ПЕТР ЛЕВАШОВ

НОВЫЕ ФИНАНСЫ

БЛОКЧЕЙН, DEFI, WEB3
И КРИПТОВАЛЮТЫ

Петр Левашов

Новые финансы: блокчейн, DeFi, Web3 и криптовалюты

«Питер»
2024

УДК 336.727.:004.738.5
ББК 65.9(2)262.6:32.988.02

Левашов П. Ю.

Новые финансы: блокчейн, DeFi, Web3 и криптовалюты /
П. Ю. Левашов — «Питер», 2024

ISBN 978-5-4461-2146-5

В современном мире, где криптовалюты и блокчейн-технологии стремительно набирают обороты и вытесняют традиционные валюты, для каждого финансово успешного человека становится критически важным уверенное понимание данных тем. Автор щедро делится своими уникальными знаниями и опытом. Он открывает читателю всю глубину мира децентрализованных финансов, предлагая теоретические основы и практические инструменты, которые помогут читателю не только быть в тренде, но и защитить и преумножить свои цифровые инвестиции.

УДК 336.727.:004.738.5
ББК 65.9(2)262.6:32.988.02

ISBN 978-5-4461-2146-5

Содержание

Левашов П. Ю.
Новые финансы: блокчейн, DeFi, Web3 и криптовалюты

ISBN 978-5-4461-2146-5

* * *

Введение

В постоянно развивающемся мире цифровых финансов понимание тонкостей криптовалют, технологии блокчейн, децентрализованных финансов и кибербезопасности крайне важно для инвесторов, энтузиастов и тех, кто хочет обезопасить свои цифровые активы. В книге даются ценные сведения о сложной и быстро меняющейся сфере цифровых валют.

Опираясь на свой уникальный опыт и знания, автор подробно исследует тему криптовалют: от инвестиционных стратегий и управления рисками до экологического воздействия майнинга и будущего децентрализованной финансовой системы. В книге рассматриваются такие вопросы, как диверсификация, управление рисками, устойчивые решения и новые варианты использования, что делает ее незаменимой для всех, кто хочет ориентироваться в постоянно меняющемся мире цифровых финансов.

Поскольку криптовалютная экосистема непрерывно развивается, для достижения успеха важно оставаться информированным и быть готовым к изменениям. Это руководство предоставляет читателям знания и инструменты, необходимые для принятия взвешенных решений, защиты своих инвестиций и грамотного использования потенциала криптовалют и технологии блокчейн.

Об авторе

Петр Юрьевич Левашов, известный как Peter Severa, – бывший российский хакер из Санкт-Петербурга, который стал специалистом по информационной безопасности, а также достиг успеха в торговле криптовалютой. Имея интригующее прошлое и уникальный взгляд на мир кибербезопасности, Левашов получил два высших образования в области компьютерной безопасности и экономики.

Когда-то известный своим участием в создании и управлении тремя крупными спам-ботнетами, Левашов сегодня использует свои знания и опыт, чтобы помочь другим защитить свои цифровые активы. Он является автором книги «Кибербезопасность: всестороннее руководство по компьютерной безопасности» и предлагает услуги по торговле криптовалютой, приносящей впечатляющие доходы.

Благодаря своему обширному опыту в области компьютерной безопасности и криптовалютной торговли Петр Левашов стал ценным источником информации для частных лиц и организаций, стремящихся понять и защитить свои цифровые активы. Будучи автором книги, которую вы сейчас держите в руках, Левашов рассказывает о пройденном им пути, делится опытом и накопленной мудростью, помогая читателям уверенно ориентироваться в будущем финансового мира. Узнайте больше о Петре на сайте **https://SeveraDAO.ai/**.

Петр также хотел бы выразить благодарность своему сыну Никите, без пытливых вопросов которого эта книга вряд ли увидела бы свет, и своей любимой жене Марии за ее постоянную поддержку, заботу и любовь. А также великолепному адвокату Ольге Леонидовне Исянамановой за ее профессиональную работу. Потрясающее владение УК РФ и его правоприменительной практикой, огромный опыт, честное и открытое общение с клиентами и адекватный подход к ценообразованию – что еще нужно от адвоката? Проблемы? Лучше звоните Ольге!

От издательства

Ваши замечания, предложения, вопросы отправляйте по адресу **comp@piter.com** (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На веб-сайте издательства **www.piter.com** вы найдете подробную информацию о наших книгах.

Глава 1. Введение в блокчейн, криптовалюты и новую финансовую эру

Первые децентрализованные цифровые валюты

Рождение Биткоина

История *Биткоина* – первой и самой известной криптовалюты – началась в 2008 году во время последствий мирового финансового кризиса. Анонимный человек или группа людей под псевдонимом Сатоши Накамото (Satoshi Nakamoto) опубликовали документ под названием «Биткоин: система электронных денег от человека к человеку». В нем была описана революционная система цифровой валюты, позволяющей осуществлять одноранговые транзакции без участия посредника, такого как банк или финансовое учреждение.

Идея децентрализованной валюты не нова: в прошлом предпринимались многочисленные попытки создать системы цифровых денег. Однако эти усилия не увенчались успехом из-за целого ряда сложностей, включая проблему двойного расходования, когда цифровой *токен* тратится более одного раза. Сатоши гениально решил данную проблему с помощью комбинации криптографических методов и механизма распределенного консенсуса под названием Proof of Work (PoW). Такой прием лег в основу технологии *блокчейн*, на которой базируется Биткоин и другие криптовалюты.

Третьего января 2009 года был добыт первый блок, известный как Genesis Block (генезис-блок или «Бытие»), что ознаменовало официальный запуск сети Биткоин. Первая зарегистрированная транзакция прошла 12 января 2009 года, когда Сатоши отправил десять биткоинов программисту по имени Хэл Финни (Hal Finney). Поначалу Биткоин использовался в основном небольшим сообществом энтузиастов, которые добывали и совершали операции с криптовалютой с помощью персональных компьютеров. По мере того как все больше людей узнавали о цифровой валюте, ее стоимость начала расти, а сферы применения – расширяться.

Одна из вех в истории Биткоина произошла в мае 2010 года, когда программист из Флориды по имени Ласло Ханиеч заплатил 10 000 биткоинов за две пиццы, что стало первым известным случаем покупки реального товара за цифровую валюту. Это событие, которое теперь ежегодно отмечается как «День Биткоин-пиццы», иллюстрирует ранние дни использования Биткоина в качестве средства обмена.

За время своего существования Биткоин столкнулся с рядом проблем, включая контроль со стороны регулирующих органов, угрозы безопасности и высокую волатильность. Несмотря на эти трудности, цифровая валюта доказала свою устойчивость, а ее распространение продолжает набирать обороты. Сегодня Биткоин широко рассматривается как надежное средство сохранения стоимости, защиты от инфляции и потенциальная альтернатива традиционным *фиатным* валютам. Успех Биткоина послужил источником вдохновения для создания тысяч других криптовалют, что привело к появлению яркого и стремительно развивающегося мира цифровых активов, который мы видим сейчас.

Появление альткоинов

После создания Биткоина криптовалютная экосистема начала быстро разветвляться, поскольку разработчики и предприниматели увидели потенциал технологии блокчейн и стремились создать новые цифровые активы с разнообразными возможностями и функциями. Эти криптовалюты, известные как *альткоины* (alternative coins), были призваны устранить некоторые из предполагаемых ограничений Биткоина или предоставить новую функциональность.

Один из первых и наиболее известных альткоинов – Litecoin – был создан Чарли Ли в 2011 году. Litecoin задумывался как «серебро» в сравнении с «золотом» Биткоина и ставил своей целью обеспечить более быстрые транзакции, больший общий объем эмиссии и другой алгоритм добычи. Появление Litecoin ознаменовало начало волны инноваций в криптовалютном пространстве.

В 2012 году компания Ripple Labs представила XRP Ledger и свою собственную криптовалюту XRP, разработанную для быстрого и недорогого проведения трансграничных транзакций. В отличие от Биткоина, XRP Ledger не опирается на PoW, вместо этого используется механизм консенсуса, потребляющий гораздо меньше энергии.

Следующий значительный прорыв в области криптовалют произошел в 2015 году с запуском Ethereum (Эфириум) – блокчейн-платформы, разработанной командой специалистов во главе с Виталиком Бутериным. Ethereum представил концепцию *смарт-контрактов* – самоисполняющихся контрактов, в которых условия соглашения записаны непосредственно в коде. Позволив разработчикам создавать децентрализованные приложения (DApps) на платформе Ethereum, эта инновация открыла новую эру возможностей для технологии блокчейн.

С момента запуска Ethereum были созданы тысячи альткоинов, которые обладают своими уникальными особенностями, способами использования и базовыми технологиями. Например, Cardano – блокчейн-платформа, основанная на научных исследованиях и ориентированная на масштабируемость и устойчивость, Binance Coin – собственный токен популярной криптовалютной биржи Binance, Chainlink – децентрализованная оракульная сеть, связывающая смарт-контракты на блокчейне с реальными данными и событиями вне блокчейна.

Распространение альткоинов значительно расширило масштабы и потенциал криптовалютной экосистемы. Благодаря постоянному развитию новых блокчейн-платформ, цифровых активов и децентрализованных приложений мир криптовалют становится все более разнообразным, предлагая пользователям широкий спектр возможностей для инвестиций, платежей и других финансовых операций. По мере роста отрасли возникает уверенность, что альткоины продолжат прогрессировать и совершать величайшие прорывы в мире цифровых активов.

Ключевые принципы криптовалют

Децентрализация

Децентрализация – это фундаментальный принцип криптовалют и лежащей в их основе технологии блокчейн. Она означает распределение власти, полномочий и контроля в рамках сети, в отличие от централизованной системы, где вся власть принадлежит одному субъекту. В контексте криптовалют децентрализация означает отсутствие единоличного контроля над сетью, выпуском новых токенов или подтверждением транзакций со стороны отдельного лица, организации или правительства.

Децентрализация в криптовалютах достигается благодаря сочетанию технологий, криптографии и механизмов консенсуса. В децентрализованной сети множество узлов (компьютеров или серверов) участвуют в поддержании и защите блокчейна, гарантируя, что ни одна точка отказа не сможет скомпрометировать систему.

Преимущества децентрализации в криптовалютах многочисленны. Перечислим и кратко опишем некоторые из них.

• **Безопасность.** Распределение управления между несколькими узлами делает децентрализованные сети более устойчивыми к кибератакам и системным сбоям. Если один узел скомпрометирован, остальная часть сети без проблем продолжит функционировать.

