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.

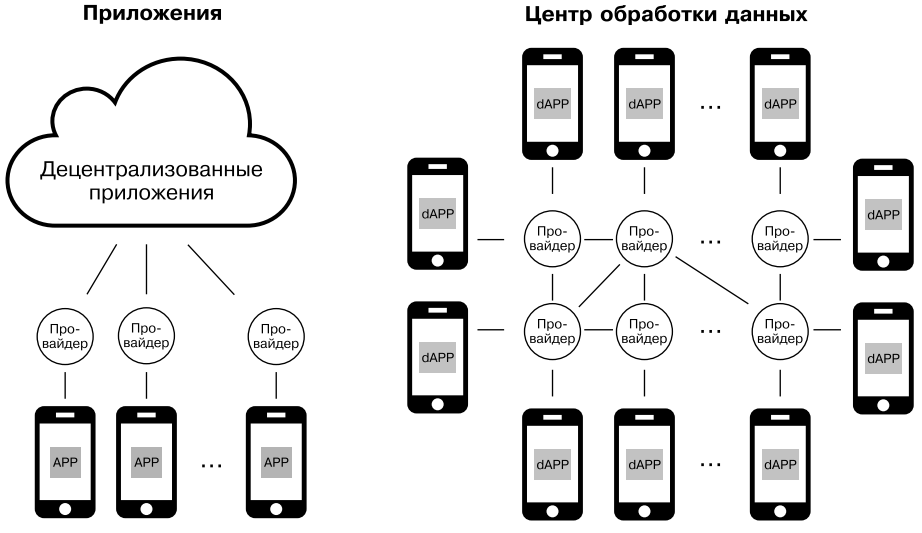
Распространение альткоинов значительно расширило масштабы и потенциал криптовалютной экосистемы. Благодаря постоянному развитию новых блокчейн-платформ, цифровых активов и децентрализованных приложений мир криптовалют становится все более разнообразным, предлагая пользователям широкий спектр возможностей 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.

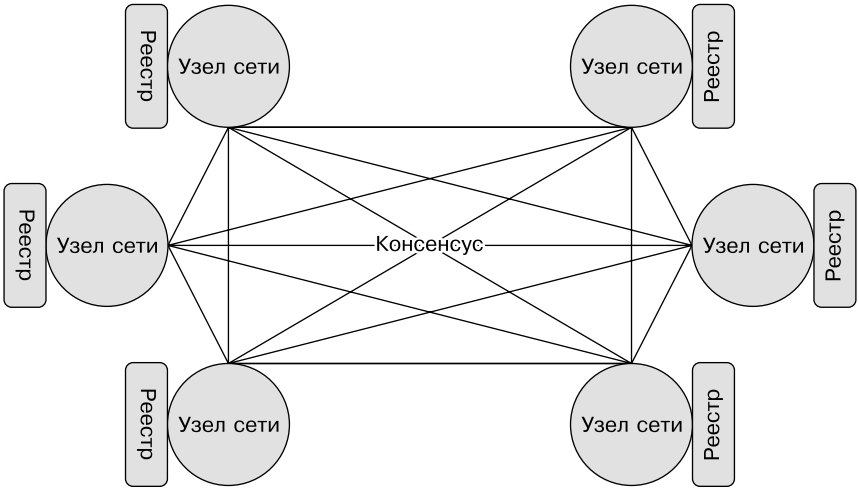


Преимущества децентрализации в криптовалютах многочисленны. Перечислим и кратко опишем некоторые из них.

- **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.

Как работает Блокчейн

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 предприятиями 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.