**Применение блокчейн технологий к классическим банковским операциям**

**Субботин Павел**

**Ноябрь 2022**

1. **Введение.**

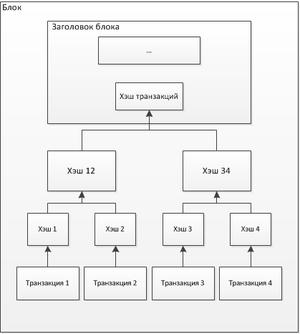
В 2008 году Сатоши Накамото опубликовал документ под названием «Биткоин: электронная одноранговая платежная система», содержащий описание схему работы криптовалюты. А уже 3 января 2009 года был сгенерирован первый блок и первые 50 биткойнов. В то время данные события прошли почти незамеченными, однако именно они положили начало новый эры цифровых валют. Сейчас курс биткоина колеблется около отметки в 20000 долларов, а на пике стоимость 1 биткоина составляла более 60000 долларов.

Такой ошеломительный успех во многом связан с применением новой технологии «блокчейн» для подтверждения транзакций. В данной работе я бы хотел подробнее рассмотреть эту технологию и составить обзор на возможность ее применения для классических банковских операций.

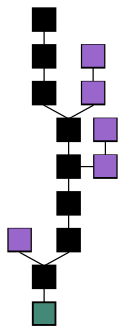


1. **Обзор технологии блокчейн.**

Исходя из названия уже можно понять, что блокчейн является некой цепью. Это действительно так: технология представляет из себя последовательную непрерывную цепочку блоков, составленную по некоторым правилам. Для обеспечения правильного порядка блоков и неизменности информации в уже имеющихся узлах цепи используются хеш-суммы. Более подробно данный процесс я рассмотрю на реализации блокчейна в системе Биткоин.



В данной системе используется цепочка блоков транзакций для подтверждения осуществления переводов криптовалюты между пользователями. Транзакция считается завершённой и подтверждённой, когда проверены её формат и подписи, и когда сама транзакция объединена в группу с несколькими другими и записана в блок. Содержимое блоков может быть проверено, так как каждый блок содержит информацию о предыдущем. При этом, блоки выстроены в одну цепочку, которая содержит информацию обо всех совершённых когда-либо операциях в базе. Вся цепочка блоков является открытой и общедоступной. В каждом блоке содержится его хеш, хеш предыдущего блока, а также хеши транзакций, которые необходимо обработать и записать. Одна из записанных транзакций является наградой майнеру (тому, кто предоставляет свои вычислительные мощности для расчетов) за выполненную работу. Созданный блок будет принят остальными пользователями, если числовое значение хеша заголовка равно или меньше определённого целевого числа, величина которого периодически корректируется. Изменение данного параметра нужно для того, чтобы скорость создания новых блоков оставалась примерно постоянной и не зависела от текущей подключенной вычислительной мощности. Создание блоков происходит на множестве реплик главной цепочки по всему миру и при помощи ограничений всегда сохраняется главная последовательность блоков, что позволяет избежать дублирования транзакций.



Пока транзакция не включена в блок, система считает, что количество биткойнов на некотором адресе остаётся неизменным. В это время есть техническая возможность оформить несколько разных транзакций по передаче с одного адреса одних и тех же биткойнов разным получателям. Но как только одна из подобных транзакций будет включена в блок, остальные транзакции с этими же биткойнами система будет уже игнорировать. Например, если в блок будет включена более поздняя транзакция, то более ранняя будет считаться ошибочной. Есть небольшая вероятность, что при ветвлении две подобные транзакции попадут в блоки разных ветвей. Каждая из них будет считаться правильной, до момента выбора главной последовательности блоков, в которую попадет только одна из транзакций. При этом не будет иметь значения время совершения операции. Теоретически есть возможность изменение одного из уже подтвержденных блоков транзакций, что приведет к некорректному перераспределению криптовалют, однако данная возможность на практике ограничена тем, что для изменения старого блока нужно будет пересчитать хеши всех последующих, то есть потребуется вычислительная мощность эквивалентная затраченной на расчет измененного и всех следующих после него блоков, что на практике практически невозможно. Благодаря описанным ограничениям, за все время существования биткоина ни разу не было зафиксировано двойного расходования средств, что говорит о надежности процесса совершения транзакций криптовалют при помощи блокчейна.