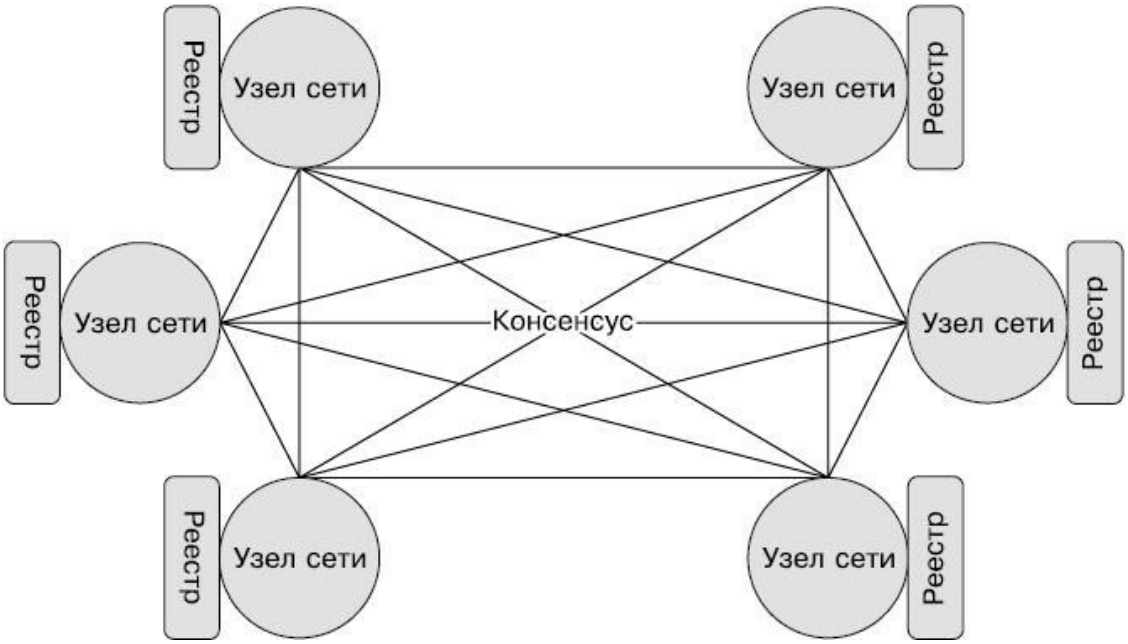
• **Недоверие.** В децентрализованной системе пользователям не нужно полагаться на некий центральный орган для подтверждения транзакций или поддержания целостности сети. Вместо этого прозрачность, неизменность и безопасность всех транзакций обеспечивают математические и криптографические принципы, лежащие в основе блокчейна.

• **Устойчивость к цензуре.** Децентрализованные сети по своей природе устойчивы к цензуре, поскольку ни один субъект не может манипулировать потоком информации или транзакциями. Поэтому правительствам или другим организациям сложно ограничить доступ к криптовалютам или манипулировать их стоимостью.

• **Финансовая доступность.** Децентрализованные криптовалюты позволяют пользователям участвовать в глобальной финансовой системе, минуя традиционные банковские услуги, которые могут быть недоступны или слишком дороги для некоторых людей. Устраняя барьеры для входа и снижая зависимость от посредников, криптовалюты могут расширить возможности пользователей и способствовать финансовой доступности.

• **Инновации.** Децентрализация поощряет прогресс, позволяя разработчикам создавать новые приложения, платформы и финансовые инструменты поверх существующих сетей блокчейн. Это способствует развитию конкурентной и динамичной экосистемы, которая стимулирует технологический прогресс и разработку новых вариантов использования.

Несмотря на все преимущества децентрализации, существуют кое-какие проблемы и компромиссы, которые необходимо учитывать. Например, децентрализованные сети могут быть менее эффективными, чем их централизованные аналоги, из-за необходимости достижения консенсуса между несколькими узлами. Кроме того, отсутствие центрального органа может затруднить применение правил или разрешение споров внутри сети.



Неизменность

Еще одной ключевой характеристикой криптовалют и технологии блокчейн является *неизменность*. Это означает, что записанные данные невозможно изменить или подделать после подтверждения транзакции и добавления ее в книгу учета. Данное свойство крайне важно для обеспечения целостности и безопасности сети, так как оно оставляет проверяемый след всех транзакций и препятствует злоумышленникам манипулировать системой.

Неизменность блокчейна достигается благодаря его уникальной структуре данных и использованию криптографических методов. В блокчейне транзакции группируются в блоки (blocks), каждый из которых содержит ссылку на предыдущий, включая его уникальный *хеш* (hash) – произвольный массив данных, преобразованный в строку фиксированной длины, которая генерируется криптографической хеш-функцией. Это создает цепочку (chain) блоков, отсюда и название «блокчейн» (blockchain).

Когда новый блок добавляется в цепь, он проверяется узлами сети с помощью механизма консенсуса, такого как Proof of Work (PoW) или Proof of Stake (PoS). После того как блок

подтвержден и добавлен в блокчейн, изменение его содержимого потребует преобразования не только самого блока, но и всех последующих блоков в цепи. Это связано с тем, что любая модификация блока приведет к пересмотру его хеша, а поскольку каждый блок содержит хеш предыдущего, подделанный блок и все последующие станут недействительными.

Учитывая децентрализованный характер сетей блокчейн, где множество узлов участвуют в поддержке и защите распределенного реестра, практически невозможно изменить данные без консенсуса большинства узлов. Следовательно, затраты и усилия, необходимые для внесения изменений в блокчейн, делают невозможной подделку данных злоумышленниками, что обеспечивает неизменность системы.

Неизменность дает несколько преимуществ в контексте криптовалют, таких как:

• **доверие** – благодаря неизменности создается прозрачная и защищенная от взлома история всех транзакций, что способствует укреплению доверия между пользователями и снижает необходимость в посредниках;

• **аудируемость** – неизменная природа блокчейна облегчает проверку и аудит транзакции, что особенно ценно в таких областях, как управление цепочками поставок, финансы и соблюдение нормативных требований;

• **безопасность** – неизменность защищает сеть от мошенничества и двойного расходования, поскольку невозможно отменить транзакции или манипулировать ими после их добавления в блокчейн;

• **целостность данных** – неизменность блокчейна обеспечивает точность, последовательность и надежность данных, что позволяет пользователям принимать обоснованные решения на основе информации, хранящейся в распределенном реестре.

Несмотря на многочисленные преимущества, неизменность несет в себе и ряд недостатков, например сложность исправления ошибок или обновления данных в блокчейне. Кроме того, неизменность может привести и к проблемам с конфиденциальностью, поскольку любая информация, однажды занесенная в блокчейн, не может быть удалена. Это стимулировало постоянные исследования и разработку решений, таких как доказательство с нулевым разглашением и конфиденциальные транзакции, для преодоления данных ограничений при сохранении основных принципов технологии блокчейн.

Прозрачность

Прозрачность – еще одна важная характеристика криптовалют и лежащей в их основе технологии блокчейн. В контексте цифровых активов прозрачность подразумевает открытый и публичный характер блокчейна, позволяющий пользователям просматривать и проверять все транзакции в сети. Эта особенность имеет важное значение для укрепления доверия, обеспечения подотчетности и содействия справедливой и открытой финансовой системе.

Прозрачность в криптовалютах достигается за счет использования публичных реестров, содержащих все данные о транзакциях и доступных для просмотра любому человеку с подключением к интернету. В этих реестрах можно увидеть такие детали, как суммы транзакций, адреса отправителей и получателей, а также временные метки, что обеспечивает высокий уровень открытости и прозрачности.

Стоит отметить некоторые преимущества прозрачности в криптовалютах:

• **доверие и подотчетность** – предоставление прозрачной записи транзакций позволяет пользователям проверять точность и подлинность данных, способствуя доверию и подотчетности внутри сети;

• **предотвращение мошенничества** – прозрачность затрудняет манипулирование системой или мошенничество, поскольку эти действия будут видны всей сети;

• **улучшение процесса принятия решений** – доступ к прозрачным и точным данным о сделках позволяет пользователям принимать взвешенные решения относительно своих инвестиций и финансовой деятельности, способствуя более эффективному и хорошо функционирующему рынку;

• **соблюдение нормативных требований** – прозрачность может помочь регулирующим органам в мониторинге деятельности криптовалютных сетей, обеспечении соблюдения соответствующих законов и нормативных актов, а также в борьбе с незаконной деятельностью, такой как отмывание денег и финансирование терроризма.

Хотя прозрачность и дает множество преимуществ, она также может вызывать опасения по поводу конфиденциальности, поскольку финансовые операции и баланс пользователей могут быть видны общественности. Это привело к созданию криптовалют, ориентированных на конфиденциальность, таких как Monero и Zcash, в которых используются передовые криптографические технологии для скрытия деталей транзакций и защиты частной жизни пользователей при сохранении основных принципов технологии блокчейн.

Безопасность и конфиденциальность

Безопасность и конфиденциальность представляют собой основополагающие принципы криптовалют. Они обеспечивают защиту средств и личных данных пользователей от несанкционированного доступа, кражи или манипуляций. Сочетание криптографических методов, децентрализованных сетей и различных технологий, направленных на повышение конфиденциальности, способствует общей безопасности и конфиденциальности цифровых активов.

Безопасность в криптовалютах достигается несколькими способами.

• **Криптография.** Для обеспечения безопасности транзакций и пользовательских данных криптовалюты опираются на передовые криптографические технологии, такие как криптография с открытым ключом. Ее суть в использовании пары ключей – *открытого* и *закрытого* – для осуществления безопасной связи и аутентификации. Открытый ключ применяется для создания адреса, а закрытый необходим для подписания транзакций и доступа к соответствующим средствам. Сохраняя конфиденциальность закрытого ключа, пользователи могут защитить свои средства от несанкционированного доступа.

• **Децентрализованные сети.** Децентрализованная природа сетей блокчейн способствует их безопасности, поскольку контроль и принятие решений распределены между несколькими узлами. Это создает сложности для злоумышленников, пытающихся взломать систему или манипулировать данными, поскольку им необходимо получить контроль над большинством узлов сети.

• **Механизмы консенсуса.** Криптовалюты используют различные механизмы консенсуса, такие как PoW и PoS, для проверки и подтверждения транзакций в сети. Эти механизмы предотвращают двойное расходование и различные мошеннические действия, а также гарантируют, что в блокчейн добавляются только действительные транзакции.

Конфиденциальность же в криптовалютах достигается сочетанием анонимности, псевдонимности и технологий, повышающих конфиденциальность.

• **Анонимность и псевдонимность.** Хотя большинство криптовалют не обеспечивают полную анонимность, они предлагают определенный уровень псевдонимности, используя публичные адреса, которые не связаны напрямую с реальной личностью пользователей. Это позволяет людям сохранять некоторую конфиденциальность при проведении финансовых операций, хотя публичный характер блокчейна все же допускает возможность провести сложный анализ для выявления их личности.

