Биткоин, а не блокчейн

Преобладающее мнение заключается в том, что внедрение блокчейна поможет сделать многие системы безопасными, дешёвыми, надёжными и прозрачными. Однако, реальность этого понятия такова, что, во-первых, блокчейн сам по себе едва ли может решить какую-то из этих проблем, а во-вторых крайне плохо подходит для тех сфер, в которых его пытаются применить. Во многих смыслах, биткоин остаётся почти что единственным и самым удачным экспериментом по применению блокчейна в то время, как множество других так и не показали свою жизнеспособность или провалились: например, R3, крупнейшая в мире блокчейн-исследовательская фирма, ведущая консорциум из 200 компаний, за всё время своего существования смогла представить только один продукт, который, при этом, по их же заявлениям, никак с блокчейном не связан, а сама сейчас находится на грани разорения.

Блокчейн впервые был внедрён в работающую систему — биткоин — в 2009 году. В самом описании биткоина термин «блокчейн» (blockchain) не употреблялся, вместо этого использовалось понятие «цепь блоков» (chain of blocks). Сама цепь блоков не была и не является основным компонентом работы или безопасности биткоина: последняя достигается совмещением множества разных решений. Смотреть только на блокчейн, отметая или изменяя сопутствующие ему механизмы обеспечения безопасности — фундаментальная ошибка, которую совершают желающие внедрить блокчейн в свои процессы, отбрасывая при этом всё остальное.

Для того, чтобы подробно разобраться в вопросе применимости блокчейна, сперва следует установить его понятие и свойства. Блокчейн, в общем виде, — криптографически связанная последовательность блоков, где каждый блок особым образом ссылается на предыдущий. Если информация в предыдущем блоке меняется уже после создания следующего, то ссылка становится недействительной: из представленной информации становится очевидно, что последующий блок ссылается не на тот предыдущий, что нам представлен. В таком виде блокчейн — не более, чем особенная вариация базы данных со своими правилами их хранения и внесения (возможно только добавление).

Поэтому использование блокчейна неразрывно связано с некоторыми представлениями о том, как должна работать окружающая его система и какими свойствами она должна обладать. Например, если блокчейн хранится только в одном месте, то внести изменения в предыдущие блоки можно путем пересоздания всей цепочки; поэтому важным его свойством является безопасность хранимых в нём данных, достигаемая через децентрализацию: записи должны храниться у многих участников системы и быть легко аудируемыми, чтобы никто не мог совершить подмену.

В связи с особенностями системы, у данных, хранимых в ней, есть вполне определённые свойства: они должны быть неизменными (возможно только добавление, перезапись старых данных невозможна), непротиворечивыми (существует определённая внутренняя логика системы, которой все данные должны следовать для избежания внутренних конфликтов), иметь информацию о владельце (любые данные в блокчейн кто-то добавляет, они не могут появиться из ниоткуда) и являться каноничными (все участники системы считают истинной информацию, записанную в блокчейне).

Последнее свойство, скрепляющее и дополняющее все остальные — это децентрализация, означающая отсутствие единой точки отказа в системе. Если такая точка есть, то система централизована. Централизация и децентрализация — не бинарные понятия, а скорее спектр, на котором к тому же крайне сложно ориентироваться: даже на первый взгляд децентрализованная система может считаться централизованной, если кто-то имеет возможность вмешаться в её работу. Децентрализованной можно считать систему, которая, во-первых, распределена настолько, что шансы вмешаться в её работу ничтожно малы, во-вторых, со временем благодаря своему устройству стремится к ещё большей децентрализации.

Стоит отметить, что децентрализация — не самоцель, а лучший из ныне известных нам способов добиться доказуемой правдивости, неизменности и общедоступности данных. Если бы мы могли построить абсолютно защищённый центральный сервер с защищёнными и гарантированными соединениями или положиться на абсолютно честных и независимых доверенных лиц, то, вероятно,

так и стоило бы сделать. Однако, вся история компьютерных систем говорит нам о том, что ни то, ни другое на практике недостижимо. Имея в виду, что любой отдельный узел сети достаточно легко скомпрометировать, идея децентрализации диктует нам необходимость иметь такое число узлов, обменивающихся информацией по определённым надёжным правилам, чтобы скомпрометировать сколь-либо значимую их часть было бы практически невозможно, а значит, система в целом оставалась бы работоспособной.

