И. Белоусов Элиот Крон
А. Пискунов В. Попов С. Симановский

WEB 3.0.

ЧАСТЬ I. НАСТОЯЩЕЕ ВЧЕРАШНЕГО ЗАВТРА

WEB 3.0.

Часть I. Настоящее вчерашнего завтра

Издательские решения
По лицензии Ridero
2020

УДК 004
ББК 32.973
W37

Авторы: Белоусов И., Крон Э., Пискунов А., Попов В.,
Симановский С.

Шрифты предоставлены компанией «ПараТайп»

Web 3.0. : Часть I. Настоящее вчерашнего завтра / И. Белоусов [и д. р.]. — [б. м.] : Издательские решения, 2020. — 348 с.
ISBN 978-5-4498-4250-3 (т. 1)
ISBN 978-5-4498-4251-0

W37

Это первая часть первой русскоязычной книги о Web 3.0. Не только о том, каким будет, но и о том, каким видится разным людям: от разработчиков до предпринимателей. Кроме того, это совместный труд сразу нескольких специалистов, что делает прочтение полезным для тех, кто с технологиями и на ты, и на вы.

УДК 004
ББК 32.973

16+ В соответствии с ФЗ от 29.12.2010 №436-ФЗ

ISBN 978-5-4498-4250-3
ISBN 978-5-4498-4251-0

ОГЛАВЛЕНИЕ

Общие вводные 11
Как правильно читать книгу? 14
Официальное определение 15
глоссарий сокращений 18
Дисклеймеры 19
Web 3.0: начала 21
От автора главы 23
Введение к главе первой 25
Что же такое Web 3.0? 28
Интерпретации Web 3.0 29
В поисках новой концепции 35
DNS на блокчейне 35
Взаимодействие сайтов с блокчейн-системами 39
Децентрализация провайдеров 40
Децентрализация хранения данных 41
Децентрализация идентификации и репутации 43
Протоколы взаимодействия 45
Codius — слон, не видимый в комнате? 47
W3C: Web Payments и Web Authentication 49
DeFi: децентрализованные финансы 53
Послесловие к главе первой 56
Глава II. Карта местности — архитектура Web 3.0, или О чём не стоит забывать 59
Великая паутина 62
Большие пушки 64
История жизненно важна 72
Больше, чем просто технология 75

Глава III. Краткие итоги истории 77
Парадокс ничьей и ИИ 82
Свобода: смарт-контракт и GDPR-крепостные 84
Централизация и Web 3.0: коротко 86
Дапсы и локальные глобальные сети — находка архитектуры Web 3.0 88
Глава IV. Web 3.0 — этап эволюции систем 93
Опять эволюция? 96
Токенизация — новый и необходимый рынок 99
Экономика действий — сфера новаторов 102
ГСР/СГР 105
Основные ошибки рейтинговых систем 106
Залог репутации 110
Отрицательная репутация 111
Социальный капитал и ГСР 112
ГСР и транзакционные системы 113
Алгоритмы консенсуса 115
История появления алгоритмов консенсуса 118
Децентрализованные платформы — следующий этап в истории развития консенсусов 122
Базовые алгоритмы консенсуса децентрализованных систем 124
Коллегиальный поэтапный алгоритм консенсуса 126
Алгоритм консенсуса «Поэтапный с лидером» 129
Алгоритм консенсуса «Лидер с собственной случайностью» 130
Алгоритм консенсуса «Лидер со связанной случайностью» 132
Алгоритмы консенсуса для платформ 137
Первый вариант PoS-алгоритма 138
Алгоритмы децентрализованных платформ с централизацией 139
Шардинг 143
Скоростные децентрализованные платформы 145
Смещение акцентов 148

Ускорение за счёт консенсуса с централизацией 150
Отказ от стандартов 152
Протоколы второго уровня 154
Шардинг 159
Шардинг состояния 162
Метод регистрации межшардовых взаимодействий 163
Прямое взаимодействие шард 164
Проверка межшардинговых транзакций 165
Управление шардами 167
Примеры платформ с шардингом 168
Zilliqa 168
QuarkChain 169
Kadena 170
Holochain 170
The Power 171
Интероперабельность 173
Перенос или обмен активами 178
Приватность 179
Масштабируемость и производительность 180
Контроль. Регулирование. Новые активы 181
Расширение функциональности и исследования 182
Известные проблемы 183
Технологическое различие платформ 183
Отсутствие бизнес-применения 184
Существующие подходы 186
Атомарные обмены 187
Мосты и нотариальные схемы 188
Релейный блокчейн, или релейная передача 190
Перспективы развития технологических решений интероперабельности 191
Выводы 193
Основные проблемы и перспективы 195
Аппаратные проблемы 198
Проблемы восприятия 200

Новые бизнесы и профессии ... 202
Будущее, которое уже наступило ... 205
Коммунизм вне политики, или Мир №X ... 208
Терминатор возвращается ... 211
Смелые мечты о наступившем или назад в...? ... 215
После послесловия ... 221
Приложение №1. Как и почему зародился Web 3.0? Краткое изложение от Сергея Симановского ... 225
Что же такое Web 3.0? ... 228
Итак — Web 3.0 ... 235
P2P-сети — примеры и какой от них толк? ... 248
Немного примеров в действии ... 249
Всё выше и выше... ... 250
Смарт-контракты, IoT и роботы ... 251
Новые виды организаций ... 252
Завершение для приложения ... 253
Приложение №2. Перспективы развития блокчейн-решений — неочевидные тенденции ... 255
О сути ... 257
Анонимность разного рода ... 259
Открытость ... 262
Автоматизация доверия ... 267
Распределённость ... 270
Квантовый блокчейн и иные тенденции ближайших лет ... 272
Приложение №3. Перевод статьи Т. О'Рейли о Web 3.0 ... 275
Приложение №4. Переводы текстов про Web 3.0 Н. Спивак ... 283
Резюме о Web 3.0: Radar Networks, Powerset, Metaweb и другие... ... 285
Семантическое социальное программное обеспечение ... 286
Наша платформа приложений Web 3.0 ... 287
Что не делаем? Поиск на естественном языке ... 288

Что делаем? Семантическая паутина ... 290
Семантическая разметка ... 291
Простые примеры семантики ... 294
SPARQL и новая веб-страница данных ... 296
Обоснование: следующий рубеж после поиска ... 297
Дифференцируя игроков ... 298
Web 3.0 только начинается ... 299
Решение проблемы перегрузки информацией ... 300
Web 3.0 — следующий шаг для Web? ... 303
Gartner ошибается насчёт Web 3.0 ... 305
Приложение №5. Видео про W3 ... 309
Все мы живём в коробке ... 312
Приложение №6. Почему доверия Apple, Facebook, Microsoft и другим гигантам больше нет? ... 317
Полезные ссылки ... 325
История Web 3.0 ... 327
Термины и дефиниции ... 328
Проекты ... 329
Система глобальной репутации ... 331
Примечания ... 332

Посвящается Д. Ассанжу и всем, кто пострадал от рук виновных

ОБЩИЕ ВВОДНЫЕ

Компания AOL когда-то считала, что массовое создание сайтов возможно только после «прыжка веры». Как видим, он таки случился…

Данный труд является совместным сразу для нескольких криптоэнтузиастов: И. Белоусова (The Power), А. Пискунова (Viz), В. Попова (Synergis & Menaskop), Э. Крона (Псевдоним), С. Симановского (Blocksult). Написана книга *для всех*, но в первую очередь для тех, кто хочет создавать по-настоящему инновационный бизнес (предпринимателям), а равно и тем, кто желает помогать его развивать (архитекторам систем, разработчикам и так далее). В начале представлены позиции относительного того, а что же есть Web 3.0 (**далее — W3**), чем так примечателен и как именно его можно использовать. Затем следуют разделы по разным направлениям. Пожалуй, самым важным для нас, авторов, является то, что книга — первая[1] в своём роде, а значит, с её помощью можем прочувствовать пульс рынка: кому именно нужен тот стек технологий, который заложен в Web 3.0? Кто готов вкладывать свои силы, время, деньги, чтобы он эволюционировал? Какие кейсы получат наибольшее развитие сегодня, а какие — в ближайшем будущем? Как бы там ни было, стоит помнить, что блокчейн, пришедший к нам более десяти лет назад, уже породил множество альтернативных инструментов, которые на полную мощность могут применяться только в парадигме Web 3.0, но и это — не всё: эволюция p2p — прямое свидетельство необходимости следующего шага. Если нравится участвовать в создании чего-то новаторского — обязательно свяжитесь с выпускающим редактором, найдя в одной из социальных сетей ник **Menaskop**, или даже по почте — menaskop@gmail.com.

А пока — приятного чтения и важных выводов: встретимся в заключении!

КАК ПРАВИЛЬНО ЧИТАТЬ КНИГУ?

Поскольку авторов несколько, каждый из них по-своему уникален, а значит — субъективен, книгу можно читать с любой части: для начинающих рекомендуем приложение №1, а затем — введение и далее, для опытных, — любую главу.

ОФИЦИАЛЬНОЕ ОПРЕДЕЛЕНИЕ

Как ни странно, но оно есть (и даже Wiki на этом настаивает): по вот этой ссылке[1]. Процитируем: «Некоторые люди спрашивали меня (*Д. Калаканиса — прим. авт.*) о чётком определении термина Web 3.0. Web 3.0 определяется как создание высококачественного контента и услуг, производимых талантливыми людьми с использованием технологии Web 2.0[2] в качестве платформы, предоставляющей подобную возможность. Сервисы Web 2.0 в настоящее время являются коммодитизированной платформой[3], а не конечным продуктом. Мир, где социальная сеть, вики или сервис социальных закладок могут быть построены бесплатно и в одно мгновение, есть, что дальше?

Сервисы Web 2.0, такие как digg[2] и YouTube, превращаются в сервисы Web 3.0 с дополнительным уровнем индивидуального мастерства и сосредоточенности. В качестве примера приведу funnyordie.com[3], сервис, который использует все стандартные наборы функций Web 2.0, та-

---

[1] https://calacanis.com/2007/10/03/web-3-0-the-official-definition/

[2] https://digg.com/

[3] https://www.funnyordie.com/

кие как синдикация и социальные сети, добавляя к ним слои особого таланта и доверия…

Web 3.0 — возвращение к тому, что было великим в средствах массовой информации и технологии до Web 2.0: признание таланта и опыта, право собственности на контент и справедливость (повсюду). Пришло время развиваться».

Есть и другая позиция на сей счёт, высказанная Н. Спиваком[4] также в 2007 году (подробней об этой дискуссии можно прочесть в приложении №3): «Джейсон только что написал в блоге об официальном определении Web 3.0 — в его случае он определяет его как лучший контент, созданный с использованием технологий Web 2.0. Было много ответов на сей счёт, но так как я один из основных соавторов страницы Википедии по термину[1] Web 3.0, то подумал, что должен бросить и забить свою шайбу в эти ворота.

Web 3.0, на мой взгляд, лучше всего определить как третье десятилетие[5] Сети (2009—2019), в течение которого несколько ключевых технологий будут широко использоваться. Главными среди них будут RDF и технологии развивающейся Семантической паутины. Хотя Web 3.0 не является синонимом Семантической паутины (в этот период произойдёт ещё несколько *важных* технологических сдвигов), он будет в значительной степени характеризоваться семантикой в целом.

Web 3.0 — эра, в которой модернизируем бэкенд Сети после десятилетия фокусировки на фронтенде (Web 2.0 в основном был посвящён AJAX, тегам и другим инновациям фронтенда для пользователей). Web 3.0 уже начинает появляться в таких стартапах, как Radar Networks (и наш продукт — Twine), но на самом деле станет мейнстримом[6] примерно в 2009 году.

---

[1] https://en.wikipedia.org/wiki/Talk%3AWeb_3.0

Почему определение Web 3.0 лучше, чем любое другое возможное определение этого термина? Во-первых, это дефиниция, которая не может быть легко экспроприирована[7] любой компанией или частным лицом под какую-либо конкретную технологию или продукт. Это совершенно однозначное определение и относится к определённому периоду времени и всему, что происходит в веб-технологиях и бизнесе в течение этого периода. Это положит конец дебатам о том, что означает сей термин, и перенесёт его в область полезного обсуждения, а именно: какие технологии и тенденции *на самом деле* станут важными в грядущем десятилетии Сети?».

Что ж, последние 10—12 лет подтвердили верность второго и относительную ошибочность первого подхода, но произведение наше как раз о том, что не всё так просто...

ГЛОССАРИЙ СОКРАЩЕНИЙ

ГСР/СГР — глобальная система репутации / система глобальной репутации

ДРС — децентрализованные и/или распределённые системы

ПО — программное обеспечение

SaO — субъект и объект (внутри ДРС)

W3 — Web 3.0

ДИСКЛЕЙМЕРЫ

Поскольку книга написана несколькими авторами, а равно — подвержена была общей редактуре, то позиции одного из участников могут не совпадать с другими, а порой — коренным образом расходиться, но в этом и прелесть децентрализации: можно увидеть как можно больше разного. Пусть это не смущает.

Второе замечание заключается в том, что в книге (по крайней мере — в электронном варианте) множество ссылок: при первом прочтении их можно смело опустить, а при повторном и последующих — использовать в качестве ***справочника****. Иногда (в силу особенностей вёрстки) приходилось заменять ссылки русскоязычной Википедии на англоязычную: вы всегда можете сменить язык в нижнем левом углу на сайте wikipedia.org.*

WEB 3.0: НАЧАЛА

ОТ АВТОРА ГЛАВЫ

«Web 3.0 — эра, в которую будем обновлять бэкенд сети после десятилетия фокуса на фронтенде».

Н. Спивак

Привет! Меня зовут Анатолий Пискунов[8], уже более пятнадцати лет изучаю интернет-технологии. Всё начиналось как хобби, переросло в небольшие проекты, эксперименты, изучение разных решений, десятки (если не сотни) прочитанных книг, профильное и самостоятельное изучение всего, что связано с Сетью. Верстал, программировал, администрировал, пробовал разные подходы, падал и (снова) вставал, устраивался на работу, менял компании, руководил разработкой сервисов, работал с тендерами, брался за разные, даже невозможные на первый взгляд проекты и завершал их. В 2016 году ушёл с работы и нырнул в блокчейн-сферу: целиком и надолго.

Думаю, у каждого блокчейн-энтузиаста своя специализация и свой спектр увлечений. И я не исключение: больше всего интересует именно Интернет и новые возможности, которые привнесут в него системы распределённого реестра. Возможно, мой взгляд на Web 3.0 не покажется «стандартным», но, постарался донести и передать словами то, что вижу. Надеюсь, после прочтения почувствуешь

«это», получишь заряд энергии и воодушевления (а может, и новые вопросы).

Буду рад отзывам и комментариям!

ВВЕДЕНИЕ К ГЛАВЕ ПЕРВОЙ

«Нумерация Интернета?!
Что за глупости, Интернет есть Интернет!
Или всё же...»

Аноним

Предположу, что часть читателей застали эпоху dial-up-Интернета[9]. Что в то время было? Адресная строка и каталоги сайтов. Сайты на Народе (сервис бесплатного размещения от Яндекса), html-страницы, баннеры на дружественные ресурсы, которыми обменивались вручную, js-скрипты, которые использовались зачастую для эмуляции падающего снега, летающих за мышкой картинок, и тесты на одной странице. CGI[1]-модули для гостевых книг и борьба с KOI8-R[2].

Переход от Web 1.0 к Web 2.0 был постепенным. Серверные скрипты на Perl сменялись PHP, автоматические механизмы регистрации, первые капчи, панели администрирования, модульные надстройки над форумами (привет, PHP-Nuke[3]!). Хостинг-провайдеры конкурировали

[1] https://ru.wikipedia.org/wiki/CGI

[2] https://de.wikipedia.org/wiki/KOI8

[3] https://ru.wikipedia.org/wiki/PHP-Nuke

за пользователей, предлагая всё новые версии PHP и MySQL (позже стали внедрять cPanel[1]). Flash-анимация, ActionScript и видеоигры в браузере.

Предлагаю оставить термин Web 2.0[2] для справочников и энциклопедий. Кто впервые публично произнёс термин, что в это вкладывал — всё в прошлом и не так важно. Интернет эволюционирует постоянно. Это происходит и сейчас. Мы — свидетели чуда. Так ли значимо, в каком году появился AJAX[3], когда родилась библиотека JQuery и прекратили обновлять страницу в почтовом сервисе для того, чтобы проверить, а пришли ли новые письма? Когда алгоритмы стали автоматически маркировать спам? Когда появилась технология потокового видео и YouTube? Когда люди стали переходить из ICQ в Jabber, а позже в Skype? Когда онлайн-созвон, чтобы совместно играть в MOBA[4], стал нормой?

Социальные сети создали точку сбора: формирование сообществ и групп перенесло живое общение в онлайн. Эволюция — процесс постепенный. Какие-то инновации потерпели крах, какие-то стали естественным продолжением нас. Теперь у каждого есть смартфон с возможностью осуществления социального взаимодействия дабл-тапом по фотографии в Инстаграме. Слои социума поделены между глобальными соцсетями. Для трудоголиков и профессионалов есть LinkedIn от Microsoft. Для старшего поколения — ламповые «Одноклассники» (которые мудро изменили позиционирование, переименовавшись в ОК). Для творческих натур и визуализаторов — Инстаграм. Для любителей читать суть — Твиттер (или TL; DR[5], который

---

[1] https://en.wikipedia.org/wiki/CPanel

[2] https://en.wikipedia.org/wiki/Web_2.0

[3] https://ru.wikipedia.org/wiki/AJAX

[4] https://ru.wikipedia.org/wiki/MOBA

обходится модными картинками с текстом или кликбейт-заголовками[6]). Телевизор с пропагандой успешно заменён на YouTube, где сформированный пользователем круг подписок создаёт замкнутый мир по интересам.

WebSocket[7] и WebAssembly[8] прямо сейчас закладывают фундамент для следующей ступени развития. Адаптивная вёрстка уже необходимость: способ потреблять информацию изменился, и для основной массы выбор очевиден[9]. Впереди — VR/AR-революция, и есть опасения, что человечество собственноручно откажется от реалистичного восприятия в угоду реалистичной картинке[10].

Исторически сложилась простая истина: инновации и технологии сталкиваются с испытаниями временем (Flash уже проиграл Canvas и HTML5), удобством (noSQL[11] всё чаще замещают реляционные базы данных), адаптацией под настоящее (осознание вреда экологии от … — *острая* повестка для всего человечества). Выжившие камень за камнем выкладывают мозаику под названием Интернет[10]. И главное: мы — участники и свидетели процесса.

---

[5] https://ru.wikipedia.org/wiki/TL;DR

[6] https://en.wikipedia.org/wiki/Clickbait

[7] https://ru.wikipedia.org/wiki/WebSocket

[8] https://ru.wikipedia.org/wiki/WebAssembly

[9] https://www.perficientdigital.com/insights/our-research/mobile-vs-desktop-usage-study

[10] https://youtu.be/Is8eXZco46Q

[11] https://ru.wikipedia.org/wiki/NoSQL

ЧТО ЖЕ ТАКОЕ WEB 3.0?

Все сервисы или компании, которые применяют термин Web 3.0, добиваются ровно одного: привлечь внимание к своей технологии, заявить о себе как об инновации, которая займёт нужное и важное место в истории. Это одновременно и метка, и маркетинговый ход, и заявка на общественное внимание. Сколько людей в своё время обогатилось, вложив в пионеров[11] — Amazon, eBay, Facebook, Alphabet (в прошлом Google)? Они правильно разглядели тренды, потенциал продуктов и решений, которыми занимались те или иные компании. Думаю, уже закрадывается сомнение, что спустя несколько лет в справочнике появится запись: «Web3.0 — это… технологическое решение, которое использовало инновационную парадигму… и предоставило пользователям решение актуальной проблемы…». *Мы находимся в состоянии Web 3.0* Шрёдингера[1]. Осознание, что Web 3.0 наступил, придёт тогда, когда придёт. Остаётся быть созидателями инноваций и движителями парадигм. Предлагаю рассмотреть существующие интерпретации новой главы Интернета от компаний и персон, готовых приложить усилия и имеющих смелость заявить о том, что именно они — часть этого нового.

---

[1] https://en.wikipedia.org/wiki/Schr%C3%B6dinger%27s_cat

ИНТЕРПРЕТАЦИИ WEB 3.0

С популяризацией криптовалют начал происходить концептуальный сдвиг в понимании экономики и ценности среди пользователей, обладающих достаточной технической грамотностью. Биткоин доказал свою жизнеспособность и состоятельность криптографических децентрализованных систем. Привлечение внимания общественности к цифровой ценности породило большую волну участников рынка, которые верят в развитие блокчейна (или, как стали называть эту технологию в научной среде, DLT[1][12]). Как итог — появились новые системы самого разного назначения. Не обошлось и без мошенников, рисующих красивые обёртки для сбора средств путём краудфандинга[2][13]. Но реальный новый сектор DLT уже невозможно остановить. Интеллектуальный вклад в развитие этой IT-находки раскрывает отрасли шаг за шагом.

Открытость, доказуемость действий, возможность независимого аудита и распределённость привели к смене парадигмы в умах сознательных людей. Именно люди стали переносить концепцию нового мышления на привыч-

[1] https://en.wikipedia.org/wiki/Distributed_ledger

[2] https://en.wikipedia.org/wiki/Crowdfunding

ные вещи. Биткоин сделал это в рамках финансового мира. Но остаётся столько[14] всего!

Приватность. Защита персональных данных. Право на тайну[15] личной переписки. Договоры и сделки без посредников (смарт-контракты).

Идея о том, что можно исключить посредника, начала поступательное движение на все элементы привычного Интернета. Энтузиасты и разработчики стали озираться по сторонам, выискивая бизнес-процессы, где есть посредники. Можно ли от них отказаться? Вот краткий список:

— Доменные имена? Есть продавец и посредники-реселлеры, которые по желанию левой пятки могут поднять цену или заблокировать домен по жалобе регуляторов. Можно отказаться от них и разработать собственные беспристрастные механизмы общего пространства[16] имён!

— Сертификационные центры (SSL)? Посредники есть! Браузеры[17] не доверяют самоподписанным сертификатам и помечают такие сайты как ненадёжные. Почему бы не разработать решение на DLT, где пользователи могут[18] сами заявлять о доверии определённым сертификатам с привязкой к доменному имени?

— Платёжные провайдеры, ограничивающие переводы средств, требуют подтверждения личности, но подвержены взломам и похищению средств.

— Облачные или хостинг-провайдеры — по жалобе заблокируют счёт, сервер, не дадут сохранить данные, могут повысить цену, будут насильно заставлять платить VAT (по мнению отдельных участников рынка, Интернет должен оставаться межгосударственным и межтерриториальным пространством).

— Социальные сети передают (продают!) персональные данные третьим лицам, используют публикуемые материалы и связи для таргетированной рекламы.

— Можно продолжать почти бесконечно…

Безусловно, большинство провайдеров услуг добавляют удобства, взамен — пользователь делегирует право распоряжаться (своими) данными. Добровольно ограничивает себя. Цель многих энтузиастов — донести мысль о том, что в современном мире должна быть и будет альтернатива. Сердцем её является цифровая экономика: децентрализованная, с открытым кодом и доступная для аудита; цифровые сущности внутри — криптографически защищены.

В 2019 году стала набирать популярность тема совместимости разных блокчейн-систем (interoperability). С появлением HTLC (Hash Time Locked Contract[1]) начали развиваться разные концепции: ILP (Interledger Protocol[2]) или IBC (Inter-Blockchain Communication[3]). Благодаря им в будущем не будет привязки к конкретному[19] блокчейн-решению.

Поэтому термин Web 3.0 сшит с криптографией, контролем за передаваемыми данными, отказом от посредников, взаимодействием в замкнутых системах с собственной экономикой[20]. *Именно в блокчейн-разработках общество видит признаки новой главы Интернета*[21] — *инновации, которая вернёт контроль за данными в руки пользователей.*

Но всё опять не так просто. Общество состоит не только из сознательных людей. Неужели верите в осознанный выбор большинства?[22] Красная таблетка только для избранных, остальные будут рады принять синюю[4]. Сознательный отказ от посредников приводит к самостоятельному контролю: за своими данными, за своими паролями,

---

[1] https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts

[2] https://interledger.org/

[3] https://cosmos.network/docs/spec/ibc/

[4] https://en.wikipedia.org/wiki/Red_pill_and_blue_pill

за своими средствами, за своими финансами. Готовы ли люди отвечать за свои решения? Сомневаюсь. **А вы?**

Да, осознанным людям новая концепция Интернета даст выбор. «Бесплатно» пользоваться социальной сетью, принадлежащей корпорации, или держать данные на одном из хабов (например, gaia от blockstack[1]), расплачиваясь внутренней криптовалютой за хранение и обработку, а может, и получая токены за просмотр нативных рекламных объявлений (как в Brave). Бесплатно скачивать торрент-файлы, оплачивать повышение скорости или получать токены за раздачу файлов[23] — возможно всё!

***

Большинство не сможет этим пользоваться. Без адаптации в привычные для всех приложения результат определён. Нужен так называемый mass adoption.

Общественная приспосабливаемость возможна в случае принятия правовых норм[24], регуляторных решений и трактовок по разным криптовалютам. Тогда стоит рассчитывать на постепенное внедрение технологий в стандарты, которые имплементируют в браузеры общего назначения (Chrome, Firefox, Opera). Несмотря на то что World Wide Web Consortium (W3C[2]) работает в направлении разработки стандартов по интеграции криптографических инструментов в браузеры, обществу нужно пройти

[1] https://github.com/blockstack/gaia

[2] https://www.w3.org/

длинный путь по фильтрации концепций и Web3.0-интерпретаций[25].

Компании и разработчики следуют вперёд, используя все доступные средства: как специализированные сайты, применяющие js-библиотеки или браузерные расширения (Metamask[1] и другие web-кошельки) для взаимодействия с блокчейн-системами, так и отдельные приложения (Scatter[2]). В некоторых случаях разрабатываются даже отдельные браузеры (Brave, Puma[3], CYB). Но всё это может столкнуться с простой цензурой на смартфонах со стороны корпораций, владеющих маркетплейсами (AppStore для iOS, PlayMarket для Android). Например, приложения социальной сети Gab[4] постоянно находятся под блокировками и подвергаются критике в СМИ (естественно, с политическим контекстом, так как речь идёт о свободе слова). Многие приложения, использующие криптографию, не проходят модерацию от Apple и Google. О какой общественной адаптации тогда может идти речь?[26]

Альтернативой приложениям, устанавливаемым через централизованные маркетплейсы, могут являться сами веб-сайты, если будут адаптированы и переделаны в прогрессивные веб-приложения (PWA[5]). Подавляющее большинство уже поддерживают адаптивную вёрстку. Следующим этапом будет поддержка PWA и взаимодействие с блокчейн-системами напрямую (посредством подключаемых библиотек).

Web 3.0 — вызов всем. Какие технологии будут востребованы? Что выберут пользователи? Могут ли приложения

---

[1] https://metamask.io/

[2] https://get-scatter.com/

[3] https://www.pumabrowser.com/

[4] https://ru.wikipedia.org/wiki/Gab

[5] https://habr.com/ru/post/418923/

к ДРС быть простыми и доступными? Как ответит финансовый сектор и регуляторы на зарождающуюся цифровую экономику в замкнутых системах?

Вопросы и ответы содержатся в нас. Общество сделает выбор. Каждый.

В ПОИСКАХ НОВОЙ КОНЦЕПЦИИ

В данном разделе представлен список интересных сервисов, связанных с развитием Интернета. Не все заявляют о себе как о Web 3.0, а те, кто заявляют, не всегда предоставляют что-то концептуальное и интересное.

DNS НА БЛОКЧЕЙНЕ

Хорошо было бы отказаться от посредника-монополиста в виде ICANN[1]. И это возможно именно с применением ДРС. Право владения, возможность передачи, заложенная в смарт-контрактах, распределённые DNS-записи[27] — созданы, чтобы одними из первых получить развитие.

ICANN за 20 лет сильно пустили корни в Интернете и уже стали стандартом. Многие просто привыкли, что

[1] https://ru.wikipedia.org/wiki/ICANN

за домен нужно платить мзду каждый год. Поэтому альтернативы, которые создаются, часто копируют систему, созданную ICANN. Есть как отдельные смарт-контракты, например, eosdns. x[1] на EOS или https://unstoppabledomains.com/ на Zilliqa (а теперь и на Ethereum), так и более универсальные решения (ENS[2], документация[3]). Сложность заключается в фактическом использовании. Современная Сеть уже полна правил и механизмов. Безопасность пользователей в браузерах довела до абсурда связь между доменами и SSL-сертификатами[4] (подробности — ниже).

Сейчас норма — использовать https-протокол, но он настолько строго вмонтирован[28] в браузеры, что без разрушения старых правил — новые не построить. Кто-то пытается обойти их в виде расширений (eosdns в Chrome Webstore[5], исходники[6]), с перезаписью PAC-скрипта для управления прокси. Кто-то вносит правки в сами «просмотрщики» или разрабатывают свой аналог на electron (например, демо от unstoppable[7]). И нельзя точно предсказать, какой подход победит. В EOS, например, есть имена аккаунтов, которые выступают в виде доменных имён[29], и короткие просто так не зарегистрируешь (есть специальный аукцион на конкурентной основе, остатки продают разные сервисы, например, eosnameservice.io[8]).

---

[1] https://bloks.io/account/eosdns.x

[2] https://ens.domains/

[3] https://docs.ens.domains/

[4] https://ru.wikipedia.org/wiki/SSL

[5] https://chrome.google.com/webstore/detail/eosdns/bapgppgkkohoiadofnmhphkjclmmmiac

[6] https://github.com/eoscafe/dns-extension

[7] https://github.com/unstoppabledomains/unstoppable-demo-browser

[8] https://www.eosnameservice.io/en

Вот и получается, что браузеры мешают пользователю, если он идёт на сайт, защищённый персональным сертификатом. Центры же выдают разрешения только за деньги и стягивают на себя такой объём ценности, что просто представить сложно. Появление инициативы Let's Encrypt[1] (в России *заблокировано*[30] Роскомнадзором: всё ради защиты детей!) сильно изменило существующий рынок, но в глобальном плане сложно модифицировать парадигму. Массовому внедрению мешают и действующие нормативы. Только разработка новых сервисов с более гибкими правилами позволит что-то изменить. Для этого нужно:

— пользователям посещать сайты с самоподписанными сертификатами[31];

— доменам хранить в DNS-записях информацию о сертификате, чтобы выявлять вмешательство в виде man in the middle[2] (для специалистов: да, конечно, для бизнеса в реальном мире хочется иметь «знак качества» от третьей стороны, в современном мире этим занимаются сертификационные центры, но для обычного использования уже доступен Let's Encrypt, который выступает поверенным, что сертификат сформирован на сервере и прошёл проверку размещением файлов определённого содержания. Стоит отметить, что домен и сервер, который его обслуживает, — две разные сущности, обслуживаемые обычно одним владельцем, поэтому считаю TXT-запись в домене слепком сертификата, достаточным для проверки и защиты от man in the middle. В таком ракурсе поверенные нужны для утверждения, что сертификат соответствует определённому юридическому лицу в реальном мире);

---

[1] https://letsencrypt.org/ru/

[2] https://en.wikipedia.org/wiki/Man-in-the-middle_attack

— user'ам голосовать своим стеком/активностью в публичных блокчейн-системах, проявляя таким образом доверие такому сертификату;

— устанавливать расширения для работы с scheme (например, для ввода нового пространства имён eos://) и прозрачно делать https-запросы по определённым в блокчейне ip-адресам.

Закрадываются сомнения: сделают ли это лидеры рынка браузеров? Или они работают на интересы групп ICANN и разных CA (Certification Authority, список от Mozilla Foundation[1])?

Возможно, это будут совершенно новые браузеры или модификация существующих, но под иным брендом. Только время покажет, какой из экспериментов выживет и даст пользователям необходимую гибкость.

P. S. Для вопросов по децентрализации SSL-сертификатов рекомендую изучить Remme[2] и DNSChain[3] (сервер с поддержкой Namecoin[4]). Сводка по ценам на домены в блокчейн-системах — peername.com.

---

[1] https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReport

[2] https://remme.io/

[3] https://n0where.net/blockchain-based-dns-dnschain

[4] https://github.com/okTurtles/dnschain/blob/master/docs/setting-up-dnschain-namecoin-powerdns-server.md

ВЗАИМОДЕЙСТВИЕ САЙТОВ С БЛОКЧЕЙН-СИСТЕМАМИ

Если со сложными консольными приложениями разобраться могут не все, то массового потребителя можно привлечь через простые и понятные разработки. К таким стоит отнести веб-приложения (или их обёртку в виде полноценных приложений для разных операционных систем) и браузерные расширения.

Веб-приложения, которые держат данные в хранилище браузера, работают по определённым принципам: зашифровывают приватные ключи для безопасности, позволяют завести несколько аккаунтов или адресов для быстрого переключения между ними, имеют предустановленные возможности для конкретной системы (зачастую это получение информации об активном аккаунте или адресе, инициация подписи данных, запрос на отправку токенов) и настроены на взаимодействие с конкретными публичными нодами.

Интеграция с веб-сайтами — непростая задача, но вполне решаемая с помощью расширений, например, того же Metamask[1] для Ethereum или Waves Keeper[2] для Waves. Часто аддоны выполняют роль кошелька и трансформируются в десктопные приложения через Electron[3], так как сталкиваются с цензурой маркетплейсов (так, например, и случилось с Scatter[4] для EOS).

Механизм работы интеграции обычно выглядит так: подключение js-скриптов для передачи данных расшире-

---

[1] https://metamask.io/

[2] https://github.com/wavesplatform/waveskeeper/blob/master/README_ru.md

[3] https://ru.wikipedia.org/wiki/Electron

[4] https://get-scatter.com/

нию или приложению, сайт инициирует запросы, приложение запрашивает подтверждение у пользователя и транслирует его решение обратно. Часто этот процесс и называют Web-3, так как происходит взаимодействие стороннего сайта с блокчейн-системой через приложение, которым управляет пользователь.

Подобные инструменты решают проблемы авторизации, отказа от посредников, где двухфакторная аутентификация заменяется паролем для подтверждения операций или интеграцией с Hardware Wallet (Ledger[1] или Trezor[2]).

ДЕЦЕНТРАЛИЗАЦИЯ ПРОВАЙДЕРОВ

Любые посредники могут быть заменены p2p-системой с внутренней экономикой. Интернет-провайдеры находятся в зоне риска из-за развития IoT (Internet of Things[3]), 5G[4], mesh-сетей[5]. Несмотря на то что теми же mesh-сетями интересовались энтузиасты давным-давно[6], популяризация блокчейн, развитие смежных технологий, таких как 5G, и потенциальное покрытие спутниковым Интернетом всё больших территорий позволили появиться проектам, которые заявляют о себе как о децентрализованных mesh-

[1] https://www.ledger.com/

[2] https://trezor.io/

[3] https://en.wikipedia.org/wiki/Internet_of_things

[4] https://ru.wikipedia.org/wiki/5G

[5] https://en.wikipedia.org/wiki/Mesh_networking

[6] https://habr.com/ru/post/196562/

сетях. Заявки серьёзные — для многих это выглядит как далёкая фантазия: расшарить Wi-Fi, связаться с другими узлами, получать вознаграждение за связность сети и предоставление услуг передачи данных, пользоваться сервисами других провайдеров, оплачивая их аналогичными токенами. В этой фантазии замечательно всё, но возможна ли она — покажет время. Многие проекты, которые собирали средства через ICO, ещё демонстрируют признаки жизни (SmartMesh[1], RightMesh[2], AMMBR[3]). Возможно, на их фоне (и на фоне открытых разработок) будут взращены те, что докажут свою жизнеспособность и необходимость всеми миру.

ДЕЦЕНТРАЛИЗАЦИЯ ХРАНЕНИЯ ДАННЫХ

В эпоху Web 2.0 развитие получили облачные провайдеры. Пионеры в этом — Amazon Web Services (AWS[4]): довольно крепко закрепились на рынке услуг, в том числе в cloud storage[5]. И если Dropbox, iCloud, Google Drive, Яндекс. Диск в первую очередь были нацелены на retail-услуги (для конечных пользователей), то корпоративный сегмент заняли SaaS-решения[6]. Так, S3 от AWS[7] и часть

[1] https://smartmesh.io/

[2] https://www.rightmesh.io/

[3] https://www.ammbr.com/

[4] https://aws.amazon.com/ru/what-is-aws/

[5] https://en.wikipedia.org/wiki/Cloud_storage

других CDN полностью захватили рынок. Конкурировать с ними по распределённому хранилищу, резервному копированию и доступности (uptime[8]) стало сложно. Корпоративный подход свёл ситуацию почти к монополии между крупными корпорациями. Новым провайдерам сложно запускать какие-либо услуги, так как предоставить какие-то конкурентные преимущества попросту невозможно. И тут на сцену вновь выходят ДРС.

IPFS[9] стал первым успешным примером работы распределённой файловой системы (про торрент чуть позже). Несмотря на отсутствие экономики в IPFS, протокол популярен: на нём создают сайты, которые обращаются к файлам, скриптам и другим элементам через IPFS-шлюзы (публичные провайдеры, готовые кэшировать и предоставлять доступ к файлам из IPFS посредством HTTP- и HTTPS-протоколов). В связке с возможностью обращения к публичным нодам различных блокчейн-систем через JSON RPC такие сайты стали своего рода децентрализованными.

Основная проблема подхода — отсутствие экономического стимула содержать IPFS-ноды и публичные шлюзы (всё пока на плечах или, точнее сказать, «кошельках» энтузиастов и идеологов). Поэтому есть проекты, которые ставят своей целью решить данную проблему, например, FileCoin[10] и BTFS[11] (который будет использовать токен BTT на сайдчейне TRON). Проблем, связанных с хранением и доступностью файлов, как технологических, так и экономических, — много. Посмотрим, какой подход найдёт

---

[6] https://en.wikipedia.org/wiki/Software_as_a_service

[7] https://ru.wikipedia.org/wiki/Amazon_S3

[8] https://en.wikipedia.org/wiki/Uptime

[9] https://ru.wikipedia.org/wiki/IPFS

[10] https://filecoin.io/

[11] https://www.bittorrent.com/btfs/

больше сторонников и займёт часть ниши, но нужно понимать: старая парадигма с облачными решениями никуда не денется. Часть рынка в виде потребителей может перейти на новые, что изменит экономику всей экосистемы. Циркуляция данных, их ценности и способ оплаты услуг — всё будет постепенно уходить из централизованных финансовых систем, лишая посредников как комиссий за переводы, так и возможности взимать налоги за предоставление услуг в привычном для текущего мира понимании (например, VAT[1] в России составляет 20%[32]).

ДЕЦЕНТРАЛИЗАЦИЯ ИДЕНТИФИКАЦИИ И РЕПУТАЦИИ

В настоящее время мало проектов занимаются репутационными моделями. Зачастую они носят локальный характер (внутри определённого сообщества или замкнутой модели оценки). Методология расчётов может быть сложна или наоборот — вызывает вопросы своей простотой. Часто в подобных системах обсуждается центр сертификации, своего рода паспортный контроль для учёта аккаунтов после прохождения KYC[2].

Транслировать в новую парадигму распределённых реестров старые принципы — *пустое и бестолковое занятие*. Как только возникает вопрос учёта голосов из реального мира, например, при участии в выборах,

[1] https://en.wikipedia.org/wiki/Value-added_tax

[2] https://en.wikipedia.org/wiki/Know_your_customer

сразу технически подкованные люди хватаются за голову.

Старый подход в виде «1 персона имеет 1 голос» — может и кажется социально справедливым, но совершенно не подходит для учёта заинтересованности сторон. Компромисс в виде социального уравнивания подходит государству, но в цифровом пространстве вызывает вопросы.

Поясню: экономика в распределённом реестре — центр экосистемы. Почему аккаунт с 0,01 токена даже в теории должен иметь аналогичный по весу голос по сравнению с держателем 100 токенов? Это банально несправедливо, так как заинтересованность в благополучии и работоспособности системы у второго выше в 10 000 раз!

А системы дропов в реальном мире, когда люди продают свою личность для получения банковских счетов, адреса для любых посылок или телефонные номера? Именно в распределённом реестре с экономическим ассетом человечество начинает просыпаться и осознавать необходимость долевого голосования[33]. Почему система в реальном мире зачтёт голос продажного пьяницы, а суд проигнорирует нападки этого же пьяницы на репутацию другого человека (не дал на выпивку)? Двойные стандарты?

В цифровых системах аккаунтом может владеть не человек, а робот[34] (или умное устройство, например, музыкальная колонка). Более того, аккаунт может принимать решения в сети, защищая свои интересы. *И внутренние механики не должны ограничивать роботов в цифровых правах*. Как только появляется идея ограничить аккаунты участием в голосовании в виде требования прохождения верификации и выдачи сертификата (или паспорта) — можно сразу ставить крест на подобной системе: уже на этапе проектирования имеем уязвимое место — центр верификации или выдачи сертификатов.

Покупка голосов, коррупция, злоупотребления на местах — пережитки старых систем, которые старались социально уравнивать персон. В цифровом пространстве с собственной экономикой доверять можно тем, которые основаны на справедливом долевом участии, где серьёзность намерений можно доказать заморозкой активов на длительный срок.

Системы идентификации носят больше рекомендательный характер, так как не могут гарантировать честность посредника (проверяющего и удостоверяющего центра). Например, существует проект KeyBase[1], который используют сами пользователи, предъявляя доказательства (криптографического, естественно, характера) связанности своего аккаунта со своими профилями в социальных сетях.

ПРОТОКОЛЫ ВЗАИМОДЕЙСТВИЯ

Бурный рост проектов с использованием распределённого реестра привёл к новой проблематике — как связать их воедино? Как добиться их взаимодействия, желательно бесшовного? Постепенно энтузиасты нашли решение в виде Hashed Time-Locked Contract (HTLC, также известные как атомарные свопы[2]) и его разновидностей. С рождением возможного решения выявились и новые проблемы:

---

[1] https://keybase.io/

[2] https://vc.ru/crypto/66308-chto-takoe-atomic-swaps-i-kak-eto-realizovat

— Как связать два блокчейна?

— Что будет делать проверяющая сторона — обращаться в другой блокчейн?

— На чём будет основано доверие другой ноде и её состоянию? Верю — не верю?[35]

Логика подсказывает, что нужен какой-то доверительный узел или канал связи между разными блокчейнами. И тут либо работать напрямую с узлами сети (доверие или проверка через нескольких оракулов[1]), либо через посредников (шлюзы, которые будут играть роль доверенных хранителей токенов, выполняя роль custodian-сервисов). В итоге имеем два разных подхода: ILP (Interledger Protocol[2]) и IBC (Inter-Blockchain Communication[3]). Вполне вероятно, что оба докажут свою жизнеспособность и будут использоваться[36]. Взаимосвязь разных распределённых реестров — часть W3-концепции. Web 2.0 научился жить с аутентификацией через другие сайты (OAuth[4]), Web 3.0 не останется в стороне, только уже в современном Интернете с сотнями блокчейн-систем.

---

[1] https://en.bitcoinwiki.org/wiki/Oracle

[2] https://interledger.org/

[3] https://cosmos.network/docs/spec/ibc/

[4] https://ru.wikipedia.org/wiki/OAuth

CODIUS — СЛОН, НЕ ВИДИМЫЙ В КОМНАТЕ?

Перед тем как состоялся Ethereum[1], в лаборатории Ripple родился Codius[2]. Codius превратился в самостоятельный проект[3] и после появления блокчейн-платформ со смарт-контрактами был временно заморожен. Пока мир не распробует набравшую популярность виртуальную машину[37] «Эфириума», нет смысла концентрироваться на «Кодиусе». Но трудно его игнорировать, так как успешная имплементация в современные финансы может составить значительную конкуренцию любым ДРС.

