SBER CIB

Глубокое погружение в технологию блокчейн

29 ИЮНЯ 2023

Технологию блокчейн стало невозможно игнорировать

По оценке Всемирного экономического форума, к 2027 году блокчейн-технологии будут обеспечивать до 10% мирового ВВП. По расчетам Citigroup, к 2030 году рынок цифровых активов может привлечь до $5 трлн новых средств. Основными драйверами станут рост популярности стейблкойнов, внедрение цифровых валют центральных банков (CBDC) и токенизация реальных активов. Банки, государственные структуры и бизнес активно интересуются применением технологии блокчейн. Согласно исследованию консалтинговой компании McKinsey, у финансового сектора самые широкие возможности практического применения блокчейна. При этом, по их мнению, внедрение технологии блокчейн заметнее всего повлияет на государственный и технологический сектора.

В этом обзоре мы рассмотрим базовые и «продвинутые» понятия блокчейна. Это позволит получить более глубокое понимание технологии. Кроме того, мы:

- рассмотрим историю и причины зарождения блокчейнов,
- проанализируем, какие бывают блокчейны и в чем их отличия,
- выделим основные преимущества блокчейна для обычного пользователя и бизнеса,
- проанализируем практические примеры применения блокчейна в корпоративном и государственном секторах,
- рассмотрим, какие инициативы применения блокчейна рассматриваются в России,
- развеем самые распространенные мифы вокруг блокчейна и криптовалют.

Герман Греф,
глава Сбера

"Токенизация ресурсов, цифровизация ресурсов и хранение их на технологии блокчейн может составить до 10% мирового ВВП к 2030 году. В ближайшие 5-7 лет, как нам кажется, эта технология будет иметь огромное влияние на развитие экономики."

Ritchie Torres,
американский политик

"Криптовалюта - это будущее. Она позволяет бедным слоям населения осуществлять платежи и денежные переводы без длительных задержек и высоких комиссий. Благодаря криптовалютам художники и музыканты могут зарабатывать на жизнь. Криптовалюты бросают вызов концентрированной власти крупным технологическим компаниям и Уолл-стрит."

Larry Fink,
исполнительный директор BlackRock

"В сфере цифровых активов происходят очень интересные события. На многих развивающихся рынках - таких как Индия, Бразилия и некоторые страны Африки - мы наблюдаем значительный прогресс в области цифровых платежей, снижающий затраты и способствующий расширению доступа к финансовым услугам. Напротив, многие развитые рынки, включая США, отстают в инновациях, в результате чего стоимость платежей значительно возрастает."

Lloyd Blankfein,
генеральный директор Goldman Sachs

"Все еще размышляю о Bitcoin. Нет мнения - не одобряю и не отвергаю. Знаю, что люди также скептически отнеслись, когда бумажные деньги вытеснили золото."

Виталик Бутерин,
сооснователь Ethereum

"В то время как большинство технологий склонны автоматизировать работников на периферии, выполняющих рутинные задачи, блокчейн автоматизирует центр. Вместо того чтобы лишить таксиста работы, блокчейн лишает работы Uber и позволяет таксистам работать с клиентом напрямую."

Bill Gates,
основатель Microsoft

"Биткоин - это технологическое совершенство."

Разрушаем мифы

Концепция блокчейна и криптовалют не проста для понимания, и потому вокруг этих понятий возникло много мифов. Ниже мы разберем наиболее распространенные из них.

Миф	Как на самом деле
 **Блокчейн и криптовалюты – это пирамида**	Такое мнение распространено среди аудитории, которая не знакома с практическими примерами применения. Блокчейн - это технология с большим количеством сфер применения. 86 компаний из списка 100 крупнейших публичных компаний уже используют блокчейн в своей деятельности. Среди них Apple, Alibaba, McDonalds. Более того, центральные банки около 100 стран анализируют возможности реализации цифровых валют на базе этой технологии.
 **Блокчейн – это биткоин**	Многие считают, что криптовалюты, такие как биткойн, это то же самое, что и блокчейн. На самом деле, это не так. Блокчейн – это технология, которая делает существование биткойна возможным. Как двигатель запускает в действие автомобиль.
 **Блокчейн являетя полностью анонимным**	На самом деле, это не так. Действительно, чтобы совершать транзакции в публичной сети блокчейна, не нужно подтверждать личности и показывать паспорт.Однако, все транзакции в блокчейне хранятся в общедоступном реестре, каждый участник имеет возможность ознакомиться с информацией о всех транзакциях и убедиться в ее корректности. Отследить цепочку платежей и выйти на конечного пользователя при должном желании и наличии навыков не составит больших проблем.
 **В крипте много мошенников и нелегальной деятельности**	Это мнение также ошибочно и строится на предыдущем мифе о том, что в сети соблюдается полная анонимность. По данным аналитической платформы Chainalysis доля преступных транзакций в 2022 году составила лишь 0,24% в общем объеме транзакций на блокчейне.
 **Майнинг биткоина загрязняет планету**	В действительности 60% биткойнов добывается за счет источников возобновляемой энергетики. Компании, занимающиеся майнингом криптовалют в промышленных масштабах, сконцентрированы в основном в регионах с развитой инфраструктурой возобновляемой энергетики: в канадском Квебеке, где имеется доступ к дешевой гидроэнергетике, и в Техасе, где развита ветряная энергетика. Китайские майнеры сконцентрированы в регионах с развитой гидро- и солнечной энергетикой. Также высока активность криптомайнеров в Исландии и Швеции, где тоже развита возобновляемая энергетика.

Базовые понятия

В этом разделе мы рассмотрим базовые понятия и историю зарождения блокчейна, а также его основные преимущества.

Что такое блокчейн? Блокчейн – от англ. «block» и «chain» – цепочка блоков. Они содержат информацию и связаны друг с другом хронологически. Новый блок создается каждый раз, когда добавляется новая информация или вносятся изменения. Информацию, которая хранится в блокчейне, невозможно удалить или подделать. Это обеспечивается благодаря тому, что «цепочка» блоков принадлежит не конкретному лицу или компании, а сразу всем участникам системы. Каждый может присоединиться к системе и стать ее хранителем.

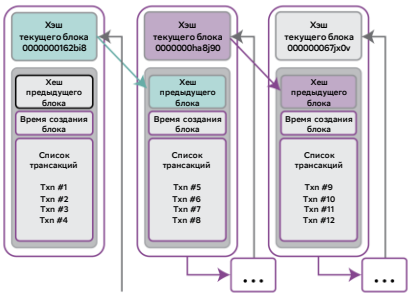
Блокчейн можно сравнить с большим ежедневником, в который записывают все важные события. Собственников этого ежедневника огромное множество, и все они хранят его постоянно обновляемую копию. Если одну из копий испортят, другие собственники помогут восстановить всю историю. Прежде чем добавить новую запись, ее должно подтвердить большинство.

Таким образом, блокчейн – это электронная база данных, состоящая из серии последовательных неизменяемых блоков. Отличительной особенностью такой базы данных является децентрализация.

Зачем нужен блокчейн? Блокчейн облегчает процесс регистрации транзакций и отслеживания активов. Активы могут быть материальными (дом, автомобиль, деньги, земля) или нематериальными (интеллектуальная собственность, патенты, авторские права). Практически все, что имеет ценность, можно отслеживать и обменивать в блокчейне. Например, отслеживать заказы, платежи, счета, производство и многое другое. Поскольку у всех участников сети есть общая одинаковая информация («картина истины»), они могут видеть все детали транзакции от начала до конца, что дает больше уверенности.

Какие бывают блокчейны? Блокчейны классифицируют по доступу к данным: публичные, частные и консорциумные. Рассмотрим каждый из типов подробнее.

Составляющие блока блокчейна



Источник: Nakamoto S., A Peer-to-Peer Electronic Cash System

Что такое хэширование?

– это процесс преобразования произвольного объема данных по определенному алгоритму в строку фиксированного размера.