• **Криптовалюты, ориентированные на конфиденциальность.** Некоторые цифровые активы, такие как Monero, Zcash и Dash, специально разработаны для обеспечения

повышенной конфиденциальности. Данные криптовалюты опираются на передовые криптографические методы, такие как доказательство с нулевым разглашением, кольцевые подписи и смешивание (микширование), для скрытия деталей транзакций и защиты конфиденциальности пользователей.

• **Решения второго уровня и протоколы конфиденциальности.** Для повышения конфиденциальности существующих криптовалют было разработано несколько решений второго уровня и протоколов конфиденциальности. Например, Lightning Network для Bitcoin позволяет проводить транзакции вне цепи, а протокол Aztec для Ethereum – конфиденциальные транзакции в сети.

Безопасность и конфиденциальность являются фундаментальными составляющими криптовалют, однако и они не лишены сложностей. Такие вопросы, как безопасность кошельков, обучение пользователей и соблюдение ряда норм, требуют постоянных усилий для обеспечения безопасного и ответственного использования цифровых активов. По мере развития криптовалютной экосистемы технологические достижения и передовой опыт будут способствовать дальнейшему повышению безопасности и конфиденциальности цифровых активов, их принятию и интеграции в мировую финансовую систему.

Понимание основ технологии блокчейн

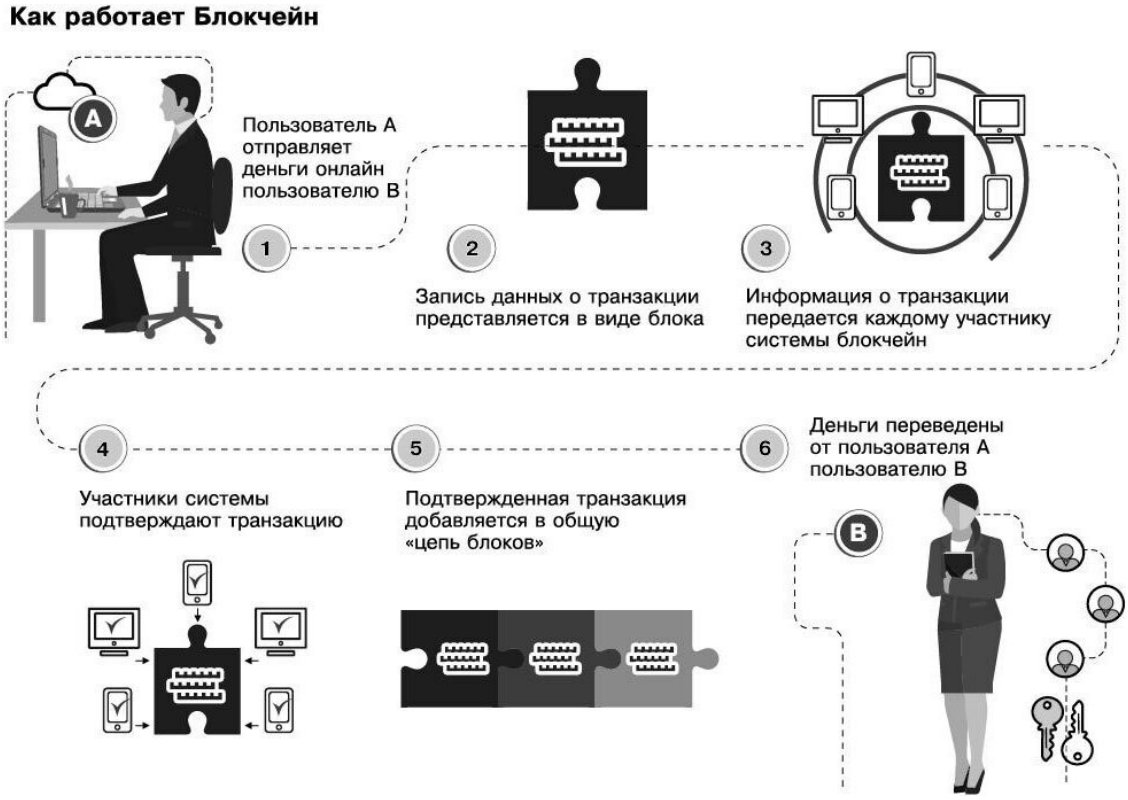
Как работает блокчейн

Технология *блокчейн*, лежащая в основе криптовалют, представляет собой революционный подход к хранению, проверке и защите данных децентрализованным и прозрачным способом. Для понимания работы блокчейна необходимо ознакомиться с основными принципами и компонентами, составляющими эту революционную технологию.

Блокчейн состоит из ряда связанных единиц данных, называемых *блоками*. Каждый блок содержит группу *транзакций*, представляющих собой передачу стоимости или информации между пользователями. Транзакции объединяются в блоки, которые затем последовательно проверяются и добавляются в общую цепочку – блокчейн.

Ключевым принципом технологии блокчейн является применение *криптографического хеширования* – математической функции, которая преобразует данные в выходной сигнал фиксированного размера, называемый хешем. Каждый блок в блокчейне содержит уникальный хеш, который действует как отпечаток пальца для блока. Когда создается новый блок, он включает в себя хеш предыдущего блока, эффективно связывая их вместе и формируя цепочку блоков.

Для поддержания безопасности и целостности блокчейна используется *механизм консенсуса*, гарантирующий, что все участвующие узлы согласны с достоверностью транзакций и добавлением новых блоков. К распространенным механизмам консенсуса относятся Proof of Work (PoW) и Proof of Stake (PoS). В PoW майнеры конкурируют в решении сложных математических задач, и тот, кто первым решит такую задачу, получает право добавить новый блок в цепочку. В PoS валидаторов выбирают на основе количества токенов, которыми они владеют и которые готовы использовать в качестве залога, что дает им возможность подтверждать транзакции и создавать новые блоки.



Одним из основных принципов технологии блокчейн является *децентрализация*, то есть контроль и принятие решений распределяются между несколькими узлами, а не выполняются центральным органом. Эта распределенная сеть узлов взаимодействует для поддержания и обеспечения безопасности блокчейна, гарантируя, что ни один субъект не может контролировать или манипулировать данными.

Как уже упоминалось, технология блокчейн обеспечивает *неизменность* и *прозрачность* благодаря своей уникальной структуре данных и криптографическим методам. Как только транзакция подтверждена и добавлена в блокчейн, она не может быть изменена или удалена, что гарантирует целостность данных. Кроме того, блокчейн, как правило, является открытым и публичным, поэтому пользователи могут просматривать и проверять всю историю транзакций.

Роль узлов

В сети блокчейн узлы играют решающую роль в обеспечении безопасности, децентрализации и общей функциональности системы. *Узел* представляет собой компьютер или сервер в сети, который участвует в хранении, проверке и передаче данных транзакций. Существуют различные типы узлов, каждый из которых выполняет определенные обязанности, включая полные, майнерские и облегченные узлы, также известные как узлы упрощенной проверки платежей (Simplified Payment Verification, SPV). Понимание ролей и функций этих узлов необходимо для восприятия внутренней работы сети блокчейн.

Полные узлы отвечают за поддержание полной копии блокчейна, обеспечивая децентрализованность сети и ее устойчивость к цензуре или манипуляциям. Они выполняют проверку и передачу транзакций и блоков, соблюдая правила консенсуса, помогая таким образом поддерживать целостность блокчейна и защищая сеть от вредоносных действий. Полные узлы

также служат источником информации для легких узлов, которые не хранят весь блокчейн и полагаются на полные узлы для проверки транзакций.

Майнерские узлы – это особый тип узлов в блокчейн-сетях, работающих по принципу PoW (таких как Биткоин). Эти узлы отвечают за решение сложных математических задач в процессе, называемом *майнингом* (от англ. mining – добыча полезных ископаемых). *Майнеры* – пользователи, «добывающие» криптовалюту, – соревнуются между собой, чтобы первыми найти решение и добавить новый блок в блокчейн. За свою работу майнеры получают вознаграждение в виде вновь добытой криптовалюты и платы за транзакции. Майнерские узлы играют важную роль в обеспечении безопасности сети, поскольку вычислительная мощность, которую они вкладывают в майнинг, затрудняет возможность атаковать сеть или манипулировать данными.

Облегченные узлы, или *узлы упрощенной проверки платежей* (SPV), представляют собой более экономичный способ взаимодействия пользователей с блокчейном. Вместо хранения всего блокчейна SPV-узлы хранят только часть данных и полагаются на полные узлы для проверки транзакций и других задач. Этот подход позволяет устройствам с ограниченными ресурсами, таким как мобильные телефоны или устройства интернета вещей (IoT), участвовать в сети и проводить транзакции. Хотя узлы SPV способствуют повышению общей доступности сети, они также зависят от полных узлов в плане безопасности и функциональности, что делает их более уязвимыми для определенных типов атак или дезинформации.

Публичные и частные блокчейны

Хотя концепция технологии блокчейн является единой для различных ее реализаций, существуют разнообразные типы блокчейна со своими особенностями и сценариями использования. Две основные категории блокчейн – это *публичные* и *частные* блокчейны, каждая из которых имеет собственные уникальные характеристики, преимущества и недостатки. Понимание различий между публичными и частными блокчейнами необходимо для определения подходящих сценариев использования и приложений для каждого типа.

Публичные блокчейны, также известные как блокчейны, не требующие права доступа, открыты и доступны для всех, у кого есть интернет. Участники, присоединившиеся к сети, могут создавать и подтверждать транзакции, а также вносить вклад в процесс консенсуса без необходимости получения разрешения от центрального органа. Примерами публичных блокчейнов являются Bitcoin, Ethereum и Litecoin.

Публичные блокчейны имеют следующие характеристики:

- **децентрализация** – ни один субъект не контролирует сеть или данные;
- **безопасность** – обеспечивает высокий уровень безопасности от атак и манипуляций за счет распределенной природы и механизмов консенсуса, таких как PoW или PoS;
- **прозрачность** – позволяет пользователям просматривать и проверять всю историю транзакций в сети;
- **анонимность и псевдонимность** – публичные блокчейны предлагают различные уровни анонимности и псевдонимности, в зависимости от конкретной реализации и особенностей конфиденциальности;
- **масштабируемость и производительность** – публичные блокчейны могут столкнуться с проблемами масштабируемости и производительности, поскольку растущее число пользователей и транзакций приводит к перегрузке сети и увеличению времени обработки транзакций.

Частные блокчейны, также известные как блокчейны с ограниченным доступом, представляют собой закрытые сети, для присоединения к которым и участия в них требуется разрешение центрального органа или консорциума. Такие блокчейны обычно используются пред-

приятиями и организациями для решения конкретных задач, таких как управление цепочками поставок, межбанковские транзакции или управление данными.