Идея в том, что построение смарт-контрактов может быть выполнено вне блокчейн-окружения. Добавить скриптам распределённость, взаимодействие с платёжными инструментами (такими, как Interledger Protocol[4]) — и для взаимодействия участников контракта это будет проще, чем работать в рамках блокчейн-платформы. Почему проще? Потому что стоить будет гораздо дешевле, поиск исполнителей расширится до веб-разработчиков, позволяя опираться на данные вне блокчейн-окружения (отсутствие аналога оракулов — большая проблема в текущем поколении p2p-систем).

Codius — своего рода открытая платформа для продажи в аренду серверных ресурсов и мощностей. Запущенная и настроенная, она автоматически принимает оплату от инициатора, разворачивает у себя Docker-контейнер

---

[1] https://ru.wikipedia.org/wiki/Ethereum

[2] https://codius.org/

[3] https://elevenews.com/2019/06/02/stefan-thomas-codius-to-prime-the-ripple-xrp-ecosystem/

[4] https://interledger.org/

с необходимым окружением и берёт плату за использование ресурсов. Можно назвать Codius хостинг-провайдером для приложений в контейнерах. И это отличное описание.

Проект явно опередил время и теперь ждёт своего часа. Уже сейчас блокчейн-сервисы, предоставляющие исполнение смарт-контрактов, задумываются о пиковой нагрузке. Учитывая общий распределённый реестр и характер формирования блоков, можно сказать, что вся активность на подобной блокчейн-платформе ограничена одним топовым сервером. Создание и разделение цепи на пара/сайд/подцепи (шардирование[1])[38] поможет. Но стоит понимать, что ограничения в рамках одной платформы никуда не денутся (вычислительные ресурсы общие). И переплачивают за это конечные пользователи (комиссиями за транзакции) или создатели приложений, арендуя мощности за счёт заморозки токенов, которые подвержены инфляции.

Именно проблема в виде масштабирования и подтолкнёт сообщество к изучению альтернатив в виде Codius. Smart-contracts на любом языке программирования в Docker-контейнере возможны: одним из таких примеров является проект Hot Pocket (GitHub[2]) — прототип универсального распределённого реестра со смарт-контрактами.

Сейчас же сервис ждёт: нужно всестороннее развитие контейнеров (Kubernetes[3] и Kata Containers[4]), Web Payments, внедрение и расширение охвата Interledger Protocol и критическая нагрузка на блокчейн-платформы (EOS, например, пострадал от таковой, создаваемой смарт-контрактами EIDOS[5] в 2019 году, а Ethereum — в 2017).

---

[1] https://youtu.be/kVpQ2MkfhNM

[2] https://github.com/codetsunami/hotpocket

[3] https://kubernetes.io/

[4] https://katacontainers.io/

Поэтому слону, Codius торопиться не надо[6] — он уже давно в комнате и его определённо заметят.

W3C: WEB PAYMENTS И WEB AUTHENTICATION

Нынешний Интернет настолько связан с разными протоколами и услугами посредников, что вопрос выживания того или иного подхода лежит уже не в плоскости технологий, но в стандартизации и имплементации в существующие решения. Именно вторым и занят Консорциум Всемирной паутины[7], он же World Wide Web Consortium, он же W3C. Рекомендации именно от W3C находят применение в современных браузерах. Google, Mozilla Foundation, Opera — малая часть участников W3C, полный же список можно найти на официальном сайте (их около 460[8]).

Конфликты внутри таких объёмных объединений неизбежны, поэтому в 2004 году представители индустрии основали WHATWG[9] (GitHub[10]), которая перетягивала стандартизацию HTML5 на себя, и только в 2019 году стороны

---

[5] https://blog.coinbase.com/eos-enters-congestion-mode-due-to-eidos-airdrop-3d3f82081074

[6] https://coil.com/p/wilsonianb/Codius-Host-2-0-Preview/xj-5cIC4u

[7] https://en.wikipedia.org/wiki/World_Wide_Web_Consortium

[8] https://www.w3.org/Consortium/Member/List

[9] https://ru.wikipedia.org/wiki/WHATWG

[10] https://github.com/whatwg

подписали меморандум[1], который представлял компромисс.

Когда говорим о Web 3.0 и размышляем о судьбе распределённого реестра, стоит задуматься: какие именно технологии дойдут до конечного потребителя (массового пользователя)? И через какие инструменты?

Логично предположить, что браузер — краеугольный камень во всём этом процессе. С развитием WebAssembly[2] и его поддержки технологическими гигантами — вполне возможно, что нативные приложения постепенно перейдут в браузерное окружение. Поэтому стоит присмотреться, кто из существующих пионеров блокчейн-технологий взаимодействует с W3C. Изучив список членов, можем найти представителей:

— Ethereum Foundation (ETH);
— Brave (BAT);
— Ripple (XRP, ILP);
— Coil (ILP);
— ConsenSys (ETH);
— Facebook (Libra).

Именно они работают над стандартами для того, чтобы создать условия простого взаимодействия с пользователями. И основными направлениями для стандартизации технологий, связанных с блокчейном, являются Web Payments (сайт рабочей группы[3]) и Web Authentication (сайт рабочей группы[4]).

Стандарт Web Payments даёт спецификации (Payment Request API[5], Payment Method Identifiers[6], Payment

[1] https://www.w3.org/2019/04/WHATWG-W3C-MOU.html
[2] https://ru.wikipedia.org/wiki/WebAssembly
[3] https://www.w3.org/blog/wpwg/
[4] https://www.w3.org/blog/webauthn/

Method: Basic Card[7], Payment Handler API[8], Payment Method Manifest[9]) для платежей в Интернете через браузеры (вводное руководство от Google[10]). Уже сейчас Chrome и Firefox позволяют запоминать введённые данные с пластиковых карт, что значительно ускоряет покупки через тех или иных агентов. Предполагаемый стандарт позволит проводить транзакции проще и быстрее как для получателя средств, так и для пользователя. Учитывая наличие в рабочей группе представителей Facebook, можно говорить об интеграции не только в браузеры, но и в целевые приложения, связанные с большим количеством пользователей[39] (социальные сети). А наличие ISO 20022 Registration Authority[11] подчёркивает важность данного стандарта (именно ISO 20022[12] объединяет разработки из современного мира финансов).

Блокчейн-компании и программисты сами порождают свои механизмы оплаты, пусть и без сохранения единого стандарта. Так, например, в bithomp.com есть возможность войти, используя холодные кошельки от Ledger[13], Secalot[14] и Ellipal[15]. А большинство сервисов для EOS требуют наличия приложения Scatter. Увидим ли в будущем адаптацию стандарта Web Payments для поддержки криптовалют —

---

[5] https://www.w3.org/TR/payment-request/

[6] https://www.w3.org/TR/payment-method-id/

[7] https://www.w3.org/TR/payment-method-basic-card/

[8] https://www.w3.org/TR/payment-handler/

[9] https://www.w3.org/TR/payment-method-manifest/

[10] https://developers.google.com/web/fundamentals/payments/payment-apps-developer-guide/web-payment-apps

[11] https://www.iso20022.org/registration_authority.page

[12] https://ru.wikipedia.org/wiki/ISO_20022

[13] https://www.ledger.com/

[14] https://www.secalot.com/

[15] https://www.ellipal.com/

не знает никто, но упрощение процесса, устранение посредников и высоких комиссий в уже привычных феноменах может значительно повлиять на привычный Интернет.

Стандарт Web Authentication[1] ставит целью дать браузерам (и их пользователям) единую спецификацию для взаимодействия сайтов с комплексом инструментов (и, надеюсь, единым интерфейсом), связанных с внешними аппаратными носителями (через USB, Bluetooth или NFC)[40]. И если с современными смартфонами не возникает вопросов (туда всё чаще встраивают чипы и технологии для сбора биометрии), то с персональными компьютерами всё непросто. Опять опираемся на агентов в виде сертификационных центров, поэтому стандарт уже ограничивает блокчейн-имплементации, которые могли бы как раз заменить этот слой. Не удивляйтесь, если в будущем стартапы наподобие BiChip[2] (twitter[3]), которые вживляют в руку RFID/NFC-чип, захватят мир, начиная с Африки. Зачем людям кошелёк, когда можно приложить руку (в настоящем — смартфон) к считывающему устройству?

Подводя итоги, можно выразить надежду, что блокчейн-компании и энтузиасты смогут отстоять хотя бы малую часть аутентичности. Иначе разного рода посредники навсегда сохранят своё положение в мире.

---

[1] https://www.w3.org/TR/webauthn/

[2] https://www.bichip.store/

[3] https://twitter.com/bichipdk

DEFI: ДЕЦЕНТРАЛИЗОВАННЫЕ ФИНАНСЫ

Криптовалюты позволили людям отказаться от оравы централизованных посредников при передаче ценности, оставив операторов учёта (майнер, блок-продюсер, делегат). Это послужило мощнейшим толчком для развития как технологий, так и финансовых взаимоотношений. Переводы токенов набирали обороты и при росте общей капитализации рынка выстрелили в современный мир финансов.

DeFi — открытые инструменты или протоколы в распределённых системах, так или иначе решающие какие-то финансовые задачи. Часто у конкретного решения есть свои члены правительства, которые принимают решения по управлению параметрами системы.

DeFi на момент написания данных строк больше воспринимается как смарт-контракты и возможности в той или иной блокчейн-системе, которые предоставляют финансовую услугу. Даже есть целые ресурсы, которые делают списки из подобных проектов[1], ведут рейтинги[2]. Аналитики выделяют несколько категорий DeFi:

— Decentralized Exchanges (так называемые распределённые обменники, они же DEX) и открытые протоколы обмена (0x[3], UniSwap[4], Kyber Network[5], Bancor Network[6], Ren[7], IDEX[8], BitShares[9]);

---

[1] https://defipulse.com/defi-list

[2] https://defipulse.com/

[3] https://0x.org/why

[4] https://uniswap.io/

[5] https://kyber.network/

[6] https://www.bancor.network/

[7] https://renproject.io/

— Lending and Borrowing (кредитование и заимствование: MakerDAO[10], Compound[11], Dharma[12]);

— Derivatives, Margin Trading & Prediction Markets (деривативы[13], маржинальная торговля[14] и рынок предсказаний[15]: Augur[16], CDx[17], dYdX[18], bZx[19], Daxia[20]).

Особенность DeFi в единой распределённой системе — возможность взаимодействия протоколов друг с другом и производными токенами. Именно поэтому наибольшую популярность DeFi получили на Ethereum.

Но на фоне уже разработанных продуктов и инструментов происходит кое-что другое: идёт подготовка существующего финансового мира к вступлению в игру на рынке систем распределённого реестра. Множество крупных компаний, сотни и тысячи разработчиков трудятся над переносом потребностей современного человечества. Достаточно открыть список клиентов[21] и партнёров того же R3 (Википедия[22]) или Hyperledger[23]. Разработки ведутся

---

[8] https://idex.market/faq

[9] https://bitshares.org/

[10] https://makerdao.com/en/

[11] https://compound.finance/

[12] https://www.dharma.io/

[13] https://ridero.ru/link/6SsaQjlduQgt1G

[14] https://en.wikipedia.org/wiki/Margin_(finance)

[15] https://en.wikipedia.org/wiki/Prediction_market

[16] https://www.augur.net/

[17] https://cdxproject.com/

[18] https://dydx.exchange/

[19] https://bzx.network/

[20] https://www.daxia.us/

[21] https://www.r3.com/customers/

[22] https://en.wikipedia.org/wiki/R3_(company)

[23] https://en.wikipedia.org/wiki/Hyperledger

во всех направлениях:

— Страхование? Есть[1].

— Идентификация? Есть[2].

— Торговля металлами? Есть[3].

— Клиринговая палата? Есть[4]!

— Патенты, здравоохранение, медицинское страхование? Всё это есть[5].

— Кредитование? Тоже есть[6].

Важно! Всё это уже не просто прототипы — это реальные сервисы, которые ждут одного: одобрения[41] регуляторов. Как только это произойдёт — станем свидетелями массового перехода существующего мира на новую парадигму. И вместе с провайдерами услуг на рынок хлынут их клиенты с деньгами в виде ценности, объём которых превышает текущую капитализацию криптовалют во множество раз. Нас ждёт много интересного после конца 2019 — начала 2020 года, но уже сейчас можно встать на ступеньку выше и окунуться во вселенную распределённых финансов. Нужно лишь начать интересоваться и изучать. Благо, информации так много, что надолго хватит.

---

[1] https://www.r3.com/customers/insurance/

[2] https://www.r3.com/customers/digital-identity/

[3] https://marketplace.r3.com/solutions/vaultchain

[4] https://marketplace.r3.com/solutions/three-parties-dvp-atomic-tx

[5] https://www.r3.com/customers/healthcare/

[6] https://marketplace.r3.com/solutions/voltron

ПОСЛЕСЛОВИЕ К ГЛАВЕ ПЕРВОЙ

Усиление централизации до абсурда, монополия технологических гигантов, смена парадигмы бизнеса и концентрация внимания на рынке услуг, где люди — товар в том или ином виде. Эволюция технологий приводит нас к очередной развилке. *Идти подобным путём или выбрать децентрализацию?*

Возобновляемые источники энергии, саморазвитие, самоуправление, самодисциплинирование, самоосознание? Префикс «само...» не всегда значит в одиночку. *Он значит осознанный выбор и действие*. Единомышленники найдутся и сплотятся там, где необходимо. Децентрализация — не про «переложить ответственность», а именно про «взять её на себя». Многие забывают об истинном значении слов. Интернет — не исключение.

Кто-то воспринимает Web 3.0 по методичке тех, кто его подготовил. Безусловно, есть много взглядов на то, что такое Web 3.0. В блокчейн-технологиях чаще встречаем упоминание этого термина в связке с проектами Ethereum, Cosmos, Waves, BlockStack, Polkadot, IPFS. Но по-настоящему независимыми и свободными можем стать, только если поднимем свои сервера и будем хранить информацию тоже сами. Невозможно отказаться от FB и отправлять

фотографии родственникам без хранения и передачи файлов. Кто их будет хранить, кто будет передавать, какие у них будут экономические стимулы? Кто, если не вы?

Web 3.0 и блокчейн — не волшебная таблетка[42] и не решение всех проблем. Хранение данных стоит денег (или другой ценности). Передача данных по каналу (трафик) стоит денег. Содержать инфраструктуру серверов тоже стоит денег (даже такие распределённые сервисы, как Mastadon[1], требуют электричества для работы сервера, самого сервера и оплаты канала связи).

Общество прошло тот этап, когда бесплатный сервис, широко улыбаясь, не использовал ваши данные: бесплатные сервисы успешно выжидали, наращивая пользовательскую базу, и искали бизнес-модель. Теперь они успешно продают: **вас**.

Альтернатива — замкнутые экономические модели, где прозрачны правила игры для держателей инфраструктуры (администраторы, майнеры, валидаторы, блок-продюсеры — получают часть от эмиссии), сервисов (веб-клиент, веб-сервис, блок-эксплорер, интерфейс к данным — показывают рекламу) и для самих участников сети (пользователи сервиса, сайта, услуги — вознаграждение за действие, покупка токенов для усиления влияния, оплаты услуг или комиссий системы). Отказ от излишних посредников или взаимовыгодное открытое соглашение.

Вот что такое *Web 3.0, помимо технологий — концепция выбора и свободы*.

[1] https://en.wikipedia.org/wiki/Mastodon_(software)

ГЛАВА II. КАРТА МЕСТНОСТИ — АРХИТЕКТУРА WEB 3.0, ИЛИ О ЧЁМ НЕ СТОИТ ЗАБЫВАТЬ

Автор данной части — криптоэнтузиаст, ecosystem development lead в cyber~Congress, основатель консалтингового агентства Blocksult Сергей Симановский. Контакты: @serejandmyself.

ВЕЛИКАЯ ПАУТИНА

Давайте начнём неправильно. Давайте начнём с того, что эта история не расскажет. Моя история не расскажет, как разбогатеть. Она не расскажет, как быть успешным. Но она расскажет о том, как с помощью растущей (и давно существующей) технологии стать *свободным*. Жить в довольно простом мире. Чувствовать себя нужным. Слышится так, будто это не те ценности, которые пытаемся изменить с помощью технологий. Но тогда что?..

Web 3.0, или Великая паутина, — коммуникационная структура, если можно так сказать. Взаимосвязь старых и новых протоколов, технологий и алгоритмов, которые переносят (нас) в прошлое. Почему именно в прошлое? Потому что так же, как и Bitcoin, W3 — реверсивный стек. Он возвращает к истокам с помощью технологий. То, что было так долго недоступно для многих, теперь становится общепринятым[43].

Один из моих любимых вопросов: где размещается W3? Является ли это приложением? Является ли это сетевым протоколом? Да, немного всего этого сразу.

Но начнём с начала: Bitcoin[1]. Bitcoin помог людям по-

[1] https://www.bitcoin.com/bitcoin.pdf

нять текущую финансовую систему: мы должны отвечать за свои финансы и не доверять никому другому.

Является ли Bitcoin частью W3? Думаю, да. Blockchain в целом является частью Web 3.0. Что-то, что позволяет общаться app-2-app. Peer-2-Peer. Сеть-2-Сеть. Но разве блокчейн не является прикладным уровнем? Да, это наверняка так, но и наверняка НЕ так. Blockchain одновременно является приложением, но может быть и протоколом взаимодействия: может быть шифровальным уровнем в целом. Но дело не в этом.

Закончим введение и перейдём сразу к пониманию того, кто является крупнейшими игроками за столом в данный момент. И попытаемся понять, как W3 работает на более высоком уровне.

Как говорил выше, W3 функционирует, помогая идейному вдохновителю действовать напрямую, без посредника. Он отменяет цепочки больше трёх: HTTP, DNS и URL, — позволяя общаться напрямую.

Почему коммуникация важна?

Коммуникация — абсолютный и самый важный протокол. Это то, как функционируем, думаем, рождаемся, умираем, обмениваемся деньгами, сигналами и т. д. Коммуникация — всё. Мы — социальные существа. Как и другие существа на нашей планете и, возможно, за её пределами.

БОЛЬШИЕ ПУШКИ

Несколько игроков W3 могут помочь понять, как этот феномен работает сейчас и как он (вероятно) будет работать в будущем. Давайте рассмотрим их и попробуем построить технологический стек, который поможет осознать, как можем создавать глобальные сети, от аппаратного обеспечения до персонального блога на вашей собственной (!) операционной системе.

Постараюсь разнести проекты по блокам, по категориям и опишу, что они сделают в кратчайшие сроки по отношению к W3 и как это поможет построить новый коммуникационный протокол.

Во-первых, Bitcoin — новая глобальная валютная система. Деньги, которые не требуют третьей стороны. Деньги, которые всегда отправляются: независимо от цели. Деньги без границ, которые функционируют 24 часа в сутки 7 дней в неделю: без удостоверения личности, банка или любой другой сущности («any other bingo bullshit»). Bitcoin закладывает основу для нового коммуникационного стека, на котором можем строить (что угодно). Мы общаемся через деньги. Говорим о деньгах. Это наш язык. Наш базовый протокол.

Polkadot[1] и Cosmos[2] — возможно, должны быть последними в моём списке, но это не так. Что они позволя-

ют — так это создать по-настоящему интероперабельную[3] систему связи: ту, в которой можем передавать ценность между сетями безо всякого беспокойства. Там, где владеете своей сетью, если хотите. И можете поделиться сетью с другими. Но главное — можете общаться со всеми безопасным и очень эффективным способом.

Polkadot и Cosmos важны, потому что они обеспечивают столь необходимое соединение между автономными блокчейнами, приложениями и протоколами, развивая необходимый сервис. Если Bitcoin — деньги, то этих двоих можно рассматривать как маршрутизаторы, которые помогают передавать информацию.

Отдельная часть головоломки, которую необходимо упомянуть, — IBC от Cosmos. IBC[44] — протокол, который склеит все «чейны» Tendermint[4] вместе: позволит осуществить одну простую, но мощную вещь — передачу данных между цепочками (следует отметить, что на момент написания этой главы IBC уже протестирован и готов к окончательному публичному тестированию через 1—2 месяца).

Передача данных при этом может означать и передачу токенов. Токены — технические данные внутри конкретного блокчейна. Если распахнёте свой разум и подумаете о бесконечных возможностях, которые может создать подобный подход, — сильно удивитесь! Скажем, если блокчейн имеет какую-либо утилиту (нас не интересуют те, которые не интересуют), то можем сделать обмен: по любой цене / набору правил и на любую схожую сущность. Пусть мой блокчейн производит рейтинг для контента, а ваш — создаёт репутацию для писателей: теперь же можем уста-

---

[1] https://polkadot.network/

[2] https://cosmos.network/

[3] https://en.wikipedia.org/wiki/Interoperability

[4] https://tendermint.com/

новить правила торговли между двумя упомянутыми ДРС. Но так как объём проектов практически бесконечен, сие дарует уникальную возможность и для бесконечных (новых) рынков.

Есть много потрясающих и эффективных, современных, компьютеров, о которых нужно упомянуть, говоря о W3: Ethereum 2.0[1], Aeternity[2], Cardano[3], Holochain[4] и другие. Это автономные двигатели, которые работают в одном направлении: создают экосистемы, в которых могут участвовать программисты, — с открытым исходным кодом, предоставляя нужные инструменты для работы. Они создают столь необходимую инфраструктуру для децентрализованных приложений (Dapps), которые могут напрямую взаимодействовать друг с другом с помощью вычислительных правил и кода. Каждое из оных имеет отличную точку зрения на технологическое восприятие окружения. Но реальность такова, что все они — цепочки общего назначения и делают один и тот же трюк — дают нам (нужные!) инструменты.

IOTA[5] и FOAM[6] — два удивительных проекта с миссиями мирового значения. Оба могут быть размещены в пространстве Интернета вещей. IOTA пытается децентрализованно установить связь между всеми устройствами в мире, а FOAM хочет составить основу инновационной картографии, которая, в свою очередь, даёт свободу в таких направлениях, как логистика, геотегирование и т. д.

---

[1] https://clck.ru/MFQWH

[2] https://aeternity.com/ru/

[3] https://www.cardano.org/en/home/

[4] https://holochain.org/

[5] https://www.iota.org/

[6] https://foam.space/

Aragon[1] — проект, который призван создать свободную юрисдикцию (вернее, убедиться, что единственная юрисдикция — код) для организаций. Стоит понимать, что нам нужны какие-то системы управления. Локальное управление будет иметь (первичную) тенденцию. На протяжении всей истории местные общины процветали и функционировали лучше (Швейцария, Лихтенштейн, Люксембург, Монако и т. д. остаются одними из самых богатых и счастливых стран в мире на сегодняшний день) иных. «Арагон» помогает сформировать судебные системы, организации и многое другое, а общинам предоставляет возможность самоуправления.

Decentraland[2]. Собственное царство. Не без минусов и препятствий, но тем не менее проект с огромными амбициями. Помечтайте о полностью цифровой и виртуальной реальности. Той, которая защищена от бюрократической и утомительной скуки современного мира. Это виртуальная реальность высшего порядка: место, где люди могут найти убежище от суеты мира. Начните новый бизнес, установите новые правила, создайте города и районы, где только позволит воображение — сквозь горизонт.

IPFS[3] и Filecoin[4]. Возможно, самые важные упоминания в этом списке. IPFS — протокол, который создан для того, чтобы сделать Интернет быстрее, безопаснее и открытее. IPFS позволяет распространять большие объёмы данных и хранить каждую версию файлов. IPFS упрощает настройку сетей для зеркалирования данных[5]. Это означает, что данные практически неизменны, а если

---

[1] https://aragon.org/

[2] https://decentraland.org/

[3] https://ipfs.io/

[4] https://filecoin.io/

[5] https://habr.com/ru/post/126134/

возможно — то и вечны. IPFS способствует дальнейшему распространению сетей среди коллег (пользователей). Она обеспечивает постоянную доступность — с интернет-подключением или без: помогает обмениваться файлами и просматривать их, управлять большими кусками данных, создавать приложения и т. д.

С другой стороны, Filecoin — проект, целью которого является внедрение IPFS в массы. Это рынок данных. Неиспользованные ресурсы, лежащие в основе большинства домашних хозяйств[45] в современном мире. С помощью экономических механизмов и посредством IPFS Filecoin может стать первым проектом, которым будет использоваться в ближайшие годы всякий, кто даже никогда и не слышал слово blockchain.

Cyber[1] создаёт совершенно новый протокол для добавления и поиска информации на графе знаний[2] (компиляция фактов о чём-то, что наполняется смыслом). И ранжирует эту информацию. Различные типы пользователей создают связи между IPFS-хэшами и размещают их на графе, тратя так называемые пропускные полосы[46] (количество данных, которое может быть передано за определённый период времени). Затем контент динамически ранжируется с помощью цифровых маркеров и текущих параметров нагрузки сети. Это делает ранжирование динамическим[47] (то есть оно характеризуется постоянным изменением, активностью или прогрессом).

Всё это вычисляется программой или компьютером, который отвечает за проверку достоверности чего-либо. Валидаторы делают это с помощью вычислительных ресурсов. Это позволяет искать данные в сети, ранжировать их, делать запросы и создавать базы данных знаний без по-

---

[1] https://github.com/cybercongress

[2] https://ru.wikipedia.org/wiki/Knowledge_Graph

средников и/или «чёрного ящика» (третьих лиц, которые пытаются цензурировать информацию, скрывать или подсовывать определённые результаты, чтобы получить вознаграждение, отслеживать данные и т. д.).

«Кибер» использует DURA (распределённый единый адрес ресурса), который является эквивалентом URL (аббревиатура для унифицированного локатора ресурсов), который видите в браузере при посещении W2-сайта. Вся идея DURA проста: просматривайте контент, не полагаясь на какие-либо реестры (ICANN). Это означает, что не будете рассчитывать на третью сторону при маршрутизации пакетов. Никакой цензуры и т. д. Кроме философского[1] вклада, DURA поможет обеспечить безопасность, глобальность и постоянную связь на нужном уровне.

Гиперссылки формируют Интернет. Они его построили. Мы же основываем наши знания, наши политические, экономические и образовательные решения на Сети: учимся у Google. Google — наш отец, учитель, источник знаний, социальная жизнь и т. д. Но как можем доверять Интернету, если он был сформирован чем-то, что само по себе не вызывает доверия? Не можем. Киберссылки, с другой стороны, верифицируются и поддерживаются проверенными и проверяемыми механизмами. Это означает, что с их помощью можем создать доверенную модель всей информации во Вселенной!

Страницы (содержимое) добавляются в индекс, когда кто-то отправляет CID или создаёт киберссылку. Это транзакции (они требуют той самой «полосы пропускания», которая служит механизмом защиты от спама). Транзакции проверяются валидаторами (компьютерами, которые обеспечивают баланс для отправки транзакции) и добавляются

[1] https://www.litres.ru/vladimir-popov-7629101/blokcheyn-filosofiya-chast-i/chitat-onlayn/

в граф, к которому затем обращается тот, кто делает запрос в базу. Страницы ни в коем случае не исключаются из индекса. Каждая транзакция важна и должна быть маршрутизирована (передана по назначению, какой бы она ни была).

Cyb[1] — дружелюбное приложение-робот / персональный браузер. С одной стороны, простой браузер. Но это не так. Проблема в том, что на данный момент нет такого слова, которое бы описывало, что такое Cyb. Это браузер в том смысле, что он позволяет искать нечто (какие-то «вещи»). Но это и ваши личные приложения, которые могут понять многое другое: например, Cyb может действовать как кошелёк; как база данных; содержит ваших киберпространственных роботов. И да, он работает через DURA, а не через обычный DNS/HTTP/URL и с помощью полных узлов маршрутизации информации между собой и пользователями.

Интересно, что такой простой механизм позволяет создать множество мощных инструментов. Например, унифицированная семантика, инструменты SEO, автономные роботы, доступ к собственной базе знаний и многое другое. Наряду с IPFS, Cyber формирует самый важный рынок будущего — обмен информацией. Это золото, нефть и бриллианты завтрашнего дня. Идея заключается в том, что Поиск — глобальный механизм, который понятен всем независимо от языка, расы, возраста и т. д. Это в некоторой степени основной инстинкт (поиск пищи для выживания и т. д.). В цифровом мире с помощью поиска получаем ответы на вопросы, которые всегда задаём. Поиск помогает построить модель вокруг любой интересующей темы. С помощью него можем создать базы, которые могут привести к большому количеству полезных инструментов.

---

[1] https://cyb.ai/

Urbit[1]. Один из самых безумных проектов в дикой природе. «Урбит» — своего рода последний рубеж для W3 и децентрализации в целом. Наряду с такими проектами, как Cyber, IPFS и другие, способен полностью изменить игру.

Urbit — персональный защищённый сервер с вашей (!) операционной системой и идентификатором. Подумайте об этом. Мир контролируется такими компаниями, как Amazon, которые ввели надзор за самыми большими кусками информации в мире (хостинг серверов CIA и другие государственные серверы). Могут ли все эти проекты стать децентрализованными, если стоящие за ними вычисления принадлежат одним и тем же гигантам? Нет. «Урбит» намерен изменить это. Более того, это совершенно новый технологический веб-стек, меняющий облик компьютерной науки с помощью своего языка Hoon[2] и минималистического подхода к системам.

Неужели всё это звучит слишком, чтобы принять? Да. Необъяснимо, но так и есть. Уже обрабатываем за день больше информации, чем люди 100 лет назад за жизнь! Чтобы идти в ногу с развитием, должны желать учиться. Но как это связано с W3? Что ж, давайте сделаем ещё один шаг назад.

---

[1] https://urbit.org/

[2] https://bitnovosti.com/2016/12/27/can-urbit-reboot-computing/

ИСТОРИЯ ЖИЗНЕННО ВАЖНА

Если масштабируем известную историю по годовому календарю (13,2 миллиарда лет, которые можем наблюдать), то вся она помещается в последние 7 секунд. Это включает в себя целые цивилизации, войны и т. д. Современная история… мгновение ока.

Точка зрения проста. Если хотим перемен, то должны учиться, должны тратить время, чтобы понять, что долго говорили об идеях прямого общения, частных деньгах, свободном мышлении и т. д., которые были рядом с нами столько, сколько знаем (себя). Сегодня наконец-то появилась удивительная возможность использовать технологии для реализации этих идей.

Не могу оставить без внимания аргументы, которые слышу от многих (увы, из-за отсутствия необходимых знаний). Перечень их таков.

«Хорошо, понимаю, что W3 — сочетание всех сервисов, которые когда-либо хотели, — частных денег, свободы слова, удивительных технологий и всего остального… Но… что будем делать, когда вырежут Интернет, а?»

Обычно на этом этапе спорящий человек выглядит таким счастливым, что одержал победу над всеми идеями, стоящими за W3. Только для того, чтобы признать, что сам

по себе аргумент не имеет никакого смысла. Во-первых, в нашей истории было много раз, когда приходилось ждать технологического прорыва, чтобы что-то изменить (например, телескоп). Более очевидный аргумент — наука. Тот факт, что кто-то перерезает кабели, не помешает общаться.

Давайте попробуем понять, как эти вещи работают, не заходя слишком далеко. Обмен электромагнитными импульсами — просто обмен нулями и единицами чем-то, способным их передавать (кстати, земля тоже на это способна, просто не очень удобна). Нельзя забывать, что код и электроны никем не контролируются. Они существуют как часть Вселенной. Изобретение телеграфа стало прорывом в этой области. Но возможность создания сетей не может быть отнята у кого-то, если только не отняты знания. Более того, сегодняшняя технология позволяет обмениваться сигналами другими способами: например, по радиочастотам, Wi-Fi и др.

Всё это показывает, что возможно создать «локальные ячеистые сети», которые соединены с другими сетями, не контролируются каким-либо субъектом, включая правительство. Это — вопрос знаний и фундаментальной науки. Вопрос одного шага, который отделяет от создания собственных физических сетей. Они уже существуют и используются. Вопрос только в том, а насколько широко? Но было время, когда большинство людей прилипли к Библии (не имея реальной способности читать её), вместо того чтобы понять, как свет от звёзд достигает Земли[48] и что Земля обладает доказанными и объяснимыми (с точки зрения науки) качествами.

Если возьмём эту информацию и доведём до современных технологий, то с помощью Wi-Fi, триангуляции[1]

[1] https://en.wikipedia.org/wiki/Direction_finding

или любой другой технологии построения сетей, включая ethernet (или любого другого способа разделения пропускной способности) и, очевидно, набора узлов, которые должны общаться друг с другом, сможем создать любые уникальные сети, то есть компьютеры — машины, которые могут считать (8 бит, 16 бит и т. д.). Если одна машина подключена к другой через кабель или антенну, она может передавать нули и единицы к другой машине. Это изображения цветов, цифр, строк, слов и т. д. Нам пришлось бы шифровать и расшифровывать данные. Убедиться, что они были приняты правильным аппаратом и т. д.

Звучит знакомо?

Конечно, так работает маршрутизация данных. Суть проста. Восстановление этого не требует больших усилий, как думали ранее. Более того — теперь кажется, что децентрализованные одноранговые[1] сети не менее, но, возможно, даже более приспособлены к такой работе!

[1] https://en.wikipedia.org/wiki/Peer-to-peer

БОЛЬШЕ, ЧЕМ ПРОСТО ТЕХНОЛОГИЯ

Могу описать W3 следующим образом: это — следующий эволюционный шаг в развитии Паутины. Шаг, который уводит от централизации поисковых и социальных служб и от вещей, которые зависят от единой функциональной единицы (имеют центральный источник полномочий). Это шаг, который хочет, чтобы вовлечённые контрагенты и приложения общались друг с другом напрямую. По согласованию друг с другом: в то же время — быть мотивированным к такому поведению. И, как результат, добиться более безопасной маршрутизации данных и пакетов (обмен информацией) в сети.

Но это — технологическое описание. Текст составлен таким образом, чтобы могли думать и решать, может ли технология помочь выйти за пределы технических возможностей. Всё это — инструменты, позволяющие понять гораздо более крупные и важные вещи в жизни. Инновации и ответственность. *Что мир, свободный от цензуры, принуждения и коррупции, уже существует*. Нам просто нужно потянуться к нему.

Последний вопрос, который остаётся без ответа: когда именно всё это произойдёт?

Что ж, позвольте дважды разочаровать в одном абза-

це. Во-первых, он уже функционирует. Это инфраструктурный этап. Проблема (фича, но не баг) в том, что мир живёт в эпоху информации и люди всюду видят её. И это хорошо. Но когда что-то видите — хотите это почувствовать и сразу же попробовать. К сожалению, сейчас это не так для пользователей технически не продвинутых[49]. Второе — нужно подождать ещё пару лет, прежде чем «все эти штуки» перейдут на прикладной уровень. Более того, это, скорее всего, не приведёт к массовому внедрению. Но, может быть, через 5—10 лет увидим, как массы будут использовать некоторые основные применения коммуникационной технологии W3.

ГЛАВА III. КРАТКИЕ ИТОГИ ИСТОРИИ

Умные устройства всё чаще порождают глупых людей.

Menaskop

Глава написана криптоэнтузиастом и создателем Synergis B. Поповым (aka Menaskop).

Web 3.0 не родился с первого раза: строго говоря, впервые о нём заговорили ещё в 2007 году, но на тот момент не было ясно, как именно соединить всё то, чем W3 должен отличаться. И всё же ряд наследственных звеньев — существуют до сих пор. Другой вопрос — можно ли их массово применять ныне?

Скажем, RDF (Resource Description Framework) — целая модель для представления любых, в том числе — и метаданных. Цитирую[1]: «RDF является стандартом для кодирования в семантическом вебе (Semantic Web). Благодаря семантическому вебу компьютерные программы могут использовать возрастающие объёмы структурированных данных, распределённо и децентрализованно рассеянные по Сети в настоящее время. RDF представляет собой абстрактную модель, обеспечивающую способ разбиения знаний на дискретные части».

Зачем? В первую очередь для того, чтобы процесс получения знаний стал… децентрализованным: удивительно, как человечеству приходится раз за разом открывать и переоткрывать очевидные истины, но это факт[50], и его нужно принимать во внимание.

Ещё три звена наследственности — DAML, OIL и OWL. Кратко и о них: первый расшифровывается как язык моделирования цифровых активов; второй — онтологический уровень выводов; третий — язык веб-онтологии. При этом онтология в данном случае понимается не в философском,

[1] https://ru.bmstu.wiki/RDF_(Resource_Description_Framework)

а в сугубо прикладном значении[1] как «попытка всеобъемлющей и подробной формализации некоторой области знаний с помощью концептуальной схемы».

OWL[2] является своего рода переработкой OIL и DAML[51], и в его случае вновь возвращаемся к Uniform Resource Identifier, то есть унифицированному идентификатору[3] ресурса, поскольку OWL способен описать что угодно в модели «объект-свойство».

Но всё это прекрасно, пока не возвращаемся к тому, что указанные стандарты описаны и созданы W3C, а их практическое применение вне описанных концепций W3 — скорее теоретическое.

Другое же достижение прошлых лет — граф знаний[4], добавленный в Google в 2012 году. Подробное описание можно изучить по ссылке — во всё той же Википедии[5], но хочется отдельно акцентироваться на следующих моментах:

— Опыт — прекрасное подспорье для развития инноваций, но ещё важнее — контекст использования: если просто принять кем-то заданные стандарты, то это не решит основной проблемы — не сможем создать нескольких независимых (ещё точнее — положительно взаимозависимых) точек развития, как это есть на сегодня, когда IoT, AI / big data, ДРС развиваются и стандартизируются, но при этом не имеют уже столь сильной зависимости от гигантов экономики: включая и «железные»[52] решения, поскольку open source сначала овладел ПО, а теперь перешёл и к оборудованию.

---

[1] https://en.wikipedia.org/wiki/Ontology_(information_science)

[2] https://ru.wikipedia.org/wiki/Web_Ontology_Language

[3] https://ru.wikipedia.org/wiki/URI

[4] https://ru.wikipedia.org/wiki/Knowledge_Graph

[5] https://en.wikipedia.org/wiki/Semantic_network

— Не стоит, с другой стороны, пытаться избавиться от субъекта как такового (ошибка тех, кто считает, что только (!) код — закон): всё же технологии создаются для человека, а не человек — часть технологии. Мысль звучит банально после «Матрицы», но, к сожалению, как показано в приложении №1 — всё ещё актуальная.

— Безусловно, можно вспомнить, откуда именно пошло понятие «семантический веб»[53], но в рамках настоящей книги важно несколько иное: «Семантическая паутина изначально представлялась исключительно как надстройка над существующим Интернетом (тогда ещё, естественно, web 1.0). То есть в качестве носителя семантически размеченных данных мыслились обычные страницы и другой контент миллионов разношёрстных веб-сайтов. Предлагалось каждый объект — каждую веб-страницу, файл, описание офлайн-объекта на веб-странице — наделить унифицированным идентификатором и, используя эти ссылки, объединить весь сетевой контент в единую семантическую сеть… Так вот, даже этого знания о планах плетения семантической паутины уже достаточно, чтобы понять их бесперспективность. Очевидно, что самым слабым звеном в этом проекте является использование в качестве его основы обычных веб-страниц».

И именно поэтому, с одной стороны, важен процесс децентрализации, а с другой — изменение парадигмы представления, поиска и развёртывания информации внутри Сети нового поколения.

Выскажу по этому поводу ряд значимых соображений.

ПАРАДОКС НИЧЬЕЙ И ИИ

Недавно в очередной раз сражался с алгоритмом, играя в шашки на смартфоне, и обнаружил[54] проблему, которая давно витала где-то, но не выкристаллизовывалась.

Дело в том, что скрипты игры были настроены так, чтобы побеждать, когда же речь шла о явной ничьей — начался изматывающий процесс: однотипные ходы по кругу. И уже через сорок-пятьдесят таких итераций мой мозг устал, а вот компьютеру было всё равно: на то он и компьютер?

И в этот момент явственно ощутил, что таких аспектов, когда машине безразлично, а человек должен мобилизовать всю свою выдержку, терпение и прочие сопутствующие качества, будет крайне много.

Взять хотя бы Siri или Алису[1]: не раз приходилось слышать, как они заблуждаются насчёт речевых обращений своих «хозяев». И в итоге — раздражение. Но как бы ни извинялись помощницы — они не испытывают эмоций. Никаких. Поэтому приходится констатировать, что в подавляющем большинстве случаев при ничьей у роботов возникает явное преимущество.

При чём тут W3?

---

[1] https://yandex.ru/alice

Если принять во внимание глобальную систему репутации (см. ниже), где объект и субъект изначально равны, то получим, что на самом деле ситуаций подобного паритета будет с каждым годом всё меньше и меньше, за счёт как количественного увеличения устройств (один только рынок IoT[1] может насчитывать 30 млрд устройств при 8 млрд людей на планете), так и качественного, поскольку нейронные сети обучаются ежесекундно.

Но это далеко не единственный парадокс внутри W3 — рассмотрим и другие…

[1] https://youtu.be/n6Kl33jtxxk

СВОБОДА: СМАРТ-КОНТРАКТ И GDPR-КРЕПОСТНЫЕ

Недавно в Сети зашёл спор о том, что смарт-контракт есть ограничение свободы. Прежде чем развёрнуто ответить на тезис, а также вывести от него логическую связку к цифровому рабству, создаваемому через тестовый документ под вязкой аббревиатурой GDPR[1], обратимся к диаграммам Эйлера[2] — два непересекающихся круга: обычно люди примерно так представляют уровни свободы индивидуумов, но на самом деле в 99% случаев выглядит это иначе — как круги пересекающиеся, и довольно плотно.

То есть из уровней «зависимость — независимость — взаимозависимость» высшим всегда остаётся последний. Поэтому взаимное ограничение свободы на основе полученного волеизъявления и есть то высшее благо, за которое должен бороться всякий мыслящий человек в эпоху тотального перехода к регрессии формаций по К. Марксу[55].

Отсюда и возникает набор следующих условий:

---

[1] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

[2] https://en.wikipedia.org/wiki/Euler_diagram

— Смарт-контракт как определённая степень взаимных ограничений ради достижения общего результата (ограничения не имеют в данном контексте негативного нарратива) достигается через обоюдную договорённость сторон и никак иначе: проще говоря, «спущенные сверху» умные контракты противоречат собственной природе, как и акцептованные в одностороннем порядке.

— Кроме того, цель смарт-контракта не есть ограничение свободы субъекта (или объекта), а именно автоматизация конкретных действий (в случае DAO — набор расширяется, в случае Dapps'ов — масштаб увеличивается до глобального), то есть тем самым создаются условия для устранения рутинных операций для, что крайне важно (!), высвобождения времени под социальные транзакции более высокого уровня — творческих и подобных. Но никак не наоборот!

— И именно по этой причине smart-contract'ы, созданные[56] вне публичных блокчейнов или dag-подобных решений, не могут гарантировать ни собственного исполнения, ни взаимозависимости связанных через себя субъектов/объектов.

И в этом смысле W3 — не идеальное, возможно, но вполне допустимое решение, где каждая цепочка взаимосвязей может быть продиктована разной мотивацией и мотиваторами (будь то токены, социально полезная деятельность или что-то ещё).

ЦЕНТРАЛИЗАЦИЯ И WEB 3.0: КОРОТКО

Опять же, о полезности споров (но не дискуссий). Намедни, общаясь с одним из ведущих разработчиков, выявил два важных тезиса:

— Сайт может быть[57] централизован, но отдать юзерам «управление» своим пространством.

— Единая авторизация[58] предполагает и единый ключ шифрования данных для взаимодействия с другими участника.

Действительно, такой подход имеет место быть, но как он соотносится со степенями свободы, выраженными в разнопорядковых цифровых отпечатках личности?

Никак.

Потому как кастомизация интерфейса на сегодня доступна и в Web 2.0, а что касается единой авторизации, то это — техническая «надстройка» над Oauth 2.0[1] и аналогами. При этом всегда возникает вопрос «рубильника», потому как никакого распределения ответственности de facto не существует и администратор самостоятельно определяет правила, когда и кто имеет право на те или иные дей-

[1] https://ru.wikipedia.org/wiki/OAuth

ствия. Банальные чёрные списки (читай — антисписок Шиндлера).

Но важнее другое: никакая децентрализованная система не допускает ограничений для централизованных система apriori. Тогда как обратное — вполне объяснимо и существует сплошь и рядом.