Преимущества каждой из описанных моделей

	Тип блокчейна		
	Публичный	**Частный**	**Консорциумный**
Общедоступный?	Да	Нет	Нет
Кто видит историю транзакций?	Кто угодно	Только приглашенные пользователи	Зависит от правил каждого конкретного блокчейна
Кто может согласовывать транзакции?	Кто угодно	Только авторизованные участники	Только авторизованные участники
Владелец	Никто	Одна организация	Несколько организаций
Известны участники (узлы)?	Нет	Да	Да
Скорость транзакций	Низкая	Высокая	Высокая

Источник: SberCIB

Публичные (открытые) блокчейны – базовый вид блокчейна, который управляется децентрализованно. К ним относятся биткойн, эфириум, а также сотни других блокчейнов с открытым исходным кодом. Любой пользователь может присоединиться к публичному блокчейну.

При этом существуют блокчейны, которые создаются, контролируются и поддерживаются центральным органом. Они называются **частными.** Частные блокчейны имеют несколько фиксированных участников, и к ним нельзя присоединиться без авторизации центральным органом. Такие блокчейны разрабатываются корпоративным сектором. Централизация позволяет значительно снизить комиссии в сети и увеличить скорость подтверждения транзакций. Частные блокчейны используются в тех случаях, когда критично соблюдение требований комплаенса и высокого уровня конфиденциальности. К таким сценариям использования относятся:

- финансовые услуги,
- здравоохранение,
- сделки с недвижимостью,
- управление цепочками поставок,
- страхование,
- розничная торговля,
- международная торговля,
- государственные сервисы.

Однако и у частных, и у публичных блокчейнов есть недостатки: одни требуют больше времени и ресурсов для верификации транзакций, другие подвержены рискам мошеннических действий со стороны единого органа управления. Для преодоления этих недостатков были созданы **консорциумные блокчейны.** Они сочетают в себе преимущества обоих типов блокчейнов. Такие блокчейны управляются несколькими организациями, которые работают вместе в качестве консорциума. В консорциумной сети валидаторами выступают несколько одинаково влиятельных сторон. Такие системы наиболее эффективны в ситуации, когда нескольким организациям из одной отрасли необходима общая база для проведения транзакций или передачи данных. Наиболее частые сценария использования здесь такие же, как и у частных блокчейнов.

С чего все началось? Способ записи и отслеживания информации в блокчейне стал революционным. Однако эта новая технология основана на базе открытий, которым уже несколько десятков лет.

Идея, которая легла в основу прорывной технологии, зародилась еще в 1991 году. Тогда двое ученых Стюарт Хабер и Уэйкфилд Скотт Сторнетта описали использование цепочки криптографически защищенных блоков со штампом времени, который служил защитой от подделки или изменения содержимого задним числом. В этом виде технология не получила распространения, и в 2004 году, за 4 года до создания биткойна, патент на него истек.

В октябре 2008 года неизвестная личность или группа людей под псевдонимом Сатоши Накомото опубликовала документ, положивший начало эпохе блокчейна. В нем были описаны основные аспекты первого и самого известного на сегодняшний день блокчейна – биткойна. 3 января 2009 года Сатоши Накомото добыл первый блок, за который получил вознаграждение в размере 50 BTC. Первая транзакция произошла уже 12 января, когда основатель биткойна перевел 10 BTC криптографу Хэлу Финни. В 2010 состоялась первая покупка за биткойн: американец купил две пиццы Papa John's за 10 тыс. BTC (по текущему курсу это около $260 млн). На 14.06.2023 в сети биткойн создано 794 тыс. блоков и подтверждено свыше 851 млн транзакций.

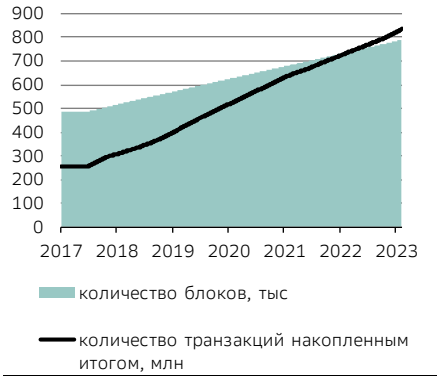
Биткойн был создан как альтернатива фиатным валютам, выпуск которых контролируется государством (доллар, рубль, евро и др.). Он создавался с целью предоставить пользователям возможность совершать платежи напрямую, без посредников, таких как банки и платежные системы. Первая криптовалюта и блокчейн не случайно появились именно в 2008 году, когда произошел мировой финансовый кризис. Он выявил риски, связанные с традиционной банковской системой, и подорвал доверие к ней.

С момента изобретения первого блокчейна технология стремительно развивалась и набирала популярность. Переломным моментом стало появление в 2014 году блокчейна второго поколения – эфириум. Его отличительной особенностью стала поддержка полноценного языка программирования, с помощью которого можно написать алгоритм (смарт-контракт) под любую задачу. Таким образом, эфириум – первый программируемый блокчейн общего назначения. Вычисления в сети эфириум выполняются на Ethereum Vitrual Machine (EVM), аналоге мирового децентрализованного виртуального компьютера. Любой разработчик может использовать мощности этого компьютера и написать собственную программу. Благодаря этому на базе эфириума появились децентрализованные приложения, возможность выпускать токены, в том числе NFT. Более подробно о EVM, применении смарт-контрактов и принципах работы децентрализованных приложений мы рассказывали в обзоре «Web 3.0. Каким будет интернет будущего?».

Почему технология блокчейн заслуживает внимания? Этот сектор становится слишком большим, чтобы его игнорировать. Блокчейн может совершить переворот в большинстве отраслей. На финансовом рынке уже происходит революция. В таких секторах, как недвижимость, торговля и здравоохранение этот процесс идет медленнее, но он уже запущен.

По данным CoinMarketCap, совокупная капитализация криптовалют превышает $1 трлн. Криптовалюты – это лишь одно из применений блокчейна. По оценке Citigroup, к 2030 году рынок цифровых активов может привлечь до $5 трлн новых средств. Основными драйверами роста будут рост популярности стейблкойнов, внедрение цифровых валют центральных банков (CBDC) и токенизация реальных активов. Для сравнения, совокупная капитализация всех компаний на Гонконгской фондовой бирже, которая является седьмой по капитализации в мире, составляет $5 трлн.

Блокчейн биткойн состоит из более чем 794 тыс. блоков, которые содержат 851 млн транзакций



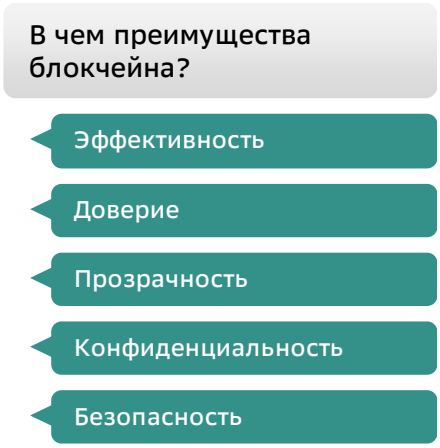
Источник: CryptoCompare, SberCIB

История развития технологии блокчейн

Источник: SberCIB

В чем преимущества блокчейна для обычного пользователя или бизнеса?

- **Эффективность.** Блокчейн позволяет сократить время и расходы на обработку транзакций благодаря отсутствию посредников.
- **Доверие.** Пользователи могут доверять информации в блокчейне, поскольку ее невозможно, изменить и фальсифицировать.
- **Прозрачность.** Вопреки распространенному мнению, транзакции в блокчейне не являются анонимными. В публичном блокчейне все транзакции хранятся в общедоступном реестре, каждый участник может ознакомиться с информацией о всех транзакциях и убедиться в ее корректности.
- **Конфиденциальность.** Хотя пользователь может отследить все транзакции, у него нет возможности идентифицировать получателя или отправителя информации.
- **Безопасность.** Блокчейн создает защищенную среду для хранения и передачи данных. Каждая транзакция в блокчейне защищена криптографией.



Анатомия блокчейна

В этом разделе мы познакомим читателя с концепциями блокчейна, которые позволят получить глубокое понимание технологии.

В основе каждого блокчейна лежит набор правил, определяющий, как его участники («ноды») приходят к общему мнению насчет источника истины (консенсус) в глобальной распределенной сети.

Нода (от лат «nodus» – узел)– это подключенный к блокчейну компьютер или сервер, который обменивается информацией о блоках и транзакциях с другими участниками.

Чем больше узлов поддерживают блокчейн, тем более защищенным и децентрализированным он является. Например, сеть биткойн поддерживает более 17 тыс. участников, и это число постоянно растет.