[https://web.archive.org/web/20160307000342/https://blockchain.info/ru/charts/n-orphaned-blocks?timespan=all&showDataPoints=false&daysAverageString=1&show\_header=true](https://web.archive.org/web/20160307000342/https:/blockchain.info/ru/charts/n-orphaned-blocks?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true)

Закончить данный блок хотелось бы подведением некоторых промежуточных итогов и выделением преимуществ и недостатков использования транзакций на базе блокчейна.

Плюсы:

1. Отсутствие посредников при совершении операций: в данном случае посредники на самом деле есть, но они деперсонализированы и не вступают в прямой контакт с участниками транзакции, что делает процесс более «рыночным» и прямолинейным
2. Гибкость комиссии: люди совершающие операции могут сами устанавливать вознаграждение за ее выполнение, тем самым влияя на скорость ее выполнения

Минусы:

1. На поддержку системы тратится большое количество электроэнергии и железа, что приводит к росту цен на видеокарты по всему миру, а также негативно сказывается на экологии.

<https://www.forbes.ru/tehnologii/377899-bitkoin-gubit-planetu-uglerodnyy-sled-mirovogo-mayninga-raven-vybrosam-krupnogo>

<https://www.forbes.ru/newsroom/tehnologii/422179-rost-kriptovalyut-privel-k-povysheniyu-sprosa-na-poderzhannye-videokarty>

1. Обязательное наличие комиссии за совершения операции. При отсутствии вознаграждения за выполнение операций исполнителям становится невыгодно ее обсчитывать, что приводит к тому, что операция не будет произведена.
2. Сложность в обмене на традиционные валюты. Чтобы обменять криптовалюту на обычную или наоборот, необходимо использовать специальные обменники, которые зачастую имеют немалую комиссию, не регулируются государством, часто привлекают внимание регулирующих органов, а также могут сливать информацию о пользователях. Так же операции с криптовалютой в России могут привести к блокировке счета в банке по 115-ФЗ

<https://www.rbc.ru/crypto/news/61a8b1e89a794759b30063e6>

Неоднозначные моменты:

1. Анонимность пользователей: сложно дать точную оценку того, насколько анонимным является, например, биткоин, не являясь экспертом в данной области, поэтому в данном пункте я дам комментарий основываясь на предположении, что пользователей действительно нельзя отследить.

* Плюсом анонимности является большая свобода пользователей, сохранность личных данных и отсутствие контроля за оборотом средств со стороны государства.
* Отсутствие контроля за транзакциями имеет, в том числе, и негативные последствия, так как анонимная платформа может использоваться для торговли многими нелегальными товарами, сильно снижая риск быть пойманным.

<http://www.consultant.ru/document/cons_doc_LAW_158661/>

1. Общий доступ к совершенным транзакциям:

* С одной стороны, данная особенность делает систему прозрачной и повышает доверие пользователей
* С другой стороны, если владелец конкретного кошелька будет идентифицирован, полная информация о его транзакциях может быть использована против него.

1. Операция с криптовалютой не может обрабатываться моментально, так как для ее осуществления необходимо подтверждение. Если сравнивать с банками, то, кажется, что по скорости перевода денег технологии на основе блокчейна проигрывают, однако без задержки переводы через банки происходят далеко не всегда и не во всех странах и при сравнительно небольших суммах перевода.

Как можно видеть из описанных факторов, транзакции на базе блокчейна довольно неоднозначны и имеют как немало минусов, так и преимущества, которые практически невозможно получить другими известными методами.