Блокчейн во всей этой парадигме — лишь одна из составных частей, обеспечивающих децентрализацию. Использование блокчейна в централизованной системе не несёт никакого смысла: получившийся продукт будет одновременно совмещать риски доверенных третьих лиц и недостатки блокчейна, а не комбинировать их достоинства. Гораздо проще и дешевле использовать обычную базу данных.

Биткоин

Практика показывает, что самым продолжительным, удачным и востребованным экспериментом по использованию блокчейна является биткоин. Сеть биткоина успешно работает уже девять с половиной лет, и за всё это время перебои в её работе составили в сумме всего лишь несколько часов. За это же время никто ни разу не смог взломать сам протокол системы, нанеся другим участникам вред, и никто не смог изменить фундаментальных правил её работы или установить над ней контроль. Платежи в биткоине по-прежнему транснациональны, нецензурируемы, абсолютно надёжны и необратимы. Все эти характеристики поддерживаются за счёт широкой децентрализации биткоина, подкреплённой огромным количеством оборудования и затрачиваемой электроэнергии. В некотором смысле, биткоин — это самая большая в мире премия за обнаружение уязвимостей: любой, кто обнаружит хотя бы один критический баг, имеет в своём распоряжении систему стоимостью более ста миллиарда долларов.

Биткоин минимизирует доверие между участниками, так как весь программный код и сам блокчейн биткоина доступны для аудита любому желающему. Заинтересованный участник сети может самостоятельно, с помощью своего компьютера, проверить состояние сети вплоть до последней транзакции и единолично убедиться в том, что все правила работы по-прежнему соблюдаются, и ни одна транзакция не является мошеннической. В биткоине нет необходимости обращаться к доверенным лицам или серверам, чтобы вести свою экономическую активность. За счёт полной проверяемости и непрекращающегося мониторинга участниками по всему миру, биткоин остаётся платёжной системой, производящей достоверный результат несмотря на отсутствие доверия между участниками.

Работа сети

Однако, такой эффект не достигается даром: для этого в устройстве биткоина приняты множественные компромиссы, которые существенно отягощают систему исключительно в угоду децентрализации и безопасности. Один из таких компромиссов — пропускная способность биткоина на уровне базового протокола. В блокчейн биткоина в лучшем случае можно записать около пяти тысяч транзакций каждые 10 минут — примерно в десять раз меньше, чем проходит в мировых платёжных системах каждую секунду. Если бы вся система находилась на одном-единственном стареньком ноутбуке, то он без проблем смог бы обрабатывать тысячи транзакций в секунду, однако, ради того, чтобы любые, даже самые слабые, компьютеры участников по всему миру успевали получать и проверять последнее состояние сети, ни на кого не полагаясь, лимит было необходимо снизить до таких значений. Повышение лимита (то есть, увеличение пропускной способности) сузит круг участников, способных независимо аудировать сеть, приводя её к централизации. «Выпавшие» из процесса участники отныне будут вынуждены полагаться на свидетельства оставшихся в сети и тем самым потеряют свою независимость. Таким образом, десятиминутный интервал записи и ограниченная пропускная способность сети — компромисс между безопасностью и удобством. Более быстрый темп приведёт к централизации и другим техническим проблемам, а более медленный — к нецелесообразности использования такой системы.

Примерно раз в десять минут в сети биткоина появляется новый блок, содержащий в себе набор недавно выпущенных участниками транзакций. Каждый следующий блок определённым образом

ссылается на предыдущий; цепь таких блоков в контексте биткоина и называется блокчейном. Блокчейн биткоина берёт своё начало 3 января 2009 года и непрерывно тянется до нынешнего момента, демонстрируя наличие связной и непротиворечивой истории на протяжении более чем девяти лет. Производитель блока, помимо наполнения его корректными транзакциями, также вынужден потратить определённое количество энергии на его создание: такой принцип называется доказательством работы (proof-of-work). Наличие доказательства работы предотвращает жульничество: у производителя нет никакого более простого способа создать корректный блок кроме затрат определённого количества энергии, а проверяющий может довольно легко в этом убедиться, посмотрев только на конечный результат.