И хотя все ноды в сети равноправны, они могут выполнять разные функции. Так, например, в блокчейне биткойн ноды выполняют 4 функции:

- маршрутизация
- хранение базы данных блокчейна
- майнинг
- обслуживание кошельков.

Есть также и «полные» ноды, которые совмещают все четыре функции.

Таким образом, нода– это важнейший участник системы, который поддерживает работоспособность сети. Каждый раз, когда в блокчейне проводится транзакция, запись о ней сохраняется и отправляется на проверку на каждую ноду в сети. Чтобы транзакция была добавлена в блок, все узлы должны прийти к единому мнению относительно правомерности транзакций, то есть достичь консенсуса.

Методы достижения консенсуса устанавливают правила, которым должны следовать узлы. Методы консенсуса в блокчейне должны гарантировать, что все участники сети смогут договориться о едином источнике «истины», даже если некоторые узлы выйдут из строя.

Наиболее распространенные методы достижения консенсуса – консенсус Накамото и алгоритм pBFT (практическая византийская отказоустойчивость).

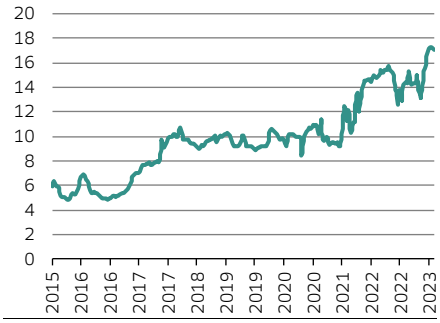
В протоколах консенсуса Накамото узлы приходят к консенсусу вокруг самой длинной цепочки. Окончательность транзакций в таких сетях всегда является «вероятностной», поскольку вероятность отмены транзакции уменьшается по мере увеличения длины цепочки. Например, большинство участников сети обычно ждут шести подтверждений в сети биткойн, чтобы окончательно убедиться в подтверждении транзакции. Транзакция получает очередное подтверждение каждый раз, когда блок добавляется в цепь.

Что такое нода (узел)?

– это подключенный к блокчейну компьютер или сервер, который обменивается информацией о блоках и транзакциях с другими участниками.

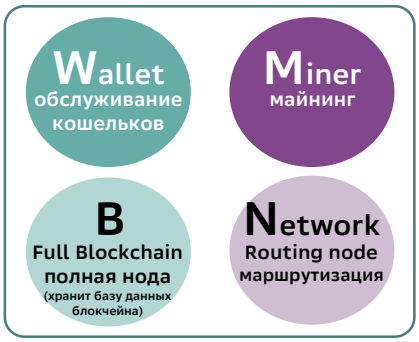
– это важнейший участник системы, который поддерживает работоспособность сети.

Динамика количества нод в сети биткойн, тысяч



Источник: coin.dance

Четыре функции нод в сети биткойн



Источник: Mastering Bitcoin

Транзакции в сетях типа pBFT являются «детерминированными». В них правила определяют, кто может голосовать по транзакции, и сколько именно голосов необходимо, чтобы все согласились с тем, что транзакция завершена на 100%. Как только транзакция достигает окончательности, более длинная цепочка существовать не может.

Одной из основных функций методов является предотвращение атак Sybil.

Атака Sybil – это атака на блокчейн, при которой небольшое количество субъектов пытается взять под контроль всю сеть, используя несколько узлов или компьютеров, чтобы добиться подавляющего влияния на сеть. Наиболее известная атака Sybil – «атака 51%», когда злоумышленники захватывают большую часть вычислительной мощности сети. В таких случаях они теоретически могут влиять на порядок транзакций, предотвращать подтверждение новых транзакций и дважды тратить свои криптоактивы.

Механизмы защиты от атак Sybil – это факторы, которые стимулируют узлы сети к честному поведению и одновременно препятствуют недобросовестным участникам. Суть подобных механизмов заключается в том, чтобы каждый узел сети имел личную заинтересованность в добросовестном подтверждении транзакций посредством:

- поощрения участников к достижению консенсуса,
- награды за подтверждение блоков и комиссий за транзакции,
- наказания недобросовестных участников потерей денежных средств, ресурсов или репутации.

Чаще всего для защиты от Sybil атак используются механизмы Proof-of-Work (PoW) и Proof-of-Stake (PoS). PoW и PoS – экономические сдерживающие факторы для атак Sybil, поскольку они требуют от пользователей затрат энергии или залога для участия в валидации сети.

- **Proof-of-Work или PoW (доказательство работы) –** алгоритм подтверждения транзакции, основанный на решении математических задач с использованием вычислительных мощностей компьютеров-майнеров. Мощные компьютеры соревнуются в том, кто первым подтвердит серию транзакций, называемую блоком, и добавит блок в блокчейн. Чем больше вычислительная мощность, тем выше вероятность добычи блока. Тот, кто первым решит криптографическую задачу, получает вознаграждение за добытый блок. Наиболее известный блокчейн, который использует этот алгоритм – биткойн. Сейчас вознаграждение за добытый блок в этой сети составляет 6,25 BTC (по курсу на 14.06.2023 – около 13 млн руб.). Вознаграждение сокращается вдвое примерно каждые четыре года (этот процесс называется «халвинг» – halving). Последний раз халвинг BTC произошел в 2020 году.
- **В Proof-of-Stake или PoS (доказательство доли владения)** транзакции проверяют не майнеры, а так называемые валидаторы — лица, которые внесли залог в виде криптовалюты в специальный пул. Если в блокчейн будет записан неправильный блок, они потеряют свои средства. Эфириум – наиболее известный блокчейн с использованием этого алгоритма.

Что такое консенсус?

это способ разрешения конфликтов при принятии решений

Методы достижения консенсуса устанавливают правила, которым должны следовать узлы

Какие существуют методы достижения консенсуса?

Накамото (Nakamoto consensus).

Практическая византийская отказоустойчивость (pBFT).

Что такое механизм защиты от Sybil атак ?

это факторы, которые стимулируют узлы сети к честному поведению и препятствуют недобросовестным участникам.

Какие механизмы защиты от Sybil атак наиболее распространенные?

Proof-of-Work или PoW (доказательство работы).

Proof-of-Stake или PoS (доказательство доли владения).

PoW и PoS выбирают автора блока и защищают от атак Sybil, но сами по себе не описывают метод консенсуса блокчейна. Вместо этого метод консенсуса сочетает в себе механизм защиты от Sybil и правило выбора цепочки, которое определяет, какая версия блокчейна является достоверной.

Механизмы устойчивости к атакам Sybil совместимы с различными методами консенсуса.

Другое важное определение для понимания работы блокчейна – **метод учета транзакций.**

В блокчейнах есть две модели учета транзакций: модель UTXO (выход неизрасходованных транзакций) и модель, основанная на счетах (account based model).

В блокчейнах есть две модели учета транзакций:

- модель UTXO (аналог расчета наличными)
- модель, основанная на счетах (аналог банковских счетов)

В модели UTXO транзакции создаются путем расходования существующих UTXO и создания вместо них новых.

Биткойн – самый известный блокчейн, который использует эту модель записи транзакций.

Каждый UTXO можно сравнить с купюрой или монетой. Если у вас есть 1 тыс. руб. наличными, то возможно несколько разных комбинаций: одна купюра в 1 тыс. руб., десять купюр по 100 руб., две купюры по 500 руб. и так далее.

В каждом из этих случаев, несмотря на разное количество купюр, у вас всегда будет ровно 1 тыс. руб. Когда пользователь видит единый баланс в своем криптокошельке, на самом деле он видит сумму всех UTXO, которую код криптокошелька просуммировал для удобства пользователя.