1. **Как работают операции в банках.**

Деятельность банков регулируется государством, в котором этот банк работает. Например, в России проведение банковских операций должно соответствовать Гражданскому Кодексу РФ и законодательству, прописывающему нормы банковского хозяйствования. Это Федеральный закон от 2 декабря 1990 г. № 395-1 "О банках и банковской деятельности". Данный закон накладывает на банки множество ограничений и дает людям некоторые гарантии сохранности их капитала. Банки – это хорошо знакомая всем структура, которой мы пользуемся каждый день, поэтому я не буду подробно расписывать все механизмы проведения банковских операций и перейду сразу к преимуществам и недостаткам.

Плюсы:

1. Государственные гарантии. Как я уже писал выше деятельность банков регулируется государством, поэтому имеются неплохие гарантии сохранности денег и выполнения банком своих обязательств, однако в зависимости от страны и экономики даже государство не всегда может быть хорошим гарантом.
2. Простота использования и доступность. Чтобы начать пользоваться банковским продуктами и совершать операции, сейчас даже не обязательно приезжать в отделение, так как некоторые банки предлагают доставку карточек, а также имеют удобные многофункциональные приложения, в которых за пару минут можно сделать практически любые необходимые действия
3. Системы лояльности. Чтобы сохранить клиентов банки предлагают все больше сервисов и спецпредложения для своих клиентов, что позволяет легко получать скидки или, например, кэшбек.

Минусы:

1. Зависимость от государства. Так как государство регулирует деятельность банков на своей территории, то оно может устанавливать правила, которые ему выгодны, поэтому сейчас осуществляется контроль операций физических и юридических лиц со стороны государства, а также возможна блокировка средств третьих лиц по инициативе государства.
2. Большие затраты на поддержание стабильности системы переводов и приложений со стороны банка.
3. Утечки данных. Так как банк должен иметь информацию о своих клиентах, он хранит ее на серверах и иногда мы можем видеть утечки данных пользователей.
4. Комиссия банков за операции по картам. В России банки берут комиссию в размере 1-2% за переводы денег через них при покупках через терминалы, что не выгодно продавцам.

<https://www.sravni.ru/biznes/ekvajring/>

По итогам написанного выше мы видим, что банк в качестве посредника между людьми и деньгами довольно удобен, однако имеет ряд недостатков, с которыми сложно бороться.

1. **Смарт-контракты**

В данном блоке я бы хотел описать один из методов взаимодействия с использованием блокчейна без посредников между пользователями, который может выступить аналогом некоторым операциям, которые сейчас происходят через банк.

Сам термин был придумал Ником Сабом в 1994 году, однако практическая его реализация стала возможна с появлением блокчейна. Смарт-контракт разрабатывается на одном из языков, спроектированных для трансляции в байт-код виртуальной машины Ethereum. Самым популярным языком на данный момент является Solidity. Суть смарт-контракта заключается в том, что в нем кодируются определенные действия, которые автоматически исполняются при выполнении описанных в контракте условий. Стороны подписывают умный контракт, используя методы, аналогичные подписанию отправки средств в действующих криптовалютных сетях. После подписания сторонами контракт сохраняется в блокчейне и вступает в силу. Для обеспечения автоматизированного исполнения обязательств контракта непременно требуется среда существования (например узлы блокчейна Ethereum), которая позволяет полностью автоматизировать выполнение пунктов контракта.

**Объекты умного контракта — это**

* **Подписанты** — стороны умного контракта, принимающие или отказывающиеся от условий с использованием электронных подписей. Прямым аналогом является подпись отправителя средств в сети Bitcoin, которая подтверждает внесение транзакции в цепочку блоков.
* **Предмет договора**. Предметом договора может являться только объект, находящийся внутри среды существования самого умного контракта, или же должен обеспечиваться беспрепятственный, прямой доступ умного контракта к предмету договора без участия человека.
* **Условия**. Условия умного контракта должны иметь полное математическое описание, которое возможно запрограммировать в среде существования умного контракта. Именно в условиях описывается логика исполнения пунктов предмета договора.
* **Децентрализованная платформа**. Для распределенного хранения смарт-контракта необходима его запись в блокчейне этой платформы.

Имея в арсенале такой инструмент, мы можем переходить к обзору возможностей использования блокчейн технологий в банковских операциях.

