
TOP
BUSINESS
AWARDS

William Mougayar

The Business Blockchain_

Promise, Practice, and Application of the Next Internet Technology

> foreword by Vitalik Buterin

Уильям Могайар

Блокчейн для бизнеса_

> предисловие Виталика Бутерина

Москва
2018

УДК 004.08
ББК 32.81
М74

THE BUSINESS BLOCKCHAIN:
Promise, Practice, and Application of the Next Internet Technology

William Mougayar, foreword by Vitalik Buterin

Могайар, Уильям.

М74 Блокчейн для бизнеса / Уильям Могайар ; предисл. Виталика Бутерина ; [пер. с англ. Д. Шалаевой]. — Москва : Издательство «Эксмо», 2018. — 224 с. — (Top Business Awards).

ISBN 978-5-699-98499-2

Блокчейн — технология хранения и обработки данных, способная преобразить мир вокруг нас. Блокчейн выглядит как распределенная база данных, система, при которой информация хранится не на каком-то одном централизованном носителе, а одновременно на всех компьютерах, которые есть в данной системе.

С этой системой становятся невозможными многие виды нарушений и преступлений.

Купить красивый номер для автомобиля? Невозможно. Один недобросовестный сотрудник больше не сможет изменить вашу очередь и выдать номер «под заказ». Остальные компьютеры, которые задействованы в процессе, такую операцию не подтвердят. Подобные преступления, а также многие виды системных ошибок скоро канут в Лету.

Различные сделки, торги, покупка недвижимости, страхование, медицина, выборы — эта технология может отследить и зафиксировать все необходимые действия без участия посредников.

УДК 004.08
ББК 32.81

ISBN 978-5-699-98499-2

Моим родителям,
чью поддержку я продолжаю чувствовать.
Морин, с которой все становится возможным.

И нашей любимой собаке Паше,
маленькому отважному бишону фризе.
Ты в моем сердце навсегда.

Содержание

Предисловие 9

Благодарности 14

Пролог 16

Введение 20

Глава I
Что такое блокчейн? 26

Глава II
Как блокчейн завоевывает доверие 55

Глава III
Препятствия, вызовы и косность мышления 90

Глава IV
Блокчейн и финансовые услуги 115

Глава V
Передовые отрасли и новые посредники 141

Глава VI
Реализация технологии блокчейна 155

Глава VII
Децентрализация как путь вперед 178

Эпилог 197
Избранная библиография 200
Дополнительные ресурсы 203
Об авторе 205
Предметный указатель 207
Примечания 212

Предисловие

Текущее десятилетие – интересное время развития децентрализованных технологий. Несмотря на все усилия, которые на протяжении предыдущих тридцати лет прикладывали криптографы, математики и кодировщики, разрабатывая строго специальные усовершенствованные протоколы для защиты конфиденциальности и гарантий аутентичности различных систем — от электронной валюты до голосования и передачи файлов, — достигнутый прогресс был невелик. Инновационно блокчейн — или, вообще говоря, инновационный общественно-экономический консенсус, предложенный в 2009 году Сатоши Накамото, — оказался тем самым недостающим фрагментом головоломки, который смог придать этой индустрии импульс для гигантского скачка вперед. Дополнительным стимулом послужила политическая обстановка: глубокий финансовый кризис 2008 года породил растущее недоверие к правительствам и корпорациям, которые как раз и должны контролировать финансовые потоки; он послужил внутренним толчком, который многих заставил искать альтернативные варианты. И наконец, «вишенкой на торте» стали откровения Эдварда Сноудена в 2013 году, пролившие свет на активность государства в сферах, которые граждане считали конфиденциальными. Хотя технологии блокчейна в результате не получили всеобщего признания, несомненно, идеи децентрализации поднялись на новую высоту.