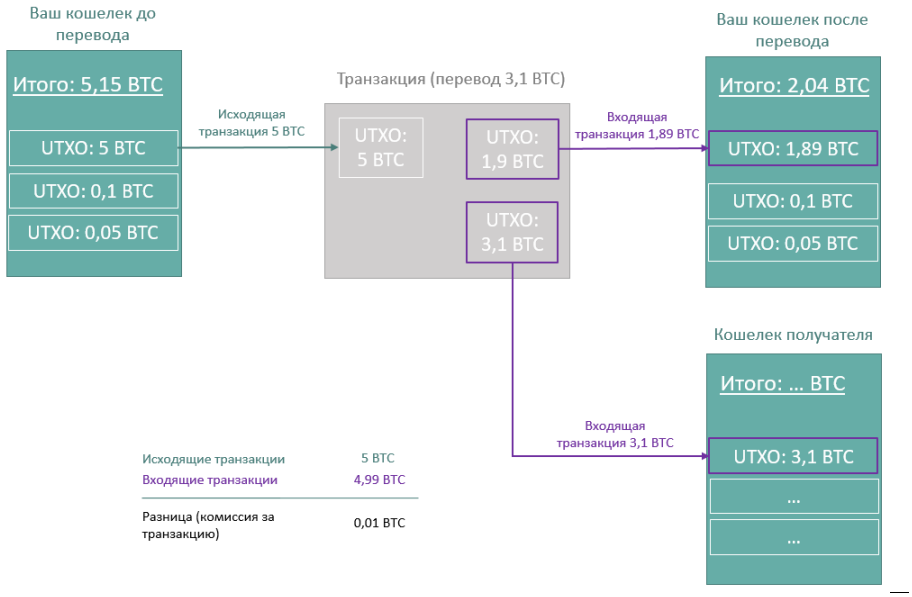
Как и купюры, UTXO не могут быть разделены. Возьмем для примера покупку чашки кофе, которая стоит 300 руб. Если у вас в кошельке только купюра 500 руб., вы должны сначала переплатить (отдать 500 руб.) и получить сдачу – в данном случае 200 руб.

UTXO работают аналогичным образом. Вы не можете оторвать часть от купюры в 500 руб., чтобы заплатить за кофе, и точно так же не можете отправить часть UTXO. В отличие от физических банкнот и монет, UTXO не имеют стандартных номиналов. В UTXO может храниться любое количество биткойна.

Представим, что вы хотите отправить кому-то 3,1 BTC, но на вашем кошельке только три UTXO стоимостью 5 BTC, 0,1 BTC и 0,05 BTC. В этом случае ваш кошелек отправит получателю UTXO стоимость 5 BTC, а затем вернет сдачу, как при оплате наличным. Однако, в отличие от операций с наличными, в качестве сдачи вам вернется меньшая сумма, за вычетом комиссии за транзакцию. Размер комиссии не отражается в транзакции как отдельная запись. Комиссией будет разница между суммой входящих и исходящих транзакций. Зачем нужны такие комиссии и от чего зависит их размер, мы разберем в разделе про транзакции.

Таким образом, при переводе получатель получит 3,1 BTC, а оставшиеся 1,89 BTC «сдачи» за вычетом комиссии (для примера – 0,01 BTC) будут отправлены обратно на ваш адрес в виде нового, более мелкого UTXO.

Схема транзакции в UTXO модели блокчейна



Источник: SberCIB

Модели, основанные на счетах, проще, чем модели UTXO. Их можно рассматривать как аналог банковских счетов. При переводе средств от одного пользователя к другому баланс счета отправителя уменьшается на сумму транзакции, а получателя – увеличивается на эту же величину.

Примеры блокчейна с использованием этой модели – эфириум и большинство альтернативных сетей, поддерживающих смарт-контракты.

В модели на основе счета, в отличие от UTXO, остатки могут быть частично потрачены. Например, если у вас есть 5 ETH, вы можете отправить кому-то 3 ETH прямо со своего счета, и в результате этой транзакции у вас останется 2 ETH, а у другого человека – 3 ETH. Вам не нужно отправлять полные 5 ETH, а затем получать «сдачу» в размере 2 ETH, как это в цепочке UTXO.

Преимущества каждой из описанных моделей

	UTXO-модель	Модель, основанная на счетах
проще для разработчиков		●
обеспечивает большую конфиденциальность	●	
возможно ли отследить историю каждой "монеты"?	●	
более масштабируема		●
более защищена от атак с двойным расходованием средств	●	

Источник: SberCIB

Для понимания технологии важно разобрать еще один момент – **комиссии за транзакции.** Они являются неотъемлемой частью большинства блокчейнов. Пользователь сталкивается с необходимостью платить каждый раз, когда он отправляет или обменивает криптовалюту, а также при взаимодействии со смарт-контрактами.

Зачем они нужны? Плата за транзакции в блокчейне необходима, поскольку это стимулирует майнеров подтверждать транзакции и предотвращает спам-атаки. Если бы транзакции в блокчейне были бесплатны,

злоумышленники могли бы угрожать ее работоспособности, наводняя сеть транзакциями.

Сейчас майнеры получают вознаграждение в двух формах: за добытый блок и от комиссий за транзакции. В сети биткойна доход от комиссий на текущий момент несущественный, однако к 2140 году, когда будет добыт последний биткойн, комиссии станут единственным источником мотивации майнеров.

От чего зависит размер комиссии и почему они могут быть очень высокими? В блокчейне биткойна стоимость транзакции зависит от загруженности сети и размера транзакции в байтах. То есть сети неважно, переводите вы $10 или $1 млн, – комиссия для обеих транзакций, скорее всего, будет одинаковой. Для сети важно, сколько «весит» транзакция. Чем больше UTXO необходимо объединить для перевода, тем транзакция дороже будет. Если на кошелек поступали небольшие суммы, например, 10 UTXO по 0,01 BTC, то для оплаты покупки стоимостью 0,1 BTC, сети необходимо будет объединить все 10 UTXO. Если же на счете был UTXO стоимостью 1 BTC, то для оплаты той же покупки пользователь заплатит значительно меньшую комиссию.

Средний размер комиссии в блокчейнах эфириум и биткойн

Источник: bitinfocharts.com

В блокчейне эфириум плата за транзакцию зависит от вычислительных мощностей EVM, которые необходимо задействовать для выполнения операции. Чем сложнее транзакция, тем дороже она будет стоить.

При этом в обоих типах блокчейнов, помимо технических параметров транзакции, на размер комиссии влияет загруженность сети. Если в сети совершается большое количество транзакций, то приоритетность их добавления в блок зависит от размера комиссии, которую пользователь выставил за обработку своей транзакции. В периоды высокой нагрузки на сеть стоимость транзакций может быть довольно высокой. Например, в периоды пиковых нагрузок медианная комиссия в сети эфириум достигала $200, в сети биткойн – $60.

Как оплачивается комиссия? У каждого блокчейна есть собственный нативный токен. Он представляет собой криптовалюту, которая используется для оплаты комиссий в сети и управления. Кроме того, майнеры (или валидаторы) получают вознаграждение за поддержку сети именно в нативной валюте блокчейна. Чем более востребована сеть, тем дороже должен стоить ее нативный токен.

Для сети биткойна нативная монета – биткойн (BTC), для эфириума – эфир (ETH). Однако название нативного токена не всегда соотвествует названию блокчейна. Например, в блокчейне Cardano нативным токеном является ADA, а в сети Polygon – MATIC.

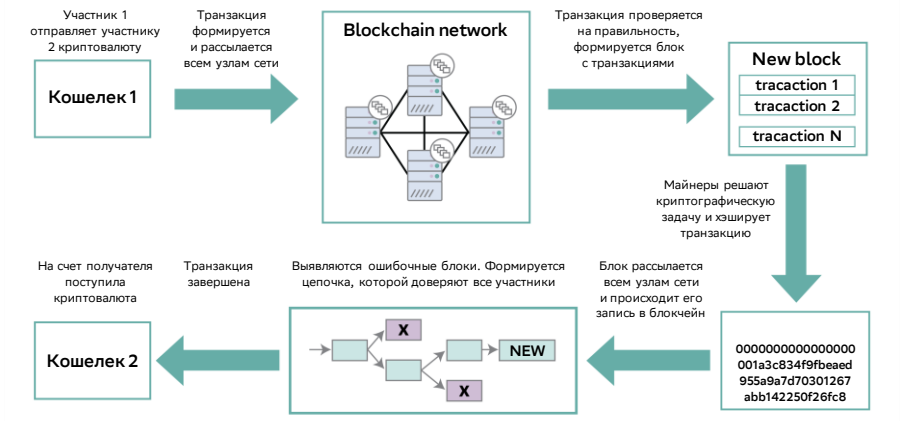
После знакомства с основными понятиями разберем механизма работы блокчейнов.