Блок, в котором хотя бы одна транзакция нарушает общепринятые правила, не пройдёт проверку ни у одного из независимых участников сети и довольно скоро исчезнет из неё (никто не желает далее пересылать или хранить некорректную информацию), а сам производитель блока не получит за него награды, за счёт которой он мог бы скомпенсировать затраченные ресурсы. Такая же судьба ждёт и блок, на который было потрачено недостаточно много энергии. Наличие такого дисбаланса между трудоёмкостью производства и проверки приводит к тому, что производителям блоков становится крайне невыгодно пытаться обмануть окружающих: цена каждой попытки невероятно высока, а шанс её успеха ничтожно мал.

За счёт наличия в блоках указателей на их предшественников, блокчейн формирует неразрывную цепь блоков, вмешательство в которую становится затруднительным. Каждый блок (кроме самого первого) содержит ссылку не просто на номер предшествующего блока, а на его уникальный идентификатор, который зависит от содержания блока. Попытка поменять его приведёт и к изменению уникального идентификатора блока, поэтому ссылка от следующего блока к данному станет недействительной. Попытка поменять ссылку, в свою очередь, поменяет уникальный идентификатор следующего блока, так как ссылка на предыдущий блок также является частью содержания

Безопасность

Таким образом, общая безопасность сети достигается только за счёт существенных материальных затрат её участников. Попытка снизить последние приведёт и к удешевлению попыток мошенничества, в то время как затраты на верификацию дальше снизить уже невозможно (кроме как полностью отказаться от верификации и оказаться в доверенной системе). неизменность блокчейна биткоина является следствием вышеописанных экономических стимулов, а не его особой структуры. С помощью доказательства работы ресурс из реального мира (электроэнергия) трансформируется в неизменяемую цифровую историю. Именно использование доказательства работы для решения проблемы подлога в открытых сетях, не полагающихся на доверие, является настоящей инновацией — и именно её почему-то больше всего стараются не замечать или упразднить, что, в совокупности с непониманием реальной области применимости блокчейна, способно привести только к трате времени впустую.

Что блокчейн не может

Правдивость

Блокчейн не решает проблемы правдивости или уникальности хранимых в нём внешних данных. Никто не мешает кому-то записать в блокчейне, что автор Мона Лизы — он, а не Леонардо да Винчи; в качестве демонстрации британский программист Теренс Иден так и сделал, навеки оставив лжесвидетельство в блокчейне биткоина. Иметь голосование на блокчейне бессмысленно, если списки голосующих, внесённые в систему, сфальсифицированы. Использовать блокчейн для хранения документов бесполезно, если кто-то выдаёт липовые справки.

Проблема внесения достоверных данных в блокчейн известна как «проблема оракула». Оракулом называют некую сущность, способную вносить в систему достоверные данные из реального мира. Полагаться на централизованных оракулов, помимо очевидной проблемы доверия, проблематично: во-первых, по сути, система централизуется вокруг такого участника, так как новые данные в блокчейне всецело от него зависимы, во-вторых, каждый независимый участник вынужден

обращаться к оракулу за информацией, что создаёт существенную нагрузку на оборудование последнего. Остаётся только использование децентрализованных систем установления внешней истины, но такой подход порождает множество других проблем, решения которых ещё не изобретены или пока не считаются достаточно надёжными. В целом, по сей день проблема оракула остаётся нерешённой.