Различные приложения, начиная от телефонов Apple до WhatsApp, стали оснащаться столь мощными системами шифровки данных, что взломать их не под силу даже компаниям, создающим софт и управляющим серверами. Для тех, кто предпочел корпорации правительственному монстру, появление «экономики совместного потребления 1.0» продемонстрировало все признаки невыполнения первоначально данных обещаний. Вместо того чтобы ликвидировать укоренившуюся олигополию посредников, такие гиганты, как Uber, просто заняли их место, отнюдь не всегда лучше выполняя их функции. Блокчейн и спектр связанных с ним технологий, которые мы называем «крипто 2.0», гарантируют исправление этих недостатков. Вместо того чтобы просто надеяться на честность наших контрагентов, мы внедряем технологические системы с такими свойствами, которые будут обеспечивать необходимые гарантии даже в случае, если многие наши партнеры поведут себя нечестно.

Все транзакции в рамках «крипто 2.0» могут быть подтверждены криптографическими доказательствами. Децентрализованные одноранговые (peer-to-peer) сети могут использоваться для уменьшения нагрузки на любом одиночном сервере; с помощью открытого программного кода можно создать идентификационные блокчейны. Более сложные математические приемы, включая кольцевую подпись, гомоморфное шифрование и доказательство с нулевым разглашением, гарантируют конфиденциальность, позволяя пользователям таким образом хранить данные, что некоторые их составляющие можно проверить и даже вычислить, не раскрывая личную информацию. Первых приверженцев этой технологии особенно удивило, сколь быстро произошло ее институциональное принятие за последние два года. С 2011 по 2013 год адепты блокчейна — тогда это в основном касалось только биткоина — отличались духом анархии, это были революционеры-идеалисты всех мастей, увлеченные новыми возможностями «противостоять властям» (или, точнее, обойти их). Сегодня, в 2016 году, наиболее захватывающие перспективы касаются сотрудничества, о чем сообщили IBM и Microsoft, исследование, проведенное Банком Англии, или банковский консорциум, куда вошли новые члены.

Что же произошло? Я бы сказал, что криптоанархисты недооценили, насколько гибкими, технологически прогрессивными и даже идеалистически настроенными могут быть банки и крупные корпорации. Мы часто забываем, что корпорации тоже состоят из людей, чьи ценности и представления вполне могут совпадать с воззрениями обычных людей, которых мы встречаем на каждом шагу. Может показаться, что новый «механизм доверия», как назвал его *The Economist,* просто пришел на смену прежним централизованным «гарантам доверия», опиравшимся на реальную репутацию и регулирующий надзор и в финансовой сфере, и в других областях, но действительность гораздо сложнее. Честно говоря, различные институты точно так же не доверяют друг другу, как и обычные люди; аналогично централизованные институты в одной отрасли обеспокоены централизацией в других отраслях. Энергетические компании, производящие и продающие электроэнергию, с равным удовольствием поставляют ее на централизованный и на децентрализованный рынок. Возможно, они даже предпочтут децентрализованный, если там будет меньше ограничений.

Более того, многие отрасли промышленности уже децентрализованы — просто многие люди, не занятые в них, об этом не задумываются. Кроме того, они децентрализованы крайне неэффективно: у каждой компании все равно есть своя инфраструктура, через которую взаимодействуют пользователи, проводятся транзакции и обмен данными и которая требует согласования с другими компаниями при каждом взаимодействии. На деле консолидация вокруг одного рыночного лидера сделала бы эти отрасли более эффективными. Но ни конкуренты потенциального лидера, ни антимонопольные регуляторы не желают это признать, создавая безвыходное положение. Так было до сих пор. С появлением децентрализованных баз данных, которые могут технологически воспроизвести сетевой эффект, прежде доступный только монополиям, каждый может присоединиться к ним и действовать себе во благо, не создавая монополию со всеми ее негативными сторонами.

Именно поэтому технологии блокчейна так востребованы в сфере финансов, индустрии поставок и системах идентифика-

ции. Все они используют децентрализованные базы данных, реализуя свои цели на одной платформе, без затрат на то, чтобы договориться о том, кто получит контроль над этой платформой, а затем примириться с тем, что они попытаются злоупотреблять своим монопольным положением.