Этот процесс упрощенно выглядит следующим образом:

- Когда пользователь совершает транзакцию, она зашифровывается для повышения безопасности.
- Ноды проверяют транзакцию на безопасность и отсутствие попыток атаковать сеть.

- Далее транзакция добавляется в мемпул (от англ. «memory pool») – своего рода «зал ожидания» для транзакций перед добавлением в блок.
- Майнеры обрабатывают транзакции из мемпула и добавляют их в блок. Приоритетность добавления транзакций в блок зависит от размера комиссии, которую пользователь выставил за обработку транзакции.
- Далее блок рассылается всем узлам сети для верификации транзакций, которая осуществляется путем достижения консенсуса участниками данной сети.
- Как только блок будет верифицирован, он получит место в цепи. При этом транзакция, которую совершил пользователь, будет выполнена.

Схема работы блокчейна



Источник: SberCIB

Трилемма блокчейна и способы ее решения

Блокчейн обладает тремя ключевыми характеристиками: децентрализацией, безопасностью и масштабируемостью. Эти характеристики взаимосвязаны, и у большинства блокчейнов на высоком уровне находятся только две из них. Усиление одной характеристики приводит к ослаблению другой. Эта проблема называется **трилеммой блокчейна:** децентрализованной системе почти невозможно одновременно достичь одинаково высоких уровней для всех трех показателей.

Рассмотрим отдельно каждую из характеристик.

Децентрализация. Виталик Бутерин, основатель блокчейна эфириум, в статье «Смысл понятия “децентрализация”» выделил три основных формы децентрализации:

- **Архитектурная:** из какого количества компьютеров («нод» или «узлов») состоит система? Сколько из этих компьютеров могут выйти из строя в любой момент времени?
- **Политическая:** сколько человек или организаций контролируют компьютеры, из которых состоит система?
- **Логическая:** если разделить систему пополам, включая как провайдеров, так и пользователей, будут ли обе половины продолжать работать как независимые единицы?

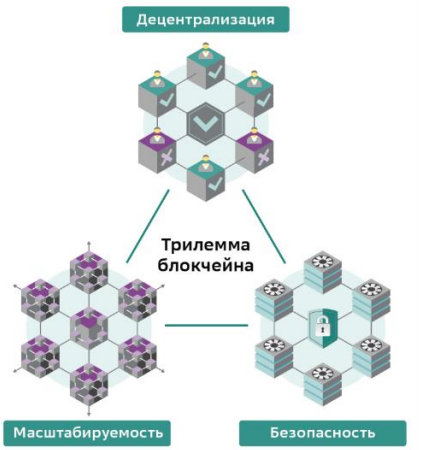
Например, традиционные корпорации централизованы политически (один генеральный директор), архитектурно (один головной офис) и логически (их нельзя разделить пополам).

Примером логической децентрализации являются языки. Носители любого языка следуют грамматическим правилам и используют оптимальные способы пользоваться языком, несмотря на отсутствие централизованного органа, который бы следил за тем, чтобы люди говорили определенным образом. Языки развиваются со временем, их структура и характер зависит от места и времени, в котором на них говорят.

В случае с блокчейном ни один человек не имеет единоличного контроля, то есть присутствует политическая децентрализация. Кроме того, инфраструктура блокчейна не имеет центральной точки отказа, из-за которой может произойти сбой во всей системе, поскольку каждый узел хранит свою копию блокчейна. Таким образом обеспечивается архитектурная децентрализация. Однако, блокчейн централизован логически, так как система ведет себя как один компьютер, несмотря на то, что она распределена по всем участвующим узлам сети.

Как можно измерить уровень децентрализации? Оцифровать уровень децентрализации блокчейнов пытается компания Input Output Global, которую возглавляет Чарльз Хоскинсон, основатель блокчейна Cardano, в партнерстве с Эдинбургским университетом. Они разрабатывают первый в индустрии блокчейна индекс децентрализации EDI. Ин-

Трилемма блокчейна

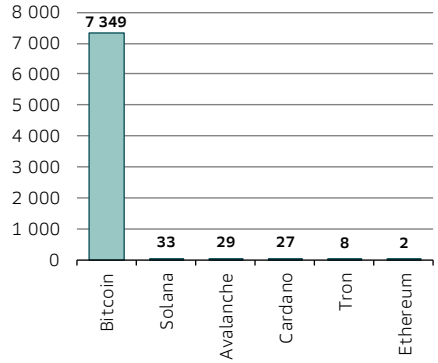


Источник: SberCIB

декс будет учитывать 8 категорий параметров, в числе которых географическое распределение узлов, концентрация нативного токена блокчейна на кошельках пользователей и даже количество производителей майнингового оборудования. На основе полученных результатов будет составлен рейтинг децентрализации для каждого блокчейна.

Пока наиболее оптимальный способ количественно оценить уровень децентрализации блокчейна – это коэффициент Накамото. Он определяется количеством операторов узлов, которые вместе контролируют более 33% всей доли в сети. Этого количества достаточно для нарушения работы сети блокчейна. Высокий коэффициент Накамото означает, что для атаки на блокчейн нужно подкупить больше участников. Таким образом, блокчейн с высоким коэффициентом Накамото более децентрализован. Самым децентрализованным блокчейном по этому параметру является биткойн.

Биткоин – самый децентрализованный блокчейн по коэффициенту Накамото



Источник: nakaflow.io, расчет SberCIB

Безопасность. В блокчейн сетях очень низкая вероятность случайных сбоев. В случае отключения одного или нескольких узлов сети система продолжит работу, если продолжит функционировать хотя бы один узел.

Кроме того, блокчейн более устойчив к атакам, так как сети распределены между большим количеством компьютеров. Чтобы осуществить атаку, злоумышленнику потребуется намного больше средств и вычислительных ресурсов, чем в централизованной системе.

Наконец, участникам децентрализованных систем гораздо труднее сговориться для осуществления мошеннических транзакций.

Масштабируемость – это способность сети обрабатывать растущий объем транзакций. Масштабируемость блокчейна измеряется количеством транзакций, которое может обработать система за секунду (TPS), скоростью совершения транзакции.

Способность блокчейнов обрабатывать большое количество транзакций – основная проблема безопасных и децентрализованных сетей.

Например, в сети биткойн обрабатывается около 7 транзакций в секунду, в сети эфириум – около 15 транзакций. Для сравнения, платежная система Visa может обрабатывать 20 тыс.транзакций в секунду. Это связано с тем, что и биткойн, и эфириум отличаются высокой степенью децентрализации и безопасности. В таких сетях часто сложно достичь высокой пропускной способности по мере увеличения базы пользователей и числа транзакций. У централизованных платежных систем, таких как Visa, Mastercard или МИР, скорость обработки транзакций значительно выше благодаря их закрытости и отсутствию публичных нод и консенсуса.

Однако это не значит, что блокчейны не могут соревноваться с платежными системами по скорости обработки транзакций. На текущий момент существует целый ряд решений масштабируемости блокчейн- сетей без значительных потерь в уровнях безопасности и децентрализации. Такими решениями являются шардинг, блокчейны второго уровня, роллапы, сайдчейны, платежные каналы и даже смена алгоритма подтверждения транзакций.

Чтобы перейти разбору решений трилеммы блокчейна, рассмотрим основные уровни блокчейнов.

Что такое L0, L1, L2 и L3 и зачем они нужны? В индустрии криптоактивов используют концепцию слоев. Этот род категоризации блокчейнов необходим участникам отрасли для понимания, как проект может дополнять или входить в общую экосистему в криптоиндустрии.

Level 0 уровень (L0). Разработки нулевого слоя помогают блокчейнам взаимодействовать друг с другом, позволяют передавать активы между разными блокчейнами, а также разрабатывать одно приложение сразу на нескольких блокчейнах. Они создают возможность проведения быстрых и дешевых транзакций на кроссчейн-биржах (это возможно благодаря коммуникационным протоколам, которые можно использовать в L0-сетях). К блокчейнам нулевого уровня относятся Cosmos и Polkadot.

Level 1 уровень (L1). Блокчейн первого уровня – это базовый блокчейн, который самостоятельно обрабатывает и финализирует транзакции в собственной сети без участия другой сети. Примеры блокчейнов первого уровня – биткойн, эфириум, BNB Smart Chain, Tron, Cardano и прочие.