То есть при доминирующем положении в Web 3.0 p2p-систем нового уровня (нечто подобное сейчас формируется в экосистеме[1] BitTorent & Tron) сохраняется и возможность многомерного распределения, включая и классические, клиент-серверные архитектуры.

В противном же случае цифровая зависимость будет уже не красивым эпитетом, а реальностью, которая вкупе с VR/AR-действительностью поглотит нас в ближайшую четверть века. Нас — как объекты!

[1] https://www.bittorrent.com/btt/

ДАПСЫ И ЛОКАЛЬНЫЕ ГЛОБАЛЬНЫЕ СЕТИ — НАХОДКА АРХИТЕКТУРЫ WEB 3.0

Dapps'ы (децентрализованные приложения) широко пиарятся ныне, не хуже ICO в 2016—2017 гг., но чем именно они так хороши? Задумывались ли вы, что сама по себе архитектура дапсов позволяет им быть фактически бесконечно вложенными?[59]

Что имеем сегодня: есть, допустим, Facebook & Instagram — взаимозависимые приложения. Но их вложенность минимальна: можно делать перепосты, есть ретаргетинг, указание профиля и всё в этом духе. Для пользователя всё равно два разных сервиса. Даже банальные юридические формальности — разные.

С dapps'ами всё не так: в них имеем возможность не только вертикального, но и горизонтального масштабирования, за счёт связок decentralized applications решений. Но и это не всё.

Как помним, W3, в отличие от создаваемой псевдодецентрализованной системы от корпораций (почитайте про blockchain от Facebook[1] и криптовалюту JP Morgan[2]), даёт

пользователю возможность самостоятельно генерировать для нужной степени вложенности свой цифровой отпечаток и распоряжаться им по временному, количественному и прочим измеряемым критериям.

Например, псевдоним Menaskop: сегодня ник есть на том же Facebook'е и Хабре, но что могу? На Хабре чуть больше: помимо лайков/плюсов можно заработать карму и рейтинг. Но как насчёт срока действия аккаунта? Либо удаляюсь и теряю всё (к тому же — более одного раза невозможно даже обнуление на Хабре, а на FB его и вовсе нет), либо принимаю правила и работаю «как есть».

Но это ведь мои (!) данные: даже уже GDPR (General Data Protection Regulation, правила защиты персональных данных, принятые в Европе) и ФЗ №152[3] в РФ приняли и подтвердили, что мои. Но только на бумаге: de facto всё хуже: корпорации зарабатывают на этом миллиарды, я — ничего, кроме набившей оскомину рекламы. Подписки ещё создадут прецеденты цифровой нетерпимости, но пока все упорно делают вид, что толерантны. Донельзя!

И вот здесь помогают цифровые слепки W3: сам определяю, когда и сколько хочу взаимодействовать с конкретным сервисом.

Первые шаги к этому — сервисы децентрализованной идентификации, социального майнинга (SportCoin, Bitradio, Brave), медиаблокчейны (Steem, Golos[60], Decent, UOS). Соответственно, в любой момент времени могу:

---

[1] https://coinmedia.ru/glava-facebook-mark-cukerberg-vnedrenie-blokchejn-podrazumevaet-bolshe-filosofskih-voprosov-chem-tehnicheskih/

[2] https://coinmedia.ru/vysokie-investicionnye-ocenki-kriptokompanij-seli-medvedi/

[3] http://www.consultant.ru/document/cons_doc_LAW_61801/

— ограничить ширину/глубину взаимодействия конкретного цифрового слепка;

— установить временной лимит (простейший пример — через смарт-контракт);

— удалить/восстановить конкретный слепок.

Таким образом, Menaskop всегда будет в конкретном децентрализованном или распределённом приложении, но ровно по тем параметрам, которые задам ему я. Кроме того, для dapps'ов на Ethereum будет, например, слепок с полномочиями из набора №1 — предельно широкий, для EOS — из набора №3, с минимальными полномочиями, а для Sia — №2. И, соответственно, связки Ethereum + EOS + Sia начнут работать от большего к меньшему.

Схема взаимодействия «цифрового слепка» пользовательских данных в Dapps в различных блокчейнах: *что это даёт*?

Помимо правильной с архитектурной точки зрения системы саморегулирования — ещё и практическую схему неразрывной взаимосвязи принципов децентрализации, анонимности, открытости и транзакционной репутации.

А что дают эти принципы?

Во-первых, главное — *свободный* Интернет. Хотим этого или нет, но сегодня Сеть[61] стала несвободной для большинства. Да, есть те, кто ежедневно отстаивает общие интересы, но пока общий процент минимален. W3 вкупе с другими тенденциями позволит этот процент удесятерить.

Во-вторых, подобный формат создаёт безграничные возможности для предпринимателей. Можно:

— объединять усилия и достигать синергии уже не на словах, а на деле: истинные DAO (на основе методик «бирюзовых организаций») — следующий шаг вперёд;

— придумывать новые общественные решения, невозможные в заданной сейчас системе координат и в принципе, и в конкретике;

— наконец, не бояться отключения со стороны провайдера, потому как они способны создавать ГЛС — глобальные локальные сети.

Wi-Fi Aware[1], предрасположенность 5G[2] к мэш-сетям (как и bluetooth-стандарта), развитие инфраструктуры для IPFS[3]/Filecoin[62] — следующий[63] шаг, которого так не хватало: покрыть физический уровень альтернативными (Интернету) сетями — задача ближайшего десятилетия.

И в этом смысле W3 — уже не логичное продолжение W2, но и модель противостояния тем негативным тенденциям, которые заложены в современном социуме: будь то управляемые цветные революции, законы[4] о едином цифровом профиле гражданина или вовсе — мировой рейтинг, созданный по непонятным правилам непонятными структурами.

---

[1] https://www.wi-fi.org/discover-wi-fi/wi-fi-aware

[2] https://secretmag.ru/news/eksperty-k-2025-godu-5g-pokroet-dve-treti-zemli-25-11-2019.htm

[3] https://youtu.be/zcCoWBCiwkI

[4] https://vc.ru/legal/83412-gosduma-podderzhala-zakonoproekt-o-sozdanii-edinoy-bazy-dannyh-rossiyan

ГЛАВА IV. WEB 3.0 — ЭТАП ЭВОЛЮЦИИ СИСТЕМ

Глава написана создателем децентрализованного объединения Synergis, писателем, философом, криптоэнтузиастом, анархистом, известным под ником Menaskop, Владимиром Поповым.

ОПЯТЬ ЭВОЛЮЦИЯ?

Изначально эта часть появилась не как элемент книги, но как предварительные исследования по проекту iTerra. Затем, уже в полной переработке — была вшита в общую ткань сего труда. И вот почему…

Дело в том, что, как только приступил к изучению W3, а было это в начале 2018 года, обнаружил, что всё, до чего бы ни дотрагивался взгляд, в той или иной степени является новым уровнем абстракции.

Допустим, языки программирования: изначально это был просто машинный код — отсюда эта сложная система 11001001000001111110110…, перфокарты и т. д. Затем появился ассемблер: первые хакеры, да и ныне живущие и придерживающиеся основ, отличались от обычных кодеров тем, что могли оптимизировать программы самыми нетривиальными[64] способами. Затем настала эпоха языков программирования высокого уровня[65]: то с победой ООП, то с возвратом к возможностям языков функциональных[1].

Но что же имеем сегодня?

Всё больше и больше технических специалистов понимают, что и в связи со сложностью существующих бизнес-

[1] https://en.wikipedia.org/wiki/Functional_programming

и иных социальных процессов, а равно и ввиду постоянных модификаций самих языков, платформ, которые через них создаются, и всей инфраструктуры в целом, даже не паттернизация[1], а *моделирование* является следующим уровнем абстракции, который следует применять для оптимизации всё новых и новых автоматизируемых сущностей.

Но языки программирования — только начало: одна из сущностей.

Дальше можно взять операционные системы и серверы: хотя в мире и есть Windows, Mac OS, BSD, Linux — на самом деле все они представляют собой ОСи предыдущего поколения.

Попытка же создать ОС именно сетевую[66], то есть децентрализованную и/или распределённую по своей сути, предпринималась не раз, но до момента перерождения концепта W3 — почти всегда неудачно: достаточно вспомнить проект Google[2].

Как бы там ни было, но именно архитектура W3, а равно и отдельные её составные части (тот же Urbit), возвращает к этой идеи, когда ОС находится не на каком-то определённом компьютере, а в любой допустимой сущности: это может быть суперкомпьютер (Ethereum), в том числе — специализированный (Sonm[3], Golem[4]); отдельный ПК; сервер; или что-то ещё (например — совокупность Dapps, внутри которых происходит имплементация и одновременно — обмен данными).

ОС подобного типа ещё в разработке с точки зрения привычного, то есть графического вида (и в ближайший

---

[1] https://en.wikipedia.org/wiki/Software_design_pattern

[2] https://ru.wikipedia.org/wiki/Chrome_OS

[3] https://sonm.com/

[4] https://habr.com/ru/post/332300/

год-два — почти наверняка не получится): но создание DOS было, как известно, необходимой вехой для рождения WinDOS.

При этом все элементы для генезиса абстракции уровня «сетевой компьютер с нужным софтом» уже есть:

— вместо привычных HDD/SSD/Raid-массивов — Filecoin, Storj, Sia, MaidSafe (или даже великая IPFS);

— вместо оперативной памяти и процессора — мощности от SONM, Golem и других;

— монитором в разных ипостасях могут выступать — blockchain с его реестр-подходом, хэши IPFS или браузер CYB (не стоит забывать, что есть ввод и вывод данных);

— а как насчёт материнской платы? Думаю, здесь аналогом выступят мультиблокчейны и любые другие «клеи» ДРС;

— что касается систем ввода, то помимо возможностей любого смартфона, терминала и других стандартных устройств — не стоит забывать и о наличии автономных IoT-единиц, которые, с одном стороны, будут выступать в роли оракулов (децентрализованный прогноз погоды), а с другой — послужат именно новым *способом* получения данных извне.

Аналогии можно продолжить, но, думаю, суть схвачена и ясна. Продолжим лучше далее относительно уровней абстракции.

ТОКЕНИЗАЦИЯ — НОВЫЙ И НЕОБХОДИМЫЙ РЫНОК

О токенизации, с одной стороны, можно говорить много и долго[67], с другой, это не что иное, как создание полного аватара субъекта, объекта и/или процесса в цифровом мире.

На сегодня человечество может покорять три основных пространства: Космос, Океан и Виртуальную реальность. Первым занимаются И. Маск, Р. Брэнсон, Д. Безос и другие; вторым — в тех масштабах, которых достиг Ж. И. Кусто, — почти никто; зато третье — одно из самых спорных, но доступных.

И токенизация в этом смысле — ещё и перенос ценности из мира офлайн[68] в мир онлайн, но для её понимания следует отречься от старых замашек тотального контроля и принять как данность (хотя бы) следующие тезисы:

— Частных денег, систем расчёта и единиц для переноса ценности может быть сколько угодно: простой и беглый анализ coinmarketcap с 2013 по 2020 год — лучшее тому доказательство. Если к 2013 набралось несколько десятков проектов, то сегодня — многим более двух тысяч, а есть ещё множество токенов, криптовалют и иных активов (ассетов), которые находятся внутри dex-бирж, созданы на какой-то платформе для ограниченного круга лиц

и т. д. И это — не просто нормально, но и ещё один возврат к системе, существовавшей в мире примерно до середины XIX века: именно на частные во всех смыслах деньги строили первые железные дороги, создавали телеграфные линии, и даже — маяки[69].

— Измерением для btc (или другой любой глобальной валюты) должен выступать сам btc (его аналог), то есть 1 btc = 1 btc, а уже затем — он (условно) стоит сколько-то долларов, рублей, etc или других единиц. Без понимания этого — невозможен фундаментальный, тектонический сдвиг.

— Токен, как написал выше коллега, — с одной стороны, есть техническая информация, но с другой, благодаря созданию такого гениального изобретения, как блокчейн, он ещё и обладает свойством передачи ценности на расстоянии без единого/централизованного субъекта-посредника, что, в свою очередь, означает, что здесь и сейчас создаём сеть (точнее — сети) нового уровня — с возможностью передачи как информации, так и value.

И именно в последнем пункте кроется вся красота простоты ДРС — многие вот уже 11 лет кряду задают вопрос: а где же практическое применение блокчейн-технологии? — но забывают, что прежде всего одним из самых главных достижений Сатоши Накамото явилось то, что он сделал невозможное: ещё в 1980-х «доказали», что решение задачи Византийских генералов[1] нереализуемо в принципе. Пожалуй, это сравнимо с доказательством теоремы Ферма и гипотезы Пуанкаре (к которой ещё вернёмся, поскольку она идеально накладывается на то, что называю объёмным поиском, когда для нахождения используем не индекс, но граф).

---

[1] https://en.wikipedia.org/wiki/Byzantine_fault

И благодаря этому возможно развитие W3 как самостоятельной концепции.

Как именно будет происходить процесс токенизации, сказать сложно, но очевидно, что:

— в нём будет и сегментация, поскольку ряд отраслей оцифровать можно уже сегодня и довольно просто (логистика, допустим), и фрагментация, поскольку всегда есть те, кто противится изменениям (в первую очередь будут сообщества проигравшие — то есть сверхцентрализованные);

— если вопрос техники и технологии можно считать решённым — по крайней мере в основании: токенизировать можно через чипизацию, через создание стандартов разного рода меток, — то вопросы этики остаются открытыми. На мой взгляд, *токенизация внутри систем не полностью открытых*, куда относятся международные организации, правительства, банки, брокеры и прочие централизованные структуры, создаёт все возможности для той самой регрессии формаций по К. Марксу, то есть движение в сторону рабовладельческого строя или рабства цифрового;

— наконец, в апогее — произойдёт выделение самоценности во вновь созданном мире, и он не будет напрямую связан с миром материальным, что, в свою очередь, породит сообщества *цифровых сепаратистов* и различные сущности, ранее не рождаемые. Впрочем, есть DeFi, DAO, смарт-контракты, автономные IoT-устройства, которые живут не совсем по правилам «реального» мира уже сейчас.

Всё перечисленное лежит в базисе двух важнейших феноменов: первый — зарождение экономики нового типа; второй — новая репутационная модель. О каждом — чуть подробней ниже.

ЭКОНОМИКА ДЕЙСТВИЙ — СФЕРА НОВАТОРОВ

Наверняка помните, что в период промышленной революции появилось движение луддитов[1], которые отстаивали архаичное (и в хорошем, и в плохом смысле) общество, считая, что машины навсегда заберут всю работу у людей.

Но что в итоге?

В итоге США, которые выиграли от промышленных революций (а с ними — и от мировых войн) больше всего, породили новые рынки в направлении, которое раньше было или маргинальным, или нишевым, или вовсе незаметным: речь идёт о сфере услуг.

Кино, а значит, и Голливуд, и Болливуд, и даже Мосфильм — услуги. Сфера красоты и всё, что с ней связано, — услуги. А ещё: консалтинг, IT в большей своей части, транспортные перевозки и прочее. Посмотрите на ВВП США, Китая, России и многих других стран: энергетика и финансы будут занимать в них немало места. Изучите топ компа-

[1] https://en.wikipedia.org/wiki/Luddite

ний мира: 10, 30, 100. Технологические и финансовые гиганты — в первую очередь.

И сегодня, здесь и сейчас, стоим на пороге новой, уже свершившейся революции — **революции майнинга**. Нет, веду речь не о GPU или ASIC-майнинге, но о монетизации любого тривиального действия, как то: ходьба, сон, секс, сдача мусора в переработку, волонтёрство и прочее.

Монетизация социального капитала — то, что ожидает нас в ближайшие 10—25 лет. Раньше просто совершали добрые поступки, но сегодня благодаря открытости, децентрализации и передаче ценности на расстоянии посредством криптографии можем превратить любой шаг, чих, улыбку человека в чистую монету, в токен.

Уже сейчас это оценили экологи, туристический бизнес, все, кто занимаются тушением пожаров и сбором/сортировкой отходов, а равно и те, кому близка позиция маркетолога. Благодаря таким решениям, как SportCoin, Bitrad.io, Siberia. Blog и им подобным каждый может генерировать деньги собственными навыками.

И если раньше человек развивался больше «для себя», то сейчас благодаря своей эволюции в интеллектуальном, эмоциональном, физическом векторе (а равно и в духовном, который в данном случае понимаю как качественный прирост к трём названным) он может выйти на новый рынок — рынок данных — и в буквальном смысле продавать себя.

И в этом случае встаём на очень и очень тонкую грань: с одной стороны, тезис «деньги есть у всех» равен тезису «денег нет ни у кого»[70], но в первом случае попадаем или в стадию истинного коммунизма (что бы под ним ни понимали конкретно в этом, положительном, ключе), или в стадию развитого, человеческого капитализма[71] с так называемой бирюзовой[72] системой управления, которая на деле есть не что иное, как горизонтальная методология решения управленческих задач.

Поэтому на сегодня, когда автоматизация — уже не праздный термин футурологов, фантастов и визионеров, за человеком остаются три следующих крупных направления:

— где есть human touch[73], или человеческое касание: будь то интересный массаж или психологическая консультация не у AI;

— требующие максимального уровня креатива и/или индивидуальной проработки: отличные ремесленники и художники-гении в разных сферах недаром так цены на рубеже веков. Кастомизация 2.0!

— там, где человек монетизирует себя сам. Свои деяния, то есть как действия (что очевидно), так и бездействия: например, проходит 1 км и в сообществе ходоков получает 10 токенов, у бегунов — 3, а любителей сибаритства — 0. Выезжает на природу и за неоставленный мусор получает в награду 5 токенов экосообщества №0.

Но это не всё: бесконечное начисление ни за что или начисление читерам может привести к весьма пагубным и нежеланным потому последствиям. Как быть? В этом случае в силу вступает методика системы глобальной репутации.

ГСР/СГР

Обычно к названиям подхожу строже, но в данном случае Глобальная система репутации подходит как дефиниция, потому что это именно система и не локальная; а система глобальной репутации — по той причине, что делает акцент на репутации как феномене всеобщем.

Как бы там ни было, но, начав работу над ней в 2017 году, совершил, пожалуй, главную ошибку — назвал обобщающий документ как «Протокол ГСР/СГР»: имелся в виду *протокол именно социальный*, коих в жизни предостаточно (вспомните санитарные нормы), но в информационном обществе это не прижилось — сильна связь с технологическим аспектом. Поэтому на сегодня именую сие методологией системы глобальной репутации.

ОСНОВНЫЕ ОШИБКИ РЕЙТИНГОВЫХ СИСТЕМ

В настоящее время существует огромное количество рейтингов и систем их учёта, начиная от лайков внутри социальных сетей, заканчивая (около) экспертными оценками ICO/IEO/STO и других стартапов, включая банковский скоринг.

Но, изучив опыт разных сервисов и проектов, можно сделать вывод о следующих ошибках, присущих большинству из перечисленных систем:

— почти любая из таковых пробует сделать превалирующим один из трёх факторов: временной, количественный или субъективный, тогда как именно их взаимозависимость — основа нормальной и стабильной работы;

— многие рейтинги после некой «внутренней стоимости» пробуют продавать, но это ошибка, которая никак не коррелирует с опытом каждого: *репутация — залоговая, а не расчётная единица;*

— кроме того, все нюансы рейтингов на деле могут быть унифицированы в простую структуру, а она может стать частью ГСР, описанной ниже.

Второй важный момент состоит в том, что есть как минимум три существенных различия ГСР и современных подходов к оценке репутации (опять же, с оговоркой, что в подавляющем большинстве случаев под ней понимается просто рейтинг).

1. Если сегодня даже блокчейн-проекты идентификации (civic и другие[74]) исходят из субъектной идентификации, то о «классических системах учёта» (паспорт, государственный реестр недвижимости и прочее) не стоит даже и говорить. ГСР же базируется на транзакцион-

ной[75] репутации, которая может применяться как к объекту (программа, IoT-устройство, робот), так и субъекту (истинный AI, человек, животное), которые при этом могут быть как анонимны и/или скрываться за псевдонимом, так и именованы согласно какой-то системе (языка, информационной составляющей и т. д.).

2. Большинство рейтингов, включая так называемый китайский народный кредитный рейтинг, на сегодня строятся на основе системы «наказание — поощрение», но поскольку исходят они от централизованных субъектов, это чревато разного рода манипуляциями, а главное — появлением общества изгоев. По этой причине ГСР базируется на том, что репутация — в первую очередь[76] элемент поощрения. И это — второй аспект глобального характера данного феномена: человек может быть хорошим родителем, прекрасным художником и ужасным руководителем, и во всех трёх аспектах оценка его репутации будет разной: от нейтральной к положительной и до отрицательной.

3. И главное: если централизованные системы текущего времени пытаются создать некий «единый протокол знаний о рейтинге субъекта», то ГСР, напротив, предусматривает бесконечное множество вариантов, основанных на унифицированных и элементарных[77] правилах учёта факторов, а равно — степеней их взаимодействия.

***

Теперь — подробней о каждому пункте, начиная с последнего.

(минус) 1 – –– – ––0– – –– – – (плюс) 1

В любой сфере репутация может равняться одному из трёх показателей:

— ноль — когда репутация только начинает копиться, то есть человек, организация или любой иной субъект/объект[78] только входит в отрасль/направление/сферу;

— плюс один — если в результате последовательных действий SaO набирает максимальное количество баллов (100) и переходит в статус доверенного узла (это может быть эксперт, нода, валидатор или что/кто-то ещё);

— минус единица создана как показатель отрицательной репутации для ситуаций, когда SaO умышленно или неосознанно (по объективным причинам) совершил действия, нарушающие доверие к нему со стороны других подобных SaO.

Такая система может показаться примитивной, но именно в этом её основное преимущество: репутация или есть, или её нет совсем; она может быть положительной или отрицательной; в разных сферах или одной.

Конечно же, для более привычного понимания понадобится дополнительный критерий — баллы или проценты внутри нуля, единицы и минус единицы.

0– – –– – –– – –– – –––100

Набирая от нуля до ста баллов, SaO тем самым может в конкретной отрасли улучшать свою репутацию: новому

SaO присваивается репутация 0/0 (ноль ГСР и ноль в балльной системе внутри ГСР).

Далее SaO зарабатывает за каждое полезное действие согласно критериям выше (временному, количественному и субъективному) баллы: заработав 100 баллов от нуля, SaO получает репутацию в единицу (плюс один) и уже может её закладывать.

SaO может копить баллы и далее, то есть внутри единицы также может быть пройден путь от нуля до ста. При этом внутри единиц баллы зарабатывать сложнее, и вводится коэффициент 0,5, то есть за каждое действие SaO может получить уже не 1, а полбалла[79].

Достигнув уровня +1 (100), SaO получает максимум и далее в этой сфере может поддерживать свою репутацию, а равно и тратить заработанные баллы в качестве оцифрованного социального капитала, который при этом никак не монетизируется с точки зрения привычного понимания валют (крипто- или фиатных).

Критерии же детерминируются так:

— временной — какой именно период времени SaO находится в системе? Это можно определить через генезтранзакцию (регистрацию) или иным способом;

— количественный — совершение одной итерации: пост, комментарий (для «жителей» соцсетей); выпущенная книга, напечатанный рассказ (для писателя); ремонт одного автомобиля (для механика) и т. д.;

— субъективный — оценка со стороны других SaO: плохой или хороший? Понравилось обслуживание или нет? И прочее.

Каждый критерий занимает 30%: итого — 90%. Но остаётся ещё 10% — они уходят на какой-то дополнительный признак, например, для полученных данных от оракулов. Впрочем, распределение может быть и 25% на 4 критерия, но в любом случае — не выше 30%, чтобы

подделку можно было легко обнаружить: скажем, если заменим временные метки, как это часто бывает у ботов в Facebook, но не создадим за указанное время (потому как аккаунта просто не было) полезных и оцениваемых транзакций (тех же постов), то подделка будет видна сразу.

Рассмотрим кратко следующие явления:
— залог репутации;
— отрицательная репутация и её свойства;
— социальный капитал и ГСР;
— репутационная система с точки зрения транзакций.

ЗАЛОГ РЕПУТАЦИИ

Данное действие служит основой любой модели внутри ГСР — монетизирует то, что SaO делает в течение определённого времени: важно, что репутация может быть заложена (в общем случае) при наличии хотя бы двух (и более) единиц, внутри которых — не менее 50 баллов (в каждой). Это логично, потому как стоимость чего-либо в транзакционной системе определяется кумулятивным[1] эффектом транзакций.

В зависимости от сложности проекта, обоснованности риска и других факторов к залогу может быть представлено большее количество минимальных единиц. При этом *залогом служат всегда все единицы одновременно*: это со-

[1] https://en.wikipedia.org/wiki/Shaped_charge

ответствует категории «поставить всё на кон» в обыденной жизни.

Количество баллов внутри каждой единицы может изменяться для залога в сторону увеличения (но не может быть меньше 50)[80].

Таким образом, репутация позволяет копить социальный капитал и монетизировать его, а с его помощью получать капитал обычный (в фиате или криптоденьгами, основными средствами производства и т. д.).

Залоговая функция репутации является тем, ради чего подобную систему можно строить в принципе, особенно в связи с тенденциями, раскрытыми ниже.

ОТРИЦАТЕЛЬНАЯ РЕПУТАЦИЯ

Данный вид репутации возникает в тот момент, когда SaO не выполняет свои обещания, данные при залоге репутации или в системе транзакций через репутацию.

Поскольку обман может быть преднамеренным, а может — в силу объективных причин, то внутри минус единицы репутации возможна градация по баллам от минус ста до нуля.

Дабы избежать, с одной стороны, порочной системы рейтингов, когда сам по себе статус становится некой ценностью, за которую люди готовы отдать всё что угодно (простейший пример показан в том же сериале «Чёрное зеркало» через систему лайков-дизлайков), необходимо, чтобы всякий SaO при первой или даже последующих ошибках мог улучшить положение.

Для этого при залоге репутации определяется максимальный порог баллов внутри минусовой репутации (но не может быть менее 25% в общем случае[81]). Возникает коэффициент сложности: при первом получении отрицательной репутации — 0,5, далее — 0,25, далее — деление предыдущего коэффициента на 2. Тем самым за каждое действие в минусовой репутации будет начисляться в два раза меньше баллов, при повторном обнулении — в четыре и так далее.

С одной стороны, такой подход позволяет SaO исправить даже самое удручающее положение, с другой — не даёт возможности мошенникам просто так использовать доверие других и быстро зарабатывать баллы.

СОЦИАЛЬНЫЙ КАПИТАЛ И ГСР

Социальный капитал для ГСР имеет двойную природу: во-первых, сама репутация есть отражение накопленного и созданного социального капитала, во-вторых, социальный капитал может генерироваться и в результате достижения SaO в той или иной области единицы с максимальным (100) количеством баллов. В этом случае социальный капитал может быть монетизирован (конвертирован в капитал финансовый) через залог репутации.

ГСР И ТРАНЗАКЦИОННЫЕ СИСТЕМЫ

Репутация не может быть единицей расчёта, но за счёт возможности залога может быть использована для совершения транзакций. В этом смысле всякий SaO выполняет роль одной конкретной ноды[82].

Для проведения транзакции в этом случае необходим поиск двух нод, обладающих положительной (плюс один) репутацией[83] и минимальным количеством баллов (допустимый min — 1/000[84]).

Для SaO с репутацией 1/100 транзакция проводится/подтверждается такими же SaO или, в случае отсутствия других подобных SaO, SaO, наиболее близкими к заданному[85]. Все остальные транзакции проводятся SaO с репутацией равной или большей, чем у SaO, который транзакцию инициирует.

Но данные условия создают систему, где инициализация транзакции осуществляется отправителем, как и её подпись, тогда как объективный мир диктует нам условия, в которых часто транзакция инициализируется получателем.

Так, когда хочется, чтобы со мной поговорил какой-то субъект, — не обязательно инициализировать транзакцию внутри системы «телефон — станция — телефон»: могу оставить сообщение иным способом, но инициализация произойдёт уже в заданной системе коммуникации.

При ненарушении договорённостей именно так работают пенсионные фонды: пенсионер в заданной структуре имеет право на минимальную выплату, которая инициализируется одним из возможных способов по достижении условия — определённого возраста. Сейчас процедура сопровождается бюрократическими проволочками, но с по-

мощью ДАО/DeFi-фондов можно (и нужно) сделать её полностью автоматической.

Куда более удивительным является осознание, что подобные транзакции могут возникать спонтанно: скажем, на счету SaO лежит 1 000 000 единиц (SaO №x). Каждый иной SaO может в любой момент времени взять не менее 1 единицы и не более 100. Поэтому совсем скоро на аккаунте SaO №x может оказаться 1000. Но ровно так же он может взять у любого SaO, у которого сумма превышает заданный остаток, нужную сумму, если только нет заморозки (стейкинга), обусловленной исполнением уже взятой и разрабатываемой задачи.

Зачем нужен такой подход?

— Для совершения транзакций с использованием репутационных систем, когда понятие денег важно лишь для облегчения количественного учёта внутри системы.

— Для разного рода социальных проектов, которые с помощью такой единицы могут лимитировать и рассчитывать свои расходы исходя из условия, что «денег достаточно».

— В случае тестирования любых систем с социальным капиталом.

Такое видение кажется необычным, но только в заданных координатах времени и пространства, где за основу взят тезис «деньги — ограниченный ресурс». На самом же деле уже давно, как минимум с момента создания ФРС, деньги — безграничный ресурс для ограниченного числа субъектов. Почему же всякий не имеет права на подобную систему в тех или иных целях, не противоречащих принципам конкретного социального или иного образования?

И всё же ответа требует и главный вопрос, поставленный неявно выше: так в чём же связь ГСР и Web 3.0? Ответов[86] — множество, и один из главных лежит в плоскости консенсусов…

АЛГОРИТМЫ КОНСЕНСУСА

Глава написана Игорем Белоусовым — CTO The Power, одним из основателей антискам-сообщества The White Guardian, разработчиком и консультантом Synergis.

Начиная разговор об алгоритмах консенсуса, нельзя обойти само понятие «консенсус»: оно довольно обширное. Обратим внимание на следующую часть понятия:

— консенсус — способ принятия группой участников *общего решения*, в случае если отсутствуют принципиальные возражения у большинства участников.

— соответственно, алгоритм консенсуса — последовательность действий для компьютерных систем, которая, если ей следует каждая участвующая в консенсусе компьютерная система, приводит к принятию всеми участниками общего решения. То есть это набор инструкций, которые выполняет каждый компьютер, участвующий в распределённой системе, чтобы все участвующие компьютеры приняли общее решение. А вот зачем компьютеры собирают в распределённые системы и заставляют приходить к «общему решению» — рассмотрим далее…

ИСТОРИЯ ПОЯВЛЕНИЯ АЛГОРИТМОВ КОНСЕНСУСА

В процессе развития автоматизированных систем всегда присутствовали два вызова (направления) — увеличение отказоустойчивости системы и увеличение производительности. И если закон Мура[1] хорошо помогал в увеличении производительности компьютерных систем — для достижения требуемых возможностей можно просто подождать, то вопрос с отказоустойчивостью всегда стоял остро, особенно когда касался важных сфер.

Классический инженерный подход дублирования мог помочь и тут. Однако в случае дублирования инженерных систем должен быть человек, который зафиксирует факт поломки основной подсистемы и переключит систему на дублирующий контур. Введение на место человека автоматики помогает, но что же делать, *если проблема появляется в автоматике*? Дублировать? Но тогда у этой подсистемы для дублирования автоматики тоже должен быть кто-то её контролирующий, а значит, если хотим получить

[1] https://en.wikipedia.org/wiki/Moore%27s_law

в этой парадигме идеальный результат, — получаем недостижимый бесконечный круговорот.

На практике же строят не бесконечные контуры дублирования, а один, максимум два.

Другое направление в решении проблем отказоустойчивости предлагают алгоритмы консенсуса. В этом случае также существуют «дублирующие» подсистемы, однако они работают постоянно и равноправно, договариваются о результатах своей работы. Причём отказ одной из подсистем является нормальным и ожидаемым исходом при «общении» подсистем. Поэтому для такого класса систем не требуется дополнительных контуров автоматизации принятия решений, и пока количество работающих подсистем не превышает критическое, система продолжит работать.

Однако позже выяснилось, что и у систем, основанных на консенсусах, тоже есть уязвимые места. Система может перейти в ненормальный режим работы или остановиться, если одна из подсистем не просто выйдет из строя, а начнёт «болеть» — работать с ошибками. В таком случае при достижении консенсуса сообщения, отправляемые «больной» подсистемой, приводят к сбоям консенсуса или же к его постоянному поиску, что выглядит как полная неработоспособность системы.

В статье Википедии[1] приведены несколько случаев, когда в реальном оборудовании случались «византийские» отказы.

История о том, почему поведение, при котором одна или несколько подсистем при консенсусе ведут себя некорректно, было названо византийским, интересна сама по себе. Дело в том, что проблема появления «больной» подсистемы, мешающей работе консенсуса, сформулирована

[1] https://en.wikipedia.org/wiki/Byzantine_fault#Examples

и формализована Робертом Шостаком[1] и названа проблемой интерактивного согласования. Однако Лесли Лэмпорт для упрощения понимания разработал красочную аллегорию, в которой группа генералов армии планирует нападение на город. И в 1982 году эта версия описания проблемы вместе с вариантами решения была опубликована под названием «Проблема византийских генералов[2]» (The Byzantine Generals Problem).

С тех пор было предложено много различных формулировок, предложим и мы — упрощённую.

Есть город, который осадила Византия, вокруг города много византийских армий под руководством генералов, генералы не могут встретиться для принятия решения о нападении и всё время остаются в пределах своих армий. Стоит задача принять решение: или нападать в ночь на город, или отступить. Если большая часть генералов придёт к одинаковому решению, потери будут минимальны; в противном случае — проигрыш. Последняя важная особенность проблемы — среди генералов есть шпионы, цель которых — как раз поражение.

В результате все алгоритмы консенсусов делятся на CFT — устойчивые к отказам — и BFT — устойчивые к византийскому поведению.

В 1999 году опубликована работа Practical Byzantine Fault Tolerance, в которой предложен алгоритм консенсуса PBFT[3], который позволил серьёзно упростить и ускорить согласования общего решения.

В 2008 была опубликована статья Bitcoin: A Peer-to-Peer Electronic Cash System, в которой был предложен новый BFT-консенсус (названный впоследствии proof of work,

---

[1] https://en.wikipedia.org/wiki/Robert_Shostak

[2] https://en.wikipedia.org/wiki/Byzantine_fault

[3] https://en.bitcoinwiki.org/wiki/PBFT

PoW[1]), который позволял участвовать в консенсусе неограниченному кругу узлов (предыдущие консенсусы требовали того, что «византийские генералы» должны знать друг друга).

[1] https://ru.wikipedia.org/wiki/POW

ДЕЦЕНТРАЛИЗОВАННЫЕ ПЛАТФОРМЫ — СЛЕДУЮЩИЙ ЭТАП В ИСТОРИИ РАЗВИТИЯ КОНСЕНСУСОВ

До публикации статьи о биткоине все консенсусы (CFT и BFT) предназначались для повышения отказоустойчивости информационных систем, собранных из различного числа равноправных компьютерных узлов. Биткоин же стал первым представителем нового класса информационных систем — децентрализованных платформ. Оказалось, что BFT-консенсус позволяет в информационной системе, состоящей из независимых узлов, принимать общее решение для всей системы в соответствии с её (!) правилами. И если часть узлов хотят предложить решение, которое не соответствует этим правилам, то пока их меньшинство, они не смогут навязать это решение.

Пользователь в такой системе, отправляя своё задание (транзакцию), ожидает гарантированного его выполнения в случае, если оно не противоречит правилам системы. Также это свойство децентрализованной системы описывают

как гарантированное выполнение задания в недоверенной среде, где под недоверенной средой подразумеваются все узлы системы, так как часть из них может быть недобросовестными, но пользователь не знает не только, кто из узлов является недобросовестными, но и присутствуют ли среди узлов недобросовестные.

Появление первой такой децентрализованной платформы не сразу, но привело к осознанию выгод нового класса информационных систем. И вскоре начало появляться всё больше разнообразных платформ, в том числе работающих на «инновационных» консенсусах.

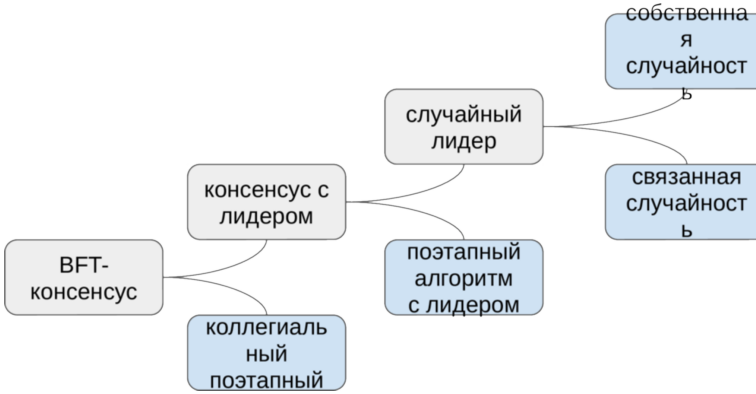
Вследствие того, что практически каждая новая платформа разрабатывала свой собственный консенсус, их набралось достаточно много, и разбираться в их особенностях стало проблематично. Поэтому далее по тексту предлагается собственная классификация алгоритмов консенсуса децентрализованных платформ.

БАЗОВЫЕ АЛГОРИТМЫ КОНСЕНСУСА ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМ

Не только своим названием алгоритмы консенсуса похожи на свой «прототип»: на самом деле, если внимательно вглядеться в действия, происходящие внутри алгоритмов, можно найти прямые аналоги действий группы людей.

Какие же способы придумало человечество для быстрого принятия общего решения?

Первое, что приходит на ум, — использование лидера. Многие древние социумы[87] так управлялись. Именно лидер даёт общее решение, а остальные участники проверяют и принимают текущим лидером решение. Но история человечества говорит о том, что лидер может или решить остаться надолго лидером, или же неожиданно подвести. Поэтому в алгоритмах консенсуса существует правило выбора текущего лидера и правило, по которому определяется необходимость выбора лидера: в зависимости от того, по каким правилам происходит выбор лидера, можно различать базовые алгоритмы консенсуса децентрализованных систем.

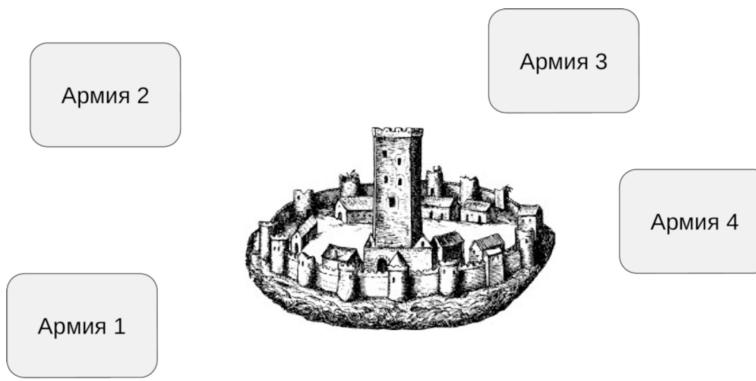


Дерево классификации алгоритмов консенсуса децентрализованных систем

На рисунке видно, что на дереве возможных вариантов алгоритмов BFT-консенсуса существует 4 листа, которые и являются базовыми видами алгоритмов BFT-консенсуса. Заметим, что, кроме трёх алгоритмов с «лидером», присутствует алгоритм консенсуса под названием «коллегиальный поэтапный». Этот алгоритм можно сравнить с механизмом явного голосования в человеческом социуме: в работе алгоритма принимают участие все участники децентрализованной платформы, это отражено в названии как «коллегиальный», а для того, чтобы получить результат в случае присутствия недобросовестных участников, все взаимодействия разбиты на стандартизированные этапы, что отражено в названии.

КОЛЛЕГИАЛЬНЫЙ ПОЭТАПНЫЙ АЛГОРИТМ КОНСЕНСУСА

Для того чтобы показать, как работают алгоритмы формата «поэтапный коллегиальный», приведём пример, который использовался для решения задачи византийских генералов в самом начале её появления.



Задача византийских генералов

На рисунке у нас показан частный случай, в котором

всего четыре армии атакуют город. Пусть генерал третьей армии является шпионом. Для принятия общего решения генералам нужно передать друг другу данные о количестве войск.

Само решение задачи состоит в поэтапном выполнении алгоритма, всеми участниками:

— каждый генерал отправляет остальным данные о своей армии (X_i);

— затем каждый генерал дожидается такой же информации от остальных троих генералов (X_k, X_n, X_m);

— и на следующем этапе посылает всю полученную информацию всем генералам (X_i — данные первого этапа, X_{jk}, X_{jn}, X_{jm} — данные второго этапа).

В результате окончания этих этапов у каждого генерала появляется копия всех сообщений генералов, переданных в рамках принятия решения. Если бы не было шпиона, данные у всех генералов были бы одинаковые. Однако, так как предполагается, что он есть, его надо выявить. Для этого все полученные данные у каждого генерала заносятся в таблицу.

	Генерал 1	Генерал 2	Генерал 3	Генерал 4
От Генерала 1	x	(1,2,x,4)	(1,2,x,4)	(1,2,x,4)
От Генерала 2	(1,2,y,4)	x	(1,2,y,4)	(1,2,y,4)
От Генерала 3	(a,b,x,d)	(e,f,y,h)	x	(i,j,z,l)
От Генерала 4	(1,2,z,4)	(1,2,z,4)	(1,2,z,4)	x

Изучив таблицу, каждый из трёх добросовестных генералов придёт к выводу, что третий генерал — шпион, и больше не будет доверять тем данным, которые он прислал. Вычеркнув эти данные, все добросовестные генералы получат одни и те же данные, на основании которых

принимается одно и то же решение.

Как видите, в алгоритм вовлечены все участники, которые взаимодействуют на каждом из этапов, без выделения какому-то участнику дополнительных прав. Именно поэтому этот тип алгоритмов и называется поэтапным, коллегиальным.

Основным недостатком алгоритма из приведённого примера является большая вычислительная и сетевая нагрузка на систему. Так, в приведённом примере с четырьмя генералами нам нужно обработать матрицу 4 на 4, но при ста генералах матрица уже будет 100 на 100.

АЛГОРИТМ КОНСЕНСУСА «ПОЭТАПНЫЙ С ЛИДЕРОМ»

Вот и начали рассмотрение первого типа алгоритма с лидером. Как уже отмечалось, основное его отличие от других в том, как происходит захват лидерства. У данного типа консенсуса получение «звания» лидера происходит вследствие правил поэтапного согласования. Эта часть очень похожа на уже описанный поэтапный, коллегиальный алгоритм, но особенность в том, что здесь она применяется не для формирования общего решения, а только для выбора лидера: уже лидер в течение некоторого времени будет формировать общее решение, которое затем будут подтверждать остальные участники. В человеческом социуме близкий аналог — корпорация, в которой управляет генеральный директор, избранный советом директоров.

У этого алгоритма есть две фазы: первая — когда лидер выбран и он работает нормально; вторая — избрание нового лидера. За счёт двухфазности алгоритмы типа «поэтапный с лидером» в случае отсутствия проблем с лидером обычно быстрее поэтапных коллегиальных.

АЛГОРИТМ КОНСЕНСУСА «ЛИДЕР С СОБСТВЕННОЙ СЛУЧАЙНОСТЬЮ»

Есть ещё один способ, кроме «согласования» для того, чтобы выбрать лидера, и, как всегда, есть аналог из опыта человечества — отдать такой выбор на волю случая.

Тут известны как минимум два варианта «случайности». В алгоритмах консенсуса типа «лидер с собственной случайностью» все участвующие изначально равноправны в борьбе за лидерство и должны сами добиться счастливого случая, а потом его предъявить для доказательства остальным участникам.

Если говорить образно, то собственная случайность похожа на классические способы получения случайных величин из теории вероятностей — бросание монетки или костей, то есть для того, чтобы выиграть лидерство, надо, например, бросая четыре кости, получить на всех четырёх по 6 очков. И тот, кто первый сложит перед всеми остальными участниками такую комбинацию, становится лидером.