В первые четыре года после того, как Сатоши внедрил биткоин в январе 2009 года, много внимания уделялось электронной валюте, включая платежный аспект и ее функции как альтернативного средства накопления. В 2013 году в центре внимания оказались приложения «блокчейн 2.0»: те же технологии, что обеспечивают децентрализованность и безопасность биткоина, теперь распространены на приложения, касающиеся самых разных областей — от регистрации имени домена до финансовых контрактов, краудфандинга и даже игр. Основная идея моей собственной платформы, Ethereum, сводилась к тому, что язык программирования, введенный в протокол на базовом уровне, был полной абстракцией, что давало возможность пользователям создавать приложения, руководствуясь логикой любого бизнеса или для иных конкретных целей, реализуя преимущества, которые предоставляет блокчейн. Примерно в это же время стали появляться такие системы, как платформа децентрализованного хранения «Межпланетная система файлов» (InterPlanetary File System, IPFS). И криптографы предложили новые мощные средства, которые можно использовать в комбинации с технологией блокчейна для большей конфиденциальности, например, zk-SNARKs или доказательство с нулевым разглашением Succinct Non-Interactive ARgument Knowledge. Сочетание тьюринг-полного блокчейна с децентрализованной сетью, использующей сходные технологии кодирования, и интеграцию блокчейна с усовершенствованной криптографией я решил назвать «крипто 2.0» — возможно, название выглядит амбициозно, но оно наилучшим образом отражает смысл технологии в самой широкой форме.

Что такое «крипто 3.0»? Отчасти — продолжение направлений, заложенных в «крипто 2.0», в частности, использование обобщенных протоколов, обеспечивающих максимальную абстрактность и конфиденциальность. Но не менее важен и такой «слон в посуд-

ной лавке», как масштабируемость в сфере блокчейна. В настоящее время все протоколы блокчейна выстроены так, что каждый компьютер в сети должен обработать каждую транзакцию, — это свойство обеспечивает максимальную отказоустойчивость и безопасность ценой того, что вычислительная мощность сети фактически ограничивается вычислительной мощностью одного компьютера.

«Крипто 3.0» — по крайней мере, как я его вижу, — должен каким-то образом преодолеть эти ограничения и достичь уровня, достаточного для его массового распространения[1].

Затем, разумеется, встает вопрос адаптации. Помимо возможностей электронной валюты, в 2015 году многие интересовались «крипто 2.0», но пока разработчики выпускают базовые платформы, а не какие-либо значимые приложения. В 2016 году мы видим уже и стартапы, и подтверждения наших концепций институциональными игроками. Конечно, большинство их ни к чему не приведет и постепенно сойдет на нет. Это неизбежно в любой области. В предпринимательстве существует трюизм: 90% любого бизнеса терпит крах. Однако оставшиеся 10% со временем будут оценены по достоинству, и этот продукт будет востребован миллионами людей — тут-то и начнется самое интересное.

Возможно, книга Уильямса вдохновит вас на то, чтобы присоединиться к работе над усовершенствованием блокчейна для бизнеса.

Виталик Бутерин,
разработчик платформы Ethereum
2 апреля 2016

[1] Технически подкованные читатели, возможно, слышали о *lightning networks* — децентрализованной системе для мгновенных микроплатежей, *state channels* — технологии платежных каналов, позволяющих проводить большие объемы транзакций за пределами основного блокчейна и *sharding* — приеме, который позволяет распределять данные между разными физическими серверами. – *Прим. перев.*

Благодарности

Есть мнение, что написать книгу – все равно что признаться в любви, и я согласен с этим мнением. Я чувствую себя так, будто я собрал пазл на холсте, а теперь вставляю его в рамку. Писать книгу — все равно что обмениваться подарками. Автор тратит огромное количество времени на то, чтобы изложить свои мысли на бумаге. Взамен читатели тратят свое время, читая. Иногда между ними возникает взаимосвязь. Я буду рад ответить каждому, кто напишет мне по адресу: wmougayar@gmail.com.