Хранение значимой информации на блокчейне связано и с другой проблемой: поначалу это не кажется очевидным, но, кроме представленности самой информации, нам нередко нужно быть уверенными, что в системе нет другой информации, опровергающей эту или нивелирующей её ценность. Например, если мы ведём учёт неких документов на блокчейне, то нам недостаточно иметь справку о том, что, например, A подчиняется X; мы также должны быть уверены в отсутствии справок о том, что A теперь не подчиняется X, или A подчиняется Y (при условии, что A не может подчиняться X и Y одновременно), и так далее. Так как в блокчейне хранится вся история системы, ничто не мешает злоумышленнику предъявить оттуда достаточно старые данные, заявив, что они являются актуальными. Чтобы проверить такое утверждение, мы должны иметь возможность просмотреть весь блокчейн, а это требует хранения всех данных в открытом виде, что либо недопустимо, либо ставит вопрос о том, зачем в случае полной открытости вообще нужен блокчейн.

Более простой пример — предсказание исходов каких-либо событий. Кто-то может указать прогнозы всех возможных реалистичных исходов футбольного матча, а потом указать только на сбывшееся предсказание: другие люди ничего не смогут узнать о существовании несбывшихся, пока им кто-нибудь явно на них не укажет.

Неизменность данных

Блокчейн сам по себе также не способен обеспечить неизменность данных: если он достаточно централизован, то заинтересованное лицо или злоумышленник может произвольно добавлять или удалять данные, сохраняя весь блокчейн валидным. Это достигается путём пересоздания всей цепочки с момента желаемого изменения. Конечно, в таком случае кто-то из следящих за блокчейном может забить тревогу. Но, во-первых, тогда осведомителю самому придётся доказывать, что он не злоумышленник (то есть что он не пытается, наоборот, подменить «правильный» блокчейн своей вариацией), а, во-вторых, даже при успехе такого мероприятия, возвращение к старому состоянию может оказаться непростым: нужно договориться, какое состояние является правильным, и у кого-то оно должно до сих пор храниться. В любом из этих случаев мы вынуждены всецело положиться на социальные способы установления истины, в то время как основное смысл блокчейна заключается в её установлении преимущественно технологическим путём, без социальных взаимодействий.

Внутренняя непротиворечивость данных также не может обеспечиваться сама по себе: она должна независимо валидироваться каждым из заинтересованных участников. Если мы в этом вопросе вынуждены полагаться на заверения других лиц, то мы лишь скрываем проблему доверия к посторонним лицам за магией блокчейна. При этом, если блокчейн достаточно громоздок для полной валидации отдельными участниками, то владельцы более мощного оборудования смогут записывать в блокчейн невалидные данные — иным словом, мухлевать, — не опасаясь того, что это раскроют владельцы более слабых компьютеров.

Как уже описывалось выше, блокчейну мало свойства очевидного обнаружения вмешательства: нужна также и устойчивость к нему, которую сам по себе блокчейн не обеспечивает. Для этого нужна устойчивая экономическая модель, воплощение которой за пределами использования блокчейна в качестве платёжной системы, возможно, и нереализуемо.

Цифровые активы

Владение цифровыми активами также вызывает много вопросов, особенно теми, что предоставляют права владения на реальные объекты. Как поступать, если владельцу цифрового актива отказывают в доступе к привязанному к нему имуществу? Каким образом будут исполняться судебные решения? Как человек, потерявший доступ к цифровому активу, может восстановить доступ к нему? Ответ на все эти вопросы приводит к необходимости существования некого обеспечителя или арбитра, обладающего расширенными полномочиями в системе. Однако, опять же, если такое лицо

существует, то оно фактически является средоточием централизации. Зачем тогда использовать блокчейн?

Похожей проблемой будут обладать и так называемые обеспеченные криптовалюты, на которые возлагают надежды многие участники традиционных финансовых рынков: наличие обеспечение неминуемо подразумевает сам факт наличия обеспечителя, который вправе отказать в обмене криптовалюты на товар обеспечения любому пользователю, будь то по своему желанию или вследствие государственных законов или судебных решений. Наличие такой уязвимости ставит под сомнение идею децентрализации такой криптовалюты, по сути превращая её в традиционную банковскую систему, в том числе позволяя обеспечителю практиковать частичное резервирование своей криптовалюты.