Частные блокчейны обладают такими характеристиками, как:

• **централизация** – частные блокчейны более централизованы, чем публичные, поскольку они контролируются и поддерживаются центральным органом или группой доверенных лиц;

• **безопасность и конфиденциальность** – хотя частные блокчейны из-за своей централизованной природы могут быть менее безопасными, чем публичные, они предлагают улучшенную конфиденциальность и контроль доступа благодаря контролируемому доступу и расширенным функциям конфиденциальности;

• **эффективность и масштабируемость** – частные блокчейны способны обрабатывать большее количество транзакций с меньшими задержками и потребностями в ресурсах, чем публичные блокчейны;

• **настраиваемость** – частные блокчейны могут быть адаптированы к конкретным требованиям организации или консорциума, что обеспечивает большую гибкость и адаптируемость для различных сценариев использования. Это позволяет создавать блокчейн-решения, оптимизированные под конкретные бизнес-процессы и потребности сторон.

Как уже было сказано ранее, публичные и частные блокчейны обладают уникальными особенностями, преимуществами и ограничениями, которые определяют их пригодность для различных задач и ситуаций. Публичные блокчейны хорошо подходят для децентрализованных, прозрачных и безопасных систем, в то время как частные обеспечивают большую эффективность, масштабируемость и настраиваемость для корпоративных и организационных сценариев использования.

В отличие от публичных блокчейнов, частные обычно ориентированы на ограниченный круг участников, что обеспечивает большую конфиденциальность и более контролируемую среду. При этом они могут предлагать различные уровни децентрализации, от полностью централизованных до децентрализованных с ограниченным количеством узлов.

Понимая различия между публичными и частными блокчейнами, предприятия, разработчики и пользователи могут принимать взвешенные решения при выборе технологии для своих конкретных нужд.

Распределенные банки данных и механизмы консенсуса

Proof of Work (PoW)

Proof of Work (PoW), или доказательство работы, – это механизм консенсуса, используемый в различных сетях блокчейн, включая Bitcoin и Ethereum (до перехода к PoS). PoW был первым алгоритмом консенсуса, реализованным в мире криптовалют, и до сих пор остается популярным выбором для многих децентрализованных сетей. Основная цель PoW – обеспечить безопасность, целостность и неизменность блокчейна, которая достигается путем выполнения участниками сети сложных математических вычислений.

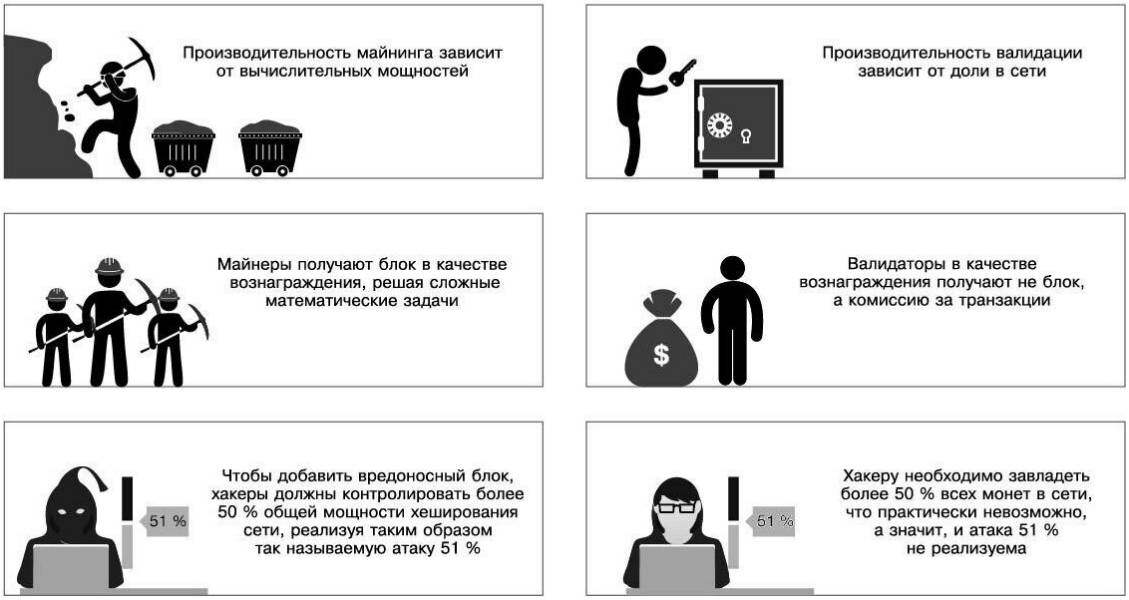
• **Процесс майнинга.** В блокчейн-сетях на основе PoW майнеры отвечают за подтверждение транзакций и добавление новых блоков в блокчейн. Майнеры соревнуются в решении сложной математической задачи, основанной на криптографической хеш-функции. Первый майнер, нашедший ответ, известный также как nonce, передает его в сеть, и, если он подтверждается другими узлами, майнеру разрешается добавить новый блок в блокчейн. За свою работу майнер получает вознаграждение в виде новой криптовалюты и комиссионных от подтвержденных транзакций.

• **Вычислительная мощность и корректировка сложности.** Сложность математической задачи в сетях PoW периодически корректируется для поддержания постоянной скорости создания блоков. По мере увеличения общей вычислительной мощности сети сложность задачи также увеличивается, сохраняя стабильную скорость создания новых блоков. Этот саморегулирующийся механизм способствует обеспечению безопасности и стабильности сети.

• **Энергопотребление и вопросы экологии.** Одной из основных претензий в адрес механизмов консенсуса PoW является их высокое энергопотребление. Поскольку майнеры конкурируют в решении математических задач, им требуется значительная вычислительная мощность, что приводит к существенному потреблению энергии. Это вызвало озабоченность по поводу воздействия криптовалют, основанных на PoW, на окружающую среду, что подтолкнуло к разработке альтернативных механизмов консенсуса с более низкими требованиями к энергии, о которых мы поговорим совсем скоро.

• **Атака 51 %.** Сети PoW потенциально уязвимы для особого типа атак, называемого «атакой 51 %». В этом сценарии, если организация или группа сговорившихся майнеров получит контроль над более чем 50 % вычислительной мощности сети, они потенциально смогут манипулировать блокчейном, дважды расходуя монеты, блокируя или даже переписывая историю транзакций. Однако стоимость и ресурсы, необходимые для осуществления подобной атаки, например, на сеть Биткоин, непомерно высоки, что делает их маловероятными.

Алгоритмы консенсуса Proof of Work и Proof Stake



Proof of Stake (PoS)

Proof of Stake (PoS), или доказательство доли, – это альтернативный механизм консенсуса, который приобрел популярность благодаря своей энергоэффективности и более высокому уровню безопасности по сравнению с PoW. Блокчейны на основе PoS, такие как Ethereum 2.0, Cardano и Polkadot, полагаются на *валидаторов*, которые «оставляют в залог» свою криптовалюту для обеспечения безопасности сети и подтверждения транзакций. Используя иной подход к достижению консенсуса, PoS стремится решить некоторые проблемы, связанные с PoW, такие как высокое потребление энергии и потенциальные уязвимости.

• **Процесс валидации.** В блокчейн-сетях на основе PoS валидаторы выбираются для создания новых блоков и подтверждения транзакций на основе количества токенов, которыми они владеют и готовы внести в качестве залога. Делая ставку на свои токены, валидаторы демонстрируют свою приверженность безопасности и целостности сети. Процесс отбора валидаторов обычно основан на комбинации факторов, таких как размер их доли, продолжительность участия в сети и процесс рандомизации, чтобы обеспечить справедливое и децентрализованное создание блоков.

• **Вознаграждения и штрафы.** Обычно валидаторы в сетях PoS получают вознаграждение за проверку транзакций и создание новых блоков в виде вновь добытой криптовалюты и комиссии за транзакции. Однако в отличие от PoW, где майнеры получают вознаграждение за решение математических задач, в PoS величина вознаграждения для валидаторов зависит от размера их доли и их участия в обеспечении безопасности сети. Валидаторы могут быть наказаны, например, потерей части заложенных токенов, если их уличат в злонамеренных действиях или попытках манипулировать блокчейном.

• **Энергоэффективность.** Одним из основных преимуществ PoS перед PoW является его энергоэффективность. PoS не требует от валидаторов выполнения сложных математических вычислений, что значительно снижает потребление энергии. Это делает PoS не только более экологичным, но и позволяет большему числу участников обеспечивать безопасность сети, укрепляя децентрализацию системы.

• **Безопасность и атака 51 %.** Считается, что сети PoS более устойчивы к атакам 51 % по сравнению с сетями PoW. В системе PoS для манипулирования блокчейном злоумыш-

леннику необходимо контролировать значительную часть токенов, оставленных в залог, что обычно сложнее и дороже, чем приобретение большинства вычислительных мощностей в сети PoW. Кроме того, поскольку злоумышленнику нужно владеть подавляющим количеством родной криптовалюты, он также заинтересован в сохранении безопасности и стоимости сети.

Другие механизмы консенсуса

Хотя Proof of Work и Proof of Stake являются наиболее известными механизмами консенсуса, существуют и другие подходы для решения уникальных задач и требований различных сетей блокчейн. Эти альтернативные механизмы консенсуса предлагают различные преимущества и компромиссы, в зависимости от их конкретного дизайна и реализации. Давайте кратко рассмотрим эти механизмы.

Delegated Proof of Stake (DPoS)

Делегированное доказательство доли (DPoS) – это разновидность модели PoS, в которой выбор валидаторов осуществляется через систему, аналогичную репрезентативной демократии. В DPoS держатели токенов голосуют за определенное количество делегатов, которые затем становятся ответственными за подтверждение транзакций и обеспечение работы сети. Такой подход направлен на повышение эффективности, масштабируемости и принятия решений в сети. Однако он также может привести к усилению централизации, поскольку делегаты могут накопить значительное влияние. Примерами проектов блокчейн, использующих DPoS, являются EOS и Lisk.

Proof of Authority (PoA)

Proof of Authority, или доказательство полномочий, представляет собой механизм консенсуса, в котором ограниченное число заранее отобранных доверенных валидаторов отвечает за безопасность сети и подтверждение транзакций. PoA особенно эффективен для частных и разрешенных блокчейн-сетей, где поддержание высокого уровня контроля и доверия имеет решающее значение. Несмотря на повышенную эффективность, масштабируемость и пропускную способность транзакций, PoA жертвует децентрализацией, поскольку выбранные прежде валидаторы имеют значительный контроль над сетью. Примером блокчейн-проекта, использующего PoA, является блокчейн VeChainThor.

Byzantine Fault Tolerance (BFT)

Византийская отказоустойчивость (BFT) – это механизм консенсуса, разработанный для решения классической проблемы, известной как «проблема византийских генералов». Она возникает в распределенных вычислениях, когда некоторые узлы системы могут быть неисправными или злонамеренными. Механизмы консенсуса на основе BFT сосредоточены на обеспечении достижения консенсуса в сети, даже при наличии неисправных или ненадежных узлов.