1. **Применение блокчейн технологий к классическим банковским операциям.**

Раннее в тексте я довольно подробно рассказал о применении блокчейна для транзакций между пользователями, однако неосвященной осталась одна проблема, которая, на мой взгляд, имеет большое значение, если рассматривать внедрение систем на основе блокчейна в привычные транзакции. Проблема заключается в высокой волатильности криптовалют. Люди хотят иметь точное представление о имеющемся у них количестве денег, поэтому необходимо либо при переводе совершать 2 обмена, что приведет к большой стоимости операции за счет нескольких комиссий, либо искать другой выход. Этим выходом могут стать «стейблкоины». Stablecoin – это общее название криптовалют, обменный курс которых стараются стабилизировать, например, привязывая котировки к обычным валютам или биржевым товарам (золото, нефть). Одним из наиболее известных примеров стейблкоина является USDC – криптовалюта, курс которой всегда примерно равняется одному доллару.



<https://ru.investing.com/crypto/usd-coin/chart>

Токенизация доллара США в USDC происходит в три этапа:

1. Пользователь отправляет доллары США на банковский счёт эмитента монеты.
2. Эмитент использует смарт-контракт USD Coin для создания эквивалентного количества USD Coin.
3. Недавно отчеканенные монеты в долларах США отправляются пользователю, а заменённые доллары США хранятся в резерве.

USDC управляется консориумом Centre, основанным компанией Circle. По заявлению Circle, каждая монета USDC обеспечена долларом, находящимся в резерве, или другими «утверждёнными инвестициями», хотя они не детализированы. Как можно видеть не графике такой концепт действительно работает и курс USDC весьма стабилен.

Однако из-за такой системы стейблкойны имеют очевидный недостаток - необходимый для поддержания курса уровень доверия к централизованному механизму обмена противоречит децентрализованной природе криптовалют.

Данную проблему решить сложно, однако в банки все равно зависят от государства и не смогут свободно использоваться нерегулируемые технологии на основе блокчейна, поэтому, на мой взгляд, на этот компромисс придется пойти, чтобы использовать другие преимущества блокчейна и криптовалют. Если же пытаться организовать рынок банковских продуктов без самих банков, то на смену им скорее всего придут другие аналогичные организации, так как государство хочет сохранять контроль над денежными операциями пользователей.

Тема стейблкоинов сейчас довольно популярна, и в России также планируется создание криптовалюты, обеспеченной рублем.

<https://www.banki.ru/news/lenta/?id=10059732>

Пользуясь допущением о влиянии государства на торговлю на базе блокчейна, можно перейти к рассуждению на тему того, как блокчейн можно использовать в других банковских продуктах, а именно кредитах и вкладах.

Механизм предоставления средств в долг или наоборот вклада средств в криптовалюте на базе блокчейна уже реализован, и я бы хотел дать его подробное описание. Основным подходом для заимствования средств сейчас является *overcollaterisation* или избыточное обеспечение. Суть данной модели заключается в том, что чтобы взять в долг x условных единиц, ты должен сначала вложить y условных единиц, где y \* *liquidation factor >=* x.

Суть данного механизма заключается в том, что вложенные y условных единиц являются вкладом, и за них клиент получает проценты большие, чем платит за заимствование денег. x денег после внесения вклада можно использовать, как собственные средства, однако после завершения срока займа необходимо внести их на счет вместе с процентами, иначе твой аккаунт будет заблокирован, а внесенные y условных единиц вместе с процентами будут изъяты. Выполнение данного соглашения фиксируется смарт-контрактом. То есть, по сути, данная система избавляет людей от посредника в виде банка, если внутри системы поддерживается необходимый капитал. Из плюсов метода избыточного обеспечения хочется выделить отсутствие для кредитодателя риска не получить деньги обратно, что позволяет, например, не проводить процедуру скоринга заемщика, однако это порождает и минус для заемщика – невозможно получить деньги, если у тебя их нет.

На мой взгляд, данный подход к кредитованию весьма интересен и может захватить часть рынка вкладов и кредитования, где люди и компании используют кредиты и клады, как финансовый инструмент для увеличения или сохранения уже имеющегося капитала.

