ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИИ БЛОКЧЕЙНА

С. З АБДАЗИМОВ
Преподаватель кафедры Информационных технологий
Академии Министерства внутренних дел Республики Узбекистана

Аннотация: *В данной статье рассматривается технология блокчейн и ее применение, а также ее роль в обеспечении экономической стабильности общества.*

Ключевые слова: *кибербезопасность, технология блокчейн, цифровой экономики, системы клиринга, консенсус.*

Annotation: *This article discusses blockchain technology and its application, as well as its role in ensuring the economic stability of society.*

Keywords: *cybersecurity, blockchain technology, digital economy, clearing systems, consensus.*

В настоящее время технология блокчейн стремительно развивается и имеет перспективные шансы на внедрение в нашу повседневную жизнь. Данная технология имеет множество преимуществ, которые помогли бы оптимизировать различные процессы во многих сферах общественной жизни человека: экономической, политической и т.д., однако наличие определенных проблем мешает ее масштабному внедрению. Она может быть применена в различных секторах экономики: реальном, аграрном, финансовом. Рассмотрим использование блокчейн-технологии в финансовом секторе, ведь сегодня в условиях цифровой экономики появляется необходимость использования системы распределённого реестра, который обладает большим потенциалом и может привнести простоту, прозрачность и эффективность в финансовую область.

Блокчейн (от английского "block" – блок, "chain" – цепь) – распределенная база данных, содержащая информацию обо всех проведенных участниками системы транзакциях. Информация в данной системе хранится в виде «цепочки блоков», в каждом из которых записано определенное число произведенных операций. Основным свойством такой системы является распределенность. Это говорит о том, что не существует единого места хранения всех записей реестродержателя. Такой распределенный реестр хранится у всех участников системы одновременно [1].

Главной особенностью блокчейна является использование алгоритмов математического вычисления, а также исключение человеческого фактора при принятии решения системой. Блокчейн практически сводит к нулю вероятность внесения новых несанкционированных блоков и хакерских взломов. Общедоступность и защищенность технологии блокчейн обеспечивается:

- трудными математическими алгоритмами;
- специальными программами криптографирования;

•мощными компьютерами, включенными в систему, между которыми распределяются все данные [2].

•Каждый блок, появляющийся в системе, тесно связан с предыдущим, и в его названии заключены ссылки на прошлый блок. Процесс хеширования необратим, и в случае изменения данных в документах произойдут изменения в цифровых подписях. Несоответствие будет мгновенно выявлено в системе, о чем она просигнализирует.

•Основной прорыв технологии блокчейн произошел в 2009 г. и связан с появлением и реализацией криптовалюты биткоин. С 2009 г. уже прошло 11 лет, но технология блокчейн используется лишь локально и преимущественно частными компаниями или только в сфере цифровых денег. Так или иначе, уже сейчас становится понятно, что такая технология будет двигателем прогресса экономики, в частности финансового сектора, в ближайшие годы.

•С учетом того, что в настоящее время глобальная банковская деятельность в отрасли составляет 134 триллион. промышленности, технология блокчейна и DLT могут лишить посредников ключевые услуги, которые предоставляют банки, включая:

•Платежи. Путем создания децентрализованной бухгалтерской книги для платежей (например, Биткойн) технология блокчейна может способствовать более быстрым платежам при более низких комиссионных, чем в банках.

•Системы клиринга[52] и расчетов: Распределенные регистры могут снизить эксплуатационные расходы и приблизить нас к операциям в реальном времени между финансовыми учреждениями.

Сегодня технология блокчейн имеет большую возможность изменить финансовый сектор. Согласно проведенному исследованию IBM C-Suite Study 2017, более 30% компаний, которые проводят эксперименты, а также способны внедрить блокчейн в 2017 г., относятся к финансовой области [3]. Внедрение распределенного реестра в широкую практику коснется деятельности розничных банков, банков, обслуживающих крупных клиентов, инвестиционных банков, брокерских фирм, платежных сетей и т.д.