Варианты BFT включают практическую византийскую отказоустойчивость (Practical Byzantine Fault Tolerance, PBFT), федеративное византийское соглашение (Federated Byzantine Agreement, FBA) и делегированную византийскую отказоустойчивость (Delegated Byzantine Fault Tolerance, DBFT). Каждый из них предлагает свои подходы к достижению отказоустойчивого консенсуса. Примеры блокчейн-проектов, использующих механизмы консенсуса на основе BFT, включают Hyperledger Fabric (применяет PBFT), Stellar (использует FBA) и NEO (основан на DBFT).

Directed Acyclic Graph (DAG)

Направленный ациклический граф (Directed Acyclic Graph, DAG) – это механизм консенсуса, который использует структуру графа вместо линейного блокчейна. В системе на основе DAG транзакции напрямую связаны друг с другом и подтверждаются последующими транзакциями, создавая структуру, напоминающую веб. Такой подход обеспечивает большую масштабируемость, поскольку транзакции могут обрабатываться параллельно, и не требует традиционного вознаграждения за блок или майнинг. Однако системы на основе DAG могут быть более запутанными и сложными в плане безопасности по сравнению с традиционными сетями блокчейн. Примерами проектов, использующих механизмы консенсуса на основе DAG, являются IOTA и Nano.

Подводя итог, можно сказать, что мир механизмов консенсуса выходит за рамки PoW и PoS и включает в себя множество альтернативных подходов, разработанных для решения конкретных задач и требований. Понимая эти различные механизмы консенсуса и их компромиссы, разработчики, предприятия и пользователи могут принимать обоснованные решения при выборе подходящей технологии для своих конкретных сценариев использования и целей.

Эволюция криптовалютных бирж

Централизованные биржи

Централизованные биржи (Centralized Exchanges, CEX) сыграли важную роль в развитии и принятии криптовалют, предоставив пользователям платформу для торговли цифровыми активами. Централизованные биржи выступают в качестве посредников между покупателями и продавцами, позволяя им эффективно совершать безопасные сделки. Хотя биржи CEX обладают рядом преимуществ, они также не лишены недостатков, в первую очередь из-за своей централизованной природы. В этом разделе мы рассмотрим основные характеристики, преимущества и недостатки централизованных бирж.

Централизованные биржи предоставляют пользователям *привычный* и *удобный* интерфейс, похожий на традиционные фондовые биржи. Как правило, они поддерживают широкий спектр криптовалют и торговых пар, позволяя участникам торгов обменивать одни цифровые активы на другие и даже на фиатные валюты. Централизованные биржи получают доход за счет торговых комиссий, которые часто взимаются в виде процента от суммы сделки.

Централизованные биржи имеют ряд таких преимуществ, как:

• **ликвидность** – благодаря огромному числу пользователей и наличию большего количества торговых пар централизованные биржи способны обеспечивать быстрое исполнение ордеров по конкурентоспособным ценам;

• **пользовательский опыт** – централизованные биржи часто предоставляют более удобный опыт работы, с интуитивно понятными интерфейсами, передовыми торговыми инструментами и отзывчивой поддержкой, что делает их привлекательным вариантом как для новичков, так и для опытных трейдеров;

• **ввод фиатных средств** – позволяют покупать криптовалюты напрямую за местную валюту, что способствует более широкому внедрению и доступности цифровых активов;

• **кастодиальные услуги** – позволяют хранить средства пользователей от их имени, что может быть удобно для клиентов, которые не хотят управлять своими закрытыми ключами или разбираться со сложностями хранения криптовалюты.

А также недостатков:

• **централизация** – может создавать риски для пользователей, поскольку CEX уязвимы к взломам, мошенничеству со стороны инсайдеров или возможному отключению регуляторов. За последние годы на централизованных биржах произошло несколько громких краж, что привело к серьезным потерям для клиентов;

• **контроль над средствами** – когда пользователи размещают свои средства на централизованной бирже, они отказываются от контроля над своими закрытыми ключами и, следовательно, активами, что приводит к риску потери средств в случае взлома или неправильного управления биржей;

• **соответствие нормативным требованиям** – централизованные биржи часто подчиняются строгим нормативным требованиям, что сказывается на конфиденциальности пользователей и доступности определенных криптовалют или торговых пар. Чтобы соответствовать нормативным требованиям, CEX обычно применяют строгие процедуры проверки личности, которые могут отнимать много времени и быть инвазивными для пользователей.

Децентрализованные биржи

Децентрализованные биржи (Decentralized Exchanges, DEX) представляют собой альтернативу централизованным биржам, предлагая пользователям более безопасный и прозрачный способ торговли криптовалютами. Используя технологию блокчейн и смарт-контракты, DEX устраняют необходимость в центральном органе, облегчая транзакции и позволяя пользователям сохранять контроль над своими средствами и торговать напрямую друг с другом. В этом разделе мы рассмотрим ключевые особенности децентрализованных бирж, а также их преимущества и недостатки.

Децентрализованные биржи работают по принципу *peer-to-peer* (p2p): пользователи заключают сделки напрямую друг с другом через смарт-контракты. Отсутствие посредников повышает эффективность и уменьшает затраты на торговлю. DEX не хранят средства пользователей и не управляют их закрытыми ключами. Это означает, что пользователи имеют полный контроль над своими активами. Децентрализованные биржи обычно поддерживают широкий спектр криптовалют и токенов, особенно тех, которые построены на одной блокчейн-платформе, например Ethereum. Это позволяет пользователям торговать разнообразными активами без необходимости перехода между биржами.

Преимущества децентрализованных бирж:

• **безопасность** – поскольку пользователи сохраняют контроль над своими закрытыми ключами и средствами, риск потери средств из-за взлома биржи или неправильного управления сводится к нулю;

• **конфиденциальность** – пользователям обычно не требуется предоставлять свои персональные данные и проходить сложные процессы проверки личности, что обеспечивает более высокий уровень конфиденциальности и анонимности по сравнению с централизованными биржами;

• **децентрализация** – не зависят от центрального органа или регулятора, так как у них нет центральной точки контроля или отказа. Это означает, что пользователи имеют большую свободу и независимость в проведении торговых операций;

• **открытость** – децентрализованные биржи, как правило, более доступны и инклюзивны, поскольку они позволяют любому желающему размещать токены и торговать ими без необходимости получения разрешения от центрального органа.

Стоит отметить и недостатки децентрализованных бирж:

• **ликвидность** – из-за меньшего числа пользователей и поддержки ограниченного количества торговых пар на децентрализованных биржах более высокая волатильность и медленное время исполнения ордеров;

• **пользовательский опыт** – для новичков DEX могут показаться довольно сложными в использовании из-за требования знаний основ технологии блокчейн, управления кошельками и смарт-контрактов. Кроме того, по сравнению с CEX на биржах DEX могут отсутствовать передовые торговые инструменты и привычная многим поддержка клиентов;

• **интероперабельность** – большинство децентрализованных бирж ограничены торговлей токенами, созданными на одной платформе блокчейна, что затрудняет торговлю межсетевыми активами. Однако для решения этой проблемы разрабатываются новые решения и технологии, такие как межсетевые мосты и атомарные свопы.

Биржи Fiat-to-Crypto и Crypto-to-Crypto

По мере расширения криптовалютной экосистемы появились разнообразные типы бирж, которые удовлетворяют различным потребностям трейдеров. Одним из ключевых различий

между криптовалютными биржами является то, поддерживают ли они операции обмена между фиатными деньгами и криптовалютой (Fiat-to-Crypto) или только между криптовалютами (Crypto-to-Crypto). В данном разделе мы рассмотрим основные характеристики, преимущества и ограничения бирж, поддерживающих как обмен фиата на криптовалюту, так и криптовалюты на криптовалюту.

Фиатные криптобиржи, такие как Coinbase, Kraken и Bitstamp, позволяют пользователям покупать и продавать криптовалюты с помощью *фиатных денег*. Эти биржи выступают в качестве моста между традиционной финансовой системой и миром криптовалют, давая возможность людям входить и выходить на рынок, используя свою национальную валюту (доллары, евро, иены и т. д.).

Преимущества бирж Fiat-to-Crypto:

• **доступность** – возможность свободно обменивать обыкновенные деньги на цифровые активы предоставляет пользователям простой и удобный способ выхода на криптовалютный рынок, что способствует более широкому распространению криптовалют;

• **разнообразие торговых пар** – позволяют торговать различными криптовалютами за местную фиатную валюту, благодаря чему люди могут создавать разнообразные и индивидуальные портфели, соответствующие их инвестиционным предпочтениям.

Недостатки бирж Fiat-to-Crypto:

• **соответствие нормативным требованиям** – данные биржи обычно подчиняются строгим нормативным требованиям, что может повлиять на конфиденциальность пользователей и ограничить доступность определенных криптовалют или торговых пар. Чтобы соответствовать нормативным требованиям, эти биржи часто применяют строгие процедуры проверки личности, которые могут отнимать много времени и быть инвазивными для пользователей;

• **комиссии** – подобные биржи часто взимают более высокие комиссии за ввод, вывод и конвертацию фиатных средств по сравнению с транзакциями криптовалют. Со временем эти комиссии могут увеличиваться, особенно для активных трейдеров.

Биржи криптовалют, например Binance, Poloniex и KuCoin, специализируются на торговле исключительно криптовалютами. Эти платформы не поддерживают операции с фиатными деньгами и требуют, чтобы пользователи уже обладали криптовалютами для торговли на них.

Преимущества бирж Crypto-to-Crypto:

• **более широкий выбор криптовалют** – предоставляет пользователям более широкий спектр торговых и инвестиционных возможностей;

• **более низкие комиссии** – низкие торговые комиссии достигаются за счет отсутствия необходимости работать с фиатными деньгами, что делает данные биржи более рентабельными для активных трейдеров.

Недостатки бирж Crypto-to-Crypto:

• **доступность** – биржи криптовалют могут быть менее доступными для новичков, поскольку для торговли необходимо, чтобы пользователи уже владели криптовалютой, а это создает дополнительный барьер для тех, кто хочет выйти на криптовалютный рынок;

• **волатильность** – на биржах криптовалют пользователи могут остро ощущать повышенную рыночную волатильность, поскольку на платформе отсутствует возможность конвертировать свои цифровые активы обратно в фиатные валюты. В таких случаях пользователям может потребоваться перевести свои активы на криптовалютную биржу или использовать так называемые стейблкоины (о которых мы подробнее поговорим в следующей главе) в качестве временного средства сохранения стоимости в периоды колебания рынка.