[Здесь](https://github.com/PavelSubbotin/blockchain_instead_of_banks/blob/main/compound.rs) вы можете ознакомиться с моей реализацией смарт-контракта на основе акторной модели взаимодействия. Как можно видеть, код занимает небольшое количество строк, но, тем не менее, может использоваться для вложения средств и кредитования, если будет подключен к необходимой инфраструктуре. Далее я хотел бы рассмотреть плюсы и минусы данной реализации.

**Плюсы:**

* Скорость: акторная модель взаимодействия позволяет использовать распараллеливание процессов, что ускоряет вычисления

<https://libeldoc.bsuir.by/bitstream/123456789/47650/1/Sorogovets_Preimushchestva.pdf>

* Масштабируемость и отказоустойчивость: так же благодаря акторной модели мы можем легко добавить возможность обработки больших данных, кроме того, обмен сообщениями позволяет отлавливать ошибки отдельных частей процесса.

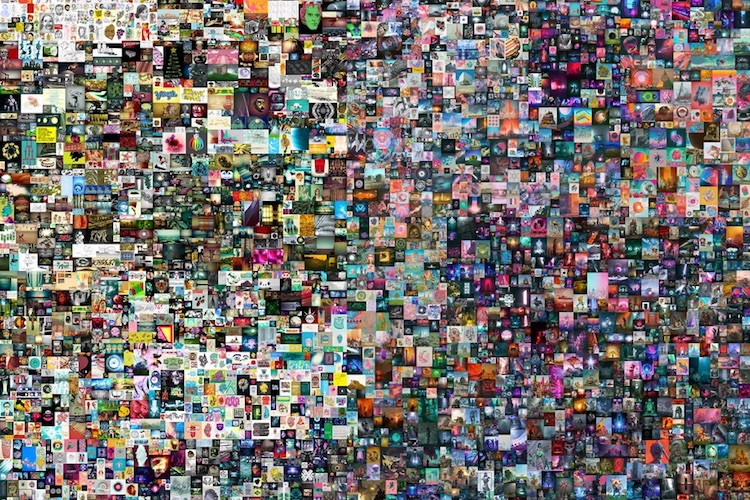
<https://habr.com/ru/post/322250/>

* Простота реализации: аналогичные контракты с измененными условиями несложно написать, что позволяет без особых усилий писать контракты под различные нужды.
* Прозрачность: имея базовые навыки программирования и комментарии автора контракта довольно легко понять, что делает контракт, поэтому пользователи могут самостоятельно убедиться в безопасности его использования

**Минусы:**

* Ограниченность применения: данный смарт-контракт является учебным примером и может применяться для весьма ограниченного числа сценариев.
* Общее хранилище: в данной реализации для сохранения информации о пользователе используется единая структура BTreeMap, что будет негативно влиять на производительность при большом числе пользователей.
* Ограниченный функционал: в коде нет поддержки ликвидаций (бана пользователей, которые нарушили концепцию избыточного обеспечения) и пула резерва (хранилища денег, изъятых у тех, чьи аккаунты заблокировали).

Еще один банковский продукт, который я хотел бы рассмотреть – это ипотека. В наше время ипотека пользуется большим спросом, так как самостоятельно накопить капитал для покупки жилья подавляющему большинству людей сложно или просто невозможно, причем покупка квартиры в ипотеку может оказаться выгодной сделкой из-за инфляции. Из рассмотренных инструментов, которые работают с блокчейном нет тех, которые способны подтверждать право собственности на что-либо, однако такой инструмент потенциально может существовать и это NFT. NFT расшифровывается как *non-fungible token,* что означает невзаимозаменяемый токен. Это вид криптографических токенов, каждый экземпляр которых уникален и не может быть обменян или замещен другим аналогичным токеном, хотя обычно токены взаимозаменяемы по своей природе. Сейчас NFT подвергается большой критике из-за высоких затрат на электроэнергию и большого выброса углерода в процессе проверки транзакций, а также из-за использования NFT мошенниками. Под сомнение ставится и полезность установки права собственности на зачастую нелегальном нерегулируемом рынке. Однако уже сейчас NFT активно применяется для покупки прав обладания цифровым искусством при помощи смарт контрактов, причем суммы сделок в какой-то момент стали просто огромными. Например, NFT на цифровая картина «Первые 5000 дней» был продан почти за 70 миллионов долларов, хотя копию данной картины я бесплатно приложу ниже.