С тех пор как я стал интересоваться технологиями блокчейна, на мой образ мыслей и открытия повлияли многие люди, но самым большим авторитетом для меня стал Виталик Бутерин, создатель платформы Ethereum и ее главный исследователь. Я навеки в долгу перед ним за время и знания, которыми он со мной щедро делился.

Я благодарен всем создателям, новаторам, предпринимателям, лидерам, исполнителям и практикам, находящимся на передовом крае новой технологической революции — спасибо, что вы помогли мне соединить звенья цепи в одно целое. Это ваши огни манят меня вперед, помогая преодолеть темноту. Наше общение бесценно. Спасибо, что позвали меня в первый ряд, а то и за кулисы вашего восхитительного представления.

Боясь не назвать кого-то из близких мне профессиональных кругов, я хотел бы выразить особую благодарность Мунибу Али, Яну Аллисону[2], Хуану Бенету, Паскалю Бувье*, Крису Алену, Джер-

[2] Отмечены те, кто согласился почитать главы моей книги в процессе работы над ней. (*Прим. автора*).

ри Брито, Энтони ди Лорио, Леде Глиптис, Брайану Хоффману*, Эндрю Кизк, Хуану Лланосу, Джозефу Любину, Адаму Людвину, Джоэлю Монегро, Крису Оуэну, Сэму Паттерсону, Денису Назарову, Рудольфу Новаку, Майклу Перклину, Роберту Сэмсу*, Вашингтону Санчесу, Эмбер Скотт, Райану Селкису, Барри Зильберту, Райнану Ши, Эджеенсену Шри, Нику Салливану, Нику Жабо, Тиму Свонсону, Симону Тейлору*, Вейн Воган, Джесси Вальден, Альберту Венгеру, Джеффри Уилки, Фреду Вильсону и Гевину Вуду. Все они, так или иначе, внесли свой вклад в мое понимание биткоина, криптовалют, блокчейна, обучая меня, дискутируя со мной, разрешив мне войти в их мир, где я получал знания.

Моя особая благодарность исполнительному редактору издательства Wiley Биллу Фэллуну, который был убежден, что мы сможем сделать это быстрее, чем это вообще возможно, и Кевину Барретту Кейну, который выступил дизайнером и одновременно продюсером книги.

Наконец, я очень признателен группе моих друзей, которые помогли организовать сбор средств для выпуска книги на Kickstarter в феврале 2016 года, — это сделало задачу выполнимой. Я бы не смог сделать этого без вас и без поддержки Марго Этвелл и Джона Диматоса из Kickstarter (сайт для привлечения денежных средств на реализацию творческих, научных и производственных проектов по схеме краудфандинга).

Один из многих, Самый Щедрый сторонник — Брэд Фелд (Foundry Group). По-настоящему Щедрые сторонники: Джим Орландо (OMERS Ventures), Райан Селкис (DCG), Мэтью Споук (Deloitte). Суперособенные сторонники: Кевин Мэги, Пьет Ван Оувербек, Кристиан Георг, Джон Брэдфорд.

Супербольшие сторонники: Дэвид Коэн (Techstars), Мэтью Рожак (Bloq), Марк Темплтон, Дункан Логан (RocketSpace), Майкл Далесандро.

Большие сторонники: Ахмед Альшайя, Флойд Д'Коста, Гейно Доссинг, Лари Эрлих, Феликс Фрай, Джей Гривз, Эмиль ван дер Хок, Фергюс Лемон, Амир Мулави, Дэниэл А Гринспун, Майкл о'Лафлин, Нарри Сингх, Амар Варма, Донна Бревингтон Уайт, Нил Уоррен, Альберт Венгер.