Следует отметить, что как фиатные криптовалютные биржи, так и криптовалютные биржи отвечают различным торговым потребностям и предпочтениям трейдеров. Хотя биржи, торгующие и фиатом, и криптовалютами, обеспечивают большую доступность и поддержку

фиатных валют, они могут быть подвержены более жесткому регулированию и высоким комиссиям. С другой стороны, биржи, ориентированные на криптовалюты, предлагают широкий выбор криптовалют и низкие комиссии, однако имеют более высокий порог входа. Понимание преимуществ и ограничений каждого типа бирж может помочь пользователям принять взвешенное решение в соответствии с их потребностями и целями.

Растущая экосистема криптовалютных кошельков

Горячие кошельки

По мере развития криптовалютной экосистемы появилось множество вариантов кошельков для удовлетворения различных потребностей пользователей. Один из таких вариантов – горячий кошелек, который предлагает удобное и простое в использовании решение для хранения, отправки и получения криптовалют. В этом разделе мы рассмотрим основные характеристики горячих кошельков, а также их преимущества и недостатки.

Горячие кошельки – это цифровые кошельки, подключенные к интернету, позволяющие пользователям быстро и легко получать доступ к своим криптовалютам и управлять ими. Доступ к горячим кошелькам реализован через различные платформы, такие как браузеры, настольные приложения или мобильные устройства. Примерами горячих кошельков являются программные кошельки Exodus и MyEtherWallet, а также мобильные кошельки Trust Wallet и Coinomi.

Горячие кошельки имеют ряд таких преимуществ, как:

• **удобство** – предлагают интерфейс, который позволяет быстро и легко управлять криптовалютами, что делает их идеальным выбором для людей, которые часто торгуют, переводят или получают цифровые активы;

• **интеграция** – часто имеют встроенные функции, улучшающие пользовательский опыт. Например, они могут включать встроенные биржи, возможности стейкинга или поддержку DApps, что дает пользователям доступ к широкому спектру услуг и функций в рамках единого интерфейса;

• **поддержка мультивалютности** – многие горячие кошельки поддерживают огромное количество криптовалют и токенов, позволяя управлять несколькими цифровыми активами внутри одного кошелька, что упрощает процесс управления разнообразным портфелем криптовалют;

• **стоимость** – горячие кошельки обычно бесплатны или недороги, что делает их привлекательным выбором для новичков в криптовалютах или для тех, кто не хочет вкладываться в дорогие аппаратные кошельки.

Однако они не лишены и недостатков:

• **безопасность** – горячие кошельки уязвимы ко взломам, фишинговым атакам и вредоносным программам, поскольку они подключены к интернету. Хотя поставщики горячих кошельков применяют различные меры безопасности для защиты средств пользователей, они не сравнятся в данном вопросе с холодными кошельками, которые отключены от интернета и менее подвержены кибератакам;

• **контроль над закрытыми ключами** – некоторые горячие кошельки, особенно веб-кошельки или кошельки, размещенные на бирже, не предоставляют пользователям полного контроля над их закрытыми ключами. Это означает, что пользователям приходится полагаться на третьи лица для обеспечения безопасности своих средств, что может повлечь риск потери активов в случае компрометации или неправильного управления провайдером кошелька.

Холодные кошельки

Альтернативой горячим кошелькам выступают холодные кошельки, которые представляют собой более безопасный вариант хранения криптовалют, особенно для пользователей,

придающих высокое значение безопасности своих цифровых активов. В этом разделе мы рассмотрим основные характеристики холодных кошельков, а также их преимущества и недостатки.

Холодные кошельки, также известные как аппаратные или автономные кошельки, хранят приватные ключи пользователей в автономном режиме, защищая их от онлайн-угроз, таких как взломы и фишинговые атаки. Холодные кошельки могут быть представлены в виде аппаратных устройств, например Ledger Nano S, Trezor и KeepKey, или бумажных кошельков – печатных изображений закрытых и открытых ключей пользователя.

Преимущества холодных кошельков:

• **безопасность** – обеспечивают высокий уровень безопасности, поскольку личные ключи пользователей хранятся в автономном режиме и вне досягаемости потенциальных киберугроз. Физическая природа аппаратных кошельков добавляет дополнительный уровень защиты, так как они обычно включают такие функции, как PIN-коды, физические кнопки для подтверждения транзакций и защищенные чипы для хранения закрытых ключей;

• **контроль над закрытыми ключами** – дают пользователям полный контроль над их закрытыми ключами, гарантируя, что они являются единственными хранителями своих цифровых активов. Это исключает необходимость полагаться на третьи лица в вопросе обеспечения безопасности своих средств и снижает риск потери активов из-за неправильного управления или взлома;

• **долгосрочное хранение** – идеальное решение для пользователей, которые планируют хранить свои криптовалюты в течение длительного периода времени без частых операций и трат. Храня свои активы в безопасной, автономной среде, пользователи могут быть спокойны, зная, что их инвестиции защищены.

Ниже приведены основные недостатки холодных кошельков:

• **доступность** – менее удобны и доступны по сравнению с горячими кошельками, поскольку требуют доступа к физическому устройству или бумажному кошельку для управления криптовалютами. Это может быть недостатком для пользователей, которым необходимо часто торговать, тратить или получать цифровые активы;

• **стоимость** – обычно довольно дороги по сравнению с другими типами кошельков;

• **настройка и обслуживание** – холодные кошельки, особенно бумажные, могут потребовать более сложного процесса настройки и постоянного обслуживания для обеспечения безопасности. Пользователи должны позаботиться о хранении таких видов кошельков в надежном и сохранном месте, чтобы избежать потери, кражи или повреждения.

Аппаратные кошельки

Аппаратные кошельки, являясь популярным типом холодных кошельков, предлагают пользователям удобное и безопасное решение для хранения и управления своими криптовалютами. В этом разделе мы рассмотрим ключевые особенности аппаратных кошельков, их преимущества и ограничения.

Аппаратные кошельки – это физические устройства, разработанные специально для хранения закрытых ключей пользователей в автономном режиме. Эти устройства подключаются к компьютеру или смартфону через USB-порт или Bluetooth, давая возможность безопасно управлять своими цифровыми активами без доступа к закрытым ключам через интернет. Примерами популярных аппаратных кошельков являются Ledger Nano S, Trezor и KeepKey.

Преимущества аппаратных кошельков:

• **безопасность** – обеспечивают высокий уровень безопасности за счет автономного хранения личных ключей пользователей, что сводит к минимуму риск взлома, фишинговых атак и воздействия вредоносных программ. Они часто содержат дополнительные функции,

такие как PIN-коды, физические кнопки для подтверждения транзакций и модули безопасности для хранения закрытых ключей, что еще больше повышает их защищенность;

• **контроль над закрытыми ключами** – дают пользователям полный контроль над их закрытыми ключами, гарантируя, что только у них есть доступ к своим цифровым активам. Это исключает необходимость полагаться на третьи лица в вопросе обеспечения безопасности своих средств и снижает риск потери активов из-за неправильного управления или взлома;

• **простота использования** – несмотря на свою физическую природу, аппаратные кошельки удобны в использовании. Они предлагают интуитивно понятные интерфейсы, а также совместимы с популярным программным обеспечением (ПО) для кошельков, что позволяет пользователям безопасно управлять своими криптовалютами без ущерба для удобства.

Недостатки аппаратных кошельков:

• **стоимость** – ощутимо дороже иных видов кошельков;

• **доступность** – хотя аппаратные кошельки предлагают более удобный опыт использования, чем другие типы холодных кошельков, они все же менее доступны, чем горячие кошельки. Для управления криптовалютами пользователям необходимо подключить аппаратный кошелек к компьютеру или смартфону, что может быть менее практично для активных трейдеров;

• **потеря или поломка устройства** – как и любые физические устройства, аппаратные кошельки могут быть потеряны, украдены или повреждены. Пользователям необходимо хранить свои аппаратные кошельки в надежном и безопасном месте и иметь резервную копию *seed-фразы* для восстановления своих активов в случае утери или поломки устройства.

Криптовалюта в глобальной экономике

Криптовалюты обладают огромным потенциалом для расширения возможностей *небанковских* и *малобанковских* групп населения по всему миру[1]. В данном разделе мы рассмотрим, как криптовалюты могут выступать в качестве цифровых денег для этих групп, способствуя финансовой интеграции и предоставляя доступ к широкому спектру услуг, ранее недоступных им.

Цифровые деньги для небанковского населения

По данным Всемирного банка, около 1,7 миллиарда взрослых людей не имеют доступа к банковским счетам или другим традиционным финансовым услугам. Значительная часть мирового населения сталкивается с ограниченным доступом к финансовым услугам или вынуждена обращаться к альтернативным поставщикам таких услуг.

Криптовалюты обладают потенциалом для решения многих проблем, с которыми сталкивается население, не имеющее банковских счетов и не охваченное банковскими услугами. Предлагая децентрализованную, безопасную и доступную форму цифровых денег, криптовалюты могут способствовать финансовой интеграции и доступу к основным услугам без опоры на традиционные банковские системы.

Криптовалюты позволяют осуществлять *быстрые и недорогие трансграничные транзакции*, снижая комиссии, связанные с оплатой, денежными переводами и другими финансовыми операциями. Это может быть особенно полезно для небанковских лиц, которые полагаются на дорогостоящие альтернативные финансовые услуги или неформальные сети для отправки и получения денег.

Имея только смартфон и подключение к интернету, люди, не охваченные банковским обслуживанием, с помощью криптовалют могут *получить доступ* к широкому спектру финансовых услуг, таких как цифровые кошельки, платформы одноранговогo кредитования и приложения децентрализованного финансирования (Decentralized Finance, DeFi). Это позволяет им сохранять, инвестировать и управлять своими деньгами без необходимости открывать традиционный банковский счет.

Криптовалюты и технология блокчейн способны облегчить *доступ к кредитам* для небанковских лиц благодаря децентрализованным платформам кредитования и инновационным моделям кредитного скоринга на основе альтернативных источников данных. Это позволяет людям без официальной кредитной истории получать займы, ипотечные кредиты и другие формы кредитования, ранее им недоступные.

Предоставляя не имеющим банковского обслуживания лицам доступ к цифровым деньгам и финансовым услугам, криптовалюты могут *расширить* их возможности для участия в мировой экономике, стимулируя предпринимательство и способствуя экономическому росту в слаборазвитых регионах.

Криптовалюты как инструмент сбережения

Вокруг криптовалют не утихают споры относительно их потенциальной способности служить *средством сохранения стоимости*, подобно традиционным активам, таким как золото

[1] Групп населения, не пользующихся банками.

и фиатные валюты. В этом разделе мы рассмотрим аргументы за и против использования криптовалют в данном ключе, а также факторы, влияющие на определение их ценности.