Именно для блокчейнов первого уровня актуальна трилемма блокчейна. При этом в последнее время появилось новое поколение блокчейнов первого уровня, которые заявляют о решении проблемы масштабируемости на базовом уровне. К ним можно отнести Solana, Aptos, Near.

Level 2 уровень (L2). Второй слой – это преимущественно внешние интеграции с первым уровнем, которые могут разрешать одну из проблем трилеммы блокчейна первого уровня. Среди решений второго уровня часто встречаются следующие: 1) каналы состояний (state channels), они представляют собой обмен транзакциями вне блокчейна, после чего результат записывается в блокчейн, 2) свертки (rollups) – объединение сразу нескольких транзакций и дальнейшая обработка в сети первого уровня, 3) сайдчейны (sidechains) – гибрид вложенного блокчейна и канала состояния, используемого для обработки значительного количества транзакций одномоментно. Решением второго уровня для биткойна является канал состояния Lightning Network. Для эфириума существует целый ряд таких решений, крупнейшее из них – Polygon.

Level 3 уровень (L3). Третий слой – это уровень, на котором непосредственно размещаются децентрализованные приложения и различные протоколы, которые обеспечивают работу приложений. Среди примеров решений третьего уровня можно отметить Uniswap (децентрализованная биржа). Кроме того, некоторые приложения могут относиться к уровням L2 и L3.

Помимо блокчейнов второго уровня, трилемма решается и на первом уровне, то есть посредством изменения основной сети блокчейна. Такими решениями являются шардинг и смена механизма консенсуса. Разберем их подробнее.

Шардинг – это деление блокчейна на множество мелких сетей (шардов). В такой конструкции каждый шард управляет определенным

Примеры слоев и решений

Уровень	Название
L0	Cosmos Polkadot
L1	Bitcoin Ethereum
L2	Optimist Polygon
L3	Orbs Uniswap

Источник: SberCIB

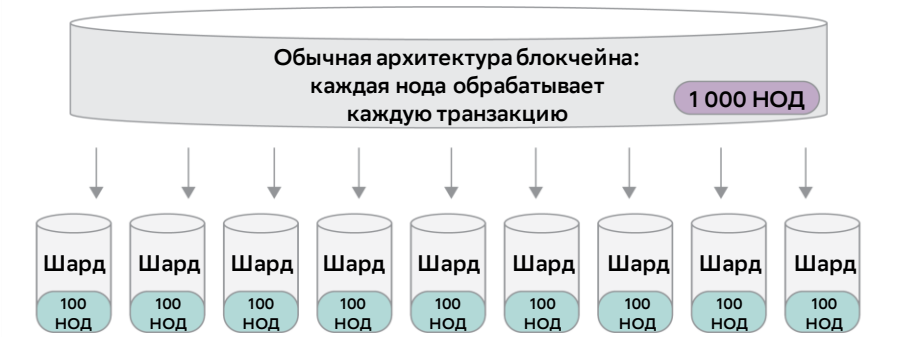
Разные слои в общей экосистеме

Уровень	Место в экосистеме криптоиндустрии
L0	Кроссчейн инфраструктура
L1	Проведение транзакций Решения одной из проблем
L2	Трипеммы блокчейнов
L3	Децентрализованные приложения

Источник: SberCIB

сегментом данных. В отличие от традиционной схемы, где каждая нода отвечает за проверку каждой транзакции в сети, шарды управляют только той частью реестра, к которой они прикреплены. Это позволяет избежать необходимости обрабатывать все транзакции в сети всеми нодами и повышает скорость обработки транзакций.

1000 узлов можно разделить на 10 шардов (по 100 узлов в каждом) для увеличения скорости в 10 раз



Источник: Web3.university

Другое решение трилеммы блокчейна, которое модифицирует основной блокчейн, – это смена алгоритма консенсуса. Proof-of-Work считается наиболее затратным алгоритмом консенсуса, так как он требует мощных компьютеров для решения криптографических задач. Из-за этого в сетях с таким механизмом скорость подтверждения транзакций крайне мала (в сети биткойн обрабатывается до 7 транзакций в секунду). Альтернативный механизм, Proof-of-Stake, не требует большого количества вычислительных мощностей, поэтому считается более эффективным решением.

В погоне за масштабируемостью блокчейн эфириум в сентябре 2022 уже осуществил переход с PoW на PoS года в рамках обновления The Merge. Помимо этого, дорожная карта сети эфириум предполагает внедрение шардинга в рамках следующего обновления The Surge. По словам Виталика Бутерина, основателя эфириум, после этого обновления блокчейн сможет обрабатывать до 100 тыс. транзакций в секунду (сейчас сеть обрабатывает до 15 транзакций в секунду).

Примеры практического применения блокчейна

Применение блокчейна в частном секторе – DeFi, GameFi, NFT, метавселенные, а также ДАО – мы рассматривали в обзоре «Web 3.0. Каким будет интернет будущего?». Теперь мы разберем практические случаи применения блокчейна в корпоративном и государственном секторах. Кроме того, мы рассмотрим, какие блокчейны наиболее популярны в частном и корпоративном секторах.

Интерес компаний к блокчейну растет по мере того, как становятся очевидными возможности применения этой технологии в других областях, помимо криптовалют. Банки, государственные структуры и бизнес активно интересуются применением технологии блокчейн.

По данным Blockdata на август 2022 года, 86 из 100 крупнейших публичных компаний разрабатывали варианты использования блокчейна в своей деятельности. При этом 44 из них уже активно использовали технологию.

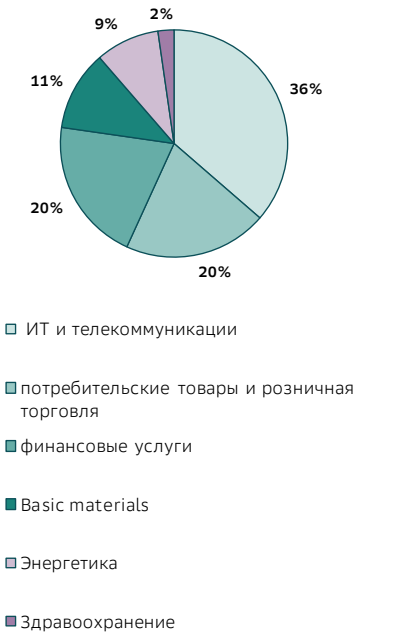
В каких отраслях использование блокчейна наиболее распространено? По данным Blockdata, наиболее активно технологию блокчейн в своей деятельности применяют компании из следующих секторов:

- ИТ и телекоммуникации (Apple, Tencent, SAP, NVIDIA, Intel, Adobe и др.);
- потребительские товары и розничная торговля (Nike, McDonald's, Walmart, L'Oreal и др.);
- финансовые услуги (Mastercard, PayPal, VISA, Bank of America и др.).

В 2022 году еще 40 из 200 крупнейших компаний по версии Forbes объявили об инициативах в области блокчейна. Большинство из них работают в финансовом секторе (19 компаний), в том числе BlackRock, Goldman Sachs, HSBC, BNP Paribas и Сбер.

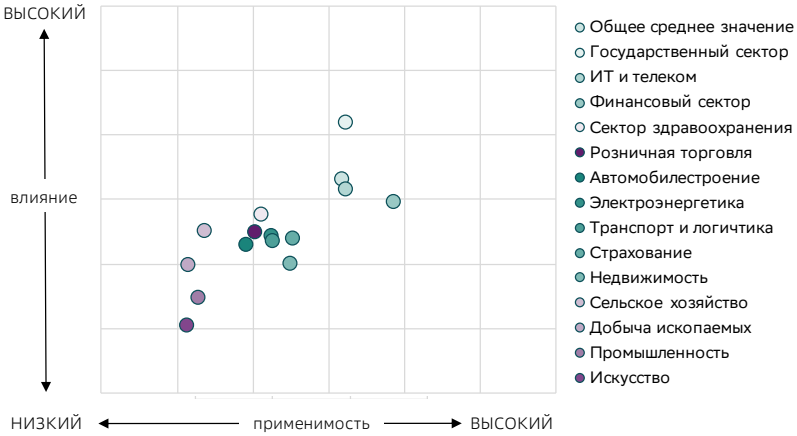
Тот факт, что именно компании финансового сектора начинают наиболее активно применять блокчейн в своей деятельности, не случаен. Согласно исследованию консалтинговой компании McKinsey, в финансовом секторе самые широкие возможности практического применения блокчейна. Кроме того, по мнению McKinsey, внедрение технологии блокчейн окажет наибольшее влияние в государственном и технологическом секторах.