<https://en.wikipedia.org/wiki/Everydays:_the_First_5000_Days>

70 миллионов долларов во много раз превышает стоимость квартиры в Москве, что свидетельствует о том, что инструмент по покупке NFT может быть применен практически для чего угодно, если добавить в механизм контроль от государства. Поэтому мне кажется, что и выдача ипотеки в скором времени может быть автоматизирована при помощи блокчейна.

1. **Заключение**

Как можно видеть из написанного выше, блокчейн может найти применение во многих сферах банковских услуг, если будут приняты соответствующие законы со стороны государства. Это позволит построить децентрализированную систему контроля операций, уменьшить издержки банков на поддержание необходимой инфраструктуры (если банки будут организаторами платформ на базе блокчейна)

<https://mgimo.ru/upload/iblock/62d/13.%20%D0%9F%D0%B0%D0%BD%D0%BE%D0%B2%D0%B0.docx>

Так же технологии на основе блокчейна могут сделать многие процессы прозрачнее для пользователей, а в долгосрочной перспективе уменьшить количество мошенников или вовсе сделать их занятие бесполезным.

<https://www.securitylab.ru/analytics/496202.php>

Мои выводы частично подтверждаются словами ведущих российских специалистов в области финансов с форума инновационных финансовых технологий в 2016 году в Иннополисе, на котором обсуждали будущее криптовалют в России и пришли к выводу, что данная отрасль будет стремительно развиваться.

<https://www.youtube.com/watch?v=xpe2qSDEZZ0>

1. **Материалы**

<https://cyberleninka.ru/article/n/bitkoin-kak-novyy-etap-liberalizatsii-finansovoy-sfery/viewer>

<http://congressavia.ru/works/konferenciya-blokcheyn-novaya-neft-rossii-ginnopolis-rt-1195-chel>

<https://www.forbes.ru/forbeslife/450565-tokeny-prevrasautsa-v-luks-10-samyh-dorogih-nft-proizvedenij-na-aukcionah-2021-goda>

<https://ru.wikipedia.org/wiki/NFT#%D0%94%D1%80%D1%83%D0%B3%D0%B8%D0%B5_%D1%81%D0%BF%D0%BE%D1%81%D0%BE%D0%B1%D1%8B_%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F>

<https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%B9%D0%B1%D0%BB%D0%BA%D0%BE%D0%B9%D0%BD>

<https://ru.wikipedia.org/wiki/USDC>

<https://vc.ru/u/903848-egor-polyanskiy/389872-chto-takoe-usdc-i-chem-on-otlichaetsya-ot-steyblkoyna-usdt>

<https://ru.investing.com/crypto/usd-coin/usdc-usd>

<https://vc.ru/crypto/250192-zaymy-na-blokcheyne-ot-lombardov-k-kreditnym-institutam>

<https://www.youtube.com/watch?v=pv0WEwkNDPQ>

<https://ru.wikipedia.org/wiki/%D0%A1%D0%BC%D0%B0%D1%80%D1%82-%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%B0%D0%BA%D1%82>

<https://lenta.ru/news/2016/10/13/blockchain/>

<https://www.youtube.com/watch?v=xpe2qSDEZZ0>

<https://www.youtube.com/watch?v=7UqrmZ89M9M>

<https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD>

<https://habr.com/ru/company/iticapital/blog/340992/>

<https://www.forbes.ru/mneniya/456381-cto-takoe-blokcejn-vse-cto-nuzno-znat-o-tehnologii>

<https://cyberleninka.ru/article/n/perspektivy-primeneniya-tehnologii-blockchain-v-bankovskoy-sfere/viewer>

Денис Баринов – разработчик смарт-контрактов в Gear Inc