Именно на платформе Bitcoin был впервые предложен цифровой аналог такому бросанию костей — консенсус PoW. При каждом согласовании общего решения к содер-

жанию общего решения применяется хэш-функция[1], в результате которой получается строка из 256 единиц и нулей. Выигрывает лидерство тот участник, который получит в начале строки определённое количество нулей. Эта хэш-функция интересна тем, что нельзя из результата строки с нужным количеством нулей получить нужное содержимое состояния. И единственный способ получить выигрышную строку — раз за разом немного изменять новое состояние, чтобы в результате вычислить выигрышную строку, что один в один похоже на кидание костей из примера.

[1] https://en.wikipedia.org/wiki/Hash_function

АЛГОРИТМ КОНСЕНСУСА «ЛИДЕР СО СВЯЗАННОЙ СЛУЧАЙНОСТЬЮ»

Второй тип получения лидерства с помощью случая больше похож на выигрыш призов из барабана: в барабан складываются присланные идентификаторы узлов, а затем один или несколько счастливчиков достаются из барабана. Именно то, что вероятность выигрыша у всех равна и выигрыш одних означает проигрыш других, отражено в названии этого типа алгоритма консенсуса — «связанная случайность».

Однако в примере с барабаном есть особенность, которая не присуща рассматриваемому типу алгоритмов, — вращение барабана добавляет действительную случайность, которую нельзя проверить и предъявить для проверки для других узлов.

Для того чтобы решить вопрос со случайным вращением барабана, была изобретена проверяемая случайная функция (Verifiable random function[1]), которая при подаче в неё переменных S — состояния платформы, V — нового

[1] https://en.wikipedia.org/wiki/Verifiable_random_function

общего решения, Id — идентификатора участника возвращает результат «случайности»: VRF (S, V, Id) = вероятность выигрыша лидерства.

Благодаря тому, что все переменные известны всем участникам, любой участник может проверить, выиграл ли «лидер» в этот раз в соответствии с правилами.

	поэтапный коллегиальный	поэтапный с лидерством	лидер с собственной случайностью	лидер со связанной случайностью
Противостояние цензуре	да	нет	нет	нет
Независимая случайность	да	нет	нет	нет
Быстрая работа при малом количестве узлов	да	да	нет	да
Тысячи и более узлов	нет	нет	да	да
Ветвление	нет	нет	да	да
Вероятность захвата постоянного лидерства	нет	нет	нет	да
Permissionless	нет	нет	да	да
Примеры алгоритмов	Resonance, Hashgraph	pBFt, Tendermint, LibraBFT	PoW, PoC	

Свойства базовых алгоритмов консенсуса

Противостояние цензуре: из-за того, что лидер всегда сам формирует общее решение и может просто часть заданий пользователей не включить в него, — влияет на содержимое, явно или неявно подвергая его цензуре.

Независимая случайность: в децентрализованных системах большие сложности со случайностью, так как у каждого участника системы при вычислении случайной функ-

ции для отражения в общем решении должно получиться одинаковое число (иначе у каждого участника будет при проверке получатся своё «общее» решение).

Поэтому для получения случайности на уровне общего решения можно использовать только VRF (S), где S — состояния системы перед принятием текущего общего решения, а значит, S — результат предыдущего общего решения. Так как знаем, что есть алгоритмы, которые позволяют лидерам цензурировать общее решение S, то, соответственно, в этих алгоритмах лидер влияет на результат VRF (S); значит — влияет на случайность, и она уже не «случайна».

Быстрая работа при малом количестве узлов — эмпирическая характеристика, показывающая, что алгоритмы с поэтапными расчётами очень быстры при малом количестве узлов в системе. В то время как у алгоритма типа «лидер с собственной случайностью» нет особой зависимости скорости от количества узлов. Из-за того, что необходимо выждать некоторое время для получения подтверждения выигрыша лидерства, его скорость примерно постоянна, получается, этот алгоритм выигрывает при работе с большим количеством узлов. Так как алгоритм типа «лидер со связанной случайностью» не требует ожидания, он одинаково хорош как при малом количестве узлов, так и при большом.

Тысячи и более узлов — дополнение к предыдущему свойству, показывает, что у алгоритмов с поэтапными расчётами существует предел по количеству узлов, после достижения которого время и мощности на согласования общего решения превышает разумные величины, в то время как у алгоритмов со случайным лидерством такой проблемы нет.

Ветвление — свойство алгоритмов со случайным лидером. Так как лидерство достигается в результате случайности, то есть вероятность, что выигрышную случай-

ность получили одновременно более одного участника. Для правил системы выигрыш всех абсолютно легитимен. Естественно, необходим механизм, который позволяет всем участникам решить, какое из ветвлений (из предыдущего состояния, как из корня, предлагаются новые легитимные общие решения, как будто новые ветви) «правильное».

Общепринятым стало правило: пока у соперничающих лидеров одинаковая длина ветки (количество принятий общего решения после ветвления), они равноправны и любой участник может сам выбирать, какую ветку поддерживать. Но в случае если чья-то ветка вырвалась вперёд, участники для продолжения работы платформы и поиска лидерства выбирают её (более длинную ветвь). Из-за элемента ветвления пользователю в таких алгоритмах необходимо ждать некоторое количество принятий общих решений, чтобы быть уверенным, что его задание было включено в общее решение.

Вероятность захвата постоянного лидерства: это свойство касается только алгоритма типа «лидер со связанной случайностью». Как уже писалось выше, из-за возможности цензуры лидер может влиять на состояние системы, а значит, влиять и на результат функции VRF (S, V, Id). И теоретически, влияя на S, может получить постоянное лидерство. Из-за того, что пока не представлено варианта, в котором доказана невозможность захвата лидерства, этот алгоритм без доработок не используется в публичных проектах и не имеет примеров своего воплощения.

Permissionless: эта характеристика свойственна алгоритму со случайным лидером. Означает, что нет необходимости любому участнику на Земле получать права на работу в системе. Для того чтобы стать лидером и участником системы, достаточно предъявить доказательство выигрыша лидерства, в то время как алгоритмам с поэтапными расчётами необходимо знать, кто именно

участвует в работе системы. Обычно в этих алгоритмах участники задаются в начале работы системы, и если необходимо добавление участника, только имеющий право может это сделать, поэтому часто такие алгоритмы также характеризуют как permissionless.

Как видно по таблице, среди базовых алгоритмов нет «серебряной пули» — алгоритма, у которого нет изъянов. Наиболее интересно (вроде бы) выглядит алгоритм с лидером со связанной случайностью. Однако из-за вероятности захвата лидерства меньшинством этот алгоритм без доработок не используется.

А что же за доработки могут быть у алгоритмов консенсуса?

АЛГОРИТМЫ КОНСЕНСУСА ДЛЯ ПЛАТФОРМ

Каждый из базовых алгоритмов, рассмотренных ранее, имеет те или иные недостатки, поэтому многие современные платформы «дорабатывают» их, вводя новые этапы, добавляя новые алгоритмические части.

На самом деле даже платформа Bitcion не использует описанный базовый алгоритм лидера с собственной случайностью: в алгоритм PoW внесён экономический фактор — токен биткоина (btc), благодаря которому, хоть и опосредованно, создаётся система безопасности платформы (майнить блоки — создавать новое общее решение Bitcoin выгодно, а значит — выгодно вкладывать деньги в оборудование майнинга; значит — злоумышленнику придётся потратить огромные деньги, чтобы попытаться взломать систему).

Некоторым не понравилась не сама экономическая составляющая, а то, к чему привело её введение: к созданию больших майнинговых пулов, на которые приходится тратить значимое[88] количество электроэнергии. Для изменения тенденции были предложены следующие доработки.

ПЕРВЫЙ ВАРИАНТ POS-АЛГОРИТМА

К алгоритму PoW биткоина предлагается добавить часть, которая позволит упрощать сложность вычисления в зависимости от количества токенов платформы у майнера.

Идея в следующем: уменьшить сложность вычисления хэша настолько, насколько большое количество токенов находится у майнеров.

Пусть обычная сложность PoW равна 20, то есть необходимо найти такой хэш, у которого 20 первых символов — нули. Допустим, у одного майнера есть одна треть всех монет, а у другого одна десятая. Тогда по правилам PoS сложность для первого получится 14 нулей (20—20*⅓ = 14), а для второго 18 соответственно (20—20*1/10 = 18).

Если сравнивать это в вычислительной мощности, то владельцу одной трети монет необходимо в 16 раз меньше (!) мощностей, чем владельцу с объёмом одной десятой от всех монет, и в 64 (!!) раза меньше, чем тем, у кого отсутствует значимый объём монет для того, чтобы вычислить выигрышный хэш.

К минусам такого улучшенного алгоритма относят тот факт, что владельцы крупных стейков могут позволить себе при минимальных затратах параллельно рассчитывать несколько ветвей, из-за чего увеличивается время необходимого ожидания для нивелирования эффекта ветвления.

Также, если попробовать представить то, как, скорее всего, будет развиваться платформа с таким алгоритмом, можно прийти к выводу, что в отдалённой перспективе будут полностью отсутствовать майнеры с неэффективным стейком. Что означает, что количество майнеров устаканится (и их стейк станет примерно одинаков) и опять начнётся гонка майнинговых мощностей.

Таким образом, несмотря на то, что такой алгоритм даёт быструю энергоэффективность сейчас, в долгосрочном периоде гонка мощностей вернётся обратно.

Рассмотренный алгоритм гипотетический: его предложили, однако никогда не использовали в проектах, поэтому его и называем PoS первого поколения. В настоящее время под названием PoS практически всегда понимается другой алгоритм, хоть и довольно сильно на него похожий.

Современный PoS-алгоритм по своим характеристикам можно включить в большую группу алгоритмов децентрализованных платформ, которые следует охарактеризовать как составные, или централизованные, алгоритмы.

АЛГОРИТМЫ ДЕЦЕНТРАЛИЗОВАННЫХ ПЛАТФОРМ С ЦЕНТРАЛИЗАЦИЕЙ

Многие проекты, создающие новые децентрализованные платформы, стараются нивелировать те или иные проблемные свойства базовых алгоритмов, описанных в таблице. Особенно часто стараются повысить общую пропускную способность системы. По таблице с особенностями базовых алгоритмов видно, что наибольшую скорость можно получить, используя алгоритмы с поэтапными расчётами.

Поэтому появился очень большой пласт алгоритмов, таких как PoS, DPoS, LPoS, PoI, которые по-разному делают схожие вещи.

Во-первых, они похожи тем, что используют составной алгоритм консенсуса. Первая часть алгоритма ответствен-

на за справедливое уменьшение участвующих в консенсусе узлов. Термин «справедливое» здесь означает, что, по мнению авторов, применяемый алгоритм уменьшения количества узлов практически не влияет на децентрализацию системы. То есть захват такой системы меньшинством настолько же вероятен, как если бы уменьшения количества узлов не было. А вот вторая часть — один из базовых алгоритмов, который показывает хорошие скорости, работая при малом количестве узлов.

Какие же алгоритмы ограничения придуманы?

— PoS второго поколения — только узлы, имеющие в собственности токены выше порогового значения, участвуют в консенсусе. Заметьте разницу: в PoS первого поколения количество токенов влияло только на сложность майнинга, и даже узлы с малым стейком могли участвовать в консенсусе. Во втором варианте их просто не допускают.

— DPoS — идея похожа на PoS, но здесь владельцы монет могут не участвовать в работе системы, а делегировать свои монеты, выбирая тех, кто им больше понравится, в производители блоков платформы, таким образом, у миноритариев есть больше прав, чем в варианте с PoS.

— LPoS — в общем-то, полный аналог DPoS с точки зрения алгоритма уменьшения узлов. Разница в добавляемой экономической мотивации. В DPoS миноритарии «голосуют» за понравившегося кандидата, а в LPoS за делегируемые токены выплачивается вознаграждение.

— PoI — идея, когда не только владение токенами платформы является мерилом, на основе которого будет происходить уменьшение узлов. Алгоритм появился на платформе Nem[1] и учитывал также активную деятельность узла на благо платформы.

[1] https://en.wikipedia.org/wiki/NEM_(cryptocurrency)

Выше были рассмотрены алгоритмы ограничения количества активных участников, в которых в той или иной мере за ограничение отвечало «богатство» участника. Однако многие критикуют такое направление ограничения и предлагают использовать другие методы. Относительно недавно появилось несколько платформ, которые применяют чисто алгоритмические способы.

Zilliqa — платформа, в которой для первичного ограничения используется алгоритм PoW, а уже после того, как появились победители-участники, начинают работать по алгоритму PBFT.

Algorand — платформа, в которой для первичного ограничения используется алгоритм с применением VRF, а уже после того, как появились победители-участники, они начинают работать по алгоритму PBFT.

Но алгоритмы консенсуса хоть и невероятно сложны, всё же не являются единственным камнем преткновения современных систем, участвующих в построении архитектуры W3. Как уже наверняка заметили, скорость — вот истинный камень преткновения при реализации любых консенсусов. И об этом — чуть подробней…

ШАРДИНГ

СКОРОСТНЫЕ ДЕЦЕНТРАЛИЗОВАННЫЕ ПЛАТФОРМЫ

Глава также написана И. Белоусовым (CTO The Power).

Скорость. В физическом смысле это метрическая величина, на которую переместится предмет относительно своего предыдущего положения за определённое время. Как видно, даже такое «простое» определение довольно сложно использовать для дальнейшего разбора скоростных платформ. Поэтому предлагаем использовать в дальнейшем слово «быстрый» и описать основные аспекты «быстроты» платформ.

Для наглядности предлагаем сравнивать понятие быстроты децентрализованных платформ с быстротой перемещения грузов.

Какие же аспекты в быстром перемещении груза?

— Конечно же, время поставки груза. Чем время доставки одного груза получателю меньше, тем сама поставка быстрее.

— Пропускная способность доставки. Чем больше грузов можно доставить одновременно, тем быстрее получается общая быстрота доставки.

— Себестоимость. Хотя быстрота доставки груза не зависит напрямую от себестоимости, но при планировании того, каким способом будет происходить отправка, себестоимость стоит чуть ли не на первом месте.

Если грубо обобщить, то, нарисовав аспекты в пересекающихся кругах и примеры реализаций, можно получить следующую картину.

Эта картина достаточно хорошо отображает зависимости между аспектами «быстроты» доставки груза.

Например, если надо получить большую пропускную способность, можно не отправлять единичный груз сразу

после получения, а накопить его, чтобы отправить большое число грузов одновременно одной поставкой. Это увеличит пропускную способность, но снизит среднюю быстроту доставки отдельных грузов (при этом себестоимость доставки, скорее всего, упадёт).

Или же можно увеличить пропускную способность, не снижая быстроты доставки. Докупить дополнительные мощности для пересылки. Тогда и пропускная способность увеличится, и быстрота доставки не изменится, но возрастёт себестоимость доставки.

Вышеперечисленные зависимости, которые можно использовать для увеличения того или иного аспекта, конечно же, могут быть использованы только в рамках одного технологического цикла. Появление и внедрение новой технологии обычно даёт существенный прирост одному или нескольким аспектам. Например, появление авиаперевозок резко увеличило «быстроту» доставок.

Что же можно «перенести» из текста про скоростные поставки груза в скоростные децентрализованные платформы?

— Рисунок трёх аспектов работает практически так же.

— Для серьёзного увеличения «скорости» нужны технологические прорывы.

— В рамках постоянства технологий можно в той или иной степени, манипулируя аспектами скорости, добиваться некоторого превосходства над конкурентами.

Соответственно, все проекты по созданию высокоскоростных децентрализованных платформ можно структурировать и разбить на следующий типы:

— увеличение скорости за счёт манипуляций с её аспектами;

— увеличение скорости через изменения технологической составляющей — алгоритма консенсуса;

— увеличение скорости за счёт частичного отказа от стандартных для остальных участников практик;

— увеличение скорости за счёт изменения технологической составляющей — парализацией выполнения.

СМЕЩЕНИЕ АКЦЕНТОВ

Как показано на рисунке выше, каждый из трёх аспектов быстроты может быть увеличен за счёт ухудшения двух других. Однако какой аспект для улучшения выбирать?

Как показывает практика, проекты зачастую выбирают улучшение пропускной способности: скорее всего, это связано с тем, что люди в первую очередь обращают внимание на красивые большие цифры в tps[1] (количество транзакций в секунду), не всматриваясь в особенности реализации, где и будут заметны изменения во времени обработки отдельной транзакции и затраты (!) на её обработку.

Самый простой способ увеличения пропускной способности, который пользуется большой популярностью, — увеличение размера блока, в который записываются транзакции. В результате за одно и то же время платформа обрабатывает большее количество транзакций. Пример такого решения — Bitcoin Cash (и BSV). Это форк оригинального Bitcoin, в котором увеличили максимальный размер блока с 1 до 8 мегабайт (сейчас это значение равно 32 мегабайтам).

---

[1] https://habr.com/ru/post/473846/

Таким образом, теоретически в Bitcoin Cash пропускная способность выше оригинального Bitcoin в 32 раза. Однако, зная, что улучшение не может появиться ниоткуда, давайте разберём последствия такого варианта.

— Увеличение блока влечёт за собой увеличение числа транзакций, то есть в блоке может быть в 32 раза больше транзакций, а значит, и вычислений при построении блока (при создании блока рассчитывается так называемое Merkle tree[1]) становится в 32 раза больше вычислений, которые необходимо сделать за то же время. Для этого вычислительные мощности каждого узла платформы должны быть выше.

— Увеличение максимального размера блока при той же периодичности влечёт за собой увеличение общего размера базы данных платформы, следовательно — возрастают требования и к подсистеме хранения на каждом узле.

— Также эти большие блоки надо передавать по сети другим узлам, а значит — необходима пропускная способность сети в разы больше. Что также предъявляет дополнительные требования как к конфигурации узлов платформы, так и к линии подключения узла к сети Интернет.

Как видим, простое решение по увеличению блока приводит к существенным изменениям в части оборудования узла.

Хотя из-за того, что время блока Bitcoin Cash 10 минут, время выполнения дополнительных вычислений составляет малую долю этого времени, а сам процесс поиска консенсуса основан на майнинге, расходы на модернизацию также составляют малую долю от всех расходов.

---

[1] https://en.wikipedia.org/wiki/Merkle_tree

Другое дело — системы с большими начальными скоростями и меньшим временем блока. Так, например, если обычный расчёт дерева Merkle tree блока занимает 1% времени блока, то при увеличении блока в 32 раза без улучшения оборудования расчёт будет занимать 32% времени блока.

Как видно, наибольшая проблема в решении увеличения блока — наличие ограничения на подобное масштабирование. Дальнейшее увеличение блока будет упираться в технологические ограничения оборудования по скорости вычисления, хранению и передачи данных.

УСКОРЕНИЕ ЗА СЧЁТ КОНСЕНСУСА С ЦЕНТРАЛИЗАЦИЕЙ

Как рассматривалось выше, почти все новые децентрализованные платформы разрабатывают свои, гибридные консенсусы. Не обошло это увлечение и высокоскоростные платформы. Только они модернизируют связку алгоритмов консенсуса именно для получения «высокой скорости». Как было описано в разделе выше, на сегодняшний момент единственный способ добиться серьёзного ускорения — внести в алгоритм этап, позволяющий уменьшить фактическое количество участников консенсуса.

Примеров таких платформ множество: все платформы, основанные на PoS, DPoS, LPoS, POI, и некоторые более экзотические, такие как (обозначенные уже) Zilliqa и Algorand.

Более подробно особенности таких алгоритмов уже рассмотрены, но здесь стоит остановиться на том, чем они все похожи.

Публичные, мировые, децентрализованные системы подразумевают под собой наличие большого количества узлов, за счёт которых и осуществляются все необычные особенности таковых. И чем больше независимых узлов, тем более децентрализованной считается система. Однако «скоростная» модернизация консенсуса сводится к тому, что для каждого нового блока число задействованных узлов для его создания резко сокращается. Таким образом, в каждый момент создания блока система значительно менее децентрализована. В частностях каждого консенсуса предполагается, что реализация конкретного алгоритма централизации направлена на то, чтобы сохранить эффекты высокой децентрализации с минимумом потерь.

Существует способ количественно подсчитать степень децентрализованной системы. Этот коэффициент равен:

D = log2 (N), где N — количество узлов системы, которые необходимо захватить или выключить, для того чтобы платформа перестала работать в соответствии с правилами.

Однако эта формула неприменима к системам с PoW, в первую очередь из-за наличия эффектов пулов, когда узлы складывают свою мощность и посчитать отдельных представителей практически невозможно. Например, по этой формуле D EOS = log2 (7) = 2,8, D Bitshare = log2 (30) = 4,9!

Также эта формула не отражает особенности, по которым происходит централизация консенсуса, а ведь из-за таких особенностей расчёт числа N может быть произведён неточно.

На рисунке эмпирически показана зависимость скорости от децентрализации: наибольшая децентрализация указана у Bitcoin, наименьшая у классической централизованной системы. Скоростные показатели, соответственно, диаметрально противоположны.

Получается, что, как и в предыдущем варианте, в угоду скорости ухудшали себестоимость либо время доставки, так, в этом варианте в угоду скорости ухудшают децентрализацию.

К сожалению, в современном комьюнити нет консенсуса по тому, как считать децентрализацию. Поэтому, хотя теоретически понятно, что чем меньше участников принимает участие в консенсусе, тем хуже, количественного показателя нет.

ОТКАЗ ОТ СТАНДАРТОВ

С тех пор как на арену вышла первая децентрализованная платформа Bitcoin, сложился некий эталон, по которому строится большинство подобных систем.

Довольно большое количество платформ старается минимально отходить от эталона: например, только вводя новый консенсус, или добавляя смарт-контракты, или же меняя экономику токенов. Однако можно добиться существенного улучшения скоростных показателей, если довольно серьёзно отойти от «эталона».

Платформа POA Network[1] работает как форк платформы Ethereum, но изменила консенсус на полностью централизованный: валидаторы POA Network — нотариусы США. Так как участников консенсуса гораздо меньше, чем в классических «эталонных» платформах и они постоянно не меняются, как в платформах с гибридными консенсусами, то они могут позволить очень высокие скорости, причём со сравнительно малой себестоимостью.

Также «эталоном» стало отношение к информационной полноте платформы.

Несмотря на то что в статье с описанием Bitcoin есть прямое упоминание возможности удаления использованных данных (входов) для экономии места на жёстких дисках, «эталоном» считается сохранение *полной истории* всей платформы.

Однако если платформа работает со скоростью 100 тысяч транзакций в секунду, то в месяц она обрабатывает 259,2 млрд транзакций. Если в среднем транзакция занимает 250 байт, то для хранения всех транзакций за месяц (!) потребуется место около 65 терабайт. Для современных технологий даже месяц хранения оказывается дорогим удовольствием, не говоря уже о времени одного года и тем более десятилетия. Поэтому для скоростных блокчейнов логичным решением является какой-либо вариант отхода от «эталона» для снижения себестоимости этой важной части работы платформы.

---

[1] https://www.poa.network/

ПРОТОКОЛЫ ВТОРОГО УРОВНЯ

В 2017 году на платформе Bitcoin было внедрено обновление протокола SegWit[1], что открыло дорогу первой платформе, построенной на протоколах второго уровня — Lightning Network[2].

Протоколы второго уровня основаны на работе децентрализованной платформы (первого уровня), но задействуют её крайне редко, а основное взаимодействие происходит без внесения данных в первый уровень.

Протокол второго уровня состоит из трёх фаз.

Первая фаза — открытие канала. Если образно представить себе децентрализованную платформу как автоматизированного нотариуса, то на первом уровне такой нотариус все сделки заверяет и оставляет в общедоступном, но защищённом хранилище. При задействовании второго уровня протокола два пользователя приходят к нашему «нотариусу» и просят подтвердить создание векселя, в котором будет заморожена некая сумма от обоих пользователей. После того как вексель появится в общедоступном хранилище и все смогут удостовериться в параметрах этого векселя, первая фаза закончена, переходим ко второй фазе.

Вторая фаза — взаимодействие на втором уровне. После открытия канала и начинается самое важное в протоколе — взаимодействие между пользователями. Имея нотариально заверенный вексель, они могут дальше обмениваться «долговыми расписками», количество которых неограниченно: главное условие — сумма долга в этих расписках не может превышать суммы, заморо-

[1] https://ru.wikipedia.org/wiki/Segregated_Witness

[2] https://ru.wikipedia.org/wiki/Lightning_Network

женной в векселе. Так как пользователи работают напрямую, без посредников в виде «нотариуса», то скорость их взаимодействия ограничена только качеством канала связи между ними и временем на выписывание «долговой расписки».

Третья фаза — закрытие канала. Совместно выписанный вексель имеет время действия (это особенность, необходимая для работы протокола второго уровня). Поэтому при любом варианте исхода взаимодействия между пользователями вексель будет «закрыт», а средства, замороженные в нём, будут заморожены. Возможные исходы:

— никто не взаимодействовал во время жизни векселя — пользователи получат обратно свои же средства;

— оба пользователя предъявят результирующую «долговую расписку» — пользователи получат средства в соответствии с договорённостями, описанными в долговой расписке между собой;

— один из пользователей отказался от согласования и совместного предъявления «долговой расписки» — пользователь получает и свои средства, и средства отказавшегося пользователя.

Конечно, если пользователь не передал в процессе взаимодействия все средства другому пользователю, ему всегда выгодно не доводить дело до пункта №3.

Выше для наглядности работа трёх фаз протокола второго уровня при взаимодействии двух пользователей описана упрощённо. Если есть интерес выяснить математические и алгоритмические подробности его, то прошу воспользоваться поиском.

Однако из описания работы протокола видно, что на второй фазе скорость его работы может быть огромна. Однако для того, чтобы любые два пользователя начали работать по этому протоколу, они в любом случае должны

пройти первую фазу, а для платформы Bitcoin это (при шести подтверждениях) занимает около часа.

В любой платформе, если необходимо единичное или любое мало повторяемое взаимодействие между пользователями, организация канала второго уровня будет медленнее, чем обычное взаимодействие на первом уровне. Для того чтобы пользователь не открывал с каждым новым пользователем новые платёжные каналы, протокол второго уровня должен быть доработан.

Примером такого доработанного протокола является платформа Lightning Network. Основная доработка — создание узлов, маршрутизирующих «долговые расписки»: если пользователь А собирается расплатиться с пользователем Б, ему не надо создавать новый общий канал, если у обоих есть каналы с узлами платформы Lightning Network. Тогда узлы, с которыми у пользователей А и Б открыты каналы, сами найдут лучший путь из узлов, с которыми у них уже есть открытые каналы, и проведут взаимный обмен «долговыми расписками». В результате на всём пути между пользователями А и Б произойдёт обмен «долговыми расписками», однако в результате только у пользователей А и Б изменится сумма долгов в их каналах.

В чём же достоинство платформ, основанных на протоколах второго уровня?

В первую очередь, это высокая скорость проведения обмена: чем больше узлов в системе — тем больше масштабируется скорость системы.

Недостатки платформ, основанных на протоколах второго уровня:

— необходимо замораживание средств, причём на весь срок векселя;

— несмотря на, казалось бы, бесплатный обмен долговыми расписками, это не так. Опосредованно: замораживание средств, оплата за поддержание узлов (оборудование, электроэнергия, каналы связи) — всё это расходы,

которые необходимо покрывать. Хотя, конечно, эти расходы на порядки меньше расходов на работу платформ первого уровня;

— у узлов появляется возможность цензуры. Так как именно узлы маршрутизируют платежи, то в случае, если узел является каким-либо окончанием платёжного маршрута, он может заблокировать проходящий через него платёж.

Особенность протокола второго уровня в том, что осуществляемое в его рамках взаимодействие работает между двумя пользователями, и хотя, например, в Lightning Network можно создавать платёжную цепочку, для этого потребовалась специализированная разработка как математического, так и программного аппарата. Из-за этого свойства протокола второго уровня работа в нём смарт-контрактов, рассчитанных на работу более чем двух участников, сильно затруднена. Насколько мне известно, до сих пор не появилось инструментария для создания таких смарт-контрактов.

Ещё одна особенность протокола — направленность на обмен средствами. Ведь залогом обмена «долговыми расписками» являются замороженные в векселе средства. Из-за этого смарт-контракты даже для взаимодействия двух пользователей в основном используются для оперирования этими средствами.

Проблема в том, что в случае взаимодействия с информацией невозможно просчитать её ценность. Для кого-то переданная информация значит очень мало, а кто-то предпочтёт отказаться от результатов расчёта смарт-контракта, пожертвовав замороженными средствами.

Из-за неоднозначности в определении стоимости как информации, так и результатов расчётов, сделанных на её основе, невозможно однозначно считать, что третий вариант закрытия канала принесёт удовлетворительную компенсацию добросовестному пользователю.

В результате получаем мощную и масштабируемую систему платежей, у которой есть небольшие особенности в виде долгого открытия и закрытия канала и замораживания средств.

ШАРДИНГ

Дословно с английского shard — осколок, а шардинг можно перевести как разделение целого на осколки, части.

Впервые его начали применять в базах данных: когда база данных становилась слишком большой для одного сервера, данные этой БД делились и переносились на несколько серверов.

Для примера возьмём успешную компанию по управлению складами, которая каждый месяц открывает один новый склад. И в результате сталкиваемся с проблемой масштабирования. Самый простой способ для подобной компании — отказаться от одной общей базы данных и выделить на каждый склад свою отдельную, добавив также одну общую базу данных, в которой будут учитываться движения между складами.

Также шардинг начали использовать и в играх. Из найденного в Сети можно предположить, что первопроходцами стали сервера World of Warcraft[89] — очень популярной онлайн-РПГ[1] того времени: в случае, если один игровой сервер не справлялся, создавался отдельный сервер с копией всех алгоритмов и части данных и туда запускали новых пользователей.

---

[1] https://ru.wikipedia.org/wiki/RPG

Эти два примера хорошо показывают технологическую сущность шардинга. В базах данных разделяется в первую очередь сохранение и изменение информации, но практически не уделяется внимание системам вычислений.

Простой пример: поступили данные переместить все шины с одного склада на другой. База данных просто учла все транзакции. А все вычисления с данными и система принятий решений о перемещении были вне.

В случае же с игрой происходит шардирование вычислений. Пользователи постоянно присылают транзакции со своими действиями, а сервер должен на их основании и по состоянию всей информации быстро обработать запросы и выдать результат.

Поэтому можно разделять шардинг по типу — *шардинг состояния и шардинг вычисления*.

Состояние информационной системы, по-английски state — совокупность всех значений, всех переменных данной системы в определённый момент времени. При получении запросов на изменения одно состояние системы переходит в другое.

Например, в самой простой обучающей программе для детей есть машина, и ей можно задать направление движения. Текущее положение машины в координатах и есть состояние такой системы. После выполнения команды «проехать два квадрата вправо или вниз» состояние системы изменяется, так как координаты машины поменяются.

Классические блокчейн-платформы также являются хорошим примером информационных систем с состоянием: в каждом новом блоке записано новое состояние по сравнению с предыдущим, а между этими блоками происходит вычисление нового состояния и согласования его по правилам алгоритма консенсуса (см. выше) платформы.

Однако, в отличие от централизованных баз данных, шардинг децентрализованных платформ — гораздо более сложная задача.

При шардинге в централизованной базе данных контроль над целостностью (подлинностью) состояния отдельного кусочка (шарды), как и в случае работы без шардирования, лежит на операторе базы данных. Таким образом, деление такой базы данных на части не имеет сложностей в аспекте валидности.

В случае же децентрализованных платформ состояние системы едино для всех участников, и если разобьём общее количество участников на несколько шард, то они станут участниками только своих шард и не будут принимать участие в консенсусе других.

Таким образом, у каждой шарды получается своё состояние, а так как все участники независимы и естественным образом контролируют друг друга в процессе консенсуса, участники из других шард больше не могут судить о том, валидное или невалидное состояние этой (заданной) шарды (так как они уже не являются участниками консенсуса такой шарды).

Решение проблемы шардинга децентрализованных платформ, в результате которого состояния отдельных шард было бы доказуемо валидно, позволило бы полностью решить многие проблемы децентрализованных платформ.

Какие плюсы могут получить децентрализованные платформы в случае применения шардинга?

— Меньший объём использования как оперативной, так и долговременной памяти в случае разделения состояния системы.

— Бесконечно масштабируемая скорость обработки обычных транзакций по изменению состояния системы.

— Высокая скорость обработки смарт-контрактов из-за шардинга вычислений.

— Общее ускорение шарда, так как можно применять скоростные консенсусы в результате уменьшения его размера.

И отдельно хотелось бы рассказать про эффект географических шард. В случае общемировой публичной децентрализованной сети сталкиваемся с физическими ограничениями — сигнал от Новой Зеландии до Франкфурта идёт около 200 мс. Поэтому такие сети должны учитывать задержки, вызванные расстояниями, и увеличивать время достижения консенсуса нового состояния. В случае же шардинга имеет смысл создавать шарды из близко расположенных узлов, для того чтобы время на достижение консенсуса не так сильно зависело от расстояния.

Какие же проблемы надо решить для того, чтобы получить полный шардинг для децентрализованной системы?

ШАРДИНГ СОСТОЯНИЯ

Полный потенциал системы может быть раскрыт только с применением шардинга состояния, когда участник любой шарды работает только с той частью данных, за которую отвечает его шарда, и не отвлекается на вычисления, связанные с состояниями других шард. Однако из-за описанных выше проблем с «полным» шардингом многие проекты полностью отказываются от такого шардинга или же применяют «оптимизации».

Самый частый способ упрощения работы с шардингом состояния — создать большинство шард с полным шардингом состояния, а, например, одну ноду оставить без шардинга состояния, и в ней и будет происходить валидация состояний из остальных шард. Назовём этот случай способом с применением «главной цепочки», так как именно в ней находятся участники с полным состоянием системы

и именно они являются гарантом валидности состояния всех остальных шард.

Ещё один экзотический способ — совсем отказаться от шардинга состояния и достичь улучшения только за счёт шардинга вычислений: в таких системах каждый участник знает полное состояние системы.

МЕТОД РЕГИСТРАЦИИ МЕЖШАРДОВЫХ ВЗАИМОДЕЙСТВИЙ

Так как шарды в децентрализованных системах — это отдельные небольшие децентрализованные подсистемы, то возникает вопрос: а как же передавать информацию между ними? Ведь как-то необходимо организовать учёт транзакций между шардами, причём в обоих шардах.

В случае если у проекта нет шардинга состояния, такой вопрос не возникает, так как любая зарегистрированная транзакция — это изменение всего состояния, а так как состояние системы на каждом узле одинаковое, то все узлы получат результат выполнения транзакции.

В случае использования «главной цепочки» чаще всего происходит следующее: транзакция регистрируется в шарде отправителя, потом в главной цепочке, а затем уже в шарде назначения.

ПРЯМОЕ ВЗАИМОДЕЙСТВИЕ ШАРД

И последний вариант — прямое взаимодействие между шардами, когда регистрация происходит в два приёма в шарде отправителя и затем в шарде назначения, но другие шарды никак не участвуют в этом взаимодействии.

ПРОВЕРКА МЕЖШАРДИНГОВЫХ ТРАНЗАКЦИЙ

Если шард получает транзакцию из другого шарда, любой участник хотел бы знать, насколько валидна эта транзакция, перед её подтверждением регистрацией в своём шарде. В идеале должна пройти полная проверка данных шарда источника, но это означало бы, что каждый участник самостоятельно должен получить состояние другой шарды и проверить преобразования с её состоянием, но так как в каждый момент времени может прийти несколько межшардовых транзакций, то в таком случае каждый узел должен постоянно получать и обрабатывать неопределённое количество состояний других шард, что отменяет все полезные стороны самого шардинга (где частники шарды должны работать над состоянием только своего шарда).

Какие придуманы способы проверки?

— Шардинг с главной цепочкой. Все транзакции всех шард проверяются в главной цепочке, перед тем как будут занесены либо сами, либо их слепки. Поэтому когда транзакция приходит в шард назначения, его участникам достаточно проверить, есть ли в блоке главной цепочки эта

транзакция либо ссылка на неё. В таких системах шарды должны безоговорочно доверять решению о валидности главной цепочки.

— Дополнительная проверка. Идея заключается в том, что любая межшардовая транзакция должна пройти дополнительную проверку не зависимыми от шарда отправления узлами. Только после прохождения такой проверки шард назначения зарегистрирует входящую транзакцию.

— Метод штрафов. По умолчанию считается, что все шарды добросовестны и большую часть времени работают добросовестно. В таком случае все межшардовые транзакции принимаются безоговорочно. Но в системе предусмотрено существование проверяющих, которые последовательно верифицируют все блоки и ищут невалидные транзакции, после нахождения которых происходит штрафование или наказание участников, допустивших эту ситуацию. С точки зрения эффективности валидации этот метод отложенной проверки гораздо лучше, чем вариант дополнительной проверки, так как при дополнительной верификации необходимо проверять в реальном времени транзакции из многих шард, а значит — проверяемый узел должен переключаться между «стейтами» этих шард, в то время как при отложенной проверке участник может полностью проверить один шард и потом переходить к следующему. Однако отложенная проверка требует системы обеспечения наказания для вредоносных участников, а также системы, которая будет разбираться с результатами включения невалидных данных в систему.

— Не решать. Да, есть проекты, в которых нет стандартного способа валидации межшардовых транзакций.

УПРАВЛЕНИЕ ШАРДАМИ

На сколько шард поделить систему? Сколько участников распределить в шардах? Делать ли географические шарды? Кто будет собирать близких участников в географические шарды? Эти и многие другие вопросы возникают при создании децентрализованных систем с шардингом.

Какие известны варианты?

— Шардинг с главной цепочкой. Именно решением её членов создаются, уничтожаются шарды, распределяются узлы в эти шарды, а также наказываются узлы за вредоносное поведение.

— Решение большинства. Все решения должны быть подтверждены большинством: большинством мощности в случае PoW, стейка в PoS или другим счётным большинством в проекте.

— Без управления. Любой может добавлять в систему свои шарды. Все шарды равноправны. Надо быть готовым, что шард может перестать работать в любой момент.

ПРИМЕРЫ ПЛАТФОРМ С ШАРДИНГОМ

После того как описали особенности реализации шардинга в децентрализованных платформах, самое время оценить, как они реализуются в реальных проектах.

ZILLIQA

Проект, на всех нодах которого хранится одинаковое состояние главной цепочки. Таким образом, каждый раз, когда создаётся и рассылается новый блок главной цепочки, все узлы получают одинаковое состояние системы.

Передача межшардовых транзакций осуществляется как с помощью отказа от шардирования состояния, так и с помощью главной цепочки. Обработанные транзакции, как внутренние, так и межшардовые, собираются от всех шард в главную цепочку и проверяются, после чего вносятся в состояние главной цепочки, которое рассылается на все узлы и становится носителем нового состояния,

в котором есть вся информация о состоянии всех аккаунтов и СК.

Проверка осуществляется в главной цепочке.

Шарды тут создаются один раз в эпоху теми узлами, которые сформировали на эту эпоху главную цепочку. Сначала владеющие (необходимым) стейком монет соревнуются в том, кто попадёт в главную цепочку, после розыгрыша мест остальные узлы соревнуются за включение узла в сеть шард, а узлы главной цепочки подтверждают выигрыш и распределяют узлы по шардам.

QUARKCHAIN

Система с разделением состояния, но с главной цепочкой, хранящей общее состояние.

В главную цепочку после проверки включаются не сами транзакции, а только хэши блоков; соответственно, в шард назначения транзакция приходит в виде дерева Merkle во главе с хэшем блока. По этим данным и данным блока из главной цепочки шард назначения может провалидировать то, что транзакция проверена главной цепочкой.

Проверкой занимается главная цепочка. Ввиду того что проверка в главной цепочке — бутылочное горлышко всей системы, в проекте предложили создавать суперноды в главной цепочке. Несколько узлов объединяются в одну суперноду, а внутри делят между собой обязанности по проверке шард пропорционально.

В документации есть указания, позволяющие сделать вывод, что управляться шарды будут из главной цепочки.

KADENA

Система получается с раздельным состоянием. Скорее всего — межшардовая транзакция будет передаваться напрямую. Блок с межшардовой транзакцией должен пройти одобрение другими шардами. Через несколько итераций такие данные о блоке и о том, кто из шард одобрил этот блок, дойдёт до шарды назначения; дальше шарда назначения будет решать, достаточно ли этих подтверждений для регистрации транзакции у себя или нет.

Нет информации о системе управления.

HOLOCHAIN

Система с раздельным состоянием. Вероятнее всего — межшардовая транзакция будет передаваться напрямую.

Проверки межшардинговых транзакций нет. Каждая шарда сама должна побеспокоиться о том, от каких шард принимать транзакции и как их проверять.

Не системы управления: каждый может запускать свою шарду.

THE POWER

Система с разделением состояния. Межшардовая транзакция будет передаваться напрямую. Каждая транзакция проверяется набором случайных валидаторов.

Управление шардами большинством. Все участники участвуют в управлении шардами.

***

...А теперь, имея нужный запас технических знаний, перейдём к ещё одной важной, интересной, не очень простой, но крайне увлекательной теме: интероперабельность!

ИНТЕРОПЕРАБЕЛЬНОСТЬ

Глава написана Элиотом Кроном (псевдоним) — архитектором распределённых систем и экспертом блокчейн-рынка, участником рабочих групп ISO по теме стандартизации технологий распределённых реестров.

Web3 — это интероперабельность блокчейн-платформ, социальных и коммерческих. Но что это значит? Давайте разбираться вместе.

В настоящее время существует значительный интерес к блокчейн-технологиям как к перспективной технологии для будущей инфраструктуры по глобальному обмену активами, которую часто называют Internet of Value[1], а также Web3[90]. Подобного рода инфраструктура подразумевает под собой интероперабельность блокчейн-платформ, но как могут блокчейн-сети безопасно и эффективно взаимодействовать друг с другом в условиях отсутствия доверия?

Нашей с вами целью является попытка сделать первый шаг к раскрытию данной темы, раскрыть понятие «интероперабельность», определить типовые сценарии использования, решаемые проблемы, а также рассмотреть основные подходы, которые используются и/или развиваются блокчейн-рынком. Не претендуем на всестороннее рассмотрение вопроса: детальное изучение данной темы оставляем пытливому читателю, который заинтересуется этим направлением в исследованиях.

Интероперабельность (функциональная совместимость) — способность компьютерных систем и/или программ обмениваться и использовать её, как это определено в стандарте терминологии ISO[2].

---

[1] https://www.mann-ivanov-ferber.ru/books/valueweb/

[2] https://en.wikipedia.org/wiki/International_Organization_for_Standardization

В блокчейн-технологии под интероперабельностью подразумевают безопасный протокол обеспечения связности логических состояний в двух и более независимых блокчейнах. Под безопасностью следует понимать аутентичность, целостность, доступность и непротиворечивость состояний.

Например, события в одном блокчейне могут происходить или не происходить в зависимости от действий в другом блокчейне. Надо понимать, что интероперабельность существует на разных уровнях взаимодействия систем (платформы, сети, криптография).

Именно интероперабельность добавляет дополнительную ценность и возможности взаимодействующим блокчейнам. Используя удобный, понятный способ обмена информацией, бизнесы, которые построены вокруг блокчейнов, получат новые возможности по налаживанию партнёрских отношений с другими участниками рынка.

Но тут нужно оговориться: рынок блокчейн-технологий делится на два сектора — публичные блокчейны и корпоративные блокчейны[91]: мы говорим про интероперабельность всех со всеми.

И тут обязательно найдётся эксперт, который скажет, что корпоративные блокчейны — вообще что-то инородное в W3. Это не так. (Просто порой в корпоративных блокчейнах существуют вырожденные случаи, которые мимикрируют под блокчейн: Ripple, Corda, Hyperledger Fabric, etc.)

Нужно посмотреть правде в глаза: W3 — не только рынок публичного Bitcoin или Ethereum. Так как первый предлагает только деньги (и ограниченный набор функций и слабенькую производительность), а второй… не совсем независимый публичный блокчейн: понимаем, что это гибрид из криптосообщества и… заинтересованной компании, которая может форкнуть сеть, если это кому-то о-о-очень сильно захочется — пример DAO помните? Поэтому

не стоит возводить китайскую стену между публичными блокчейнами и корпоративными DTL, так как модель управления у них может быть похожей[92]. Плюс ответственность за работу сети могут также нести конкретные организации.