Статистика использования блокчейна по секторам



Источник: Blockdata

Возможности блокчейна в секторах



Источник: McKinsey Digital

Для каких задач бизнес используют блокчейн?

Контроль за цепочками поставок. Компании потребительского сектора и розничной торговли используют блокчейн для повышения прозрачности и отслеживаемости цепочек поставок.

Маркетинг. Компании розничной торговли выпускают эксклюзивные коллекции в форме NFT и продвигают продукцию в метавселенных. Например, Starbucks запустил программу лояльности на базе NFT, а Tiffany выпустила эксклюзивные подвески для держателей популярной коллекции NFT CryptoPunks.

Эксклюзивные подвески от Tiffany для владельцев NFT CryptoPunks

Крупнейшие мировые бренды начали исследовать возможности Web3 с NFT

Источник: "State of crypto 2023" a16zcrypto

Токенизация активов. Это процесс превращения традиционных активов, таких как акции компаний, облигации, золото, недвижимость, в цифровой актив (токен) на блокчейне. Такой токен невозможно подделать благодаря криптографичекой защите.

Предположим, у вас есть дом, который вы хотите продать. Процедура продажи недвижимости сложна и занимает много времени. С помощью токенизации, вы можете создать новый цифровой токен на блокчейне, который будет представлять стоимость вашего дома. Такой токен будет иметь те же свойства актива, что и ваша недвижимость. Отличие в том, что он будет оцифрован на блокчейне, и его можно легко обменять или продать.

Благодаря токенизации такие низколиквидные активы, как недвижимость, могут быть быстро и безопасно куплены или проданы на открытом рынке. Кроме того, токенизация активов позволяет снизить затраты и повысить прозрачность сделок.

Многие финансовые организации видят огромный потенциал для использования блокчейна в этом направлении. Глава подразделения цифровых активов Onyx в JPMorgan на конференции Consensus 2022 представил планы токенизации традиционных активов, таких как казначейские облигации США и фонды денежного рынка. Согласно исследованию Oliver Wyman, 91% институциональных клиентов заинтересован в инвестировании в токенизированные активы.

Аналитики Citigroup считают, что токенизация активов будет способствовать массовому использованию блокчейна. По их мнению, объем рынка токенизированных активов вырастет в 80 раз до $4 трлн к 2030 году. Такой рост станет возможен благодаря тому, что почти все финансовые и реальные активы можно будет токенизировать.

В России токенизация активов происходит в форме цифровых финансовых активов (ЦФА) и регулируется законом №259-ФЗ. Выпускать ЦФА могут только компании из списка ЦБ РФ. На середину апреля в него входило 5 организаций, в том числе Сбер и Альфа-Банк.

Чем интересна токенизация активов? Она ускоряет расчеты, позволяет расширить спектр инструментов для инвестирования и обеспечить инвесторам лучшую диверсификацию, улучшает ликвидность для таких активов как недвижимость. Кроме того, выпускать токенизированные активы существенно дешевле, чем облигации и проводить дорогостоящие IPO.

Государственные и правительственные структуры наряду с центробанками либо уже применяют, либо активно исследуют возможности прикладного использования блокчейна.

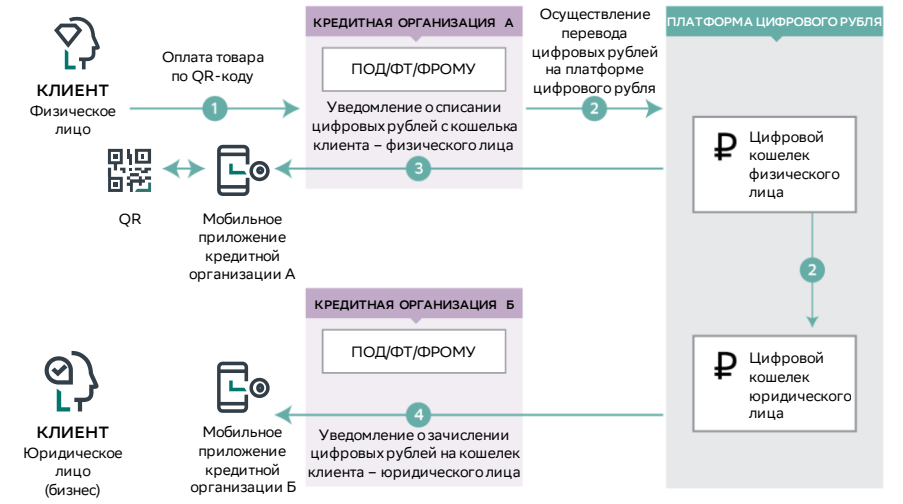
Для каких задач используют блокчейн в государственном секторе?

Цифровые валюты центральных банков

В настоящее время центробанки примерно 100 стран вовлечены в CBDC-проекты, но лишь шесть из них реализовали[1]* проект, а еще около 20 стран находятся на пилотной стадии. Один из последних примеров – объявление МВФ в апреле 2023 о запуске CBDC. На наш взгляд, с учетом растущего спроса на расчеты в локальных валютах при трансграничных транзакциях в условиях санкций использование CBDC имеет наибольший потенциал для использования во внешнеэкономической деятельности. Подробнее о цифровых валютах центральных банков мы рассказывали в криптодайджесте «Встречая новые вызовы» за 4К22.

Глобальный тренд на создание цифровых валют центральных банков затронул и Россию. Закон о цифровом рубле уже рассматривается в Госдуме, а тестирование новой формы валюты планируется начать уже в этом году.

Схема покупки товаров за цифровые рубли



Источник: ЦБ РФ

Цифровая валюта центрального банка, или ЦВЦБ (Central bank digital currency, CBDC)

это новая дополнительная форма платежного средства, которую выпускает центральный банк наряду с безналичной и наличной валютой, и которая равна этой валюте по стоимости

Что такое цифровой рубль?

– это новая, третья, форма рубля. Как наличный и безналичный рубль.

– это обязательство Банка России

Его можно сравнить со стейблкоином, эмитентом которого является не частная компания или алгоритм, а Банк России

[1] **К реализации CBDC (тестовым расчетам по сделкам) уже приступили шесть ЦБ:** Китая, Ямайки, Нигерии, Багамских островов, Камбоджи и Восточно-Карибский ЦБ (центральный банк восьми островных государств Карибского бассейна).

Государства также анализируют возможности использования **блокчейна для защиты персональных данных граждан (цифровая идентичность).**

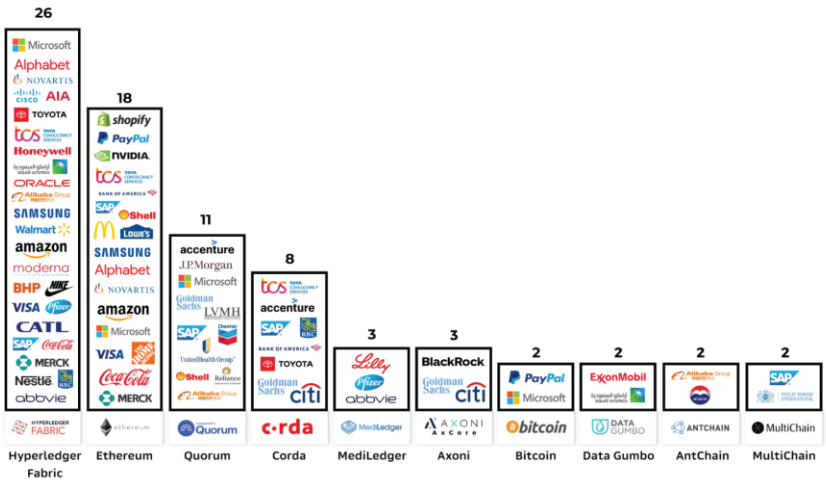
Децентрализованная цифровая идентичность – это способ хранения и использования персональных данных, который основан на использовании технологии блокчейн. В этом случае данные не хранятся, как сейчас, централизованно в одном месте, где они могут быть украдены и использованы злоумышленниками. Кроме того, каждый человек самостоятельно может контролировать, кому и когда передать свои данные.