Доводы в пользу криптовалют в качестве инструмента сбережения:

• **ограниченная эмиссия** – многие криптовалюты имеют ограниченный объем предложения, что алгоритмически обеспечивается их базовыми протоколами. Это ограничение может способствовать увеличению их стоимости, создавая дефляционную среду и предотвращая размывание стоимости через инфляцию;

• **децентрализация** – децентрализованная природа криптовалют говорит о том, что они не зависят от центральных органов власти, таких как правительства и банки. Это может быть привлекательным для людей, беспокоящихся о стабильности традиционных финансовых систем или возможном обесценивании валюты в результате монетарной политики;

• **цифровое золото** – некоторые сторонники цифровых активов утверждают, что криптовалюты могут выступать в роли «цифрового золота», обеспечивая защиту от инфляции и служа надежным убежищем в периоды экономической неопределенности. Сравнение проводится из-за их общих качеств, таких как дефицит, делимость и портативность.

Доводы против:

• **волатильность** – одно из основных противоречий в отношении криптовалют как средства сохранения стоимости связано с их высокой волатильностью. Цены на криптовалюты могут существенно колебаться в течение коротких периодов времени, что ставит под сомнение их способность сохранить вложенные средства;

• **юридическая неопределенность** – нормативно-правовая среда, охватывающая криптовалюты, продолжает развиваться, при этом некоторые правительства занимают более ограничительную позицию в отношении их использования и принятия. Такая неопределенность может представлять риск для инвесторов, рассматривающих криптовалюты в качестве инвестиционного инструмента, поскольку изменения в регулировании могут повлиять на их стоимость и легальность;

• **ограниченное распространение** – несмотря на то, что криптовалюты привлекли значительное внимание и инвестиции, они до сих пор не получили достаточно широкого распространения для повседневных операций. Такое ограниченное применение может затруднить становление криптовалют в качестве общепризнанного средства сохранения стоимости.

Факторы, влияющие на стоимость криптовалют:

• **настроение рынка** – стоимость криптовалют во многом определяется настроением рынка, поскольку инвесторы спекулируют на их будущем потенциале и принятии. Позитивные или негативные новости и события могут вызвать быстрые изменения в спросе и привести к значительным колебаниям цен;

• **значимость** – по мере того как все больше людей применяют криптовалюты для транзакций, денежных переводов и других целей, их воспринимаемая ценность может возрастать;

• **инновации** – внедрение новых технологий и усовершенствование существующих протоколов блокчейна повышают масштабируемость, безопасность, а также общую полезность криптовалют, что может способствовать росту их стоимости.

Следует отметить, что дебаты о криптовалютах как инструменте сбережения являются сложными и аргументы приводятся с обеих сторон. Хотя их дефицит, децентрализация и потенциал в качестве цифрового золота могут поддержать их использование в качестве средства сохранения стоимости, остаются опасения по поводу волатильности, неопределенности нормативно-правового регулирования и ограниченного распространения. В конечном счете способность криптовалют утвердиться в качестве общепризнанного инструмента сбережения может зависеть от их дальнейшего развития, признания и эволюции нормативно-правовой базы.

Препятствия и возможности для массового внедрения

Поскольку криптовалюты продолжают привлекать внимание и вызывать интерес, одним из важнейших вопросов является их потенциал для массового принятия. В этом разделе мы рассмотрим, какие проблемы стоят перед криптовалютами для интеграции в глобальную экономику и какие у них для этого есть возможности.

Проблемы, связанные с внедрением криптовалют в массовую практику:

• **масштабируемость** – несмотря на значительные успехи в области масштабируемости, необходимо проводить дальнейшие исследования и разработки, чтобы криптовалюты могли конкурировать с традиционными платежными системами;

• **юридическая неопределенность** – как уже упоминалось ранее, нормативно-правовая база в отношении криптовалют все еще развивается, и некоторые юрисдикции придерживаются более ограничительного подхода. Такая неопределенность может затруднить массовое принятие криптовалют, поскольку предприятия и потребители могут не решаться использовать их без четких нормативных указаний;

• **пользовательский опыт** – криптовалюты должны предлагать пользовательский опыт наравне с традиционными методами оплаты или даже лучше, чтобы получить массовое распространение. Это включает в себя обеспечение максимально быстрых, простых и безопасных транзакций, что остается сложной задачей для многих криптовалют;

• **проблемы безопасности** – громкие случаи взломов и нарушений безопасности, связанные с криптовалютами, вызвали обеспокоенность по поводу их защищенности. Чтобы получить широкое признание, криптовалюты должны решить эти проблемы и продемонстрировать, что они могут предложить безопасные и надежные средства проведения транзакций.

Возможности для внедрения в мировую практику:

• **финансовая доступность** – криптовалюты могут предоставить финансовые услуги тем слоям населения, которые не имеют доступа к банковским операциям. Это создает потенциал для экономического роста и расширения прав и возможностей. Предоставление финансовых услуг через криптовалюты может способствовать их массовому принятию;

• **снижение затрат на транзакции** – криптовалюты могут предложить значительную экономию при трансграничных транзакциях и денежных переводах по сравнению с традиционными платежными системами. Это может стать мощным стимулом для предприятий и потребителей использовать криптовалюты в повседневных операциях;

• **инновации** – разработка новых технологий и усовершенствование существующих протоколов блокчейна может помочь решить проблемы масштабируемости, безопасности и удобства использования, с которыми сталкиваются криптовалюты. По мере развития этих технологий они могут проложить путь к более широкому распространению;

• **интеграция с существующими финансовыми системами** – интеграция криптовалют с традиционными финансовыми системами может способствовать их массовому принятию. Это включает в себя разработку криптовалютных дебетовых и кредитных карт, интеграцию с платежными процессорами, а также создание финансовых продуктов и услуг на основе криптовалют.

Новая финансовая эра: блокчейн, DeFi, Web3 и криптовалюты

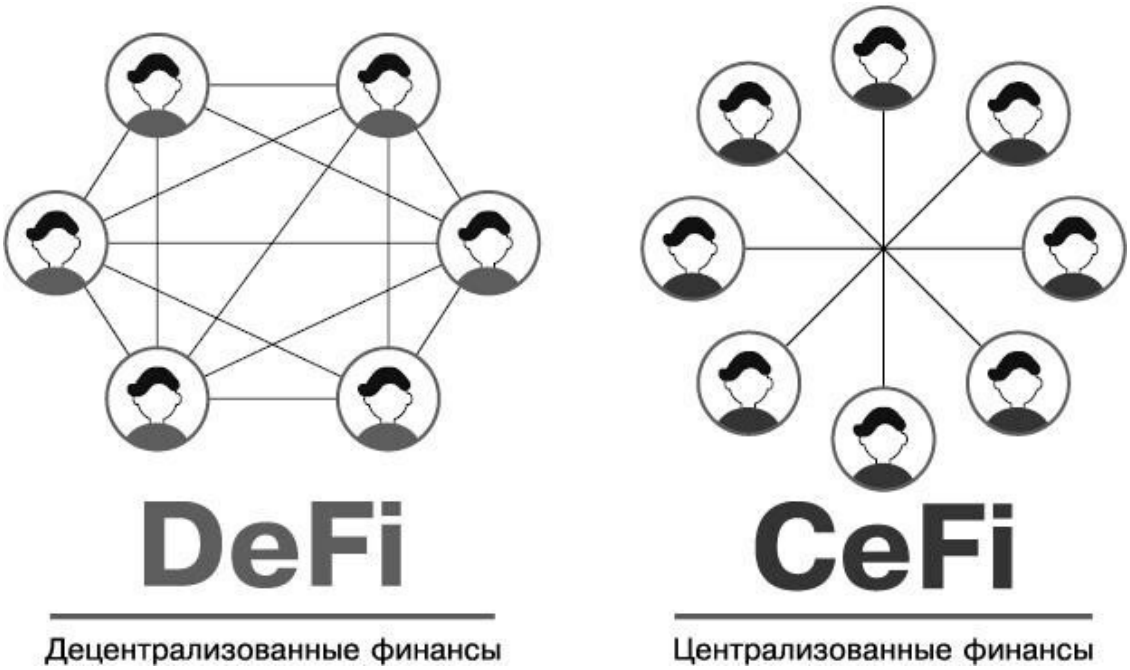
Пересечение финансов и технологий

В настоящее время мы наблюдаем слияние финансовой и технологической сфер, что приводит к появлению новаторских решений, способных изменить традиционные финансовые системы. *Цифровизация* финансовых услуг открыла путь для развития новых финансовых технологий и платформ, включая криптовалюты, цифровые кошельки и мобильные платежные решения. Эта тенденция привела к созданию более оптимальных, доступных и экономически выгодных финансовых услуг, позволяя потребителям и предприятиям эффективнее управлять своими финансами и с большей легкостью участвовать в глобальной экономике.

В последние годы сектор финансовых технологий, известный как *финтех*, переживает бурный рост: как стартапы, так и уже устоявшиеся компании используют новейшие технологии для предоставления прорывных финансовых продуктов и услуг. Это привело к усилению конкуренции и дезорганизации финансовой отрасли, поскольку традиционные финансовые учреждения вынуждены приспосабливаться и развиваться в соответствии с меняющимся ландшафтом.

Технология блокчейн, которая лежит в основе криптовалют, предлагает целый ряд приложений, выходящих за рамки цифровых активов. Она обеспечивает безопасные, прозрачные и децентрализованные транзакции, создавая фундамент для разработки новых финансовых платформ, продуктов и услуг, таких как *децентрализованные финансы* (DeFi) и *Web3*.

DeFi – это быстрорастущий сектор в блокчейн и криптовалютном пространстве, предлагающий широкий спектр финансовых услуг и продуктов, построенных на децентрализованных платформах. Цель DeFi – демократизация финансов путем использования технологии блокчейн для устранения посредников и формирования более доступных, прозрачных и эффективных финансовых систем. Ключевыми приложениями DeFi являются децентрализованное кредитование, децентрализованные биржи и токенизированные активы.



Web3 же относится к следующему поколению интернета, построенному на децентрализованных протоколах и инфраструктуре. Эта новая парадигма направлена на создание более открытого, безопасного и ориентированного на пользователя интернета, который дает людям возможность контролировать свои данные, личность и активы в Сети. Технологии Web3, такие как децентрализованные системы идентификации и децентрализованное хранение данных, могут иметь значительное влияние на финансовый сектор, обеспечивая новые формы цифровой идентификации, управления активами и конфиденциальности данных.

В конечном итоге пересечение финансов и технологий приводит к значительной модернизации финансового сектора, которая не может происходить без сбоев. Цифровизация финансовых услуг, подъем финтеха и появление технологий блокчейн, DeFi и Web3 открывают новые возможности и проблемы как для традиционных финансовых учреждений, так и для инновационных стартапов. В этой новой финансовой эре нам важно понять и принять потенциал этих технологий и их последствия для будущего финансов.