Но вернёмся к интероперабельности. В W3 интероперабельность позволит слить в глобальную кластерную сеть и корпоративные DTL с регламентированным управлением, и публичные блокчейны с «социальным» управлением. Ведь «публичные» не всегда подходят по производительности и безопасности[93] для коммерческого использования, но токеномику-то (см. выше) хочется всем, и всем бизнесам хочется иметь быстрый и высокоэффективный инструмент. Конечно, для этого придётся пойти на компромисс в плане управления своей блокчейн-сетью, но сейчас не про это.

Одним словом — интероперабельность наше всё в светлом W3-будущем, когда кластеры корпоративных DTL будут объединяться по принципу сот в глобальные сети и всё это будет идти рука об руку с публичными сетями, как связующим клеем криптоэкономики анархокапитализма.

Но давай разберёмся, чем интероперабельность может быть полезна и для чего используется.

ПЕРЕНОС ИЛИ ОБМЕН АКТИВАМИ

Чаще всего интероперабельность используется для обмена активами между блокчейнами с участием / без участия третьей стороны. При этом в случае переноса активов они блокируются (замораживаются, уничтожаются) в одном блокчейне, а их «зеркальное отображение» в другом блокчейне разблокируется (размораживается, создаётся).

При обмене между взаимодействующими участниками активы переводятся с адреса на адрес в одном блокчейне и атомарно происходит аналогичная операция перевода в другом блокчейне.

ПРИВАТНОСТЬ

Подходы к интероперабельности используются для обеспечения конфиденциальности операций, когда данные из одного блокчейна выносят в сторонний блокчейн, который обладает необходимыми свойствами конфиденциальности: там происходит взаимодействие участников. При необходимости данные возвращаются в основной блокчейн.

МАСШТАБИРУЕМОСТЬ И ПРОИЗВОДИТЕЛЬНОСТЬ

Для обеспечения большей масштабируемости блокчейн разделяется на шарды[94] или на сайдчейны, которые взаимодействуют друг с другом для обеспечения общей консистентности главного блокчейна.

В другом случае для увеличения производительности активы переносятся в связанные блокчейны, где иные, более быстрые правила обработки транзакций, с последующим возвратом результатов обработки транзакций в основной блокчейн.

КОНТРОЛЬ. РЕГУЛИРОВАНИЕ. НОВЫЕ АКТИВЫ

Возможность блокчейна к функциональной совместимости с другими блокчейнами позволяет реализовать механизмы контроля, регулирования работы блокчейна и движения активов, а также даёт возможность создавать новые виды активов, в том числе и финансовых производных.

Например, можно:

— установить правила выплаты дивидендов в блокчейне А держателям активов, зарегистрированных в блокчейне Б;

— заблокировать активы в блокчейне А и задать условия разблокировки, зависящие от активности в блокчейне Б. Типичными случаями использования являются залоги, обеспечение в финансовых деривативах, реализация исполнения судебных приказов и различные варианты использования, связанные с залоговыми депозитами.

РАСШИРЕНИЕ ФУНКЦИОНАЛЬНОСТИ И ИССЛЕДОВАНИЯ

Иногда одного блокчейна не хватает для решения специфического бизнес-кейса, тогда можно использовать сторонние решения, которые обладают необходимой функциональностью. Для этого объекты данных, над которыми необходимо произвести манипуляции, переносятся в соответствующий блокчейн или же используются данные специализированного блокчейна.

ИЗВЕСТНЫЕ ПРОБЛЕМЫ

ТЕХНОЛОГИЧЕСКОЕ РАЗЛИЧИЕ ПЛАТФОРМ

Одна из ключевых проблем при реализации интероперабельности — различия в используемых технологиях. Типичными конфликтами являются:

— несовместимость криптографии и модели консенсуса;

— разные требования к производительности, безопасности и конфиденциальности;

— различия в способах обработки транзакций;

— функциональные особенности работы смарт-контрактов;

— многое другое.

Для разрешения этих конфликтов ведутся исследования в организациях по стандартизации: на международном уровне — в Международном союзе электросвязи (Сектор стандартизации электросвязи, МСЭ-Т[1]), Международной организации по стандартизации (ИСО/ТК

[1] https://www.itu.int/ru/ITU-T/Pages/default.aspx

307 «Блокчейн и технологии распределённого реестра»), на национальном уровне — в Техническом комитете по стандартизации «Программно-аппаратные средства технологий распределённого доступа и блокчейн» (ТК 159) и Техническом комитете по стандартизации «Криптографическая защита информации» (ТК 26).

Также работы ведутся и в исследовательских группах Ethereum Research[1], Web3 Foundation[2], IOHK[3] и других группах, которые ближе всего к блокчейн-рынку. Стоит отметить, что на данный момент единства мнений в подходах к обеспечению интероперабельности нет.

ОТСУТСТВИЕ БИЗНЕС-ПРИМЕНЕНИЯ

К сожалению, классический бизнес не спешит токенизировать свои активы и участвовать в W3, так как его интересы не защищаются ни стандартами, ни законами (кроме математических). Для этого участия в криптоэкономике бизнесу нужно или выходить в серую и теневую зону рынка, или не применять инструменты токеномики вовсе. Иначе в лучшем случае он подвергнется репутационному риску и потеряет свои активы, а в худшем — к руководителям такого бизнеса возникнут вопросы со стороны регуляторов и правоохранительных органов[95]. И это всё в результате того, что нет стандартов, а нет стандартов — нет регулирования.

---

[1] https://ethresear.ch/

[2] https://web3.foundation/

[3] https://iohk.io/

Из-за этого бизнес не спешит тратить деньги на исследования интероперабельности и в целом блокчейн-технологий. Поэтому направление W3 не развивается с корпоративной стороны, поэтому и не видим массового применения блокчейна в бизнесе, токенизации активов и так далее. Замкнутый круг. Конечно, не всё так печально: те же ICO принесли на рынок много денег для исследования и развития подходов к интероперабельности.

СУЩЕСТВУЮЩИЕ ПОДХОДЫ

Технологии стремительно развиваются: на данный момент существует множество научных и околонаучных работ, которые пытаются категоризировать способы интероперабельности. Но всё так быстро развивается, что через год будут придуманы новые концепции и протоколы. На основе проводимых исследований готовы выделить (высокоуровнево) следующие подходы к реализации интероперабельности:

— атомарные кроссчейн-транзакции (атомарные обмены[96]) — самый простой тип взаимодействия, который основан на использовании криптографического протокола HTLC (Hash Time Locked Contracts). Участники протокола договариваются об использовании секретной информации, без которой невозможно произвести обмен;

— мосты и нотариальная схема. Если атомарные обмены подразумевает обмен активами, то мосты и нотариальные схемы подразумевают обмен сообщениями. Это позволяет, например, делать вызов функций одного блокчейна (смарт-контракта) из другого. Этот подход основан на наличии во взаимодействующих системах посредника (или мажоритарной группы) для передачи информации из одного блокчейна в другой;

— релейный блокчейн (релейная передача). Релейный блокчейн подразумевает создание сети из блокчейнов — так называемую релейную сеть. При этом происходит объединение различных блокчейн-платформ в единую структуру, консистентность которой обеспечивается за счёт консистентности релейной сети, лежащей в основе такой структуры. На данный момент этот подход самый сложный с технической стороны, но он активно исследуется сообществом.

АТОМАРНЫЕ ОБМЕНЫ

Атомарные обмены — самый простой способ организации межблокчейнового взаимодействия. В основе этого подхода лежит протокол Hash Time Locked Contract[97], который является самым децентрализованным способом обмена активами, так как не требует участия третьей стороны при отсутствии доверия между участниками. При всей своей простоте этот протокол является и наиболее ограниченным с точки зрения функциональности.

Важное условие: для коммуникаций двух блокчейнов нужно, чтобы они поддерживали общие криптографические протоколы, а также требуется максимальная осознанность в действиях между участниками — в том числе и большая интерактивность.

Одним из способов использования этого механизма являются так называемые off-chain транзакции. Они также основаны на HTLC, но транзакции проходят вне основного блокчейна и не сохраняются в них. В блокчейн же попадает начало транзакции с HTLC и окончательный результат

прошедших промежуточных транзакций, которых может быть (!) много. Данный подход используется, например, в Lightning Network.

В рамках HTLC подхода можно выделить протокол Interledger, который использует идеи HTLC. Напомним, что консорциум World Wide Web (W3C) предложил его как общий протокол, обеспечивающий безопасный перевод активов через любые блокчейны.

Цель Interledger — разрешить передачу активов в атомарной манере таким образом, чтобы ни одна из вовлечённых сторон не подвергалась каким-либо рискам и чтобы отправитель мог иметь неоспоримое доказательство того, что конечный получатель получил/оплатил соответствующие активы. Протокол Interledger позволяет объединять участников обмена в сети для передачи активов через различные блокчейн-сети. Разрабатывается протокол на деньги Ripple: ха-ха, но, видимо, так Ripple вносит позитивный вклад в криптосообщество, чтобы его не так строго судили за то, что Ripple усиленно мимикрирует под блокчейн.

МОСТЫ И НОТАРИАЛЬНЫЕ СХЕМЫ

Этот механизм позволяет передавать активы и произвольную информацию, вплоть до вызова методов смарт-контракта из одного блокчейна в другой блокчейн. Для этого блокчейны должны быть более или менее «равными» с точки зрения технологий, на которых они созданы.

Под мостом чаще всего подразумевается использование управляющих смарт-контрактов и сервиса-оракула,

который мониторит транзакции, прослушивает события в управляющем смарт-контракте. Мост может быть как в двух сетях одновременно, так и только в одной, получая информацию по другим каналам связи, самое главное — это криптографическая проверка аутентичности информации. Мост может также использовать возможности HTLC и атомарных обменов, но по функциональности они шире, чем атомарные обмены.

Можно сказать, что любую интероперабельность между блокчейнами можно назвать мостом. Принцип у них примерно одинаков: отправить сообщение и получить подтверждение (блокирующий вызов) или fire-and-forget[1] — неблокирующий вызов. Далее каждый из этих подходов делится по другим параметрам.

Упрощённое понимание: мост — это MITM[2] (man in the middle), только это сервис-оракул, который тратит технические расчётные единицы (например, gas[3]) на создание и отправку транзакций, при этом информация может защищаться криптографией. И нужно доверять этому MITM[98].

Своё развитие мосты находят в нотариальных схемах.

В нотариальной схеме основным звеном, которое ответственно за передачу данных, являются «нотариусы», которые могут являться валидаторами сети. Роль нотариуса заключается в проверке того, что событие произошло в одном блокчейне, сборе необходимого количества подтверждений о произошедшем событии от других «нотариусов-валидаторов» и передаче этой информации в другой блокчейн.

---

[1] https://en.wikipedia.org/wiki/Fire-and-forget

[2] https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[3] https://2bitcoins.ru/chto-takoe-gas-v-ethereum-skolko-platit-za-tranzakcii/

Основное преимущество таких схем — не нужно доверять одному оракулу: можно доверять сети в целом, в которой есть такие нотариусы на уровне системы.

РЕЛЕЙНЫЙ БЛОКЧЕЙН, ИЛИ РЕЛЕЙНАЯ ПЕРЕДАЧА

Релейный блокчейн — отдельный блокчейн, который функционирует как лёгкий клиент для связанных с ним блокчейнов, является своего рода хабом для подключённых блокчейнов. При этом под релейной передачей подразумевается возможность одному блокчейну проверить данные в другом самостоятельно. Некоторые утверждают, что релейные сети — развитие нотариальных схем, но дополняют их новыми функциями.

Общими словами: релейная передача — смарт-контракт одного блокчейна, который является «лёгким клиентом[1]» второго блокчейна, таким образом, первый блокчейн видит изменения, которые происходят во втором блокчейне.

Блокчейны-участники могут использовать информацию о других блокчейнах, обмениваясь сообщениями через релейный блокчейн, который отслеживает состояния всех соединённых блокчейнов и может обеспечивать определённый контроль над активами в этих блокчейнах.

В рамках концепции «релейный блокчейн» можно выделить концепцию сайдчейна. В зависимости от типа

[1] https://en.wikipedia.org/wiki/Thin_client

управления сетью, сайдчейн может быть или зависимым, или более независимым от своего основного блокчейна.

Основная идея сайдчейнов состоит в перемещении некоторых активов из одного блокчейна в другой блокчейн, для проведения действий над ними. Позже активы могут быть возвращены в первоначальный блокчейн.

— Распространённой причиной использования сайдчейнов является время подтверждения транзакции, так как задержки транзакций в сайдчейне обычно значительно меньше, чем в основной цепочке.

— Вторая причина использования сайдчейна заключается в том, что сайдчейн может поддерживать некоторые функциональные возможности, которые могут отсутствовать в основном блокчейне, например, возможность создания смарт-контрактов или даже экспериментальные функции.

— Третья причина: стоимость транзакции (стоимость записи данных транзакции в блокчейн) в сайдчейне может быть (значительно) ниже, чем в основном блокчейне. Сокращение времени транзакции и стоимости транзакции могут повысить масштабируемость.

ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕХНОЛОГИЧЕСКИХ РЕШЕНИЙ ИНТЕРОПЕРАБЕЛЬНОСТИ

Потребность в интероперабельности есть, но она ещё недостаточно очевидна рынку. Связано это в первую очередь с неразвитостью самого рынка и отсутствием большо-

го количества промышленных сетей, которые можно было бы объединить.

Но при этом многие соглашаются с мнением, что развитием подходов интероперабельности необходимо заниматься, так как не очевидная на данный момент потребность в функциональной совместимости будет всё больше нарастать в ближайшие годы и острая необходимость в ней возникнет, когда будем ближе к расцвету W3 и токеномики (как его части).

Наше будущее будет за отдельными, специализированными сетями, которые будут объединять в кластеры компании по юридической принадлежности, функциональности или сектору экономики. Именно за кластерными сетями будущее. И интероперабельность здесь будет и между сетями внутри кластера, и между кластерами.

Интероперабельность придаёт значительную ценность блокчейн-платформам. Говоря проще: если блокчейн-платформа не имеет доступных интерфейсов для интероперабельности, то такая сеть будет нежизнеспособной, а если механизмы интероперабельности реализованы, то это откроет новые возможности для бизнес-применения в рамках консорциумных блокчейнов.

Однако вместе с широкими возможностями по бизнес-интеграциям возникнут и проблемы, которые необходимо будет решать: взаимодействие открытых блокчейнов и консорциумных «блокчейнов». Это разные области, с разными функциональными свойствами, разными требованиями к безопасности и производительности. А самое главное — разный уровень правовой[99] ответственности у участников токеномики.

Поэтому сейчас основными барьерами для развития W3 являются:

— регуляторная политика;

— незрелость технологических решений;

— отсутствие острой необходимости подобного рода технологий у бизнеса;

— быстрые изменения на рынке;

— отсутствие стандартов интероперабельности блокчейнов…

ВЫВОДЫ

Можно сказать, что современные ДРС сталкиваются со сложной задачей обеспечения функциональной совместимости между сетями в условиях отсутствия доверия к консистентности данных в системах, к безопасности каналов связи.

Криптография на современном этапе развития способна обеспечить необходимый уровень безопасности для таких систем, но «функциональная совместимость» в блокчейн-технологиях понимается шире и подразумевает возможность и готовность блокчейнов к взаимодействию с другими блокчейнами и традиционными информационными системами.

Как видим, интероперабельность блокчейн-платформ активно изучается и развивается. Разрабатываемые решения имеют различную степень сложности: от криптографической связи транзакций в различных блокчейнах до иерархических структур с высокой масштабируемостью.

Индустрия ещё не разработала стандартов для объединения различных блокчейн-сетей. При этом участникам рынка становится очевидна необходимость стандартизации подходов к интероперабельности, так как это

упростит внедрение и эксплуатацию блокчейнов в бизнесе.

Всё чаще встречается мнение, что в будущем нас ожидают сети из блокчейнов. При этом каждая из них будет иметь свою конкретную сферу применения. Нужно понимать, что поддержку таких сетей будут вести компании и корпорации, а вот модель управления такими сетями, возможно, будет изменяться в сторону публичности. Возможно. И именно сети специализированных блокчейнов создадут инфраструктуру по глобальному обмену активами, также известную как Internet of Value, которой и будет Web 3.0.

***

И всё же технологические инновации и проблемы — верхушка айсберга. Что же скрыто от глаз?..

ОСНОВНЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Web 3.0 — не просто набор технологий, это смена не только парадигмы, но и образа действия: проще говоря — за ним скрывается множество возможностей (ещё не реализованных) для бизнеса, комфортной, хотя и насыщенной жизни и прочих сфер. Но есть нюансы (далее — мнение В.П.)…

АППАРАТНЫЕ ПРОБЛЕМЫ

Можно сколь угодно считать, что проблема рубильника, то есть когда операторы/провайдеры связи, государственные органы могут выключить конкретный сегмент сетей, — проблема надуманная, но давайте посмотрим правде в глаза: сотовая связь лицензируется и потому — напрямую зависит от власти; 5G и прочие технологии, сулящие возврат к мэш-сетям, — только начальный этап, потому как ad hoc сеть не просто должна быть, но она должна быть ещё и стабильной, одноранговой — да, но многоуровневой в то же время.

А как же насчёт проектов Google, И. Маска и других? Да, они сулят бо́льшие уровни свободы, но в то же время они — далеки от принципов децентрализации. Речь, конечно же, о раздаче интернета.

И решений здесь несколько.

— Во-первых, создание абсолютных офлайн-систем передачи информации по зашифрованным каналам, чтобы факт коммуникации сам по себе не прерывался. Так поступали арабские активисты, работая против незаконных действий США на территории своих стран: неплохо о данном аспекте рассказано в фильме «Совокупность лжи».

— Во-вторых, необходимо создание «временно доступных» сетей, то есть таких, которые будут масштабиро-

ваться в зависимости от глобальных задач в рамках единой цели: это могут быть мобильно разворачиваемые станции, те же 5G-решения, Wi-Fi надстройки и что угодно.

— В-третьих, возможно, сейчас покажется фантастикой, но это вполне достижимо в средне- и долгосрочной перспективе: необходим запуск на основе краудфандинга (любой его формы) спутников для непрерывного контроля через консенсус (PoW в новом формате). Равно возможно и решение на уровне глубоководных кабелей.

И эти проблемы нельзя решить за один присест и тем более — игнорировать: без физического уровня[1][100] все сети нового поколения будут уязвимы, в том числе и из-за отсутствия постоянного и планомерного аудита «железа».

[1] https://en.wikipedia.org/wiki/Physical_layer

ПРОБЛЕМЫ ВОСПРИЯТИЯ

Почему, собственно, Web 3.0?[101] Потому как люди хотят обновлений и стабильности одновременно и всегда, поэтому — Сеть, но нового образца. Недаром за последние годы появились труды, посвящённые маркетингу два, три, четыре и даже пять ноль; жизни 3.0[1] и так далее.

Но, как много раз говорилось на наших страницах, W3 — нечто совершенно иное: трудности начались ещё у Сатоши, когда всякий любитель криптографии твердил ему, что это (имея в виду блокчейн Bitcoin) «никогда не будет работать» или «никогда и никому не понадобится», а потом они переродились и в сложности для первичного размещения токенов (ICO/ITO/TGE/ILP/IEO), поскольку для многих, хотя и не подавляющего большинства, они стали предметом ярых спекуляций, в то время как на самом деле через такой нехитрый, инновационный, быстрый способ финансирования создавалась (и создаётся отчасти) инфраструктура для ДРС: и не только технических, но и социальных.

Поэтому W3 предоставляет уникальную возможность приспособиться к тем изменениям, которые уже застали

[1] https://www.litres.ru/maks-tegmark/zhizn-3-0-byt-chelovekom-v-epohu-iskusstvennogo-intellekta/chitat-onlayn/

нас врасплох. Всё новые и новые профессии и виды бизнеса против архаичного в ряде аспектов образования — только первая грань. Вторая — смешение офлайна и онлайна. Третья — равенство объекта и субъекта.

Чем здесь помогает W3?

В первую очередь тем, что даёт инструментарий для взаимодействия любых вновь формирующихся групп и структуры их взаимодействий (консенсусы, правила токенизации и прочее: читайте об этом выше). Во-вторых, W3 делает из глобализации по-настоящему планетарный продукт: если ещё 10—20 лет назад глобализация была продуктом скорее американским[1], то сегодня это не так. И дело даже не в образовавшемся противовесе в виде Китая, а в том, что мультикультурность стала интегрирована в Сеть, а вместе с тем люди смогли получить доступ к очень разным рынкам, знаниям, бизнесам.

Простой пример из собственной практики — Synergis: с периода формирования в 2016 году и по сей день объединение охватило порядка 30 стран, включая Россию, Украину, Беларусь, Израиль, Аргентину, Колумбию, Латвию, Китай, Перу и другие. Да, это лишь объединение, а не в строгом смысле организация или компания, но факт в том, что для совместной работы людям давно не нужен единый офис и даже CRM-система. Меж тем SCRUM-практики — это тоже про W3.

И такой подход порождает сразу несколько интересных перспектив…

[1] https://www.ozon.ru/context/detail/id/2157181/

НОВЫЕ БИЗНЕСЫ И ПРОФЕССИИ

Это не атлас новых профессий[102], но, скорее, общие тенденции.

— Во-первых, благодаря Ф. Лалу в мире стала популяризироваться идея так называемых бирюзовых организаций, которые идеально накладываются на горизонтальное масштабирование W3, а значит, уже сегодня (и это так и есть) получим невероятные возможности от наложения смарт-контрактов, DeFi, DAO (банальный пример — BNB) и методик, которые развиваются в таких компаниях, как издательство МИФ, ретейлер «Вкусвилл» и ряде других компаний[103].

— Во-вторых, W3 закладывает невероятно количество векторов, отраслей, сфер и целых экономик для рождения новых видов предпринимательства. Продажа сырых данных, как рассказано выше, есть выкачивание новой «нефти», но знаем, что куда больше ценятся переработанные продукты — бензин, пластик и даже пищевые. Того же стоит ждать от сегмента превращения данных в информацию: формирование потоков, дизайн виртуальных миров и прочее.

— В-третьих, если токенизация помогла вернуться в эпоху натурального обмена (всякий товар может быть

выражен через цифровой аватар — тот самый криптоактив), то репутационные ДРС предоставляют возможность сделать нужный и важный шаг назад к крепкому купеческому слову, которое ценно в силу сложившихся социальных транзакций. Говоря проще: сначала были цены на товары, затем — товар универсальный (деньги), затем время и внимание, а в период W3 — активность (синтетическая, а не механическая совокупность правильного деяния, времени и внимания) и креатив.

И подобных аспектов — груда: здесь и разработка нового железа для ДРС, и создание школ предпринимательства подобного формата, и сами рождаемые сервисы, и экономическое моделирование и многое другое.

Одним словом, W3 — кладезь для тех, кто любит мечтать, творить, дерзать, но в то же время W3 позволяет (наконец-то!) хоть в какой-то мере обуздать пороки, раздирающие цивилизацию мира нынешнего: речь не только о жадности и скупости, о неуважении в Сети, но и даже о войне. Аппарат насилия не приспособлен воевать с анонимом, который находится везде и сразу и нигде одновременно.

Безусловно, и на это найдутся противодействия, но без этого не будет борьбы «снаряда и брони»: W3 защищает каждого из нас от той гидры, которая обычно в теории права зовётся политической властью.

БУДУЩЕЕ, КОТОРОЕ УЖЕ НАСТУПИЛО

Всю свою сознательную жизнь[104] борюсь за позицию, которая устанавливает градацию на физиков и лириков лишь условно, потому как мир никогда не был настолько простым, чтобы и те и другие существовали как строго заданные сущности.

Но сегодня это приобретает совершенно иной оттенок. Почему? Вступаем, вне зависимости от того, нравится конкретно нам это или нет, в эпоху цифрового коммунизма.

И в этом смысле W3 — очередная попытка переложить на рельсы технологические то, что и так уже рождено в социуме. Попробую объяснить на предельно точных и коротких примерах.

КОММУНИЗМ ВНЕ ПОЛИТИКИ, ИЛИ МИР №X

Речь не пойдёт о политике или социальных теориях — не об этом наша книга. Нет, хочется поговорить о том, как уберизация[105], оцифровка социального капитала и другие современные тенденции влияют на связь технологической и общественной составляющей.

Например, что такое каршеринг и uber-такси в принципе? Это постепенный переход от частной собственности к распределённой, то есть — совместной. И если на данном этапе последним «ненужным» звеном являются деньги[106], то как раз описанные подходы позволяют устранить и их: в любой момент времени и при совпадении объективных факторов — есть доступ к общественному транспорту, включая Hyperloop в какой-то реализации, автомобиль, мотоцикл, скутер, велосипед или самокат. И это — уже повсюду: многие европейские страны (Голландия, Швейцария, Финляндия, Швеция и другие) в буквальном смысле завалены велошерингом — например, в Барселоне можно брать целые абонементы на проезд на известного (красного) цвета передвижные устройства; каршеринг в России набирает всё большие обороты, а uber-мотоциклы на Бали спасают в самых узких переулках и улочках.

И это — начало.

Система подписок превратила в мир именно в коммунистический: могу смотреть фильмы, получать продукты, даже летать на самолётах, если только мой баланс выше[107] установленного. «От каждого по способностям, каждому по потребностям»: разве не так?

Если раньше была проблема принятия, то как раз сегодня, когда коммуникационная функция всё чаще становится уделом техники и технологии, то есть автоматизируется на предельно допустимом уровне, устранена и она. Но у любого процесса есть и обратная сторона: в данном случае это опасность централизации.

Почему, собственно, в XVII — XVIII веках зародилась демократия?

Причин было несколько, но одна из основных — неравномерное распределение достояний конкретных обществ во временных рамках, проще говоря, помимо дворянства и других классических сословий появился класс буржуазии, и он заявил свои права: громко, кроваво[108] и не единожды. И что же — терять всякий раз нажитое, созданное ради простых решений? Нет: и сегодня из маргинальной теории демократия превратилась в доминирующую идеологию в мире. Да, она бывает разной — от нарочито-показательной и не работающей до сверхэффективной (прежде всего — прямая демократия в той же Швейцарии), но в любом случае это далеко не абсолютная монархия.

И что же изменилось?

Всё! Меньшинство хочет быть услышанным; экологические и прочие мировые проблемы — требуют соучастия каждого; время бежит неимоверно быстро. И демократия работает всё хуже и хуже, но мало кто говорит не о критике, а об альтернативных решениях. Меж тем — они есть и успешно функционируют.

В бизнесе это так называемые бирюзовые организации (которые, к слову, отлично накладываются на концепт

DAO/DeFi); в системе управления — консенсус, а не выборы; в разработке — децентрализованный и открытый исходный код.

В этом смысле становится ясна роль W3 — это система сервисов, помогающих принять новый общественный договор, и не просто в моменте, а именно динамически отшлифовывая и отсылая разные редакции тем группам, которые хотят его акцептовать.

Почему разные?

По той же причине, почему есть страны, модели демократии и даже великие, локальные и местные кухни: мы, люди, разные в принципе, в основании. Равны по родовому признаку, но индивидуальны по видовому.

И по этой причине обозначенный выше подход «деньги есть у всех» означает, что рождается «общественный и экономический строй, основанный на общей собственности на средства производства, чем обеспечивается социальное равенство».

Открытым же остаётся вопрос: а кто будет всё это контролировать?

ТЕРМИНАТОР ВОЗВРАЩАЕТСЯ

Не раз приходилось наблюдать с экранов телевизоров, кинотеатров, мониторов компьютеров, планшетов и смартфонов различные фильмы, которые в той или иной форме заявляли о гибели человечества или о страдании его через нападение AI[1], который мог быть как в виде каких-то конкретных роботов, так и в виде отдельно взятой программы.

Если вы представитель того редкого вида, который об этом никогда не читал, не слышал по радио и ТВ, не изучал через кадры конкретных кинолент, то вот несколько: «Терминатор» (все части); «Превосходство» (с неповторимым Д. Деппом); «Искусственный разум», «Пароль Хаус» и, конечно же, трилогия «Матрицы». Впрочем, продолжать можно долго, поскольку мир аллегорий — бескрайний: начиная с «Метрополиса» 1927 (!) года и заканчивая...

Но как бы там ни было, проблема AI — проблема в первую очередь систем централизованных. Если изучить шардинг (см. выше), а также модели взаимодействия нод

[1] https://en.wikipedia.org/wiki/Artificial_intelligence

(и их возможной компрометации) у того же Nem, The Power[1], Cosmos и других проектов, станет ясно, что захват открытых децентрализованных (и тем более — распределённых) систем для искусственного разума — дело нетривиальное, если вообще возможное.

И всё же подобная парадигма не может установиться сразу. Причин множество, но три основные (на мой взгляд) следующие:

— ДРС требуют развития личной ответственности и её проработки на самом глубинном уровне. Впрочем, уже не раз обозначенные экологические проблемы, а также и связанные с ними вопросы бедности, общего образования и прочие — вынуждают человечество идти именно этим путём. Не говоря о постоянных и надоевших большинству финансовых кризисах, которые, как и революции прошлых эпох, сметают все накопления и достижения для очень и очень многих.

— Люди откровенно боятся новаторства: взять первые годы картофеля в России, который теперь считают незаменимым продуктом на все времена, а тогда признавали чуть ли не дьявольской проделкой; сотовую связь, о вреде которой в 1990-х не говорило разве что самое ленивое СМИ. И уж тем более когда речь идёт о том, что жизнь должна быть открытой, но одновременно — автоматизированной, в том числе — за счёт ИИ.

— Наконец, люди привыкли лениться из-за потребительского императива, который внушается с детства: учимся в школе 10—11 лет, а затем повторяем в вузе пройденный материал — ещё два года; становимся совершеннолетними в 18—21 год, тогда как многие не доживают и до 55[109]. И всё приводит к тому, что труд, а тем более работа — стали ругательными словами.

[1] https://thepower.io/ru/

По этой же причине сфера развлечений растёт год за годом и в разных регионах: аквапарки и парки аттракционов, всевозможные моллы и комнаты развлечений, постоянно «горящие» туры и засилье туристических YouTube- и ТВ-программ.

Всё вкупе приводит к тому, что децентрализация требует большей осознанности от тех, кто привык жить «по течению», то есть неосознанно абсолютно.

И всё же процесс уже начался: владение приватным ключом в сфере криптовалют — единственный способ владения деньгами в принципе[110]; децентрализованное наблюдение и прогнозирование погодных условий — верный (хотя и не единственный) путь, который даёт положительные результаты[111]; общественный контроль в разных, даже самых тиранических государствах, — свои плоды: от Афганистана и до России, от США и до Сингапура.

И подобных примеров — множество.

Значит, потребуется глубинное понимание не только технологической, но и социальной основы. И о ней — коротко ещё несколько важных тезисов ниже.

СМЕЛЫЕ МЕЧТЫ О НАСТУПИВШЕМ ИЛИ НАЗАД В...?

Здесь попробую[112] кратко описать, почему не переживаю за массовую адаптацию ДРС и W3-технологий в целом. Также покажу предельно широкими мазками, что может ждать в будущем в альтернативе А и Б нас всех.

Один из ключевых вопросов данной книги, а равно и развивающегося рынка ДРС: а будет ли всё это когда-нибудь по-настоящему массовым? Имеется в виду в первую очередь успех IBM, Google, Apple, Microsoft, Facebook и прочих.

И, пожалуй, только меня (В. П.) эта задача не затрагивает абсолютно.

Почему?

Всё рождается и умирает вовремя — даже ненужное: демократия стала если не лучшим, то компромиссным вариантом выхода из кризиса сформировавшихся, новых (!) на тот момент отношений; Великая Октябрьская революция была злом для миллионов людей, но благодаря ей социальные и экономические права стали реальностью: именно противостояние Востока и Запада дало людям возможность развиваться. По этой же причине, какой бы странной и страшной ни выглядела Америка, в 1940-е годы она всё равно казалась многим лучше разрушенного СССР и тем более — нацистской Германии. Лошади — прекрасный транспорт, но они наводнили навозом города, и именно автомобиль стал искомым решением, а сегодня — и он должен кануть в Лету!

Свобода — всегда слишком высокая цена, чтобы заплатить ею за что-то: развитие государства, цивилизации, культурную революцию, генетически правильное население и так далее.

И сегодня, когда мир стоит на эпохальном переломе, то есть старые практики или работают плохо, или требуют чересчур больших ресурсов, W3 — визуальное отображение этой вечной борьбы: совместного и индивидуального, недоступного и открытого, дефицита и достатка, свободы и…

За последние три года удалось проехать несколько десятков стран, и всюду увидел одно и то же: доллар действительно всем надоел, как и сиюминутность потребительской жизни, но ещё четверть века назад было иначе, и главное — не было альтернативы как таковой.

Сегодня она есть, и в любой сфере: предприниматель из маленькой деревушки на юге Китая с помощью AliExpress может сделать свой товар доступным не только в России, но при желании и в Перу; btc как первые (цифровые) истинные p2p-деньги интернациональны по определению, и транзакции стоимостью в 1 000 000 000 долларов — не проблема; главное — всякий стал носителем устройств, мощности которых хватит, чтобы проложить курс до Луны и обратно.

Именно по этой причине не просто верю, но знаю, что концепт W3 получит сторонников в большом количестве: концлагери на территории Китая, возвращение каторги в России, инквизиционные тюрьмы США в формате Гуантанамо, гетто для богатых в Лондоне, Боготе и множестве других столиц и беспечность человечества относительно ноосферы — всё это те самые движители, с помощью которых всякий и все придут, точнее, вернутся к идее децентрализации. Бизнес и наука — в первую очередь: уже.

Но не только они: недаром начал с того, что сегодня совместная работа гуманитарного, естественно-научного и математического знания как никогда велика.

С одной стороны, к этому подталкивает постоянное взаимодействие с роботами, которые давно стали инопланетянами с нашей собственной планеты, то есть организмами абсолютно нам не чуждыми, но незнакомыми: и речь веду не только о материально воплотившихся, как в моделях Boston Dynamic, но и о тех скриптах, что разговаривают с нами в качестве ботов по телефону (привет, Siri, Alisa & Google), давая советы по онлайн-банку, или же в чатах мессенджеров, или меняя VR-маски в видеопрезентациях.

С другой — люди действительно становятся умнее: пока единственное, чего не хватает, — позитивного осмысления.

Да, с одной стороны, именно позитивное мышление сыграло с нами злую шутку[113], и то, что сотворено с Природой, — уже факт: приговор даже; но с другой — нам постоянно талдычат, что «человек — самое опасное животное на свете» или «главный двигатель рынка (торговли) — жадность»: говорят столь часто, что большинство, подавляющее, невозможно огромное по числу сторонников большинство охотно сему верит.

Но разве это так?

Меня лично окружают люди вполне порядочные, начитанные, грамотные, благородные, открытые и уважительно относящиеся к другим. Разве у вас нет таких? Почему-то над человечеством навис дамоклов меч нещадной критики: Грета кричит, что «хватит разглагольствовать» (хотя сама мало что успела сделать помимо слов); очередной президент США грозит очередной не понравившейся стране, а «русский мир» при этом — продолжает бомбить другую часть не понравившихся; Поднебесная спонсирует разного рода сепаратистов, но продолжает делать вид, что всё вполне себе, и так далее.

Но что же остаётся нам, простым людям?

Сражаться: если эпоха Возрождения была временем необходимого сепаратизма, в коем участвовали и прародители Швейцарии, и пираты; если Новое время стало периодом революций; то **сегодня период, когда поле битвы — нигде**. Благодаря транзакционной репутации нет прямой связи с субъектом, а ДРС делают его невидимым для шпионских спутников и дронов, пока используются мэш-сети, VPN, Tor и другие средства анонимизации (или электроника отключается совсем) правильно. Воевать государству (как феномену) попросту становится не с кем.

Именно по этой причине Д. Ассанж смог противостоять целой Империи, как и Э. Сноуден, а Anonymous смогли стать легендой, как и группа White Hat.

Конечно, централизованные мастодонты это понимают: Microsoft недаром скупила разработчиков Linux-решений — Red Hat и главный репозиторий времени нынешнего Github, скооперировалась с Ethereum & Ripple, а равно и имплементировала в Azure самые разные ДРС; Facebook ушла в сторону Libra (пусть это и было неудачным маркетинговым ходом); IBM взялась за Hyperledger, созданный Linux Foundation и т. д. То есть стратегически это уже победа.

Но до окончательного счёта ещё слишком далеко…

ПОСЛЕ ПОСЛЕСЛОВИЯ

Итак, попробую выделить тенденции W3, которые породят новые виды не просто бизнеса, а целые отрасли деятельности:

— интеграция сетей: IoT (включая промышленный интернет), deep/dark-net, Интернет, p2p/ДРС (в том числе — ad hoc решения через мэш-сети) и другие;

— равенство субъекта (человек/AI) и объекта (скрипты/устройства/etc);

— майнинг через активности, которые представляют собой не механическое объединение времени, внимания, деяния как новый вид экономики (моделей экономик);

— интеграция офлайна и онлайна через инновационные протоколы.

Очень значимо, что мы завершили полный цикл: натуральный обмен — деньги — внимание/репутация/время — натуральный обмен (через цифровые аватары). Таким образом, теперь у нас несколько миров, а значит — и мириады экономических моделей: условно — цифровая, реальная, личностная. Все они связаны, и связаны плотно.

Что ждёт дальше? Посмотрим…

***

Этот совместный труд — не просто компиляция записей, статей, эссе на тему W3 и всего, что с ней связано, но именно разновидение перспектив развития, и не только IT.

Именно по этой причине не стал убирать редкие, но повторы: мне (В. П.) было крайне важно показать, как

разные люди в разное время, в разных географических, социальных, экономических координатах думают об одном и том же: о том, как сделать мир чуть свободней, интересней, честнее.

Нет, никто из нас не верит, что инновации в технологиях — спасение: напротив, всякий по-своему понимает, что скорее верно обратное. Без углубления в философию, историю, психологию мир не станет более гуманным, а вот обратное — вполне допустимо.

Многие это чувствуют, но наша цель — показать, что можно делать, если не бояться: страх — не двигатель, а только часть механизма — тормоз. Движение же придаёт любопытство, интерес к общению, взаимное доверие.

Надеюсь, хотя бы часть из этого станет ближе благодаря прочитанному.

До!

ПРИЛОЖЕНИЕ №1. КАК И ПОЧЕМУ ЗАРОДИЛСЯ WEB 3.0? КРАТКОЕ ИЗЛОЖЕНИЕ ОТ СЕРГЕЯ СИМАНОВСКОГО

Данный текст составлен по презентации и вебинару С. Симановского.

— Ссылка на вебинар — см. на канале[1].

— Ссылка на презентацию — здесь[2].

В рамках предстоящего запрета на свободный Интернет в России всем категориям граждан (а также — неграждан) стоит понимать разницу между отличиями и возможностями децентрализованного Интернета и его текущей версией (стоит добавить, что запрет скорее не предстоит, а уже давно идёт полным ходом, пока ещё «плетясь» медленно, но уже уверенно. Само собой, речь идёт о пакете Яровой[3], принятом в 2016 году). И если сейчас кажется, что всё это лирика и законы в РФ никто не будет соблюдать или что у правительства нет средств на выполнение данных законов, то сама мысль о том, что вас (!) лишают базовых прав (прописанных, кстати, в Конституции[114]), как минимум должна вызывать у небезразличных людей волнения: а что, если хватит средств/сил/времени?

Но для начала необходимо немного погрузиться в некоторые детали и понять, что же такое Web 2.0 и Web 3.0, их отличия и всё, что за ними стоит.

---

[1] https://clck.ru/MCWQh

[2] https://clck.ru/MFSqn

[3] https://en.wikipedia.org/wiki/Yarovaya_law

ЧТО ЖЕ ТАКОЕ WEB 3.0?

Предполагаю, что данный термин можно прояснить двумя способами. Используя Вики: «концепция развития интернет-технологий… (которая) позволит на её основе силами профессионалов создать высококачественный контент и сервисы… определить Web 3.0 как „взаимодействие интернета с физическим миром“»; либо своими словами: Web 3.0 — свободное (не зависимое от других лиц и сервисов) общение приложений, ботов, софта (и не только его) и людей, стоящих за ними, между собой. Это формализм, в котором человеку N не нужно получать разрешение на раздачу файла, стоять в очереди за «визой на паспорт» и не нужно платить кому-то за воздух. Web 3.0 — попытка (да, это очередной виток развития, в некотором смысле — эксперимент) человечества исправить централизованные сервисы, на балу которых правят (условно) десять корпораций[115] и люди принимают политические решения на основе картинок в соцсетях.

Web 1.0 — понятие, которое родилось до первого бума доткомов[1]. Имеется в виду куча статики, HTML, маленькое количество создателей контента и много потребителей последнего. Ещё одна характеристика Web 1.0 — медленная

[1] https://en.wikipedia.org/wiki/Dot-com_company

скорость подключения к Сети и распространённая компьютерная неграмотность.

Сдвиг к Web 2.0 произошёл с появлением новых технологий, таких как более удобные браузеры, больше интерактива на самих сайтах, и с развитием высокоскоростного подключения к Интернету.

В основу Web 2.0 легло развитие проектов, сервисов, таких как социальные сети, блоги и т. д. При этом вопросы надёжности и достоверности подачи информации не являлись приоритетом. В эпоху развития Web 2.0 появляются и развиваются технологии, которые всем сегодня известны: возможность асинхронной подгрузки информации (AJAX и подобные), теги, ссылки и развитие HTTP (протокола «клиент-сервер»: сам протокол — подарок Web 1.0).

Четвёртой версией веба я бы назвал что-то, куда Интернет может уйти потенциально. Некое «чёрное зеркало», в котором, с одной стороны, всё прекрасно и автоматизировано, а с другой — всё подконтрольно корпорациям и государству. То есть огромная интерактивная паутина, в которой всё взаимодействует словно хорошая коробка передач. Вот правда как автоматическая — в той, в которой ни у кого уже нет возможности самому управлять автомобилем и самостоятельно принимать решения: даже в самый ответственный, критически важный момент!

Для того чтобы двигаться ещё дальше, нужно вникнуть в некоторые технологические понятия. Давайте попробуем очень поверхностно это сделать.

Итак, что такое протокол?

В сфере IT — просто набор данных или стандарт, который описывает взаимодействие чего-либо с чем-либо другим. То есть нечто, что определяет, как будут общаться между собой те или иные программы/интерфейсы, как будут обрабатываться ошибки и т. д.

Что такое маршрутизация?

Это слово имеет смысл, который в английском языке называется does what it says on the box, то есть путь, по которому будут следовать данные в сетях связи.

Как же передаются данные в Интернете?

В первую очередь, нужно понимать, что данные передаются пакетами. То есть чем больше кусок информации, тем (обычно) больше пакетов. Очень глупый, но хороший пример — это представить себе, что файл — паровоз, а данные в нём — вагоны, и чем он больше, тем больше у него вагонов.

В каждом пакете содержится информация о файле: откуда пришла информация, куда она идёт, информация об оригинале файла и, грубо говоря, порядковый номер (условно часть 3 из 123). Как только все пакеты «доехали» до места назначения, один из протоколов их восстанавливает.

Можно резюмировать следующее: файл в компьютере А был разделён на пакеты протоколом — пакеты, которые по отдельности пришли в новое место, — протокол пересобрал пакеты, чтобы воссоздать файл на компьютере Б — файл в компьютере Б.

Так как пути пакетов не всегда очевидны, наилучший путь помогает найти то, что зовётся роутером (компьютером-маршрутизатором).

Обычно информации приходится проделать путь через n число роутеров, чтобы найти свой пункт назначения. Стоит понимать, что путь может меняться в процессе (в идеале ради поиска оптимального маршрута), так что пакеты от одного файла могут путешествовать разными путями.

***

Возможно, стоит отойти в сторону и буквально на секунду задуматься о том, что такое компьютерная сеть и как работает Интернет.