Есть ли примеры стран, которые уже внедрили цифровую идентификацию на блокчейне? Первой страной в мире, которая выдает цифровые идентификаторы резидента, стало тихоокеанское островное государство Палау. Оно использовало платформу децентрализованной цифровой идентификации RNS.ID, которую разработала кампания Cryptic Labs. Еще один пример – Южная Корея, которая также разрабатывает решения для контроля персональных данных граждан и планирует запустить цифровой паспорт в 2024 году. Частичный функционал и цифровые водительские права на блокчейне доступны в Южной Корее с января 2022 года.

Каковы перспективы цифровой идентификации на блокчейне? Компания cheqd, которая разрабатывает продукты для защиты цифровой идентификации на блокчейне, в 2022 году оценила общий объем рынка децентрализованной идентификации в $550 млрд. По расчетам консалтинговой компании McKinsey, полный охват цифровой идентификацией только в семи проанализированных странах[2] может увеличить их ВВП в 2030 году на 3-13%.

Какие блокчейны они используют? В корпоративном и государственном секторах наибольшей популярностью пользуются частные и консорциумные блокчейны. Это объясняется возможностью ограничивать доступ к чувствительной информации пользователей, что может быть критично для целого ряда отраслей. По данным Blockdata, наиболее популярное решение для корпоративного сектора – блокчейн Hyperledger Fabric, за ним следуют эфириум, Quorum и Corda.

Наиболее популярные блокчейны для корпоративного сектора



Источник: blockdata.tech

Основные преимущества цифрового рубля

Для граждан и бизнеса	1) Операции с цифровым рублем будут проходить по единым тарифам, что позволит снизить издержки на их проведение. 2) Возможность использования без доступа к ИнтернетуВысокий 3) уровень сохранности и безопасности средств
Для государства	1) Контроль за целевым использованием бюджетных средств 2) Потенциал для упрощения проведения трансграничных платежей

Источник: ЦБ РФ

Цифровая идентичность (digital identity)

– это информация о нас в цифровом мире. Она включает в себя все наши аккаунты в социальных сетях, электронные учетные записи на Госуслугах, электронные банковские карты и многое другое. Digital identity может использоваться для аутентификации, то есть проверки личности, для входа в системы и для выполнения других действий в виртуальном пространстве.

[2] США, Китай, Индия, Бразилия, Великобритания, Эфиопия, Нигерия.

Государственный сектор отдает предпочтение Hyperledger Fabric, эфириум и Quorum. Кроме этих блокчейнов, некоторые страны выбирают XRP Ledger от Ripple для внедрения CBDC. К этим странам относятся Черногория, Бутан и Палау. Две страны, Нидерланды и Великобритания, разрабатывали прототипы CBDC на блокчейне биткойн.

Какие блокчейны пользуются популярностью у частных пользователей? За пределами корпораций и государств блокчейн используется в основном для совершения транзакций и финансовых операций (DeFi). По состоянию на середину июня 2023 года на крипторынке было 12 блокчейн-сетей первого уровня с капитализацией нативного токена свыше $1 млрд. Всего капитализация L1 сетей (их около 30) составила примерно $794 млрд, или 72% от капитализации всего крипторынка. При этом на сети биткойн и эфирум приходится соответственно 46% и 19%. Количество L2-блокчейнов гораздо скромнее — всего 13, и только у Polygon и Arbitrum капитализация превышает $1 млрд. Совокупная рыночная капитализация L2-сетей составила $9.5 млрд, или 0.9% от капитализации всего крипторынка. Однако, важно понимать, что не все L2-решения выпускают нативный токен: например, Lightning Network (решение второго уровня для сети биткойн) не имеет своего собственного токена.

Примеры блокчейнов, которые используются для внедрения CBDC

Страна	Блокчейн
Нидерланды	Bitcoin
Великобритания	Bitcoin
Канада	Ethereum, Corda
Сингапур	Hyperledger Fabric
Южная Африка	Quorum
Швеция	Corda
Тайланд	Corda, hyperledger
Гонконг	Corda
Австралия	Ethereum
Черногория	XRP Ledger
Бутан	XRP Ledger
Палау	XRP Ledger

Источник: Blockchain and central bank digital currency – Tao Zhang, Zhigang Huang

Топ-10 L1 сетей по капитализации

Токен	Тикер	Цена, $	Рын. кап., млн $
Bitcoin	BTC	25 987	504,2
Ethereum	ETH	1 746	209,9
BNB	BNB	249	38,8
Cardano	ADA	0,28	9,7
Solana	SOL	15,20	6,1
Polkadot	DOT	4,70	5,8
Avalanche	AVAX	11,90	4,1
Cosmos Hub	ATOM	8,76	2,6
Bitcoin Cash	BCH	106	2,1
Hedera	HBAR	0,05	1,5

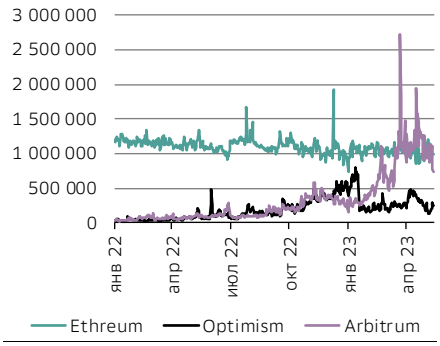
Источник: CoinGeco, по состоянию на 14.06.2023

Топ-10 L2 сетей по капитализации

Токен	Тикер	Цена, $	Рын. кап., млн $
Polygon	MATIC	0,65	6 080
Arbitrum	ARB	1,00	1 275
Optimism	OP	1,15	743
Immutable	XIMX	0,61	613
Loopring	LRC	0,22	270
SKALE	SKL	0,03	113
Coinweb	CWEB	0,03	93
Cartesi	CTSI	0,13	92
Metis	METIS	19,14	83
Boba Network	BOBA	0,14	47

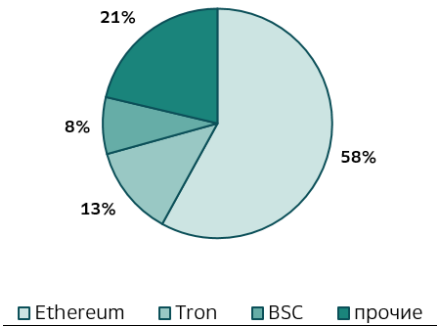
Источник: CoinGeco, по состоянию на 14.06.2023

Объём транзакций в сети Ethreum (L1), Optimism (L2) и Arbitrum (L2)



Источник: обозреватели блоков

Структура TVL в DeFi



Источник: Defillama, по состоянию на 14.06.2023

Объем транзакций L2 увеличивается. Объем транзакций в сети эфириум в прошлом году почти не менялся, поскольку сеть уже работает на полную мощность. Тем временем существенно увеличилось количество транзакций в L2- сетях (крупнейшие — Arbitrum и Optimism): их доля от всех транзакций в начале 2022 года составляла всего 5%, к концу декабря выросла до 46%, а в апреле 2023 года несколько дней достигала более 200%. Решения второго уровня продолжают набирать популярность благодаря низким комиссиям за транзакцию. С начала 2023 года по середину мая Arbitrum в течение 35 дней обрабатывал большее количество транзакций, чем основная сеть эфириум.

Насколько L1 популярны в децентрализованных финансах (DeFi)? В секторе DeFi показатель TVL (Total Value Loked) отражает объем средств, которые пользователи внесли смарт-контракты децентрализованных финансовых проектов. Значимая часть (примерно 94%) TVL – это блокчейны первого уровня. При этом на топ-3 блокчейнов по TVL— эфириум, BSC и Tron (все они относятся к L1) – приходится приблизительно

80% заблокированных средств в DeFi. При этом все большую популярность набирают L2: в период с начала 2023 года по конец апреля их совокупный TVL увеличился на 126% до $9,3 млрд, в то время как TVL L1-сетей вырос только на 45% до $78 млрд. По итогам 2022 года L2-сети тоже показали динамику лучше рынка: их TVL сократился на 41%, а у блокчейнов первого уровня – упал на 75%.

Ограничение ответственности