Инновации, определяющие будущее финансов

Сфера финансов развивается стремительными темпами, и появляющиеся технологии и платформы определяют ее будущее. Одной из таких технологий являются смарт-контракты – самоисполняющиеся контракты, в которых условия соглашения записаны непосредственно в коде. Эти программируемые контракты позволяют автоматически выполнять транзакции при заранее определенных условиях, устраняя необходимость в посредниках и повышая эффективность финансовых процессов. Смарт-контракты находят применение в различных областях финансов, таких как DeFi (о нем мы уже говорили ранее), токенизация активов и торговое финансирование.

Токенизация – это процесс представления классических активов, таких как акции, облигации, недвижимость и товары, в виде цифровых токенов на блокчейне. Это открывает возможности для создания новых финансовых продуктов и услуг, а также повышает ликвидность, снижает транзакционные издержки и делает доступнее традиционно неликвидные активы. Токенизация также способствует развитию формы привлечения инвестиций через предложение *токенизированных ценных бумаг* (Security Token Offerings, STO), которые явля-

ются более регулируемой и соответствующей нормативным требованиям формой привлечения средств по сравнению с первичными размещениями (предложениями) монет (Initial Coin Offerings, ICO).

В результате усиления взаимосвязанности мира и широкого распространения цифровых транзакций появляются все новые решения для *цифровой идентификации*. Важность систем цифровой идентификации, основанных на блокчейне, невозможно переоценить. Они способны в полной мере обеспечить пользователя безопасной, децентрализованной и управляемой им платформой для работы с цифровыми идентификационными данными. Эти решения находят применение в таких областях, как соблюдение KYC/AML, конфиденциальность данных и доступ к финансовым услугам.

По мере роста популярности криптовалют центральные банки по всему миру изучают возможность выпуска собственных цифровых валют. Цифровые валюты центральных банков (Central Bank Digital Currencies, CBDC) могут предложить ряд преимуществ, включая расширение финансовой доступности, снижение транзакционных издержек и улучшение реализации денежно-кредитной политики. Однако внедрение CBDC также вызывает озабоченность по поводу конфиденциальности, безопасности и потенциального влияния на традиционный банковский сектор.

В последние несколько лет возрос интерес к децентрализованным автономным организациям (Decentralized Autonomous Organizations, DAO). Это такие организации, которые управляются смарт-контрактами и функционируют на децентрализованной основе, а решения в них принимаются их членами. DAO могут найти применение в различных областях финансов, таких как децентрализованное управление активами, управление децентрализованными платформами и децентрализованное финансирование проектов.

Все более важную роль в финансовом секторе играют искусственный интеллект (ИИ) и машинное обучение, которые находят применение в таких областях, как выявление случаев мошенничества, кредитный скоринг и алгоритмическая торговля. Эти технологии помогают повысить эффективность, точность и результативность финансовых процессов, а также способствуют разработке новых продуктов и услуг.

Перспективы

По мере погружения в новую финансовую эру блокчейна и изучения DeFi, Web3 и криптовалют становится очевидным, что перед нами встает множество проблем, но их решение открывает окно невероятных возможностей. Быстрые темпы развития технологий в финансовом секторе подчеркивают необходимость *постоянных* инноваций. Внедрение и разработка новых технологий позволяют финансовым учреждениям, стартапам и разработчикам внести свой вклад в создание более инклюзивной, эффективной и прозрачной финансовой системы. Однако важно найти баланс между повсеместным применением нового функционала и управлением потенциальными рисками.

Будущее финансов будет определяться не только технологиями, но и *сотрудничеством* между традиционными финансовыми учреждениями, стартапами, регулирующими органами и другими заинтересованными сторонами. Работая вместе, эти различные группы могут обмениваться знаниями, ресурсами и опытом, создавая синергетический эффект, который должен способствовать разработке и внедрению новых финансовых решений. Сотрудничество необходимо для преодоления проблем, решения вопросов *регулирования* и содействия широкому распространению новых технологий. Хорошо функционирующая финансовая система требует надежной нормативной базы, которая защищает права потребителей, поддерживает стабильность рынка и способствует прогрессу. Поскольку финансовая система продолжает развиваться, для регулирующих органов крайне важно найти правильный баланс между поддержкой

инноваций и управлением потенциальными рисками. Это включает разработку четкой и гибкой нормативно-правовой базы, способствующей ответственному внедрению новых технологий и одновременно обеспечивающей безопасность и стабильность денежной системы.

Для того чтобы приблизить новое финансовое будущее, необходимо повышать *осведомленность* общественности о технологиях, платформах и решениях, формирующих это самое будущее. Эти мероприятия подразумевают повышение финансовой грамотности, предоставление образовательных ресурсов и развитие открытого диалога о преимуществах, рисках и возможностях применения новых финансовых технологий.

Растущее внимание к воздействию на окружающую среду является важным фактором для будущего цифровых финансов. Это включает в себя решение вопросов энергопотребления и воздействия криптовалют на *экологию*, а также исследование потенциала блокчейна и других технологий для поддержки устойчивого финансирования и инициатив в области охраны окружающей среды, социальной сферы и управления (Environmental, Social, and Governance, ESG).

Надо признать, что путь, который нам предстоит пройти в новой финансовой эре, полон не только перспектив, но и неопределенностей. Однако, чтобы раскрыть весь потенциал блокчейна, DeFi, Web3 и криптовалют, нужно помнить:

- о необходимости постоянных инноваций;
- сотрудничестве;
- вопросах нормативного регулирования;
- важности образования и осведомленности;
- воздействии на окружающую среду.

Глава 2. История криптовалют. От Биткоина до альткоинов

Истоки Биткоина: Сатоши Накамото и «белая книга»

Напомню, что история криптовалют началась с создания Биткоина – первой и самой известной цифровой валюты. В 2008 году некто под псевдонимом Сатоши Накамото представил миру документ под названием «Биткоин: одноранговая система электронных денег». В нем была изложена концепция децентрализованной цифровой валюты, которая позволяла бы осуществлять прямые одноранговые транзакции без участия посредников, таких как банки или финансовые учреждения.

В этом же документе было представлено несколько новаторских концепций, которые стали основой для Биткоина и более широкой криптовалютной экосистемы:

- децентрализация;
- блокчейн;
- механизм консенсуса Proof of Work (PoW);
- криптография;
- ограниченная эмиссия.

Децентрализованный характер Биткоина, обеспечиваемый технологией блокчейн, исключает возможность контроля над сетью со стороны отдельных организаций или групп (включая центральные органы власти). Блокчейн, в свою очередь, представляет собой распределенный реестр, где все транзакции записываются в связанных между собой блоках. Эта инновационная структура данных обеспечивает прозрачную, безопасную и защищенную от взлома запись транзакций, а также предоставляет механизм консенсуса, необходимый для поддержания работы сети.

Механизм консенсуса PoW, лежащий в основе Биткоина и обеспечивающий безопасность сети и справедливое распределение новых монет между участниками, требует от майнеров решения сложных математических задач для подтверждения транзакций и добавления новых блоков в блокчейн.

Для обеспечения безопасности транзакций, конфиденциальности пользователей и целостности сети Биткоин использует передовые криптографические технологии. Криптография с открытым ключом позволяет пользователям отправлять и получать биткоины, не раскрывая своей подлинной личности, а криптографические хеш-функции помогают защитить сеть от злоумышленников.

Одной из ключевых особенностей Биткоина является ограниченное предложение в 21 миллион монет, что создает цифровой дефицит и помогает поддерживать его стоимость с течением времени. Эта дефляционная модель резко контрастирует с традиционными фиатными валютами, которые могут быть дополнительно выпущены центральными банками в процессе количественного смягчения.

С тех пор, как документ был опубликован, Биткоин из нишевого проекта среди энтузиастов криптографии превратился в глобальный феномен, который привлек внимание не только частных инвесторов и широкой общественности, но и правительств! Успех Биткоина подготовил почву для создания тысяч альтернативных криптовалют (альткоинов), каждая из которых имеет свои уникальные особенности, сценарии использования и целые сообщества. В следующих разделах этой главы мы рассмотрим историю криптовалют за пределами Биткоина, выделив основные вехи и события в быстро развивающемся мире цифровых активов.

Первые дни Биткоина: майнинг, транзакции и распространение

Первые дни существования Биткоина были пронизаны атмосферой экспериментов, сотрудничества и открытий среди небольшой группы преданных энтузиастов. В этом разделе мы рассмотрим начальные этапы развития Биткоина, начиная с первых попыток майнинга и заканчивая ростом пользовательской базы и все более широким принятием в качестве формы цифровой валюты.

Сеть Биткоин ожила 3 января 2009 года благодаря майнингу блока Genesis, также известного как блок 0. Этот первый блок содержал сообщение от Сатоши Накамото, которое ссылалось на заголовок из газеты The Times: «The Times 03/Jan/2009. Канцлер на пороге очередного спасения банков». Данное сообщение рассматривается как намек на финансовый кризис и мотивацию создания децентрализованной валюты. А уже 12 января Сатоши провел первую в истории транзакцию Биткоина ныне покойному Хэлу Финни, известному криптографу и ключевому участнику проекта Биткоин. Это положило начало использованию Биткоина в качестве средства обмена между физическими лицами. В этом же году Сатоши Накамото выпустил первую версию программного клиента для своего детища, позволив пользователям добывать (майнить), отправлять и получать Биткоин. Со временем ПО развивалось и привлекало все больше разработчиков, которые вносили свой вклад в его усовершенствование и доработку. Сатоши общался с растущим сообществом через электронную почту и различные форумы, в том числе форум BitcoinTalk, обсуждая идеи, исправляя ошибки и закладывая основу для будущего развития Биткоина.

По мере роста интереса к Биткоину пользователи начали искать способы торговать им, и в 2010 году была запущена биржа BitcoinMarket.com, которая позволила людям обменивать биткоины на фиатные валюты. В это же время первые майнеры начали объединять свои ресурсы, чтобы увеличить шансы на получение вознаграждения за добычу, что привело к появлению первых *майнинговых пулов* и профессионализации майнинга.

В 2011 году был запущен печально известный даркнет-рынок Silk Road, позволявший пользователям покупать и продавать нелегальные товары, используя биткоины в качестве платежного средства. Хотя данное событие привлекло повышенное внимание к Биткоину, это также вызвало негативные ассоциации с ним из-за преступной деятельности и поставило под сомнение потенциал цифровой валюты в плане облегчения незаконных операций.

Несмотря на первоначальные трудности, сообщество Биткоина продолжало расти, а сама цифровая валюта завоевала популярность в качестве альтернативной формы денег. Новаторы, разработчики и энтузиасты со всего мира собрались вместе, чтобы изучить потенциал этой революционной технологии, заложив основы для роста Биткоина в качестве цифрового актива и развития альтернативных криптовалют.

Конец ознакомительного фрагмента.