Компьютерная сеть — сеть узлов, связанных между собой одним или другим способом (например, при помощи кабелей или мобильной радиосвязи). В роли узлов могут выступать компьютеры, сервера, мобильные телефоны, принтеры и т. д.

Есть такое страшное слово, как модель OSI[1] (кстати, расшифровывается это совсем не страшное слово как открытая система интеркоммуникации). По сути, это набор правил для поведения участвующих в ней протоколов на каждом из её семи уровней (в старой версии уровней семь, в более «новой», смотря как считать, их от пяти до шести). Но не будем уходить в разборку модели OSI.

Хочу сказать, что данную модель стоит рассматривать от верхнего уровня (уровень аппликаций — браузер, email, в некотором смысле блокчейн и другие) и понимать, что эта модель, по сути, диктует правила поведения каждому протоколу на каждом своём уровне. Нужно понимать, что у неё один физический уровень — первый, который и подразумевает системы кабелей или любую другую передачу электромагнитных импульсов (всё, что можно потрогать руками).

Это отступление делаю, чтобы понимали, что сейчас мы «как мартышки привыкли к облачной модели работы с Интернетом»[116], хотя любому p2p-приложению можно задать свой набор поведенческих правил, который не обязан следовать модели «клиент-сервер». Также можем со-

[1] https://en.wikipedia.org/wiki/OSI_model

здать и свой собственный физический уровень. Например, при помощи так называемых мэш-сетей[1].

Интернет не обязан работать по принципу «клиент-сервер». Совсем не обязан. Это нужно понять и осознать.

***

Для данного раздела необходимо понимать следующие протоколы:

TCP-IP: набор правил, решающих задачи по передаче данных, на которых базируется Интернет. Из названия понятно, что он состоит из двух частей. TCP — протокол транспортного уровня, выполняющий функцию «корректного» общения между различными системами коммуникации и стандартными протоколами. IP, или Internet Protocol — в некотором смысле объединяет отдельно стоящие компьютеры в одну большую сеть. Его задача — маршрутизация пакетов данных между узлами. Вместе они являются неким стандартом для коммуникации информации/данных.

HTTP и HTTPS: протоколы для обмена пакетами данных между сервером и клиентом. По сути, последний — всё тот же «клиент-сервер», но в зашифрованном виде. Немного иными словами, это протоколы передачи данных для получения информации с веб-сайтов.

URI и URL: некие универсальные идентификаторы. Простым языком — строка, позволяющая обозначить документ/файл/почтовый ящик и т. д.

[1] https://en.wikipedia.org/wiki/Mesh_networking

DNS: иерархическая система именования для компьютеров, сервисов и всего того, что подключено к сети. Берущая свои корни у АРПАНЕТа[1] (компьютерная сеть, созданная министерством обороны США, которая является неким прототипом текущей версии Интернета).

И ещё два термина, которые пригодятся чуть позже:

Семантическая паутина — глобальная сеть, в которой вся информация является пригодной для машинной обработки. В отличие от HTML, который пригоден для чтения и понимания человеком, в семантической паутине все элементы предназначены для машинного чтения. Имеем: предмет — связь — другой предмет на выходе. Программы-клиенты, которые получают данные и делают логические заключения.

Наконец, **p2p** — одноранговая, децентрализованная сеть, основанная на равноправии участников. Узлы одновременно выполняют роли серверов и клиентов. То есть (почти) нет посредника — субъекта.

Кстати, хочу сказать спасибо Web 1.0 за это наследство, благодаря которому пропускная способность Интернета всё ещё далека от высокой. В частности, за DNS и систему маршрутизации данных: до сих пор «стучимся» к одному серверу, запрашивая данные; и, само собой, «стучимся» к серверам по очереди. Например: не нашёл у А — иду к следующему; или: А спит — иди дальше.

Для чего это рассказываю?

Для того чтобы показать, что вся «связка», на которой построен текущий Интернет, более чем централизована. Например, домены верхнего уровня до 2012/2013 гг. (org/com и другие) вообще нельзя было регистрировать обычному смертному[117].

---

[1] https://en.wikipedia.org/wiki/ARPANET

На данный момент ICANN, которая с 2016 года является якобы независимой, продолжает администрировать домены высшего уровня (простой поиск легко выдаёт информацию о сотрудничестве с американским правительством и о том, кто на самом деле является бенефициаром в данном вопросе).

Текущие стандарты и протоколы на поверхности могут казаться децентрализованными и справедливыми. Но если немного копнуть, начинаем видеть огромное количество проблем. Таких, как отсутствие решений для безопасности и излишнее раскрытие персональных данных.

Получая доступ к таким данным (как IP-адрес), их можно подделать и получить вход в сеть, тем самым иметь фактически неограниченные возможности относительно любого набора данных внутри данной сети. Многие стандарты «зафорсены» и «запушены», при этом часть прибыли, полученная от определённых действий, связанных с работой Интернета, делится между несколькими крупными игроками (в том числе и некоторыми правительствами). Эти игроки не имеют намерений или интересов что-либо менять. Потери данных, доменная система и прочее — верхушка айсберга, гнилью которого покрылась Всемирная паутина.

Основываясь на данных выше, можно сделать пару простых выводов: до сих пор живём в зазеркальной стране ссылок Web 1.0 и 2.0 — порочный круг, который не снился и самому Данте. HTTP — URL — DNS. Пользователю необходима информация, он её запрашивает у ограниченного количества серверов (при этом порочный круг нам сам скажет, куда стучать, нас особо не спросят). Серверов мало — пользователей с каждым днём всё больше и больше.

Всё это порождает технологические проблемы и всё чаще описывается футурологами как война за Интернет (из последнего — «Первому игроку приготовиться» Спилберга). Вопрос о перегрузке не в «если», а в «когда»...

ИТАК — WEB 3.0

Но, как говорится, мир не без добрых людей. В эпоху развития Интернета на свет появляются прекрасные технологии и протоколы. Например, такие понятия как DHT и TCR. Сейчас оба используются так или иначе в архитектурных построениях баз данных и в блокчейн-сфере.

DHT, или распределённые хэш-таблицы, — децентрализованный и распределённый класс систем для обзора и поиска данных при помощи узлов-хранителей и ключей. DHT может являться своего рода инфраструктурой, например, для p2p-сетей, распространяющих файлы. Такая инфраструктура более надёжна, безопасна и главное — децентрализована.

TCR — курированные списки, в которых для пользователей существует инициатива вознаграждения чем-либо (обычно это некий токен).

И тут хочется упомянуть два прекрасных проекта, порождённых Web 1.0 и Web 2.0, без которых, как мне кажется, всё могло быть немного хуже. Это Napster[1] и Bittorrent[2].

Napster — p2p-обменник для музыки 1999 года, который перевернул сознание пользователей: оказалось, что

[1] https://ru.wikipedia.org/wiki/Napster

[2] https://en.wikipedia.org/wiki/BitTorrent

можно было свободно (ну почти — привет «Металлике[1]») обмениваться файлами с другими пользователями. Популярность «Напстера» впервые за многие годы поставила под вопросы стандарты, которые типично использовались. Суть не в том, что до «Напстера» никто об этом не знал. Суть в его популярности и в том, насколько он перевернул сознание масс в данном вопросе.

Bittorrent, который появился чуть позже (в 2001 году), — протокол для коммуникации данными и, следовательно, файлами по схеме person-to-person. Прелесть в работе «Битторрента» появилась в тот момент, когда ребята из Vuze смогли интегрировать DHT-таблицы в процесс работы сервиса и, по сути, перестали трекать[118] пользователей. Такой дизайн позволил создавать независимые друг от друга сети для каждого торрента и дал большой пуш[119] развитию p2p-технологий.

Нужно принимать во внимание, что информация, предоставленная выше, — поверхностные знания, в некоторых местах технологически не точные, но описанные более понятным языком для восприятия любым человеком, даже технически не подкованным.

Для того чтобы вникнуть и понять, как работают протоколы, требуется много лет изучения различных сфер. От построения СУБД до криптографии. Я же не являюсь экспертом по протоколам, а использую информацию выше, чтобы вывести некоторый ряд логических заключений. О которых мы, собственно, и будем говорить дальше.

---

[1] https://en.wikipedia.org/wiki/Metallica_v._Napster,_Inc.

***

Если на секунду остановиться и посмотреть на картину целиком, а точнее, на развитие разных протоколов до стадии блокчейна и таких компьютеров, как Ethereum, то можно увидеть прогресс от мультиранговых сетей, основанных на работе серверов, к модели, которая базируется на самом пользователе. Мне лично всё это напоминает развитие подачи информации от газет к YouTube (YouTube — распределённый ресурс, на который любой желающий может залить какую-либо информацию; газета же (особенно в её классическом понимании) — не просто административный ресурс, но и часто проспонсированный некими лицами для продвижения собственных целей и пропаганды).

2009 год[120] положил начало развитию эры блокчейна. Тут распределённые реестры и таблицы начали использоваться немного в ином ключе. Поинт был в «неизменной» информации, в которой каждый узел мог отслеживать информацию, но не мог её менять. Для DHT была отведена роль эффективного распределения информации в сети.

Никто и не ожидал, что какой-то там «Бейтховен» станет самым важным в истории человечества денежным протоколом, который, помимо всего, даст толчок в развитии механизмов консенсуса, затронет глобальные вопросы управления и иных прикладных ценностей (см. выше).

Собственно развитие блокчейна не заставило себя долго ждать, и здесь тоже появились 1.0, 2.0 и последующие версии, где первой ветвью был сам биткоин, который позволил решить вопрос двойной траты[1] в рамках электронных денег и обмениваться информацией децентрали-

[1] https://en.wikipedia.org/wiki/Double-spending

зованно. Спустя некоторое время родился блокчейн 2.0, или программируемое поведение цепочки (умные контракты). Ethereum — софт, позволяющий писать open source[1], unstoppable[121] код. Умный код.

За это время в блокчейн-индустрии на свет появилось много прекрасных и умных компьютеров. Таких, как Polkadot (см. выше), называемый многими Blockchain 3.0 (а за ним — 4.0 и даже 4.5). Сеть, позволяющая создавать и соединять аппликации (приложения) и другие сети, писать собственные протоколы, сайдчейны и т. д. При этом — сохранив уникальность архитектуры, и всё это — в децентрализованном виде!

Во всём этом прослеживается развитие от того, что когда-то было просто поиском через центральный сервер соединяющих сеть пиров[2], к классу децентрализованных хранилищ и сетей с мотивированными узлами, сотрудничающими в скоординированной манере при помощи кода.

Подобные сети и есть то, что называю Web 3.0!

В их непосредственном сотрудничестве между собой, прямой мотивации пользователя и узла, координации действий при помощи умных контрактов, отсутствии (ненужных) третьих лиц, безопасной маршрутизации данных и т. д. Вот в чём кроется ключевая разница между Web 2.0 и 3.0. Продолжая строить и развивать подобные сети, вступаем в новую, децентрализованную эру приложений, способную снизить расходы и дать заработок каждому участнику. Интернет, в котором каждый (вроде бы) — потребитель, но одновременно и создатель контента.

---

[1] https://en.wikipedia.org/wiki/Open-source_software

[2] https://ru.wikipedia.org/wiki/Peer

***

Давайте плавно перейдём к проблемам Web 2.0, не столько техническим, сколько более глобальным. Проблемам, которые так или иначе задевают всех пользователей Интернета, и не только их (я о том, что проблемы Сети выходят далеко за её рамки… Это, конечно, если до сих пор мыслить в категориях о том, что Интернет — не везде).

Выше немного затронул тему развития от газет к YouTube. На самом деле всё не так просто и красиво, как кажется. В некотором смысле променяли одних моголов на других. Times стал Instagram, а Fox News — Facebook. Может ли это считаться хорошо? Поменять одних диктующих мнения и разжигающих гнев политологов на других, делающих это более интерактивно и умно?

Во многом не появление YouTube стало началом новой эпохи, а удешевление смартфона с камерой: тогда информация стала доступна всем повсеместно. Люди начали выкладывать видео отовсюду. Со всех уголков Вселенной (включая Сибирь-матушку и Луну). Новостные каналы начали ссылаться на частные «видосики» и фото. Появились новые слова: мемы, тренды и другие. И с одной стороны — видим прогресс в том, как вся эта информация могла распространиться (включая независимые блоги/газеты и далее); с другой — что-то и где-то пошло не так. Люди стали принимать политические решения, основываясь на постах в ФБ[1]. Корпорации стали перепродавать информацию и данные пользователей, хранящиеся на их серверах, без оглядки друг на друга. Google знает о вас всё: даже то, чего не знает ваша супруга или муж.

---

[1] https://www.vedomosti.ru/technology/articles/2018/07/18/775875-tramp-facebook

Централизация данных и серверов (привет, Amazon) достигла пика. Всего несколько компаний в мире владеют таким количеством мощи и влиянием — что не снились даже Ост-Индской компании[1] рубежа XVII — XVIII вв.

Возникает вопрос: ну и при чём тут Web 2.0? А при том, что именно он и его структура обмена данными, стандарты, отсутствие приватности, описанная маршрутизация данных и другие элементы — позволяют превратить пользователя в слепого потребителя контента, которого машинное обучение каждую секунду кормит всякой… ерундой. При этом далеко не пользователи решают, что, куда, кому и как (хотя всё стало настолько «умным», что некоторым может показаться, что они — да, решают).

Рынок продажи данных и банальное несоблюдение правил безопасности — стало нормой. Люди больше не задумываются, передавая свои данные другим. Хотя, если подумать: именно информация и есть и золото, и нефть XXI века! Это простое, банальное и базовое право человека.

Приватность

Управление собственными решениями. Свобода слова: попробуйте запостить в ФБ то, что кто-то там в ФБ не считает нормой; попробуйте сделать поиск квартиры на Airbnb в любом городе под Win 10[2] — увидите, как винда отслеживает данные и меняет заставку под вас. Это может показаться даже полезным. И оно бы было полезным, если бы я имел от этого выгоду. В вариации, где все эти сервисы работают на технологиях W3, — это как минимум делается с моего разрешения и я получаю от этого пассивный доход в виде токенов/стекинга/репутации и т. д.

---

[1] https://en.wikipedia.org/wiki/East_India_Company

[2] https://ru.wikipedia.org/wiki/Windows_10

И, допустим, я готов продавать свои данные. Но не я, не вы, а кто-то иной получает всю прибыль, считывая вас и информацию, которую вы выдаёте, обучаясь на ваших повадках. **Зарабатывая вашими действиями…**

Вопрос, который следует задать самому себе: сколько стоит моя приватность? Банальный пример, как при помощи старых Web 2.0-приёмов продаём себя за пять копеек. Вдумайтесь, был ли у вас адрес с пройденным KYC и привязанный к централизованной бирже? А дальше прислали с этого адреса хотя бы один раз btc на любой ваш «скрытый адрес»? А ещё дальше — использовали последний или с него прислали на другой, чтобы сделать клейм на другую валюту? Вот и продажа данных при помощи старых трюков.

И как же без понимания того, что все специальные сервера принадлежат всё той же кучке корпораций, которая контролирует рынок данных. В геополитических рамках они (корпорации) способны на изменение/предотвращение/форсирование информации как, когда и где им удобно (на слушаниях в США CEO Google так и не ответил на простой вопрос о том, способны ли сотрудники Google влиять на выдачу информации).

***

И тут хочется немного уйти в сторону и поговорить об успехе. О том, как его измерять. И поясню, зачем и почему…

Считаем ли успешным Интернет 2.0? Как измерить успех интернета? Можно ли смело говорить, что успех —

то, что напрямую зависит от уровня его популярности и использования (либо от размера и/или капитализации)? Моё мнение — нет.

Выше уже упомянул все доводы о лжеинформации в СМИ при помощи интернет-платформ. Но Интернет создавался именно как свободное пространство. А теперь возьмём Linux-системы. Успешны ли они? Они есть везде, хотя о них никто не говорит. Чёрт! Даже в вашем доме сейчас их порядка ста. Датчики, телефоны, машины, техника, компьютеры. Везде! При этом[122] — бесплатны! Так кто из них успешен? И как его, успех, измерять? Доступностью? Капитализацией? Решать вам…

Мораль сей басни в том, что W3 сейчас, возможно, не кажется успешным. Возможно, сейчас тяжело измерить успех open source[123] приложений. Но на примере Unix-систем и блокчейн-платформ видим, как W3 может стать успешным. А это означает, что достаточно разобраться в том, как он работает, и начать собственный бизнес в данном направлении.

***

Теперь предлагаю поговорить о двух заключительных вещах. В первую очередь про более насущные проблемы, во вторую — немного о прикладной части, так как всё это пока может показаться слишком абстрактной информацией. Более глобальные проблемы: банковский кризис, ЕЦБ и при чём тут W3?

Не хочу сейчас ударяться в философию или детали кризиса 2008 года. Для более-менее образованного чело-

века всё и так понятно: ЦБ работают по одной и той же схеме, начиная с Великой депрессии. Их цель одна — сделать ЦБ неприкасаемым и независимым, при этом вогнать в долг государства и даже корпорации, которые считают, что они стоят у руля (хотя с появлением новых банков в виде ФБ — спорно, кто именно у руля).

Схема банальна и проста: создаётся нехватка денег, далее раздувается пузырь (кредитной политикой и процентами ставками… хотя есть более умные и извращённые способы — акции 1920-х, трейдинг в Японии, долговые обязательства и кризис недвижимости и т. д., но все они по сути одинаковы), далее начинается… апокалипсис — в прямом смысле. По итогу которого ЦБ получает то, что хочет, — независимость, печатает новые деньги бесплатно (на самом деле — за наш счёт) и производит выкуп обанкротившихся бизнесов и предприятий.

«Печатает, потому что может»!

Заметьте, что условия независимости всегда важны для ЦБ. Например, ЕЦБ вообще настолько гениально продуман, что на всей планете на данный момент не существует ни одного правительства / суда / иного рычага воздействия на данную организацию. Никто и ничто не имеет права (де-факто и де-юре) оспаривать решение ЕЦБ (нет — де-юре, конечно, можно оспорить, но тут нужна неимоверная удача).

Ещё немного лирики: когда последний раз участвовали в заседании по изменению ставок в рамках состава ФРС? Ага… А ведь эти двенадцать человек принимают решения за всех нас! Они, совместно с ЕЦБ, диктуют мировую экономику, политику и повестку дня в целом.

И теперь к W3 — и в чём разница? За десять лет протокол Bitcoin ещё ни разу[124] не был непредсказуем. Все ставки известны заранее (приток денежной массы, количество участников сети и так далее). Я и остальные участники сети принимаем решения свободно и независимо. Про-

токол Bitcoin не перестал работать ни на одну секунду[125] (что сложно сказать о ФРС или ЕЦБ).

Чувствуете разницу?

Могла бы кучка банкиров раздуть экономический пузырь, не имей они своих рычагов? Вы правда считаете, что их желание создавать «криптофиат» и другую… ерунду исходит из благих намерений?

Ещё раз о ФБ-коин (aka Libra). У меня есть статья «Вам не нужен блокчейн, вам нужен фейскоин»[126] — суть в том, что то, что создаётся данными корпорациями, создаётся на базе технологий Web 2.0 — это централизованная, коррумпированная, отслеживаемая система, которая никогда не будет иметь ни одну из тех ценностей, которые несут в себе open source криптовалюты и блокчейн-протоколы. Они будут популярнее, быстрее и дороже… но тут вам к измерению успеха — капитализацией или доступностей?

Есть прекрасный документальный фильм Princes of the Yen[1]. Если посмотреть его один раз и почитать после него немного литературы по теме, работа всех ЦБ становится более понятной.

W3 даёт рычаги воздействия. Предлагает незаменимую, безграничную, честную технологию, основанную на математике, основанную на неостанавливаемом коде. Технологию, при помощи которой у каждого в кармане (за 20 евро) появляется свой собственный банк. Блокчейн (который часть W3) — интернет денег. Это не просто база данных. Да, это набор технологий, давно уже известных человечеству. Но при всём при этом это и парадигма, при помощи которой каждый имеет возможность сделать чуть-чуть лучше. Получить распределённую ценность, пассивный доход и иметь воздействие на различные локальные вопросы (иду именно от локального к глобальному, а не наоборот).

---

[1] https://www.imdb.com/title/tt4172710/

***

Давайте попробуем разбавить всё вышесказанное прикладной частью. Буду продолжать приводить примеры и рассказывать о возможностях. Но попробую сделать так, чтобы каждому стало чуть более понятно не только, что такое W3 и чем он лучше, но и то, как можно воспользоваться для себя.

Перестроение Всемирной паутины — что с того?

В первую очередь давайте поговорим о простом и подумаем, что с этого каждому из нас. Офлайн-браузинг… его до сих пор нет. Информацию, которую получаем (которая дублирует сама себя), можно было бы кэшировать и сохранять, тем самым — снизить глобальное потребление трафика: в разы! С использованием технологии p2p и W3-решения всё могло бы происходить на локальном рынке и дать пуш развитию «локальных серверных точек». Информация была бы получена в разы быстрее и от человека с репутацией, которую подтверждает математический код, а не централизованный сервер или гугл-работники. Количество подобных сетей могло бы развиваться и расти, так как они бы были вознаграждены путём того же токена. Перепродажа данных могла бы либо «уплыть в небытие» в таких сетях, либо, наоборот, стать очередной статьёй дохода для тех, кто пожелал бы делиться[127].

Тут стоит отметить, что хранение личностей или персональных данных в W3 тоже может получить совершенно другой оборот. Ребята из CYB прогнозируют, что информация будет храниться в виде наборов секретов и кусков информации, например, через доказательство с нулевым разглашением[1] (доказательство набора информации при

[1] https://en.wikipedia.org/wiki/Zero-knowledge_proof

помощи секретов[1], грубо говоря, не раскрывая при этом ничего лишнего). Которые позволят не раскрывать личность, но всё же 100% подтверждать при любой необходимости.

Что же те, кто поддерживает все эти протоколы в новом вебе?

Майнинг (в широком смысле: от POW до DPOS) и есть новый вид глобальной поддержки распределённых сетей. И более чем уверен, что уже совсем скоро (а ещё точнее — уже наблюдаем) увидим, как майнеры становятся провайдерами. Это позволяет им (майнерам) выполнять целый ряд действий и получать доход: шардинг, защита данных, чтение данных, оракулы, он- и оффчейн-транзакции… И далее. И да, это и есть новый вид провайдера услуг в W3-пространстве, позволяющий любому участнику стать провайдером, вкладывать, развивать и получать вознаграждение.

Контент-адресации http и url нужна смена, и она есть. Для получения контента не нужно знать сервер и его местонахождение. Уже сейчас существует IPFS, которая в самой ссылке показывает, что за контент по ней лежит и как его достать. На данный момент ссылка предоставляется в виде хэша, который, да, читать сложно (но вспомним, о чём в начале говорилось, и о языке пригодным для чтения машинами).

На данном этапе в распределённых реестрах нет нормального алгоритма для обработки информации, откуда, собственно, можно получить грамотную индексацию требуемых данных (на данный момент всё ещё хуже… никто (!), включая Google, не знает, как происходит индексация данных — и это правда. Тот же Google нанимает людей, которых в W3 называют оракулами, которые поставляют

[1] https://youtu.be/NgrVJolrPU4

достоверную информацию из внешнего мира в Сеть. О них чуть позже. Результаты олимпиад и матчей «корпорация добра» обновляет вживую, работой человека, который смотрит матч. В случае любой глобальной катастрофы могут произойти огромные потери данных и понимания того, как действует механизм выдачи информации).

Индексацию, основанную на том, чем интересуется пользователь, а не на рекламе, — вот чего ждёт W3 (и мы все)!

P2P-СЕТИ — ПРИМЕРЫ И КАКОЙ ОТ НИХ ТОЛК?

В первую очередь скажу о псевдо-W3: MetaMask, Mist, Brave. Данные технологии не являются W3, хотя и могут дать некий расширенный и улучшенный функционал (например, что-либо НЕ отслеживать, насколько это возможно, (почти) напрямую работать с приложением и т. д.). Эти сервисы зависят от технологий, на которых построены, то есть от W2, и, соответственно, они имеют «болезни» W2.

В W3 браузеры, код, приложения, софт и другие сущности будут общаться с друг другом напрямую и, скорее всего, будут выглядеть очень и очень непривычно (по крайней мере изначально). Что, как ни странно, опять возвращает к мысли о новых рынках, о том, что эти просторы ещё не паханы.

На этой ноте буквально пара слов и о псевдоблокчейнах и криптовалютах — спасибо Сергею Прилуцкому[1] за гениальное сравнение. Пожалуй, процитирую: «Почему сейчас токен и немного JavaScript называют „криптоплатформой“? Потому что для того, чтобы его запустить, нужно договариваться с кучей инстанций? Слово „платформа“-то

[1] https://www.facebook.com/prilutskiy.sergey

здесь при чём? Делать будут наверняка на эфире, вейвсах или мастерчейне каком-нибудь. Свою сеть поднимать ради простого (и даже сложного) токена особого смысла нет. Откуда эти „платформы“?» Или ещё проще: если у вас есть шесть соток и вы там раз в пять лет выращиваете капусту, это не делает вас фермером.

Это о наболевшем, но уверен в том, что об этом стоит помнить, перед тем как назвать золотом всё, что блестит…

НЕМНОГО ПРИМЕРОВ В ДЕЙСТВИИ

Aeternity — проект, который перекроил (отчасти взяв из других проектов) naming system, то, что зовём DNS, а у сервиса это в будущем, скорее всего, будет именоваться ANS. Aeternity делает огромный акцент на распределённых оракулах и на том, как и в каком виде они будут поставлять данные в сеть. Где будет:

— использоваться вознаграждение в виде токенов?

— стейкинг репутационных рисков?

— распределённые репутационные системы, а где новые механизмы консенсуса?

Прелесть в том, что некоторые части из этого уже можно потрогать и пощупать; главное — почитать и изучить.

Cyb (о котором шла речь выше) — W3-browser и глобальная, распределённая система поиска. Многообещающий проект, о котором, возможно, мало кто слышал (а ты, читатель — уже целых два раза минимум!).

Polkadot — глобальная автомагистраль для других блокчейн-проектов. W3-проект, соединяющий другие за счёт собственных инноваций и распределённых техно-

логий. Грубо говоря, город, из которого «все дороги ведут в Рим», а точнее, все ведут к нему и из него.

Тут можно привести в пример создание бизнесов на основе кроссчейнов и на основе провайдеров информации «из мира — в сеть», таких как распределённые платёжные системы (начиная от человека-к-человеку и заканчивая сложными схемами: выплата по наследству по окончании n-ых действий и прочее; распределённые банки (DAI), в которых консенсус принадлежит сети и пользователям, и многое другое).

Holochain — интереснейший проект, который проектируется по совершенно иным принципам в отличие от стандартных блокчейнов. Тут нет консенсуса, зато есть распределённые хэш-таблицы, локальные хранилища данных и офлайн-доступ к сети и приложениям. Проект строится исходя из принципов того, что всё должно и будет общаться напрямую друг с другом, без какой-либо точки входа.

Skycoin — децентрализованный интернет по принципам W3. Проект, объединяющий в себя самые хипстерские технологии и все «прелести» новой парадигмы. Задача его — не только спроектировать новую всемирную паутину, но и создать новый мир по новым правилам.

ВСЁ ВЫШЕ И ВЫШЕ...

Последняя ступень и ещё одна тема, которую стоит затронуть: на её основе можно создавать не только бизнесы, но и монтировать организации, разрабатывать и согласовывать правила... Это тема скорее не технологических, а парадигмальных аспектов W3.

Говернас и механизмы консенсуса. Появление W3 породило вопросы консенсуса и управления. В свою очередь, это дало толчок развитию проблематики византийских генералов (читай подробней в главах про консенсус и шардинг). В новых схемах часто участвуют все участники, порой участвует часть (для более высокой эффективности), делегируются репутация, голоса, доли и много всего другого.

Это позволяет создавать справедливые архитектуры управления. Например, ТСЖ, в котором участники и владельцы долей — жильцы квартир. Репутация основывается на их действиях, доли — на основе размера метража, вознаграждение — в виде оплаты услуг ЖКХ; от субаренды нежилых площадей выигрывают все, а вся информация занесена в реестры (да, сейчас это может показаться фантастикой, и бабушки на скамейке нас всех победят, но, уж простит меня блокчейн, — бабушки не вечны).

СМАРТ-КОНТРАКТЫ, IOT И РОБОТЫ

Программируемые контракты создают возможность для любых видов деятельности от банально понятных в виде «заплати токены, если инвестировал», до на сегодняшний день кажущихся фантастикой в виде «ухаживай за моим местом захоронения и получай деньги по смарт-контракту после подтверждения действия».

Роботы и IoT создают просто огромную отрасль, в которой информация получает ценность. Изучая те действия, которые им позволяем, анализируя их и продавая ту информацию, которую хотим.

Опять же, от простого «умного» холодильника до глупого и смешного «смотрю эротический фильм, а робот изучает, какие моменты мне были интереснее, и продаёт информацию создателям роликов».

Примеров миллиард, но суть одна — возможность убрать посредника, получить вознаграждение за сделанное. И да: развить при этом Сеть!

НОВЫЕ ВИДЫ ОРГАНИЗАЦИЙ

«Арагон» и «Гитколони» — на примере первого можно создавать различные организации, без границ и посредников, глобальные и без бюрократических проблем. Организации, за которыми стоят пользователи, кодовая база, математика и кооперация участников.

GitColony[1] — простой пример того, как интеграция технологий W3 помогает создавать IT-команды, делать их лучше, умнее, быстрее. Всё при помощи кода. Где доказательством выступают либо коммиты, либо количество написанного кода. Где разработчики получают вознаграждение за те действия, за которые бы не получали профит без подобного рода формализма. Где легче и проще найти работу. Где легче и проще создать что-то новое, получить за это оплату и радоваться результатам.

[1] https://www.gitcolony.com/

ЗАВЕРШЕНИЕ ДЛЯ ПРИЛОЖЕНИЯ

Хочется сказать о том, что всё это уже давно не новое, но развитие как технологий, так и свободного мышления, а также доступность информации помогает строить децентрализованное. Уже сейчас выгоду подобной структуры можно описать на примере транзакционных взаимоотношений между людьми и организациями.

Человеческие взаимоотношения построены на экономической выгоде по отношению друг к другу, выражаемой в количественном или качественном эквиваленте. Частные системы с древних времён показывают свою неспособность к масштабированию и дороговизну транзакционных отношений. Проще говоря, не обеспечивают нормальное обслуживание отдаваемых в них же ресурсов. Институты же, подбирая свою деятельность под режим, не снижают транзакционные издержки, а повышают их, тем самым ставя себе палки в колёса для дальнейшего роста.

Типичное решение показано на примере первого в мире DAO, которым является Bitcoin: децентрализованная система на основе открытого кода, решает указанные проблемы путём записи транзакций в публичный и доступный реестр, тем самым показывая преимущества децентрализованных систем и распределённых экономических моделей внутри.

ПРИЛОЖЕНИЕ №2. ПЕРСПЕКТИВЫ РАЗВИТИЯ БЛОКЧЕЙН-РЕШЕНИЙ — НЕОЧЕВИДНЫЕ ТЕНДЕНЦИИ

Данный материал задумывался как отдельная статья, но идеально подходит именно для раскрытия содержания настоящей книги. Автор — В. Попов (aka Menaskop).

О СУТИ

На сегодняшний день происходит развитие технологии блочной цепи, но при этом blockchain — не только технология, но и система ценностей и взглядов (сколько раз я и коллеги уже повторили это за книгу?:). И именно благодаря принципиальным отличиям децентрализованного подхода появился Bitcoin как противостояние классической банковской системе после кризиса 2008 года.

Как известно, блокчейн зиждется на следующих посылах:

— анонимность;

— открытость;

— автоматизация доверия[128] за счёт криптографии;

— распределённость (децентрализация как начальное условие).

Развивая каждый из пунктов и совершенствуя начальные условия сети Bitcoin, появились первые форки и иные альткоины: LiteCoin был направлен на упрощение майнинга и скорости транзакций, Dash — на анонимность, Nem — на большую децентрализацию и создание собственного блокчейна и так далее.

Но сейчас вопросы стоят ещё жёстче: вскрывается сильнейший антагонизм современности — борьба государ-

ственной власти за ужесточение требований отслеживания действий граждан (достаточно вспомнить о слежке АНБ) и желание граждан противостоять данной системе всеми возможными легальными способами, включая право на тайну связи, переписки и прочее.

АНОНИМНОСТЬ РАЗНОГО РОДА

Dash, Zcash, Monero и ещё множество более мелких криптомонет дают возможность совершать транзакции анонимно. У этого пункта есть как минимум две составляющие: позитивная и негативная.

Положительный аспект состоит в том, что благодаря анонимности можно обеспечивать тайну связи, а она, в свою очередь, ограждает общество от излишних знаний о субъекте.

Негативный аспект известен: возможность спонсирования терроризма, легализация преступных доходов и прочие, неудобоваримые для обычного человека вещи, которые описаны, например, в ФЗ №115 «О противодействии...» и в стандартах ФАТФ.

И всё же именно сегодня, *в обществе тотальной мобилизации*, то есть фактического чипирования с помощью смартфона и IoT-устройств, право на анонимность для всё большего круга лиц становится приоритетным. Достаточно вспомнить Д. Ассанжа и Э. Сноудена, чтобы понять, о чём речь.

Поэтому блокчейн-философия[1] стоит на строгом соблюдении данной свободы. Но как быть с недостатками, описанными выше? Для этого и нужна система глобальной

репутации, которая не будет основана на нынешнем, потребительском подходе, когда она — результат неких действий по оценке субъекта. Нет, **репутация — побочный продукт деятельности**, который должен рассчитываться из трёх составляющих:

— субъективной оценки другими (лайки, баллы и прочее): не более ⅓;

— времени существования в определённом статусе (стаж в профессии, период создания произведения и прочее): не более ⅓;

— количественные показатели деятельности (выпущенная книга, выкованные ворота и прочее): не более ⅓.

Системы создаются фактически оторвано от этой схемы: да, есть временные решения, как, скажем, внутренний рейтинг на LocalBitcoins или Linkedin (обе при этом заблокированы в России: то есть рейтинг уже нельзя назвать глобальным), но всё это цифры локальных сервисов, которые при желании можно заработать, специально создавая положительные транзакции внутри систем. Особенно это хорошо видно по социальным сетям, где миллионы подписчиков и лайков уже давно ничего не значат. И именно поэтому на оценку всегда выдаётся не более одной трети: даже подделав конкретную составляющую — будет виден явный перекос с двумя другими и наоборот.

Кроме того, не хватает унифицированного стандарта оценки, то есть элементарной единицы репутации. И именно за этим — будущее.

И не стоит забывать, что будущее наступившее — за счёт автоматизации доверия частный сектор уже смог оптимизировать бизнес-процессы: «С начала 2017 года

---

[1] https://www.litres.ru/vladimir-popov-7629101/blokcheyn-filosofiya-chast-i/chitat-onlayn/

Сбербанк и „М-Видео“ используют блокчейн-технологии в факторинговых операциях: если раньше обмен информацией в рамках каждой сделки осуществлялся через письма и телефонные звонки и занимал до трёх дней, то теперь этот срок сократился до нескольких часов».

Недаром именно здесь видим ускорение процессов интеграции: R3, EEA, Hyperledger, Crypto Valley и другие, что позволяет оптимизировать процесс создания стандартов и принципов эволюции блокчейн-технологии, а главное — связать её с практикой.

ОТКРЫТОСТЬ

Нынешняя система взаимодействия «государство — общество» построена на весьма странных и архаичных началах, когда деятельность политической власти максимально закрыта (за счёт специальных силовых структур, использования ноу-хау в защите данных и другими способами), а социум постоянно и во всё больших объёмах открывает информацию о себе. Точнее — данные, которые в разрезе управления становятся полезными и перетекают в статус значимой информации.

Именно поэтому крупные проекты сегодня сосредоточены на big data и машинном обучении, которые вместе позволяют выявлять даже самые неочевидные потребности общества и порой — конкретных, значимых индивидов.

Для того чтобы через блокчейн открыть деятельность публичной власти — уже сегодня есть масса возможностей:

— необратимое голосование с помощью p2p-систем, подделать которые сложнее, нежели проприетарные и подчинённые единому центру системы;

— государственные реестры: частично они реализованы силами BitFury в Грузии и Украине;

— нотариальные сделки без нотариуса: нечто подобное разрабатывает система Emercoin, и такая возможность

заложена в смарт-контракты «по дефолту», как говорят программисты.

Можно выделить и другие направления, но суть будет схожей. Важнее понять, что для реализации подобных схем от блокчейна требуется модернизация как минимум по следующим направлениям:

— надёжность (верифицируемость): здесь есть разные подходы, пока наиболее интересным выглядит Nem с разработанной системой доверия к нодам, когда скомпрометированные узлы не участвуют в оценке транзакций, а также Cosmos и The Power;

— скорость: именно поэтому сегодня развивается lightning network, рождается огромное количество форков bitcoin-сети (от LiteCoin до Bitcoin Cash & Gold) а также решения, которые уходят от самого блокчейна как технологии (tangle, byteball, hashgraph и подобные)[129];

— майнинг: обычно этот аспект[130] включают в скорость (отсюда — зарождение других консенсусов, не PoW, среди которых пока победоносно чувствует себя DPoS), но хотелось бы остановиться на нём отдельно и подробно.

Дело в том, что майнинг сегодня имеет ряд очевидных проблем.

1. Майнинг не несёт в себе зачастую никакой осмысленной пользы, кроме поддержания работы какой-либо сети, подтверждения транзакций этой же сети. Из-за этого тысячи и тысячи машин фактически нарушают то, за что человечество борется последние десятилетия: нормализацию экологии. Так называемый зелёный майнинг — неполноценное (пока) решение. Поэтому будущее здесь видится в следующих направлениях:

— социальный майнинг — то есть создание криптоактивов за счёт действий субъекта или сообществ

(bitrad.io[1] — прослушивание радиопотока, SportCoin — заработок на ходьбе и прочее);

— мобильный майнинг — использование безграничных ресурсов мобильных сетей и устройств и оптимизация справедливого распределения вычислительных мощностей за счёт этого: то же создание ЛГС;

— полезный майнинг: data-майнинг (поиск новой и полезной информации в текстах); научный майнинг (сейчас к этому близок foldingcoin[2]); суперкомпьютеры по требованию (Sonm, Golem, да и сам Ethereum, но прошедший модернизацию).

2. Майнинг в большинстве случаев приводит к централизации: ярчайший пример — Bitcoin, который по факту контролируется «китайскими» майнерами (впрочем, здесь больше важен фактор географической привязки, а не гражданства). И в этом смысле все иные системы консенсуса — PoS, DPoS, LPoS и так далее — не решают главной проблемы. Видится, что именно за счёт социализации и мобилизации она может быть устранена, но для этого каждый должен разобраться как минимум в трёх важных феноменах:

— теории частных денег: их (прототипов) уже сегодня свыше 2500 по данным coinmarketcap, а будет — в сотни и тысячи раз больше;

— принципах децентрализации: неплохо механизм управления в этой системе координат описан у Ф. Лалу в «Открывая организации будущего»;

— блокчейн-философии[3], которая фактически ведёт к глобальной смене существующей парадигмы потребле-

---

[1] https://bitrad.io/?ref=10533

[2] https://foldingcoin.net/

[3] https://www.litres.ru/vladimir-popov-7629101/blokcheyn-filosofiya-chast-i/chitat-onlayn/

ния и в первую очередь учит делиться и доверять, а не забирать и защищаться.

3. Наконец, две описанные проблемы рождают самую главную: сам по себе майнинг обеспечивает защиту блокчейн-сетей, и поэтому неправильная интерпретация его важности и значимости приведёт (и уже приводит) к созданию банковской системы 2.0, которая будет осуществляться через держание нод той или иной блокчейн-сетки: стоимость может достигать сотен тысяч долларов (можно посмотреть на примеры Waves, Dash, Nem в разные периоды). И именно в этом — основное противоречие в развитии технологии и философии блокчейна.

Главное же, о чём стоит задуматься, — что оторванность технологии от социальных принципов ещё никогда не приводила к положительным эффектам: те же проблемы экологии порождены в первую очередь безалаберным отношением к производству и всем его этапам — от проектирования до ликвидации. Чтобы понять, о чём речь, достаточно посмотреть на экологическую ситуацию неправильно спроектированных производств, скажем, в Красноярске или на Урале, в Бангладеш или Китае — недаром экологические квоты становятся валютой международных отношений[131].

Те же тенденции можно выявить и в области атомной энергетики (Чернобыль и Фукусима), космических полётов (загрязнение орбиты), сельского хозяйства (генная инженерия и использование химикатов в первую очередь) — в любой сфере человеческой деятельности.

Блокчейн должен и может сделать любую деятельность прозрачной с одной стороны, а с другой — обсчитываемой: каждый исследователь способен оценить влияние того или иного фактора на окружающую среду, которая становится всё более агрессивной под давлением антропологических механизмов изменения.

Пока эту возможность мало кто осознаёт, и все фактически сосредотачиваются на более «земных» сферах: финансы и банковское дело, страхование, создание экосистемы сервисов. В фавориты выходят системы с явной централизованной схемой: Ripple и им подобные.

Но такой перекос означает, что ни о каком развитии блокчейн-философии говорить не приходится, и мы не только останемся на уровне развития потребителей, но и гипертрофируем эти взгляды до такой степени, что уже через 5—10 лет на планете фактически не останется замкнутых экосистем, таких, как есть сейчас в Исландии и на плато Путорана, на озере Байкал и даже в Антарктиде.

АВТОМАТИЗАЦИЯ ДОВЕРИЯ

Выше рассказал о данном аспекте в рамках открытости, но хотелось бы добавить ещё ряд значимых моментов.

Во-первых, государства, не имеющие нужного иммунитета к силовому влиянию США и других стран (России, Китая, Индии в первую очередь), уже сегодня осознали важность криптовалют и блокчейн-технологий: недаром Япония, Швейцария, Эстония стоят в первых рядах. Автоматизация доверия не только позволяет создавать нечто внутри страны, но и напрямую влияет на модификации внутри международного сообщества: золотовалютные запасы, повсеместно распространённый, но не обеспеченный чем-либо доллар, безумный государственный долг уходят на второй план и оставляют место для манёвра.

Во-вторых, сам институт государства начинает перестроение в специальный набор сервисов, которые могут использоваться по требованию: воевать внутри p2p-сообществ не с кем, уничтожать p2p-системы бессмысленно, запрещать p2p-валюты невозможно. Именно поэтому описанный механизм автоматизации реестров, юридических служб и прочего — начало: дальше сами государства смогут оптимизировать бюрократический аппарат и использовать его как ad hoc решения по запросу.

В-третьих, автоматизация доверия приведёт к неминуемой гибели массы профессий: нечто подобное человечество уже получило после промышленной революции, когда не просто зародилась, а фактически вышла на ведущие позиции сфера услуг и интеллектуальных разработок (сегодня ведущие компании мира — Google, IBM, Microsoft, Facebook[1][132], Alibaba — услуги того или иного порядка, и, конечно же, верхний пьедестал занят финансами и банками). Юристы — не аналитики, бухгалтеры и финансисты, водители и копирайтеры, дизайнеры средней руки и даже повара могут уйти в небытие[133] после оттачивания связки «блокчейн + искусственный интеллект + смарт-контракты + big data + роботизация».

И что же останется человеку?

Творчество и труд: труд в тех условиях, где машины немощны. В первую очередь — космос, так как там много неочевидных и новых явлений. Во вторую — совершенствование внутреннего мира. В третью — работа над собой в широком смысле.

Но для начала необходимо понять, что автоматизация доверия сама по себе не даст нам ничего, даже в потенциале. Приведу несколько примеров.

— Блокчейн должен был убить посредников, но вместо этого развитие технологии без философского переосмысления привело к их росту: биржи, обменники, оракулы, технические платформы и так далее.

— Биткоин породил автоматизацию доверия транзакций, но разве это лишило мошенников возможностей проводить необеспеченные ICO, собирать с помощью банального фишинга миллионы и обманывать доверчи-

[1] https://vc.ru/social/53459-facebook-rasskazala-ob-uyazvimosti-kotoraya-mogla-otkryt-dostup-k-lichnym-fotografiyam-6-8-mln-polzovateley

вых граждан через тривиальные и даже примитивные схемы?