Несмотря на несколько лет своей истории, цифровые активы получили применение только в качестве продаваемых так называемых «токенов» блокчейн-проектов, собирающих деньги рядовых пользователей фактически под одни обещания. До сих пор ни один из этих проектов так и не показал реального и значимого функционала, кроме, возможно, Ethereum, который и стал главной площадкой для таких распродаж. Вопрос о том, имеет ли какую-то полезность существование подобных активов на блокчейне, поднимается многими участниками, равно как и необходимость блокчейна в этом сценарии в принципе.

Обновления и работоспособность

Функционал блокчейнов также не может быть статичным: скорее всего, кто-то захочет внести в них какие-либо обновления или исправления уязвимостей. В отличие от традиционных программ, обновление программы для использования блокчейна опционально: пользователь имеет право его не устанавливать, и никто не может его заставить это сделать. Если такое обновление к тому же предполагает изменение самого протокола, то оно требует установки у абсолютно всех пользователей во избежание разделения сети: иначе обновившиеся и оставшиеся на старой версии программы пользователи окажутся в двух системах, работающих по взаимоисключающим правилам. Таким образом, вопрос согласия пользователей на обновления и их обратной совместимости становится достаточно существенным фактором, наделяющим систему огромной инерцией и исключающим любую возможность оперативно вмешаться в работу блокчейна ради исправления каких-то моментов.

Это также означает и то, что злоумышленник, обнаруживший определённую уязвимость, может безнаказанно её использовать, и ни у кого нет полномочий его исключить или как-то ему помешать. Поэтому программирование блокчейна предъявляет высокие требования к его отказоустойчивости и продуманности на будущее. Богатая статистика сбоев и успешных атак в существующих блокчейнах говорит о том, что многие разработчики не справляются с этой задачей. Более того, излишнее усложнение блокчейна в попытке добиться поддержки новых функций или большей безопасности зачастую приводит к обратным эффектам: сложная система содержит в себе больше компонентов, каждый из которых может дать сбой, и труднее проверяется. Видимое отсутствие уязвимостей в протоколе может достоверно означать только что таковые пока не были обнаружены. Свидетельством отказоустойчивости протокола может являться только испытание временем. Самый лучший результат в последнем по-прежнему демонстрирует биткоин.

Чего на самом деле все хотят

Желание использовать блокчейн для решения проблем в самых различных сферах прежде всего говорит о кризисе модернизации в них. Из-за своей специфичности и множественных ограничений блокчейн вряд ли сможет им помочь. Вместо него нужно просто использовать современные технологические решения, способные снизить издержки, повысить эффективность, улучшить прозрачность, и т.д. Или, например, работать над законодательством в определённых сферах, или принимать на вооружение современные управленческие практики. Иными словами, всё это — долгий и комплексный процесс, который нельзя заменить одним взмахом волшебной блокчейн-палочки.

Однако, неудивительно, что в ответ на такой запрос появляется множество продавцов блокчейна, обещающих решение любых проблем бизнеса или общества. Они встречаются с директорами фирм,

знающими о блокчейне только по обзорным статьям — зачастую содержащими в себе множественные ошибки — и лишь подкрепляют их неинформированное мнение, тем самым продолжая раздувать ажиотаж. Примечательно, что на фоне всеобщего роста надежд и многочисленных блокчейн-конференций только разработчики реально работающих применений блокчейна пытаются сказать, что король-то голый.

Из-за проблемы достоверности внешних данных блокчейн может только обеспечивать правдивость информации о самом себе. Вкупе с экономическими стимулами такая система имеет больше всего смысла именно для работы с деньгами. Для всего остального у нас есть довольно сносно работающая система законов, договоров и судов с тысячелетней историей, и глупо пытаться отказаться от всего этого в пользу новой технологии. Увы, технологические революции проходят стремительно и плавно только на страницах учебников, но в реальной жизни это долгие годы упорной работы многих людей. И сейчас, скорее, стоит направить эту работу туда же, куда и обычно: на совершенствование социальных институтов и технологическую модернизацию, но никак не на бездумное копирование внутренней структуры биткоина в надежде таким образом решить все проблемы.