— Наконец, даже крупные игроки, в первую очередь The DAO & Ethereum, EOS, MtGox, NiceHash, до сих пор злоупотребляют доверием в той или иной форме.

Поэтому для автоматизации доверия необходимо выработать изначальные условия такового и обучить каждого следовать им: иначе рискуем никогда не выйти из порочного круга необеспеченных обещаний и систем учёта рисков, а не возможностей.

РАСПРЕДЕЛЁННОСТЬ

Кажется, уже обо всё сказал в предыдущих разделах, единственное, что отмечу отдельно — необходимость обучения каждого, чтобы распределённость или децентрализация давала синергетический эффект.

Как показал опыт развития Bitcoin в течение десяти лет и мой собственный опыт с 2011 года, рынок не может создать себя самостоятельно, если каждый из его участников не будет обладать необходимым знанием принципов самоорганизации.

Именно поэтому первая волна ICO была направлена на построение структуры блокчейн-решений, а уже вторая — больше на реальный сектор экономики и оцифровку его в новом формате — токенизацию.

Достичь описанного механизма в действии можно следующими способами:

— обучение (курсы, тренинги, вузовские программы и прочее);

— просвещение (книги, статьи, видео);

— самообучение каждого: узнал сам — расскажи другому.

Именно это приводит к замкнутой системе, где каждый элемент является одновременно и объектом познания, и субъектом восприятия, то есть своеобразной нодой уни-

фицированного мирового блокчейна. Нечто подобное очень правильно и точно описывал В. Вернадский через ноосферу[1].

[1] https://en.wikipedia.org/wiki/Noosphere

КВАНТОВЫЙ БЛОКЧЕЙН И ИНЫЕ ТЕНДЕНЦИИ БЛИЖАЙШИХ ЛЕТ

Пожалуй, завершу описанием самых интересных перспектив развития технологии блокчейн и их соотношением с философскими началами. Первое, о чём много говорят, это создание квантового компьютера и возможный «взлом» криптовалют. На деле же есть ряд аспектов, которые мало учитываются.

— Явление декогеренции[1] уже достаточное количество лет (с 1980-х) не даёт возможности просто так взять и создать даже стокубитный квантовый компьютер. Последнее время было немало заявлений от разных групп исследователей, что они вышли на уровень нескольких десятков кубитов, но какой-то проверяемой открытой информации до сих пор нет.

— Не стоит забывать, что квантовый компьютер разрабатывают сейчас в основном или государства (США, Япония, Россия и другие), или же крупные корпорации: и они навряд ли те, кто заинтересован в первую очередь в ка-

[1] https://en.wikipedia.org/wiki/Quantum_decoherence

ких-либо взломах, особенно с учётом того, что те же IBM ратуют за развитие блокчейн-решений. Кроме того, есть куда более лакомые системы для возможного доступа: начиная от секретных архивов спецслужб, заканчивая банковскими системами и государственными архивами.

— Не стоит забывать, что есть квантовая криптография, а значит чисто теоретически любой блокчейн может получить квантовый хардфорк и тем самым станет неуязвим к новому компьютерному чуду. К тому же возможности КК явно преувеличивают СМИ: скажем, для взлома даже SHA-256 прямым перебором[134] он не годится.

Но на самом деле у КК есть куда более глобальная проблема: его пробуют создавать по канонам классической физики и технологии, тогда как любая квантовая система (в силу связанности элементарных частиц, принципа неопределённости и так далее) фактически система децентрализованная или даже распределённая. И в этом смысле пока относим такое направление, как изучение сознания через законы квантовой физики, к пограничным научным отраслям, говорить о каких-то значимых прорывах не приходится.

Кроме того, следствием этого тезиса является тот факт, что КК будет близок к уровню работы мозга, и возникает множество этических и даже психологических проблем, которые так ярко и одновременно скупо (потому как не среди человечества, а узких специалистов) обсуждаются в научных кругах относительно ИИ.

Мощь КК, уже существующая градация людей на владеющих криптоактивами и нет, рост разделения на интеллектуальную элиту и всех остальных, а также зависимость всех и каждого от технологической составляющей приведут мировой социум к неизбежным антагонизмам, которые, в свою очередь, породят проблемы планетарного масштаба. Поэтому уже сегодня должны сделать главное: решить их на этапе становления.

И сделать это можно не одним способом: скажем, развитием науки, которая на сегодня является забытой и косной — философии: именно она позволяет воспринимать мир не аналитически, а синтетически, а тем самым развивать эвристические модели, столь важные на момент генезиса явлений, которые ранее не были даже плодом фантазии для подавляющего большинства.

Это и есть Web 3.0, но уже в социальном аспекте!

ПРИЛОЖЕНИЕ №3. ПЕРЕВОД СТАТЬИ Т. О'РЕЙЛИ О WEB 3.0

Если Web 2.0[135] был таким горячим, как насчёт Web 3.0? Это была отличная тема для будущих инженеров, которые хотят позиционировать свой стартап как «следующую значимую вещь». Компания Nova Spivack начала её с описания сетей Web 3.0, но теперь у Джейсона Калаканиса есть его конкурентное определение, аккуратно *подобранное под его собственный mahalo.com*. Результат в виде бури негодования и высмеивания — (в этом смысле) ожидаем.

Теперь больше всех должен колебаться, чтобы сказать: «Web 3.0 — глупая идея», потому что, конечно, та же самая критика была применена к Web 2.0. Но есть (всё же) пара важных отличий.

Web 2.0 начинался как название конференции![136] И это название имело очень специфическую (конкретную) цель: обозначить, что Паутина была фактически забыта[137] после краха доткомов! Web 2.0 был не о технологии, а о возрождении интереса к Сети. Когда пришли к этой идее в 2003 году, многие программисты были безработными, и было общее отсутствие интереса к веб-приложениям. Но увидели, что грядёт возрождение, и спроектировали конференцию, чтобы рассказать о том, что на этот раз будет по-другому.

Затем я потратил некоторое (достаточное) время, пытаясь определить характеристики компаний, переживших банкротство в пузыре доткомов, и лучшие из новых компаний и сайтов, которые видел на подходе. Эта работа и называлась «Что есть Web 2.0?», и она была ретроспективным описанием, основанным на широком анализе спектра успешных компаний, не подогнанным под конкретную компанию или проект, который ещё не успел заявить о себе.

Так что для начала сказал бы, что для того, чтобы Web 3.0 был значимым, нам нужно увидеть серьёзный разрыв[138] с предыдущим поколением технологий. Это может

быть очередная неудача и возрождение, или, что более вероятно, это будет что-то качественно другое[139]. Мне нравятся размышления Стоу Бойда на эту тему: «Лично чувствую смутные очертания чего-то, выходящего за пределы Web 2.0, и они предполагают довольно радикальные шаги. Представьте себе Паутину без браузеров. Представьте себе полный разрыв с метафорой документа или истинное размывание приложения и информации (внутри него). Это то, чем будет Web 3.0, но уверен, что назовём это чем-то другим».

Согласен: определённо есть что-то новое, но уверен, что назовём это чем-то другим, нежели Web 3.0. И становится всё более вероятным, что он будет намного шире и более распространён, чем Сеть (нынешняя), так как мобильные технологии, датчики, распознавание речи и многие другие новые технологии делают вычисления намного более вшитыми в offline, чем это есть сегодня.

Но в любом случае следующие заметки (о W3) будут иметь (куда более) широкую основу, с большим количеством доказательств, каждое из которых будет показывать иной аспект дискретного развития. Любой, кто скажет, что его стартап — признак следующей революции, просто вне (этой) игры.

Меня особенно раздражают определения Web 3.0, которые в основном являются описанием Сети 2.0 (т. е. новых форм применения коллективного интеллекта), которые оправдывают себя как прорыв, только притворяясь, что Сеть 2.0 как-то связана с AJAX, мэш-сетями и другими технологиями на стороне клиента.

Например, можно посмотреть пост Nova Spivack, написанный в качестве ответа[140] на выступление Джейсона: «Web 3.0, на мой взгляд, лучше всего определить как третье десятилетие Сети (2010—2020), в течение которого будут широко использоваться несколько ключевых технологий. Главными из них будут RDF и технологии развива-

ющейся Семантической паутины. Хотя Web 3.0 не является синонимом Семантической паутины (в этот период произойдёт ещё несколько важных технологических сдвигов), она будет в значительной степени характеризоваться семантикой в целом».

Web 3.0 — эра, в которой модернизируем бэкенд веба после десятилетия фокусировки на фронтенде (Web 2.0 в основном был посвящён AJAX, тегам и другим инновациям фронтенда для пользователей).

У меня есть некоторые симпатии к попытке Nova спасти термин Web 3.0, привязав его к временным рамкам, а не к какой-либо конкретной технологии (Windows 95 кто-нибудь помнит?), но считаю, что идея Web 2.0 о «фронтендовых» технологиях настолько нелепа, что дискредитирует всю идею. Google — выдающаяся история успеха Web 2.0, и это всё (же) бэкенд! Каждая крупная игра Web 2.0 — бэкендовая история. Всё дело в создании приложений, которые используют сетевые эффекты, чтобы стать лучше (и оттого всё больше и больше людей используют их): и это возможно сделать только за счёт обогащения бэкенда. Nova прав, что технологии семантического веба могут всё больше внедряться на некоторых сайтах, но не думаю, что это (за) данность.

Как написал в комментарии к блогу Новы: «Увы, нахожу аргументы в пользу Web 3.0 явным доказательством того, что сторонники Web 2.0 вообще не понимают: Web 2.0 — не (только) технологии фронтенда».

Речь идёт не только о бэкенде, но и о смысловой нагрузке на него.

Настоящая разница между Web 2.0 и Семантической паутиной заключается в том, что Семантическая паутина, кажется, думает, что нам нужно добавлять новые виды разметки к данным, чтобы сделать их более значимыми для компьютеров, в то время как Web 2.0 стремится иден-

тифицировать области, где смысл уже закодирован, хотя и скрытыми способами.

Например, Google нашёл значения в структуре ссылок (триплеты RDF); Wesabe находит его в структуре расходов.

Есть сайты (на ум приходит geni.com), которые создают узкоцелевые случаи, когда люди добавляют структурированное значение, и, думаю, что найдём намного больше (подобных применений/практик). Но также думаю, что большая разница заключается в количестве фонового шума, который принимаете в своих значимых данных, когда думаете, что грамматика развивается из данных или навязывается ими. Приложения Web 2.0 являются фундаментально статистическими по своей природе: своего рода коллективным разумом, полученным из множества и множества вводимых данных в глобальном масштабе.

См. мои различные сравнения[141] Web 2.0 и семантической паутины.

Тем временем Web 2.0 был довольно дерьмовым названием того, что происходит (название от Microsoft, «живой софт», вероятно, — лучший термин, который видел), так что не понимаю, зачем распространять (его) и на Web 3.0. Но когда люди спрашивают, что думаю о Web 3.0, то вообще не думаю о Семантической паутине.

Какие вещи дадут качественный скачок за пределами того, что знаем (испытываем) сегодня?

Думаю, что это разрыв парадигмы клавиатура/экран и мир, в котором коллективный разум возникает не от людей, печатающих на клавиатурах, а от инструментов (куда более близких) нашей деятельности.

В этом смысле сказал бы, что Wesabe и Mint, которые превращают нашу кредитную карту в своего рода сенсор, рассказывающий историю через трекинг, оставленный в реальном мире; или Jaiku, превращающий телефон в сенсор для умной адресной книги; или страховка от Norwich Union в формате «платите-как-водите» — (все

они) являются ранними сигналами того, что бы назвал Web 3.0, нежели (это делать через) семантический веб.

Давайте просто использовать (выражение) «Семантическая паутина», а не нечто мутное, пытаясь назвать это же Web 3.0, особенно когда точки значимого различия[142] на самом деле те же точки, которые использовались, чтобы отличить Web 2.0 от Web 1.5. (Всегда говорил, что Web 2.0 = Web 1.0 с боковым ответвлением от. com, которое неверно истолковали).

У Nova был отличный ответ на этот комментарий, который прислали мне по электронной почте и который воспроизвожу здесь с разрешения (автора): «На самом деле я бы сказал, что согласен со многим из того, что указываете в своём комментарии к моему посту. С одной стороны: исключительно — Семантическая паутина полностью перпендикулярна вопросу о коллективном разуме. На самом деле она может быть использована как лучший бэкенд для существующего Web 2.0 или для экспертных систем — и это не просто фреймворк. Было бы неправильно с технической точки зрения говорить, что семантическая сеть — не статистика или не некое выведение структуры из того, что уже есть в данных. Семантический веб — просто способ кодирования всего, что знаете.

Так что можете использовать статистику, или майнинг[143], или мудрость толпы, чтобы разметить данные, но тогда где храните и делитесь тем, чтобы об этих данных узнали? Семантический веб предлагает более богатую основу для хранения и публикации этих метаданных. Он полностью независим от того, как генерируются метаданные. Просто лучший способ совместного использования этих метаданных.

Использование строковых тегов и микроформатов, или XML-тегов для этого материала — разные способы разметки данных. RDF и OWL являются разными способами разметки данных, но они являются ЛУЧШИМИ способами.

У них гораздо больше мощности, они более открытые, они более расширяемые, они лучше поддерживают коллективный разум «снизу-вверх».

Вот почему предлагаю, что если ДОЛЖНЫ использовать такие нелепые термины, как Web 1.0, Web 2.0, Web 3.0, то давайте не будем привязывать их к определённой технологии. Давайте просто привяжем их к десятилетиям, когда многие технологии происходят вместе.

Давайте посмотрим правде в глаза, что мир не такой нарезанный и высушенный, как хотели бы (некоторые) люди. RDF началась в Web 1.0, между прочим!

Тем не менее думаю, что со временем структура Сети значительно изменилась. RDF позволяет перенести Web с файлового сервера на что-то более похожее на базу данных. Это позволяет получить сеть данных. Он делает для данных то, что гипертекст делает для текста: и называю это гиперданными. Это, конечно, что-то новое и очень полезное, но это будет зависеть от того, что люди в конечном итоге будут с этим делать.

В Radar используем подход Web 2.0 к Web 3.0: применяем пользовательский контент и мудрость толпы, а также статистический анализ, *майнинг* и машинное обучение. В этой совокупности имеем нечто гораздо более мощное, чем когда эти элементы применяются сами по себе: настоящую платформу для коллективного разума. Тот факт, что храним данные, используя семантический веб, является удобством: это делает наши данные более расширяемыми и пригодными для повторного использования. Но в конечном счёте сами данные поступают от пользователей».

Некоторые из приведённых тезисов имеют для меня смысл: он, безусловно, прав, что семантический веб может оказаться весьма полезным для многих классов умных приложений. Но «лучшим доказательством хорошего пудинга является его поглощение», как говорила моя мама.

ПРИЛОЖЕНИЕ №4. ПЕРЕВОДЫ ТЕКСТОВ ПРО WEB 3.0 Н. СПИВАК

РЕЗЮМЕ О WEB 3.0: RADAR NETWORKS, POWERSET, METAWEB И ДРУГИЕ...

Прежде[144] всего, перед тем, как начнём, нужно кое-что прояснить. Семантическая паутина — часть того, что некоторые называют Web 3.0, но, на мой взгляд, это всего одна из нескольких сходящихся технологий и тенденций, которые определят эту грядущую эру Паутины. Я написал здесь о предлагаемом определении Web 3.0 более подробно.

Для тех из вас, кому не нравятся такие термины, как Web 2.0 и Web 3.0, хочу сказать, что согласен и что все хотим избежать быстрой серии подобных лейблов или гонки компаний, претендующих на x.0. Поэтому у меня есть практическое предложение: давайте используем эти термины для индексации десятилетий, прошедших с тех пор, как появилась Паутина. Это объективно: можем договориться о том, когда декады начинаются и заканчиваются, и если посмотрим на историю, то каждое десятилетие характеризуется различными тенденциями.

Думаю, что это разумное предложение, и оно на самом деле крайне полезно, так как позволяет избежать бесконечных анонсирований нового x.0 каждый год.

Таким образом, Web 1.0 был первым десятилетием Сети: 1990—2000. Web 2.0 — второе десятилетие, 2000—2010 гг. Web 3.0 — грядущее третье десятилетие, 2010—2020 и так далее. Каждое из этих десятилетий характеризуется (или будет характеризоваться) определёнными технологическими движениями, темами и тенденциями, и эти индексы — 1.0, 2.0 и т. д. — являются не более чем удобным способом отсылки на них. Это полезный способ обсуждения истории, и он не лишён прецедента. Например, различным династиям и историческим периодам также даются названия, что обеспечивает краткое обращение к этим периодам и их уникальным вкусам. Чтобы увидеть мою хронологию этих десятилетий, нажмите здесь[1].

СЕМАНТИЧЕСКОЕ СОЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

...Здесь, в компании Radar Networks, строим онлайн-сервис нового поколения на базе веб-технологий, который принесёт семантическую паутину потребителям и профессионалам во всей Сети. Это приложение сфокусировано на включении следующего поколения социального программного обеспечения (обратите внимание, что социальное программное обеспечение не обязательно является социальным нетворкингом — это подмножество социального программного обеспечения). Это пример того, что

[1] https://web.archive.org/web/20120221011853/http://www.kurzweilai.net/the-third-generation-web-is-coming

«Интеллектуальная паутина» может состояться. Очень взволнованы (рождением) этого сервиса и тем, что он уже делает, но ещё многое предстоит сделать, прежде чем выпустим релиз.

Наше приложение основано на Семантической паутине. Оно будет обогащать и облегчать более интеллектуальные онлайн-отношения, сообщество, контент, сотрудничество и даже коммерцию. Оно поможет перенести Semantic Web из исследований в реальность, сделав его удобным, доступным и, прежде всего, непосредственно полезным и ценным для обычных людей. Мы сосредоточены на обеспечении ценности для потребителей, а не только для разработчиков или ранних последователей…

НАША ПЛАТФОРМА ПРИЛОЖЕНИЙ WEB 3.0

Для того чтобы построить наш продукт, пришлось сначала построить новую платформу, которая поддерживала бы те функции и возможности, которые разрабатывали: не смогли найти ни одной существующей платформы, которая могла бы делать то, что хотели бы делать мы. Существующие платформы для Semantic Web были слишком ориентированы на исследования и не обеспечивали требуемого уровня масштабируемости, производительности и простоты использования.

Работали над этой платформой в течение нескольких лет и нескольких поколений нашей кодовой базы. Сейчас она очень надёжна и сложна. Считаем, что она более мас-

штабируемая и производительная, чем любая другая платформа, которую видели в семантическом веб-пространстве на сегодняшний день.

Наша платформа является всеобъемлющим, основанным на Java фреймворком для семантических веб-приложений и сервисов, который имеет некоторое сходство с Ruby on Rails (хотя он также сильно отличается от RoR, и не собираемся идти по пути рынка платформ — мы действительно больше сосредоточены на нашем приложении сейчас). Наша платформа также включает в себя множество других технологий, таких как чрезвычайно быстрый и масштабируемый уровень хранения семантических данных, мощные возможности семантических запросов, а также ряд алгоритмов для анализа данных и выполнения интеллектуальных вещей для пользователей.

Платформу можно назвать прикладной платформой Web 3.0, поскольку она по своей сути основана на RDF/OWL и развивающемся семантическом вебе. В дополнение к Web 3.0 аспектам того, что делаем, наша платформа также активно использует методы и технологии Web 2.0, такие как AJAX, REST, виджеты и RSS/ATOM, и это лишь некоторые из них.

ЧТО НЕ ДЕЛАЕМ? ПОИСК НА ЕСТЕСТВЕННОМ ЯЗЫКЕ

Прежде всего, в Radar Networks НЕ строим новую поисковую систему, чтобы конкурировать с Google, как это делают Powerset и TextDigger, — так что не конкурируем

с ними… Поиск на естественном языке не эквивалентен поиску в Semantic Web, хотя Semantic Web, безусловно, может помочь в этом процессе.

Компании, работающие специально над поиском на естественном языке, используют семантику, но только на уровне слова. Они используют сети слов, которые связаны с синонимами, антонимами, омонимами и другими вариациями. Их иногда называют семантическими сетями. Основываясь на этих сетях значений слов, могут понимать значение различных слов и выражений.

Более сложные алгоритмы поиска в естественном языке не просто смотрят на слова в одиночку, они смотрят на них в контексте, анализируя грамматику и остальное содержимое вокруг них. Смысл поиска на естественном языке в конечном счёте состоит в том, чтобы попытаться сопоставить значение слов в поисковых запросах с содержанием различных документов — и сделать это лучше, чем Google, который в основном просто сопоставляет ключевые слова, не обращая внимания на значение слов.

Поиск на естественном языке требует как минимум некоторого уровня искусственного интеллекта. Машинное понимание естественного языка является сложной проблемой, и за последние несколько десятилетий над этим было проделано немало работы. Сегодня существует много технологий, которые фокусируются на этом, но большинство из них основаны на предположении, что программное обеспечение должно делать всю работу, чтобы понять значение информации.

ЧТО ДЕЛАЕМ? СЕМАНТИЧЕСКАЯ ПАУТИНА

В отличие от естественного языкового поиска, который фокусируется на попытке вывести значение слов, подход возникающей Семантической паутины использует метаданные для кодирования значения информации.

При таком подходе значение информации может быть явно закодировано в информацию точно так же, как HTML-коды добавляются в контент сегодня, — и это могут делать люди или программное обеспечение, даже сообщества. Как только это значение, или семантика, будет явно закодировано в содержимое, оно может быть повторно использовано другими приложениями, чтобы наполнить содержимое смыслом. Стоит отметить, что явная семантика в содержании может помочь приложениям, обрабатывающим естественный язык, а также приложениям, которые не понимают естественный язык.

В подходе Semantic Web смысл информации кодируется с использованием языков разметки, таких как RDF и OWL, которые являются открытыми стандартами W3C. Слова и понятия в содержании документов и записей данных могут быть помечены выражениями RDF/OWL для обозначения того, что они означают — означает ли определённое слово или выражение, например, «Lotus», компанию, производящую программное обеспечение, программный продукт, экзотическую марку спорткара или какую-либо другую концепцию? Без сложной обработки естественного языка программному обеспечению часто трудно определить это самостоятельно. Semantic Web предоставляет коды разметки, которые прямо указывают на предполагаемое значение информации в однозначном, машиночитаемом формате.

Разметка контента дополнительными метаданными была возможна ещё до того, как Semantic Web использовала XML: можно было просто сказать <sportscar> Lotus </sportscar>, но проблема в том, что значение слова «sportcar» всё равно приходилось кодировать в приложения, чтобы они знали, что оно подразумевает. С помощью RDF/OWL это значение может быть формально закодировано вне приложений в наборе определений, называемых онтологией. Онтология определяет такие факты, как «спортивная машина — вид автомобиля», «автомобиль — наземное транспортное средство», «автомобиль — продукт», «автомобиль — устройство», «спортивная машина — рекреационное или соревновательное транспортное средство» и др.

СЕМАНТИЧЕСКАЯ РАЗМЕТКА

Пометив содержимое OWL, указывающее на то, что это спортивная машина, можно отнести это значение к соответствующим определениям в онтологии, из которых любое приложение, которое может прочитать онтологию, может затем сделать вывод об этих различных специфических значениях. Смысл здесь в том, что семантика менее двусмысленна — явно закодирована онтологией, которая функционирует как своего рода более продвинутая схема данных.

Но это упрощение — OWL и онтологии на самом деле могут пойти гораздо дальше, чем просто определение смысла понятий: они также могут определить и логические отношения. Например, как именно две вещи связаны меж-

ду собой и есть ли какие-то особые ограничения на эту связь? Например, онтология может определить, что сестра человека должна быть женщиной или что у человека может быть только одна биологическая мать и т. д.

Дополнительные подсказки о значении информации, которая может быть предоставлена метаданными Semantic Web вокруг контента, могут быть полезны для всех типов приложений. Например, даже поисковая система на естественном языке могла бы делать меньше анализов и нуждалась бы в меньшем «интеллекте», если бы могла использовать существующие семантические метаданные, которые уже содержатся[145] в контенте.

Важно отметить, что приложениям и людям не обязательно когда-либо смотреть на RDF или OWL код (и слава богу!) — они могут просто работать с объектами и формами, как уже работают в вебе, и лежащая в их основе разметка может быть создана автоматически. Никто не должен смотреть на сырой RDF и OWL (если только он действительно этого не хочет), и Semantic Web никого не заставляет делать это. Например, большинство из нас не пишет HTML, XML или CSS вручную — но если используем блоги или Вики или даже размещаем объявления на таких сайтах, как вакансии и аукционы, делаем вещи, которые приводят к созданию HTML, XML и CSS.

Из вышеприведённого раздела должно стать ясно, что естественный поиск по языку — специфический процесс, использующий семантику на уровне слов, но Semantic Web — широкий набор технологий для определения значения любого вида информации (включая слова, но не ограничиваясь ими). Semantic Web может помочь улучшить процесс поиска на естественном языке, но сегодня многие алгоритмы поиска на естественном языке не используют структуры данных Semantic Web или RDF/OWL. Однако по мере того как эти технологии начинают сближаться (как это происходит в компании Radar Networks),

увидим, что становятся возможными новые уровни точности — сочетание традиционной обработки естественного языка и богатой семантики разметки RDF/OWL позволяет улучшить машинное обучение (и понимание) и обработку текста. Тем не менее ещё раз хочу уточнить, что Radar Networks не поисковая компания — хотя и используем семантический поиск нового поколения достаточно широко в наших приложениях и платформах.

Любое приложение, которое может понять RDF/OWL, может корректно интерпретировать значение любого контента, помеченного метаданными RDF/OWL. Если новостная статья, в которой много раз упоминается слово «Париж», помечена метаданными RDF/OWL, то любое приложение, которое может понять эти метаданные, может, например, правильно определить, что статья о населённом пункте Париж штата Техас, а не о столице Франции — г. Париж и уж точно не о девушке по имени Пэрис Хилтон. Для этого приложению не нужно делать какую-либо обработку на естественном языке. Даже относительно «глупый» запрос, не имеющий возможности делать обработку на естественном языке, всё равно может иметь некий смысл в (полученном) документе, если использует RDF/OWL.

Так как же эта явная семантическая разметка в виде метаданных RDF/OWL попадает в документ в первую очередь? Это может быть добавлено автоматически каким-нибудь другим приложением, которое обрабатывало его на естественном языке, или это могло быть результатом того, что редакторы газет и/или даже читатели классифицировали и/или помечали документ тегами для мест, людей и т. д., то есть способом, не отличающимся от того, как помечают содержимое в таких сервисах, как Flickr[1] сегодня.

[1] https://www.flickr.com/

Главное здесь в том, что добавление семантических метаданных не требует от приложений, которые создают или потребляют контент, понимания естественного языка и не требует от людей быть XML-кодировщиками — даже обычные конечные пользователи могут помочь определить семантику контента, просто пометив его тегами. В этом смысле семантический веб предоставляет гораздо более богатый и выразительный набор возможностей для этого, чем доступные в настоящее время в Web 2.0 теги.

Semantic Web может улучшить понимание и обработку текста на уровне слова во многих отношениях, но обратите внимание, что он не ограничивается только приложениями на уровне слова. Semantic Web обеспечивает способ сделать любую информацию более понятной для других приложений, включая записи данных в базах, документы на рабочем столе и в Интернете, данные предприятий, фотографии, видео, музыку и даже веб-сервисы и программный код.

ПРОСТЫЕ ПРИМЕРЫ СЕМАНТИКИ

Например, сегодня существует большая проблема интеграции[146] данных между приложениями. Например, на предприятии одно приложение может определить запись, которая называется «Клиент», в то время как другое может называть это понятие термином «Клиент». Если пользователь ищет «Клиентов», он не обязательно найдёт записи *для* Клиентов. Но с помощью Semantic Web записи данных для Клиентов и Клиентов могут быть сопоставлены так, чтобы приложения могли рассматривать их как эк-

вивалентные. Любой поиск одного из них вернёт и другое. Не только записи могут быть сопоставлены друг с другом, но и поля этих записей могут быть сопоставлены вместе. Например, запись клиента может иметь поле под названием «Отложено», в то время как запись клиента может иметь поле под названием «Введено» — они могут быть отображены вместе.

Аналогичный пример может быть применён к потребительскому использованию — например, покупки: разные магазины описывают один и тот же товар по-разному — с разными терминами. В одном магазине ноутбук называется «ноутбук», а в другом — «портативный компьютер», в то время как ещё в одном — «замена настольного компьютера». Поиск любого из этих терминов должен вернуть товар, использующий любой из них. В рамках одного коммерческого сайта это не так сложно, но как насчёт поиска по многим коммерческим сайтам (что сегодня совсем не так просто сделать...)? Если бы разные коммерческие сайты использовали одни и те же определения семантических метаданных для разметки различных продуктов, то пользователи могли бы искать по продуктам с меньшим количеством проб и ошибок и получали бы лучшие результаты.

Конечно, технология разметки между базами данных не нова — есть много способов сделать это, но Semantic Web предоставляет способ, который может быть более открытым и эффективным в долгосрочной перспективе. Центральным в этом подходе является то, что организация или онлайн-сервис может использовать онтологии, которые централизованно определяют ключевые понятия строгим образом. Таким образом, вместо того, чтобы каждое отдельное приложение индивидуально сопоставлялось с другими, потенциально все приложения могут просто сопоставляться с центральной онтологией, которая функционирует как своего рода семантический коммутатор[147]. Все

приложения и запросы могут использовать общую онтологию (или их набор[148]) для унификации доступа к записям данных в различных онлайн-сервисах и базах данных. Онтологии обеспечивают способ определения и совместного использования общих языков для данных, контента, отношений и приложений.

SPARQL И НОВАЯ ВЕБ-СТРАНИЦА ДАННЫХ

Совсем недавно начала появляться новая технология Semantic Web под названием SPARQL[1]. SPARQL предоставляет общий язык запросов, такой как SQL, для запроса данных, которые хранятся в RDF. Любой сайт или база данных, содержащая данные RDF и предоставляющая интерфейс SPARQL, может быть найдена любым приложением, «говорящим» на SPARQL. Это означает, что мечта о «глубоком веб-поиске» наконец-то становится реальностью. В настоящее время существует огромный интерес к SPARQL, и уже сейчас в Интернете появляется всё больше и больше конечных точек, использующих SPARQL. Эти конечные точки для данных то же, что веб-сайты для документов. Это начало того, что некоторые называют Data Web — первый шаг к полномасштабной Семантической паутине. SPARQL также является большой частью того, что делаем мы.

[1] https://ru.wikipedia.org/wiki/SPARQL

ОБОСНОВАНИЕ: СЛЕДУЮЩИЙ РУБЕЖ ПОСЛЕ ПОИСКА

Ещё одним ключевым преимуществом использования RDF/OWL является то, что эти языки предназначены для поддержки формальных логических рассуждений. При разметке информации с помощью RDF/OWL вокруг неё может осуществляться сложный поиск, а затем и установление связей. Например, разметив различных людей и их социальные связи, можно сделать вывод, что Сью — двоюродная сестра Джейн, что Боб и Дейв — коллеги, что продукт A несовместим с продуктом B и т. д.

Такой тип логического рассуждения и умозаключений необходим для того, чтобы сделать возможным следующее поколение сети — Интеллектуальную сеть, в которой программное обеспечение и онлайн-сервисы начинают помогать людям работать, общаться и делать покупки более продуктивно. Например, это позволит сделать нечто, выходящее за рамки поиска: например, это поможет службам, которые предоставляют ответы или предложения. Это не обязательно важно для всех приложений сегодня, но в будущем это будет становиться всё более важным. Содержание, которое существует в RDF/OWL, по сути, имеет более длительный срок хранения, и (потому) в будущем его будет легче использовать повторно, интегрировать и обосновывать.

ДИФФЕРЕНЦИРУЯ ИГРОКОВ

Семантическая паутина обеспечивает всеобъемлющие и растущие рамки технологий, которые делают возможной следующую эволюцию Сети — таким образом, это гораздо более широкое и далеко идущее видение, чем естественный языковой поиск, хотя это, безусловно, (лишь) одна из областей, которая принесёт пользу. Поиск на естественном языке на самом деле сводится к сопоставлению поисковых запросов с документами путём анализа значения слов. Семантическая паутина — определение значения любых данных: слов, записей, документов, социальных отношений, списков продуктов и т. д., равно как и предоставление способа запроса таких данных, их интеграции и сопоставления согласно критерию разумности.

В нашем собственном приложении и платформе используем много обработки на естественном языке (NLP[1]), а также предоставляем возможности семантического поиска, но наше внимание сосредоточено на чём-то совершенно ином, чем поиск в Web, и потому одинаково полезном и важном для всех. Честно говоря, рад, что не работаем над поиском, как бы велика ни была возможность: думаю, что соперничество непосредственно с Google — сложная задача, и не хотел бы участвовать (в ней)! Вместо этого предоставляем новую среду, в которой люди могут начать пользоваться преимуществами Семантической паутины в областях, в которых Google весьма слаба сегодня или вообще не работает в некоторых случаях: довольно перпендикулярно работе Google и других поисковых систем.

---

[1] https://en.wikipedia.org/wiki/Natural_language_processing

Поэтому из вышеприведённого разговора должно быть ясно, что работаем над Semantic Web, а не просто над естественным языковым поиском, и поэтому сильно отличаемся от таких компаний, как Powerset, Textdigger и других, которые работают над словесным семантическим пониманием текста. Но как насчёт Metaweb — чем отличаемся от них?..

Radar Networks и Metaweb часто упоминаются как два основных стартапа, работающих над созданием семантически управляемых онлайн-сервисов Web 3.0. Думаю, что будет некоторое сходство, но различий всё же гораздо больше. Возможно, когда-нибудь даже появятся возможности для совместной нашей работы. Но всё ещё находимся в закрытом режиме, так что сегодня трудно получить конкретную информацию о наших сходствах и различиях. Одно можно сказать наверняка, 2007 год будет захватывающим как для наших компаний, как и для нового поколения компаний и продуктов в стиле Web 3.0.

WEB 3.0 ТОЛЬКО НАЧИНАЕТСЯ

В любом случае следующая эволюция Сети — то, что называем *Интеллектуальной сетью (и то, что многие также называют Web 3.0)* находится на очень ранних стадиях, и не думаю, что она действительно достигнет большого успеха до 2010 года (ссылка на шкалу[1] смены W1-W2-W3-W4)...

[1] https://novaspivack.typepad.com/nova_spivacks_weblog/2007/02/steps_towards_a.html

К счастью, Web 3.0 — большое пространство с большим количеством возможностей, и в нём есть место для сосуществования и конкуренции множества различных игроков и бизнес-моделей. Тот факт, что в настоящее время есть несколько предприятий в этом пространстве, является хорошей вещью для всех, ибо, как сказал мне один человек на днях, «восходящий прилив поднимает все лодки»... А ведь всего год назад казалось, что мы — единственный коммерческий голос дикой природы академических исследований. Сегодня венчурные фонды выстраиваются в очередь, чтобы поговорить с нами и другими компаниями...

РЕШЕНИЕ ПРОБЛЕМЫ ПЕРЕГРУЗКИ ИНФОРМАЦИЕЙ

Ключевым моментом, который стоит за всем этим интересом к семантике, является то, что поиск по ключевым словам и традиционные представления контента и данных *снижают производительность*. По мере того как Сеть становится всё шире и сложнее, а потребители должны работать с растущим количеством контента и услуг, производительность подвергается серьёзной угрозе — не только в поисковых системах, но и во всех других сферах цифровой жизни. Большинство интенсивно работающих со знаниями и информацией (проектов) уже имеют непосредственный и интуитивно понятный опыт того, как росла информационная перегрузка в последнее десятилетие. Очевидно, что с этим нужно что-то делать,

или через несколько лет все будем погребены в собственной информации.

Semantic Web обеспечивает лучшее (и действительно единственное (?)) долгосрочное решение проблемы информационной перегрузки и сложности, добавляя к данным более богатую семантику и позволив приложениям начать использовать то, что позволит помочь людям вернуть большую производительность и сделать программное обеспечение более умным — *без необходимости пытаться создавать супер-пупер научно-фантастический искусственный интеллект*[149].

Важно помнить, что Semantic Web не требует, чтобы машины понимали или рассуждали так же хорошо, как люди, — семантика может быть создана людьми и/или машинами и не должна быть идеальной, просто должна добавлять подсказки, которые делают контент менее двусмысленным и более структурированным. Напротив, как подход Google к ключевым словам, так и естественный языковой поиск таких компаний, как Powerset, если только они хотят идти в ногу с растущей сложностью веба, потребует всё более интеллектуального программного обеспечения, потому что в основном в таких системах ПО должно выполнять всю работу само по себе.

Semantic Web на самом деле в большей степени использует коллективный интеллект людей и приложений для обогащения контента — вместо того, чтобы пытаться заставить приложения выполнять всю работу самостоятельно: это будет намного яснее позже, когда появится несколько приложений в стиле Semantic Web…

Конечно, потребовалось некоторое время, чтобы реализовать Semantic Web, но если подумать, то на Web 1.0 потребовалось около пяти лет, чтобы действительно приступить к работе… Новое поколение Сети — большое дело. Пока что всем нам, работающим над чем-либо, что связано с семантикой или Web 3.0, нужно работать вместе,

чтобы начать создавать карту местности и просвещать рынок, чтобы люди (включая прессу и ранних последователей) могли более чётко понимать компании и технологии. Ирония заключается в том, что значение термина «семантика» до сих пор неоднозначно!

WEB 3.0 — СЛЕДУЮЩИЙ ШАГ ДЛЯ WEB?

Статья[150] о Семантической паутине только что вышла в онлайн. Это огромная статья. Во многом это одна из самых популярных статей, написанных о Semantic Web в прессе. В ней много подробностей о том, над чем работает Radar Networks.

Один момент для прояснения, если кому-то будет интересно…

Web 3.0 не только о машинах, но и о людях: он использует социальные сети, фолксономии[1], сообщества и социальную фильтрацию КАК СЕМАНТИЧЕСКАЯ СЕТЬ, а также применяет интеллектуальный поиск данных и искусственный интеллект. Комбинация этих технологий более мощная, чем любая другая сама по себе. Web 3.0 — Web 2.0 +1. Это НЕ Сеть 2.0 — люди. Сеть +1 — добавление ПО и метаданных, которые помогают людям и приложениям (правильно) организовывать и тем лучше понимать Сеть. Это новый уровень семантики…

Так что… мы сосредоточили большую часть наших усилий на том, чтобы «помочь людям помочь себе», чтобы

[1] https://en.wikipedia.org/wiki/Folksonomy

они могли помочь друг другу найти смыслы в Паутине. Используем удивительный интеллект человечества и дополняем его, используя Семантическую паутину, майнинг и AI. И верим, что следующее поколение коллективного интеллекта — *создание систем экспертов, а не экспертных систем*.

GARTNER ОШИБАЕТСЯ НАСЧЁТ WEB 3.0

Очень уважаю людей в Gartner, но их недавний отчёт[1], в котором поддерживается термин Web 2.0, но утверждается, что термин Web 3.0 является «лишь маркетинговой уловкой», — явное заблуждение.

На самом деле всё наоборот.

Термин Web 2.0 на самом деле является маркетинговой уловкой. Со временем у него появилось нечто, похожее на определение. Поскольку на самом деле он настолько плохо определён, (что) предлагал в прошлом, чтобы просто использовали его для обозначения десятилетия — второго десятилетия Web (2000—2010). В конце концов, нет никакой реальной технологии, которая называлась бы Web 2.0: в лучшем случае есть целый ряд вещей, которые этот термин, кажется, объединяет (не называя), и многие из них являются шаблонами дизайна, а не технологиями. Например, теги — не технология, а скорее — шаблон дизайна. Метка — ключевое слово, строка текста, и за ней на самом деле нет никакой новой технологии. AJAX также не являет-

[1] https://web.archive.org/web/20071012025026/https://www.networkworld.com/news/2007/092107-gartner-web-20.html

ся технологией сам по себе, а скорее сочетанием технологий и шаблонов дизайна, большинство из которых существовало до появления того, что называется Web 2.0.

Напротив, термин Web 3.0 относится к набору новых технологий и изменениям, которые они привнесут в течение третьего десятилетия существования веба (2010—2020 гг.). Главной среди них является Семантическая паутина. На самом деле Semantic Web — не одна технология, а множество. Некоторые из них, такие как RDF и OWL, находятся в стадии разработки в течение многих лет, в том числе — и в эпоху Web 2.0, а другие, такие как SPARQL и GRDDL[1], являются недавно появившимися стандартами. Но это только начало. По мере развития Semantic Web в головоломку будет добавляться несколько новых технологических частей для обсуждения, разработки и обмена открытыми определениями и правилами, а также (будут) предлагаться решения проблем, связанных с доверием, агентами, машинным обучением, разработкой и интеграцией онтологии, семантическим хранением данных, поиском и многими другими вещами.

По сути, Семантическая паутина позволяет постепенно преобразовывать Паутину в базу данных. Это глубокое структурное изменение, которое в конечном итоге затронет каждый слой веб-технологии. Оно преобразует технологию баз данных, CMS, CRM, корпоративного промежуточного ПО, систем интеграции, инструментов разработки, поисковых систем, группового ПО, цепочек поставок и других систем, которые и охватывает отчёт Gartner.

Семантический веб будет проявляться несколькими способами. Во многих случаях будет улучшать приложения и сервисы, которые уже используем. Так, например, *увидим семантические социальные сети, семантический поиск,*

[1] https://ru.wikipedia.org/wiki/GRDDL

семантические средства групповой работы, семантические CMS, семантические CRM, семантическую почту и многие другие семантические версии приложений, которые используем сегодня. Для конкретного примера возьмём социальные сети. Существует много разговоров об «открытом социальном графе», чтобы социальные сети были более включёнными в жизнь. В конечном счёте, чтобы сделать это правильно, социальный граф должен быть представлен с использованием стандартов Semantic Web, чтобы действительно быть не только открытым, но и легко расширяемым и интегрируемым с другими данными.

Однако Web 3.0 не является ТОЛЬКО Семантической паутиной. Большую роль могут играть и иные развивающиеся технологии. Gartner, кажется, считает, что виртуальная реальность будет одной из них. Возможно, но если быть честным, VR является феноменом Web 1.0: существует уже долгое время и не сильно изменилась за последние десятилетия. Люди в MIT (Media Lab) работали в начале 1990-х над вещами, которые далеко впереди Second Life[1] сегодня.

Так какие же другие технологии можно интегрировать в Web 3.0, которые на самом деле являются новыми? Ожидаю, что у нас будет большой рост «облачных вычислений», таких как *открытые одноранговые сетевые хранилища*[151] и вычислительные возможности в Web — дающие любому приложению по существу столько же памяти и вычислительной мощности, сколько нужно, бесплатно или очень дёшево.

На мобильной арене увидим более высокую пропускную способность, больше памяти и более мощные процессоры в мобильных устройствах, а также мощные встроенные системы распознавания речи, GPS и датчики

[1] https://ru.wikipedia.org/wiki/Second_Life

движения, позволяющие использовать их в новых[152] целях.

Думаю, что увидим увеличение мощности инструментов персонализации и персональных помощников, которые пытаются помочь пользователям управлять сложностью их цифровой жизни.

На арене поиска узрим, как поисковые системы станут умнее: среди прочего — начнут не только отвечать на вопросы, но и принимать такие команды, как «найди дешёвый рейс в Нью-Йорк», и будут учиться и совершенствоваться по мере того, как будут использоваться.

Будем наблюдать и большие улучшения в интеграции и переносимости данных и учётных записей между различными веб-приложениями. Увидим фундаментальное изменение в мире баз данных по мере того, как базы данных будут отходить от реляционной и объектной моделей в сторону ассоциативной модели данных (графических баз данных и «тройных хранилищ»).

Одним словом, Web 3.0 — новые технологии с жёстким ядром, которые окажут гораздо большее влияние на IT-менеджеров предприятий и IT-системы, чем Web 2.0. Но по иронии судьбы к такому выводу компания Gartner может прийти только после выхода Web 4.0 (2020—2030)!

ПРИЛОЖЕНИЕ №5. ВИДЕО ПРО W3

Как бы там ни было, обитаем в эпоху верховенства видео: и, прежде чем закончить книгу, как минимум для успокоения, а как максимум — для расширения понимания, следовало обратиться к этому типу контента, дабы посмотреть, а как же на день сегодняшний (декабрь 2019 — январь 2020) выглядит YT-позиция относительно Web 3.0. И вот что получилось…

ВСЕ МЫ ЖИВЁМ В КОРОБКЕ

Если точнее — в ящике: ещё точнее — внутри компьютера, который давно мимикрировал под телефон. И когда исследование началось, первое, на что наткнулся, было соглашение о кукисах: «We use cookies to provide the best experience. By continuing to use our website, you agree to our cookies policy» — на одном из сайтов. И ведь это — ровно то, против чего W3 выступает в очередь за номером ноль!

Одним из первых[1] попалось обращение на канале As Informer, которое при 320 000 подписчиков посмотрело с декабря 2018 года чуть менее 4000 человек или около 12%. Пожалуй, «популярным» является выступление на TedX[2], собравшее 25 666 просмотра на момент проверки (с 2012 года), и это при 22 600 000+ подписчиках на канале: тоже — не лучший результат?

Но самое удивительное, что действительно популярное по теме было опубликовано ещё в 2008 году[3]: свыше

[1] https://youtu.be/8tCC_UWZw_o

[2] https://youtu.be/u2w9XKASbPw

[3] https://youtu.be/bsNcjya56v8

329 000 просмотров. При этом подписчиков на самом канале — 259. Не тысяч, а именно 259 человек. Дальше ждал не менее удивительный результат: канал с 1000+ подписчиками и почти 380 000 просмотров[1]. Но все эти окольцованные кадры были, по сути, одной и той же калькой об эволюции от W1 к W3: как, например, и данный ролик[2] (единственное отличие — анимационный). В этом смысле рассказ А. Болдачева[3] выделяется двумя параметрами: он более детализированный и рассматривает не только технический, но и философский аспект W3.

Ещё несколько ссылок из этой же категории: пример[4] №1, пример[5] №2 и пример[6] №3. В последнем наблюдается явное уравнивание блокчейн-технологии и W3, что, безусловно, в корне неверно, потому как blockchain — часть бэкенда W3. Пожалуй, лучшим на момент редактуры страниц сих, по крайней мере в русскоязычной среде, по данной теме является выступление у Forklog[7] С. Садова.

Есть видео, которые акцентируются больше не на эволюции W1-W2-W3, а на основных категориях и терминах: пример[8] №1, пример[9] №2 (впрочем, в нём также немало о трудностях W2), пример[10] №3.

Существуют и ролики, описывающие конкретные реализации, скажем, от Waves[11], или раскрывающие позиции

---

[1] https://youtu.be/off08As3siM

[2] https://youtu.be/fWj4NNdJHE0

[3] https://youtu.be/6qXSUp_-las

[4] https://youtu.be/83K42ZBgOnU

[5] https://youtu.be/F_nbUizGeEY

[6] https://youtu.be/Y2mGzvvtiKo

[7] https://youtu.be/NR6lEZYK0uA

[8] https://youtu.be/wT34xGXbZ-E

[9] https://youtu.be/aPVmd7SyKfQ

[10] https://youtu.be/rVrpCi3jWzs

экспертов из различных (смежных) отраслей — как в интервью/обсуждении на TechCrunch[12]. Ещё одним — в формате исследования, но на сей раз от Microsoft, можно считать данный материал[13].

Самой продолжительной (более пяти часов контента) стоит признать данную запись[14], которая, впрочем, раскрывает разные аспекты современных технологий в принципе, нежели акцентируется именно на Web 3.0.

Конечно же, YouTube не был бы собой, если бы не хранил ролики с явным юмористическим подтекстом: как, скажем, здесь[15].

И всё же интересны практические имплементации различных составных частей W3: IoT + blockchain (ссылка[16]), коих пока — крайне мало.

***

Итог поразителен: на все миллионы роликов, миллиарды просмотров и минут видео — **очень и очень скудная подборка именно по W3**. Её скорее нет! Нет совсем… И это ещё раз подтверждает, что здесь и сейчас всё только зарождается, а значит — самое время для настоящих безумцев: предпринимателей, воодушевлённых разработ-

[11] https://youtu.be/TChEJlU93hw

[12] https://youtu.be/VJPiGgh-hjI

[13] https://youtu.be/Q7tyi1kp33w

[14] https://youtu.be/fgfQiuCOuFw

[15] https://habr.com/ru/post/47778/

[16] https://youtu.be/SMq-s9CZ8LY

чиков и первых последователей, которые не раз доказывали, что самое невероятное и невозможное — наступает и цунами накрывает всех, всё и сразу.

Удачи в этом!

ПРИЛОЖЕНИЕ №6. ПОЧЕМУ ДОВЕРИЯ APPLE, FACEBOOK, MICROSOFT И ДРУГИМ ГИГАНТАМ БОЛЬШЕ НЕТ?

Ответов множество, как и доказательств, их подтверждающих, но в этой небольшой подборке приведу несколько.

Например, совсем недавно Apple[1] «извинилась за прослушку запросов пользователей», и было это в 2019 году, а в 2020-м выяснилось, что корпорация сканирует фотографии[2], дабы найти в них «детское порно». То есть теперь корпорация №1 по капитализации в мире превратилась в полицию, какую-то секретную службу и законодательный орган с судом сразу?

В том же 2019 году выяснилось, что более 419 000 000[3] учётных записей пользователей Facebook «утекли в сеть», а приложение Instagram, которое, как известно, принадлежит «мордокниге», и вовсе хранило миллионы паролей[4]… в незашифрованном[153] виде!

Если вдруг думаете, что подобное происходит только «в последнее время», то вам небольшая подборка за десять[154] лет:

— 2009 — массовый взлом[5] сайтов и email[6].

— 2010 — помните об icq[7]? но ломали не только «аську», но и сайты[8], и почту, и другие аккаунты в сетях.

---

[1] https://www.forbes.ru/tehnologii/382619-apple-izvinilas-za-proslushku-zaprosov-polzovateley-v-siri

[2] https://secretmag.ru/news/apple-priznalas-v-skanirovanii-fotografii-polzovatelei-iphone-tak-ishut-detskoe-porno.htm?utm_source=email&utm_medium=weekly

[3] https://tjournal.ru/news/114821-baza-dannyh-s-419-millionami-nomerov-polzovateley-feysbuka-popala-v-set

[4] https://www.gazeta.ru/tech/2019/04/19/12310651/millions_instagramers.shtml

[5] https://www.securitylab.ru/news/386711.php

[6] http://mediaprofi.org/media-info/news/item/6846-vzlom

[7] https://habr.com/ru/post/101870/

[8] https://exploit.in/2010/3993/

— 2011 — а как насчёт взлома десятков миллионов[1] учётных записей[155] от Sony?

— 2012 — взлом миллионов[2] учётных записей Linkedin.

— 2013 — взлом фактически всех аккаунтов Yahoo стал, пожалуй, наиболее известным в этот год, а это свыше 3 000 000 000[3] человек.

— 2014 — взлом более 360 000 000[4] записей[156] из Adobe.

— 2015 — массовый взлом Slack, Ulmart, Twitter и других.

— 2016 — взлом более 272 000 000[5] учётных[157] записей в различных сервисах.

— 2017 — база в 320 000 000[6] пользователей в почти-свободном-доступе.

— 2018 — данные 365 дней запомнились взломом «ВКонтакте[7]»[158], а также различных CMS-систем: Drupal[8], ModX[9] и других[10].

— 2019 — и снова: взлом Instagram[11][159], массовый взлом[12] «ВКонтакте» и других соцсетей и сервисов.

---

[1] https://xakep.ru/2011/05/11/55649/

[2] https://life.ru/p/410019

[3] https://threatpost.ru/yahoo_vzlom_2013_goda_zatronul_vse_akkaunty/22615/

[4] http://holdsecurity.com/news/cybervor-breach/

[5] https://govoritmoskva.ru/news/77705/

[6] https://habr.com/ru/post/357402/

[7] https://habr.com/ru/company/owasp/blog/440352/

[8] https://revisium.com/ru/blog/drupageddon2.html

[9] https://perfkirill.ru/stati/modx/massovyij-vzlom-sajtov-na-modx

[10] https://xakep.ru/2018/09/24/mass-wp-hjack/

[11] https://iz.ru/899754/2019-07-16/indiiskii-khaker-nashel-sposob-vzlomat-akkaunt-v-instagram-za-desiat-minut

[12] https://vk.com/team?w=wall-22822305_608052

Не если, но когда захочется погрузиться в историю больших взломов, обязательно прочтите подборку[1]: с её помощью поймёте, что с 1980-х годов нам дурят голову, сообщая о безопасности, приватности и прочих вещах, которых на самом деле не существует (если только сами не берётесь за дело).

Чтобы вдруг никому не показалось, что защищаю интересы псевдоучастников крипторынка, а именно централизованных решений (будь то кошелёк, биржа, форум или что-то ещё), — приведу в пример вот эту подборку[2], которая справедливо доказывает, что только полное осознание защитной функции p2p-систем есть решение, а не прикрытие приставкой «крипто[3]», где это уместно и нет.

Одним словом, когда Twitter[4][160], Google[5], LinkedIn[6], Amazon[7], Microsoft[8][161] и другие, в том числе — и здесь не упомянутые, утверждают, что «вы в безопасности», — ложь, и ложь откровенная, наглая и ничем не обоснованная. Особенно страшно становится, когда речь заходит о таких сферах, как ядерная безопасность[9], авиаперелёты и прочие, где от верности работы устройств и программ зависят сотни, тысячи, а то и миллионы жизней сразу.

---

[1] https://republic.ru/posts/l/1139636

[2] https://bits.media/milliony-uchetnykh-zapisey-s-forumov-o-bitkoine-za-6-let-prodayutsya-v-darknete/

[3] https://www.vedomosti.ru/technology/articles/2018/02/16/751202-hakeri-kriptobirzhi

[4] https://habr.com/ru/company/pt/blog/303004/

[5] https://rg.ru/2016/05/04/rossijskij-haker-vzlomal-272-milliona-uchetnyh-zapisej-v-internete.html

[6] https://life.ru/p/410019

[7] https://xakep.ru/2017/04/12/amazon-password-reuse/

[8] https://riafan.ru/1131764-obnaruzhen-sposob-vzlomat-uchetnye-zapisi-microsoft

[9] https://www.fontanka.ru/2017/05/12/139/

И Stuxnet — просто ещё одно подтверждение этому. А как насчёт Flame и прочих?

И главное во всём этом, что нам постоянно врут: Adobe заявил об утечке всего лишь (!) 3 000 000[1] пользователей, а их оказалось *38 000 000*; Facebook хранил обет молчания после того, как узнал (?!) о хранении паролей в открытом виде, а признав своё преступление, чем именно он поплатился? Yahoo более трёх лет умудрялась скрывать самый крупный взлом, затронувший 3 000 000 000[2] человек! Или «ВКонтакте», который был взломан не раз и даже при миллионах жалоб — всё равно утверждал обратное.

Проще говоря государства, государственные корпорации, мировые IT-гиганты и банки[3] кормят постоянными байками о том, как всё слаженно и прекрасно работает, забирают за это персональные данные, комиссии и в любой момент могут вовсе лишить аккаунтов/счетов (по тем же предписаниям ФАТФ), а в итоге — НИЧЕГО НЕ ДЕЛАЮТ! Совсем. Если предыдущие цифры в этом не убедили, тогда — ещё одна: 2 700 000 000[4] учётных записей в открытом доступе или 1 000 000 000[5] подборок «почта — пароль». При этом от ⅓ до ⅔ пользователей соцсетей ежегодно[6] сталкиваются со взломами (см. также исследование[7] ESET). Еженедельно похищается

---

[1] https://3dnews.ru/773518

[2] https://meduza.io/news/2017/10/04/yahoo-soobschila-o-vzlome-treh-milliardov-akkauntov

[3] https://www.rbc.ru/business/03/10/2014/542ddd63cbb20f7901598532

[4] https://habr.com/ru/post/436420/

[5] https://tjournal.ru/internet/85004-hakery-opublikovali-1-mlrd-unikalnyh-kombinaciy-pocht-i-paroley-eto-krupneyshaya-publichnaya-baza-akkauntov

[6] https://3dnews.ru/922785

[7] https://www.esetnod32.ru/company/press/center/eset-2-3-akkauntov-v-sotssetyakh-podverglis-vzlomu/

не менее 250 000[1] паролей и логинов! И это не считая незаконной замены sim-карт, которая происходит благодаря безалаберности сотовых операторов и банков; социальной инженерии, которая работает с 1980-х годов не останавливаясь; уязвимостей нулевого уровня, существующих в закрытых системах и многих других, которые невозможно обнаружить в проприетарном коде в принципе и по определению.

Да, открытые системы тоже взламывают[2], но, во-первых, не так часто; во-вторых, проводится работа над ошибками, и в эпоху 64-битных систем и многомиллионного сообщества Linux подобных промахов становится ещё меньше.

О чём говорят эти цифры и при чём здесь снова W3?

На мой взгляд, всё очевидно: либо учимся защищать свои данные самостоятельно, как это происходит с нашим домом, где всегда есть не только окна и двери, защищающие от потери тепла, но и они же — предохраняющие нас от нежданных гостей, либо продолжаем быть пешками в чьей-то не очень честной игре, то есть потребителями, которым всё равно, что именно с ними происходит, будет происходить и как это всё повлияет на жизнь и быт в целом.

Мне не всё равно, а вам?

---

[1] https://security.googleblog.com/2017/11/new-research-understanding-root-cause.html

[2] http://www.opennet.ru/opennews/art.shtml?num=36155

ПОЛЕЗНЫЕ ССЫЛКИ

ИСТОРИЯ WEB 3.0

Интересное интро от Waves о том, как зарождался W3 и почему именно сегодня он стал актуальным — https://forklog.com/sp/web3-0/theory/

О том, как зарождался Web & Blockchain — через аналогии, весьма умело представленные проектом Bitnovosti — https://bitnovosti.com/2019/07/02/blockchain-and-internet-revolution-1/

И вторая часть этой же работы — https://bitnovosti.com/2019/07/12/blockchain-and-internet-revolution-2/

О том, почему Web 3.0 рождался дважды (и как именно), от исследователя А. Болдачева — https://habr.com/ru/post/468557/

Другая статья этого же автора, где кратко обозначен общий путь развития Web 3.0 — https://vc.ru/future/81683-web-3-0-ili-zhizn-bez-saytov

ТЕРМИНЫ И ДЕФИНИЦИИ

Официальное определение W3, которое, впрочем, устарело сразу после обнародования — https://calacanis.com/2007/10/03/web-3-0-the-official-definition/

Несколько исследований по тематике W3 от Web3.Foundation — https://web3.foundation/research/ (не все доступны, к сожалению, вне архивной версии)

Токенизация с технической стороны вопроса: в исследовании от Binance — https://research.binance.com/analysis/tokenization

Несколько материалов от Menaskop:

— О философии[1] Web 3.0

— Web 3.0 в конкретике[2] реализации (видео)

— Про Dapps[3] в социальном аспекте

— Смарт-контракты и уровни свободы

— https://en.bitcoin.it/wiki/Sidechain — одна из самых распространённых категорий последних лет.

---

[1] https://coinmedia.ru/vladimir-popov-web-3-0-dapps-i-principy-decentralizacii-anonimnosti-otkrytosti-i-tranzakcionnoj-reputacii/

[2] https://cont.ws/@menaskop/1503636

[3] https://zen.yandex.ru/media/id/5c7d297bd4b4f400b219deae/vladimir-popov-web-30-dapps-i-principy-decentralizacii-anonimnosti-otkrytosti-i-tranzakcionnoi-reputacii-5c81546c23e78700b2e15561

ПРОЕКТЫ

— https://ark.io — один из самых полномасштабных проектов

— https://brave.com — не W3-браузер[162], но важная переходная форма

— http://btcrelay.org — Bitcoin- и Ethereum-сети вместе

— https://cosmos.network — интересная реализация мультиблокчейна

— https://cyb.ai — первый W3-браузер

— https://github.com/ethereum/eth2.0-specs — Ethereum 2.0

— https://filecoin.io — распределённое хранилище

— https://interledger.org — открытый протокол платёжных интеграций

— https://www.iota.org — интернет вещей и DAG-реализация

— https://ipfs.io — та самая межгалактическая файловая система

— https://nearprotocol.com — блокчейн для разработчиков

— https://www.overledger.com — синтетическая сеть блокчейнов

— https://polkadot.network — конкурент и лучший соратник Cosmos

— https://www.skycoin.com — монета, экосистема и сервисы в стиле W3

— https://docs.tokenbridge.net — взаимодействие токенов

— https://viz.world — DAO и система поощрений

— https://urbit.org — персональный сервер где и в чём угодно

— https://www.wanchain.org — открытая финансовая сеть

Если хочется ещё больше узнать о браузерах, то есть интересный материал на сайте Forklog[1]: «На страже Web 3.0: главные блокчейн-браузеры интернета нового поколения».

Для самых же вдумчивых — путеводитель[2] за 2019 год.

[1] https://forklog.com/na-strazhe-web-3-0-glavnye-blokchejn-brauzery-interneta-novogo-pokoleniya/

[2] https://itsynergis.ru/assets/docs/blockchain_cryptocurrency_guidebook_2019.pdf

СИСТЕМА ГЛОБАЛЬНОЙ РЕПУТАЦИИ

Описание и схематичное представление на английском языке: https://docs.google.com/document/d/1SPsqSgwCrKydsLIFvSxOmF63QP5UtPWRhVxqDpT9sPA/edit?usp=sharing

Манифест шифропанков — http://www.cypherpunks.ru/Manifesto-cypherpunk.html

Манифест криптоанархистов — http://www.anarhvrn.ru/anarh/xaoc/crypto.html

Нужно больше? Всегда найдёте в нашем файле-каталоге[1], который постоянно обновляется.

[1] https://docs.google.com/spreadsheets/d/1Af_cSHNZ9JJnzOTeJaO7M5Hu5AEKOvaZhse3StyGeoo/edit?usp=sharing

ПРИМЕЧАНИЯ

[1] Полноценная о Web 3.0 на русском языке (прим. В.П.).

[2] На мой взгляд — в этом он сильно ошибался (прим. В.П.).

[3] То есть ориентированной на массовое потребление (прим. В.П.).

[4] Который опубликован по известному адресу — https://novaspivack.typepad.com/nova_spivacks_weblog/2007/10/web-30----the-a.html.

[5] Интересно, что в ответе Д. О'Рейли и в Интернете часто приводится другой период — с 2010 по 2020 годы (прим. В.П.), потому как именно и сам автор перешёл на округление до этого периода: 1990—2000, 2000—2010, 2010—2020 и т. д.

[6] Так оно и вышло: Белая книга Биткоина написана в 2008 году, а первая транзакция совершена именно в 2009-м, как и намайнен[1] первый блок.

[7] В оригинале использовано понятие co-opted (кооптация[2]), которое дословно можно перевести как смыка-

---

[1] https://www.blockchain.com/btc/address/1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

[2] https://en.wikipedia.org/wiki/Co-option

ние или же введение в состав чего-либо без дополнительного согласования, но остановился, как и везде далее, на передаче смысла, а не побуквенном переводе (прим. В.П.).

[8] Помимо прочего Анатолий является одним из создателей VIZ[1].

[9] Здесь и далее предпочитаем использовать слово Интернет, написанное с заглавной буквы, если речь идёт о всей сети в целом, поскольку часто будем говорить об альтернативах сегодняшним, пусть и наиболее глобальным, решениям (прим. В. П.).

[10] А ещё точнее — Интернет 2.0, потому как альтернативных сетей должно быть как можно больше (прим. В. П.).

[11] Но стоит помнить, что тех, кто обанкротился на пузыре доткомов[2], — значительно больше! (Прим. В. П.).

[12] Всё же для меня (В. П.) DLT и blockchain — равнопорядковые, но разные явления.

[13] Не стоит преувеличивать их значение: отчёт-исследование ico с 2013 по 2018 гг.[3] показал, что уровень скама в данной сфере не достигал и 20%, что значительно ниже, чем в отрасли банковского кредитования и в венчурном инвестировании.

[14] Можно, например, найти примеры в путеводителях Synergis за 2018 — https://itsynergis.ru/assets/docs/meta_analysis_menaskop_synergis_2018.pdf и 2019 — https://itsynergis.ru/assets/docs/blockchain_cryptocurrency_guidebook_2019.pdf годы.

[15] См. список литературы с манифестами шифропанков и криптоанархистов (В. П.).

---

[1] https://viz.world/@on1x/

[2] https://en.wikipedia.org/wiki/Dot-com_bubble

[3] https://itsynergis.ru/assets/docs/ico-report-first-half-2018.pdf

[16] Одно из решений — https://unstoppabledomains.com. Аналоги есть у Aeternity, Ethreum, Zilliqa, Namecoin, Emercoin и других.

[17] Речь именно о HE-W3-браузерах (В. П.).

[18] Именно в эту сторону движется https://cyb.ai.

[19] Хотя есть сторонники другой гипотезы, условно называемой «останется только один», что, на мой взгляд (В. П.), противоречит самой логике децентрализации.

[20] Под замкнутыми здесь имеются в виду полные и независимые экономические модели.

[21] Ещё точнее — эры Постинтернета, поскольку Сеть уже не будет единой (прим. В. П.).

[22] Я — да (В. П.).

[23] Это стало особенно актуально после IEO BTT[1] (прим. В. П.).

[24] О противоположной позиции читайте в одной следующих глав (прим. В. П.).

[25] Меж тем уже существует и развивается CYB, Beaker и другие проекты, как и дополнения к существующим (прим. В. П.).

[26] Об альтернативной — о чём и шла речь выше (прим. В. П.).

[27] Одно из первых решений в этой области — https://ru.wikipedia.org/wiki/Namecoin (В. П.).

[28] Подробней о стандартах — см. приложение №1.

[29] И не только в EOS (прим. В. П.).

[30] См. подробности https://habr.com/ru/news/t/446398/.

[31] И/или изменить саму систему создания таких сертификатов (прим. В. П.).

[32] НДС — не единственная проблема в РФ

[1] https://www.bittorrent.com/btt/

и во многих других государствах: есть нечестная таможенная политика, из-за которой покупки в зарубежных онлайн-магазинах год от года не становятся дешевле; существует ряд законов, постепенно делающих дороже конечную стоимость товаров и услуг (закон Яровой в первую очередь) и т. д. (прим. В. П.). И хочется верить, что ДРС не станут панацеей, но помогут вернуть конкуренцию.

[33] Исторически возвращаемся в эпоху XVII — XIX вв., когда имущественный ценз был, но совершенно по иным основаниям (прим. В. П.).

[34] Напомню, поэтому в глоссарии указан SaO — субъект и объект, как единая сущность, выступающая в ДРС (см. подробней ниже — В. П.).

[35] Каждый из этих вопросов раскрывается по-своему в главах ниже (В. П.).

[36] Скорее всего — их будет на каком-то этапе и многим больше (прим. В. П.).

[37] Или любой её аналог (В. П.).

[38] Читайте подробней в главах ниже.

[39] Впрочем, не стоит забывать и о проблемах Libra (В. П.).

[40] Подробнее почитать о нём можно в статьях threatpost.ru[1], hype.ru[2], habr.ru[3] и ещё habr.ru[4].

[41] На мой взгляд — только новых пользователей (В. П.).

[42] Но и не плацебо (В. П.).

[43] Со временем — общеупотребимым (прим. В. П.).

---

[1] https://threatpost.ru/webauthn-becomes-a-w3c-standart/31468/

[2] https://hype.ru/@id184/chto-takoe-webauthn-i-kak-rabotaet-protokol-j9q0bz4z

[3] https://habr.com/ru/company/1cloud/blog/445534/

[4] https://habr.com/ru/company/globalsign/blog/358622/

[44] См. также выше (В. П.).

[45] Оставил именно такой перевод как отсылку к началам экономической теории (В. П.).

[46] См. также https://ru.wikipedia.org/wiki/Пропускная_способность[1] (В. П.).

[47] О важности транзакционной репутации — читайте ниже (прим. В. П.).

[48] На самом деле сегодня живём во многом в эпоху высокотехнологичного Средневековья (В. П.).

[49] Впрочем, искренне надеемся, что данная книга исправит и сей аспект (прим. В. П.).

[50] В уже указанной ссылке https://ru.bmstu.wiki/RDF_(Resource_Description_Framework) есть дополнительные источники для изучения. Или можно обратиться к стандартной Wiki — https://ru.wikipedia.org/wiki/Resource_Description_Framework.

[51] Впрочем, ещё можно упомянуть и язык запросов поиска связанных данных — SPARQL.

[52] Один из примеров — https://habr.com/ru/post/157527/. Почему это так важно? Читайте здесь[2].

[53] Если интересно — всегда можете изучить в материале А. Болдачёва «Web 3.0, или Жизнь без сайтов» по адресу https://vc.ru/future/81683-web-3-0-ili-zhizn-bez-saytov.

[54] Данный материал был опубликован В. П. изначально в рамках статьи.

[55] То есть не от рабства к феодализму, капитализму и от него далее к коммунизму, а в эпоху цифрового рабовладельческого строя, где условно-свободным может быть лишь аватар виртуального мира, а вероятно — и он будет

---

[1] https://ru.wikipedia.org/wiki/

[2] https://vc.ru/story/47938-eto-problema-vsey-otrasli-razbor-rassledovaniya-bloomberg-o-kitayskih-shpionskih-chipah

под игом, как это показано в известном сериале[1] «Чёрное зеркало».

[56] На самом деле для меня близка парадигма, что разработчик-будущего (условно в «Тени завтрашнего солнца» называю его «модельер») создаёт некие бизнес- или же модели быта, а уже искусственный интеллект пишет собственно смарт-контракт (В. П.).

[57] Приведу верное замечание А. Пискунова: «Сайт в текущей ситуации **всегда** централизован: кто владеет доменом — может указать сервер, который будет выдаваться посетителям; кто владеет сервером — может указать скрипты/файлы для взаимодействия с пользователями; кто владеет скриптами/файлами (имеет к ним доступ) — может менять содержимое и выполнять js-код у посетителей на компьютере; пользование сайтом — акт доверия: во-первых, владельцу домена; во-вторых, владельцу сервера; в-третьих, владельцу файлов. Не бывает децентрализованных сайтов „пока“. Бывают сайты, где открыт код, который можно изучить, где можно посмотреть потоки данных и решить для себя: заслуживают ли они доверия? Сайты/скрипты могут отдать часть ресурсов/данных на управление пользователям — и всё! Дать доступ к файлам/скриптам — не могут, так как нельзя доверять их содержимому, а если дать „управлять“ файлами — то это дыра (как загрузка вредоносных скриптов и взлом изнутри уже)». Всё это так, скажу я (В. П.), но выше идёт речь именно о модели, когда условный сайт становится таким же открытым вместилищем, как и любая ДРС. Методология создания таких «сайтов» представляет собой совокупность практик совместных репозиториев (на Github или других ресурсах), построения p2p-сетей формата TOR или торрентов, а равно и консенсусные решения внутри ДРС.

---

[1] https://en.wikipedia.org/wiki/List_of_Black_Mirror_episodes

[58] Опять же — адресую к комментарию А. Пискунова: «Единая авторизация предполагает и единый ключ шифрования данных для взаимодействия с другими участниками». Не понял (этот момент): что, если Гугл решит авторизовать другого пользователя от твоего имени? Это акт доверия: исключить «доверие» можно лишь при использовании распределённых систем для получения публичного ключа, чтобы провести проверку действия, когда юзеры будут подписывать своим ключом все действия — только тогда можно убедиться, что перед тобой нужный юзер: юзер должен понимать — что ОН владелец «авторизации». Потерял ключ = потерял личину на сайте, поэтому не понимаю «единая авторизация предполагает и единый ключ шифрования данных» для взаимодействия с другими участника. Возможно, это объяснено не под тем углом: (как) говорил, единая авторизация возможна в том случае, если есть провайдер публичных личин (пространства имён) и ты можешь проверить там публичный ключ (ключ подписи). Тогда любой сайт сможет обратиться к доверительному сервису с доступом к данным из того или иного блокчейна, а может, у него своя нода для доступа к эфиру. Получить проверку — что перед ним тот аккаунт, который «доказал», что это он, с помощью криптографии. Мне не нравится предложение «единая авторизация предполагает и единый ключ шифрования данных для взаимодействия с другими участниками». Оно (несколько) путает: ключ шифрования — всё-таки другая вещь, не ключ для криптографической валидации подписи. Есть криптографические методы для нахождения shared key между двумя ключами, когда каждый участник может с помощью публичного ключа собеседника и своего приватного ключа получить shared key, который уже можно использовать для шифрования сообщений. Этот shared key получается одинаковый у обоих собеседников: никто другой не может получить его, для этого нужно знать один из приватных клю-

чей двух собеседников. Опять же, всё верно (с моей точки зрения — В. П.), но смысл фразы сводится к тому, что сегодня — эпоха мультиблокчейнов, а за ней необходимым образом следует эпоха мультихранилищ ключей авторизации/шифрования/валидации, но пока, конечно же, это лишь гипотеза.

[59] Впервые данная подглава была описана в виде отдельной статьи и опубликована в онлайн-журнале coinmedia[1].

[60] Есть, скажем, мастер-ключ, ключ для постинга и т. д.

[61] Читай подробней в приложении №1, но здесь напомню про Великую огненную стену в Китае aka государственный Firewall и автономный Рунет (В. П.).

[62] В этом смысле — полезно следить не только за новостями, но и конкретными личностями: например — https://en.wikipedia.org/wiki/Juan_Benet_(computer_scientist).

[63] Кстати, подумайте и о технологии IPv6[2] именно с этой позиции.

[64] Например, доводить до совершенства код, и так написанный в 10—12 строк.

[65] Подробней см. https://ru.wikipedia.org/wiki/История_языков_программирования[3].

[66] Впрочем, терминологически здесь всё неоднозначно — https://ru.wikipedia.org/wiki/Сетевая_операционная_система[4].

---

[1] https://coinmedia.ru/vladimir-popov-web-3-0-dapps-i-principy-decentralizacii-anonimnosti-otkrytosti-i-tranzakcionnoj-reputacii/

[2] https://vasexperts.ru/blog/bezopasnost/ipv6-texnologiya-nastoyashhego-ili-budushhego/

[3] https://ru.wikipedia.org/wiki/

[4] https://ru.wikipedia.org/wiki/

[67] Подробней — читайте в наших бесплатных книгах: https://itsynergis.ru/blog.

[68] Лучший пример — «микронные чипы на каждый кирпич».

[69] Почему это так важно — рекомендую изучить в книге А. Аузана «Экономика всего[1]» или в своей собственной «Тени завтрашнего солнца[2]».

[70] В этом смысле тенденции дня сегодняшнего — развитие идей прошлого: «Одновременно богатыми и вместе с тем бедными: богатыми — потому что у них есть всё, бедными — потому что у них нет никакой собственности, и поэтому не они служат вещам, а вещи служат им» (Т. Кампанелла, «Город Солнца»).

[71] Подробней об этом можно почитать у М. Каку.

[72] См. подробней Ф. Лалу «Открывая организации будущего».

[73] Думаю, что одним из первых этот термин стал употреблять именно с данным содержанием А. Шульгин[3] — композитор, инвестор и визионер.

[74] Подробный, но не полный список можно найти в Путеводителе-2020 — https://itsynergis.ru/assets/docs/blockchain_cryptocurrency_guidebook_2019.pdf.

[75] Удивительно, что после наших работ 2016—2017 гг. независимо и в разных направлениях, отраслях и уровнях формализации об этом стали высказываться деятели науки, искусства и других областей интеллектуальной деятельности: пример — части интервью Б. Акунина[4] о книге «Счастливая Россия».

---

[1] https://www.mann-ivanov-ferber.ru/books/ekonomika_vsego/

[2] https://www.litres.ru/vladimir-popov-7629101/teni-zavtrashnego-solnca/

[3] https://youtu.be/Se376NVai6E

[4] https://youtu.be/nrJpDBHWzyI?t=3254

[76] Подобное можно «пощупать» как раз в реализации telegram-бота системы VIZ, когда за пользу внутри чата (правильный вопрос, ответ, вовремя сказанная реплика и т. д.) можно поставить "+" и тем самым — отблагодарить не просто словом, но и делом, точнее — его цифровым выражением, то есть активом.

[77] В этом смысле она как электрон, нейтрон и протон, из которых можно сложить неимоверное количество комбинаций.

[78] Здесь и далее будем использовать термин SaO — subject and/or object.

[79] Или с любым иным коэффициентом сложности, не превышающим 0,5.

[80] Следует понимать, что методология носит рекомендательный характер.

[81] Если исходить из 50%, указанных выше для залога положительной репутации.

[82] Безусловно, нода внутри ДРС — частный случай.

[83] Впрочем, не обязательно применять tangle-подобный подход, но именно он даёт возможность создания замкнутых систем из трёх и более элементов при минимальном наборе правил.

[84] Написание 000 (трёх нулей) говорит о том, что речь идёт о стобалльной системе.

[85] Если же система функционирует как централизованная/закрытая/«частная»/проприетарная, то это ограничение по очевидным причинам может быть снято.

[86] Здесь не только консенсусы: токенизация, учёт цифровых активов для кредитования и прочее.

[87] Речь об истории государств, но не общества (прим. В. П.).

[88] А мир и без того разогрет (прим. В. П.).

[89] Если вы, уважаемый читатель, знаете другой, более ранний пример, просим связаться с Menaskop, чтобы внести правки в последующие редакции книги.

[90] Впрочем, автор указанной выше книги (К. Скиннер) как раз разводит/разделяет понятия Web 3.0 и Value Web.

[91] Как указано выше, есть понятие DTL и блокчейн. Словосочетания формата «закрытый блокчейн», «проприетарный блокчейн», «корпоративный блокчейн» — оксюмороны, которые по факту означают DTL (*прим. В. П.*).

[92] С этой позицией сложно не согласиться, что не отменяет именно категориальной градации (*прим. В. П.*).

[93] Здесь не соглашусь с автором главы, потому как исследования 2017—2019 гг. доказывают часто обратное (*прим. В. П.*).

[94] В этом и есть главная, но не единственная связь с материалом предыдущей главы (*прим. В. П.)*.

[95] Точка зрения весьма спорная, как с учётом международного опыта (начиная от законодательства Лихтенштейна с фактически полным регулированием процесса токенизации, заканчивая десятком юрисдикций, регулирующих отдельные аспекты такового), так и с пониманием, что гражданское право почти любого государства даёт бизнесу неограниченные возможности для манёвра на любом новом рынке (*прим. В. П.)*.

[96] Часто в литературе, технической документации и исследованиях можно встретить словосочетание «атомарные свопы» *(прим. В. П.)*.

[97] См. о нём также в первой главе (*прим. В. П.)*.

[98] Как видим, в блокчейн даже старое зло может обернуться новым добром (*прим. В. П.)*.

[99] Правильней сказать — законодательной, так как право всегда для всех едино (*прим. В. П.)*.

[100] Ещё подробней https://www.litres.ru/endru-tanenbaum/komputernye-seti-42227980/.

[101] Глава написана В. П.

[102] Один из вариантов можно посмотреть на сайте: http://atlas100.ru/upload/pdf_files/atlas.pdf.

[103] См. подробней: https://t.me/RussiaTeal.

[104] Глава также от В. П.

[105] Также вопрос можно изучить в статье: https://vc.ru/books/26463-register-of-things.

[106] Хотя, скажем, в каучсёрфинге и их уже давно нет, в отличие от шеринг-экономики аренды недвижимости в формате AirBNB.

[107] Будто герой фильма «Пятый элемент».

[108] 1566, 1649, 1775, 1789, 1848—1849 и другие года: всё зависит от конкретных государств.

[109] Даже при среднем максимуме в 70—80 лет 20 составляет не меньше четверти!

[110] Если же речь идёт о seed-фразе, то просто переступаем на другой уровень математической абстракции и не более: https://medium.com/@fidgett/все-про-seed-фразу-25a0aff7cf3d[1].

[111] Подробней — см. в книге «Прогноз: Как, наблюдая за погодой, научиться предсказывать экономические кризисы» от М. Бьюкенена.

[112] Снова В. П.

[113] Подробней об этом смотрите в аллегориях киноленты «Форма воды».

[114] Интересно, что материал был составлен задолго до нелегитимного изменения Конституции РФ в 2020 году (прим. В. П.).

[115] А не условно — около 50—100 конечных бенефициаров (прим. В. П.).

[116] Цитата Д. Стародубцева.

[117] Напомню, что сегодня есть решения от Namecoin, Ethereum, Ziliqa, Aeternity и других блокчейн-платформ (прим. В. П.).

[118] Определять месторасположение (прим. В. П.).

---

[1] https://medium.com/@fidgett/

[119] Толчок в развитии: от английского push — проталкивание.

[120] Хотя кто-то скажет про 2008, но это уже тонкости летописи: https://www.bitcoin.com/bitcoin.pdf.

[121] Имеется в виду не останавливаемый третьей стороной: например, держателем сервера или хостинг-провайдером.

[122] Имеется в виду софт, а не «железо», конечно же (прим. В. П.).

[123] Хотя дело Rambler VS Nginx, кажется, и здесь поставило точку.

[124] Оплошности, как в 2010 году, — о другом.

[125] В 2019 году система ФРС дала сбой, и об этой особенности биткоина сразу заговорили многие.

[126] Частично можно ознакомиться[1] на YouTube-канале.

[127] Модель уже успешно применяется в BAT-токене и браузере Brave. Отличное глобальное применение — в проекте iTerra.

[128] Сам же блокчейн создан как инструмент доверия в недоверенной среде, коей, как ни сложно это признать, является общество в большинстве своих нынешних проявлений.

[129] Подробней о достижениях в данной области можно прочесть в Путеводителе-2019 — https://itsynergis.ru/assets/docs/blockchain_cryptocurrency_guidebook_2019.pdf.

[130] Интересен в этом смысле проект скоростного PoW-блокчейна Tera.

[131] Дополню из года 2020-го, что Г. Тунберг — ещё один, новый, но предсказуемый символ, толкающий нас в эпоху репутационных систем.

---

[1] https://youtu.be/hVR8BxsOBgU

[132] См. также об их взаимосвязях — в статье[1].

[133] Читай в «Тени завтрашнего солнца» — первом бизнес-моноспектакле: https://www.litres.ru/vladimir-popov-7629101/teni-zavtrashnego-solnca/.

[134] Что не говорит о невозможности решения через сугубо «квантовые» подходы.

[135] Оригинал статьи — http://radar.oreilly.com/archives/2007/10/web-30-semantic-web-web-20.html
не доступен, но сохранился в web-архиве[2] (что само по себе — вполне аллегорично). Мы ушли от дословного перевода к смысловому.

[136] Имеется в виду http://web2con.com/.

[137] Дословно: Web was roaring back after the dot com bust.

[138] И он как раз произошёл в 2008—2009 году благодаря появлению Bitcoin (прим. В. П.).

[139] Например, блокчейн (прим. В. П.).

[140] Имеется в виду материал, часто цитируемый в Сети, в том числе — из-за представленной схемы развития веба из версии 1.0 к версии 4.0 (!): https://novaspivack.typepad.com/nova_spivacks_weblog/2007/10/web-30----the-a.html

[141] Это можно проделать по запросу «site:radar.oreilly.com semantic web».

[142] Насколько же порой родитель может ошибаться в собственных детях (прим. В. П.).

[143] Прошу обратить внимание, что материал написан в 2007 году! (прим. В. П.)

---

[1] https://vc.ru/story/53790-facebook-davala-dostup-microsoft-apple-yandeksu-i-drugim-kompaniyam-k-skrytym-dannym-polzovateley-new-york-times

[2] https://web.archive.org/web/20090131054117/http://radar.oreilly.com/archives/2007/10/web-30-semantic-web-web-20.html

[144] Даны **выдержки** материала, который акцентирует внимание сразу на нескольких W3-аспектах — https://novaspivack.typepad.com/nova_spivacks_weblog/2007/02/web_30_roundup_.html: данные материалы, на мой взгляд (В. П.), являются важными как с точки зрения хронологии, так и с точки зрения смысловой нагрузки, поскольку Нова и О'Рейли — родоначальники не просто великого спора о W3, но и многих начинаний в нём.

[145] Так, впрочем, и происходит (прим. В. П.): например, благодаря так называемой микроразметке.

[146] Вспомните о самовложенных dapps, которые описывал выше (В. П.).

[147] Не совсем ясно, почему онтология должна быть именно централизованной: естественные языки в большинстве своём развиваются многомерно и разнонаправленно — русский в модификациях украинского и белорусского или английский в американском диалекте и «классическом британском» — различны, что не мешает ни уровню их развития, ни тем более интеграции в мировое сообщество (В. П.).

[148] И это уже ближе к моей точке зрения (В. П.).

[149] На мой взгляд (В. П.) — ключевой тезис.

[150] Представлен перевод материала Н. Спивака, обозначенного на странице https://novaspivack.typepad.com/nova_spivacks_weblog/2007/07/web-30----no-hu.html.

[151] См. выше описание Filecoin (В. П.).

[152] См. опять же SportCoin (В. П.).

[153] Есть даже официальное признание в блоге компании: https://about.fb.com/news/2019/03/keeping-passwords-secure/.

[154] Ещё одну подборку можно найти https://xdrv.ru/tags/break/all. Или третья альтернатива — https://ru.hetcomputer.com/2012-s-worst-security-exploits-fails-and-blunders-58145.

[155] Про взлом Gmail[1] до сих пор — молчание.

[156] Свыше 500 000 000[2] аккаунтов Yahoo в том же году: и не помогает даже уголовное наказание (ещё пример[3]). И в целом в 2014 году речь идёт уже о цифре, превышающей 1 200 000 000[4] пользователей, а это — 1/7 часть Земли! И почти ¼ всех пользователей Сети. Часть из них занесена в Wiki[5] навечно.

[157] И ещё свыше 171 000 000[6] в одном только «ВКонтакте»!

[158] Но другие соцсети[7] ломали также, что казалось просто «фоновым режимом».

[159] Ссылка[8] для верификации.

[160] Особенно после взлома аккаунта самого генерального директора[9] Twitter и аккаунта премьер-министра[10] РФ Д. Медведева.

[161] И речь даже не о вечно «дырявой» Windows, а именно о сервисах компании.

[162] Подробней о W3-браузерах в расширенном материале от «Форклога» — https://forklog.com/na-strazhe-web-3-0-glavnye-blokchejn-brauzery-interneta-novogo-pokoleniya/.

---

[1] https://rg.ru/2011/06/02/gmail-hakery-site.html

[2] https://www.ukrinform.ru/rubric-world/2471552-hakeru-iz-kanady-dali-5-let-za-vzlom-yahoo-na-zakaz-rossijskih-specsluzb.html

[3] https://tjournal.ru/tech/71467-v-ssha-urozhenca-kazahstana-prigovorili-k-5-godam-tyurmy-za-vzlom-yahoo-v-interesah-fsb

[4] https://www.gazeta.ru/tech/2014/08/06_a_6162977.shtml

[5] https://en.wikipedia.org/wiki/ICloud_leaks_of_celebrity_photos

[6] https://habr.com/ru/company/defconru/blog/302644/

[7] https://www.gazeta.ru/tech/2018/08/14/11896147/instagram_ru.shtml

[8] https://www.gazeta.ru/tech/2019/01/26/12143245/instagram_hacking.shtml

[9] https://www.rbc.ru/technology_and_media/30/08/2019/5d6986d69a79477d2ab0f7a7

[10] https://www.tvc.ru/news/show/id/47493

И. Белоусов
Э. Крон
А. Пискунов
В. Попов
С. Симановский

Web 3.0.
Часть I. Настоящее вчерашнего завтра

Создано в интеллектуальной издательской системе Ridero

НЕ ПЕЧАТАТЬ!

ISBN 978-5-4498-4250-3