Во-первых, технология позволит осуществлять операции без посредников. Сегодня посредниками выступают специалисты по инвестиционно-банковской деятельности, компании, по венчурным инвестициям, брокеры, чьи гонорары могут достигать внушительных размеров. Вместо того чтобы обращаться к третьим лицам, например финансово-кредитным организациям, в качестве посредников при проведении транзакций, узлы блокчейн-сети используют специальный протокол консенсуса для согласования содержимого реестра, а также криптографические алгоритмы хеширования и электронно-цифровые подписи для обеспечения

[52]**Кли́ринг** (англ.*Clearing*-очистка) - безналичные расчёты между странами, компаниями, предприятиями и банками за поставленные, проданные друг другу товары, ценные бумаги и оказанные услуги, осуществляемые путём взаимного зачёта, исходя из условий баланса платежей.

целостности транзакции и передачи ее параметров. За счет этого значительно повышается скорость транзакций и частота обмена информацией. Поскольку в блокчейне нет центрального органа, проверить подлинность транзакции может любой участник системы. Так, например, «Смарт контракты» позволяют регулировать и контролировать исполнение обязательств по договору. Тем самым появляется возможность снизить размеры комиссий и предоставить клиентам услугу на более выгодных условиях.

Во-вторых, блокчейн дает возможность развития новой аналитики данных, которой будет свойственна высокая степень конфиденциальность и защита личных данных. К примеру, внедрение новой аналитики данных в финансовый сектор оптимизирует процесс одобрения заявки на ипотечное кредитование. Заемщикам будет предоставляться возможность обмена данных о личных доходах и расходах с кредиторами с применением блокчейн-технологии. С её помощью можно будет избежать большого количества ошибок и мошенничества, а также отнимающего много времени процесса ручного сбора различных документов на бумажных носителях. Информация о заемщиках с учетом высокой степени ее защиты может быть использована для осуществления анализа агрегированных данных. Результаты анализа сводных данных позволят повысить эффективность процесса кредитования и дать более точный прогноз и оценку кредитоспособности заемщика [4].

В-третьих, технология даст возможность покупать, продавать и погашать задолженность. Сегодня существует ряд дополнительных отраслей для проверки кредитоспособности, ведения кредитной истории, назначения кредитных рейтингов. Благодаря использованию блокчейн-технологии физические лица, малые и средние предприятия смогут использовать свою репутацию заемщика в виде цифровой записи для получения займов. Таким образом, появляется возможность выпускать, обменивать и урегулировать традиционные долговые обязательства напрямую, тем самым снижая не только все различные издержки, но и системный риск, повышая скорость и прозрачность кредитования. Потребители смогут получать займы непосредственно у таких же потребителей, что особенно важно для не охваченных банковским обслуживанием и для предпринимателей по всему миру [5].

В-четвертых, благодаря блокчейну можно предотвратить мошенничество, кражу персональных данных, искажение данных и DoS-атаки. Децентрализованность и распределенность данных по цепочке блокчейн вместе с криптографической защитой каждой транзакции делают финансовую систему менее уязвимой. Подлинность транзакций в системе проверяется непосредственно ее участниками. Так, например, одной из главных проблем для отрасли страхования является мошенничество, использование технологии блокчейн позволит переводить все транзакции в безопасный распределенный регистр, что уменьшит вероятность двойных платежей по одной и той же претензии или по другим мошенническим схемам [6].

В-пятых, блокчейн-технологии могут быть применены для разработки платежных систем с использованием цифровых валют, которые подкреплены фиатными денежными средствами. Такие платежные системы позволят упростить взаимодействие центральных банков стран и обеспечат при партнерстве с коммерческими банками мгновенное проведение трансграничных платежей. Центральные банки стран начнут покупать цифровые активы и на основе технологии блокчейн в режиме реального времени будут использовать криптоактивы как средство обмена ценностями [7].

В-шестых, блокчейн-системы могут быть применены для управления ценными бумагами. В октябре 2017 г. центральный банк Канады, TMX Group вместе с компанией Payments Canada начали тестирование применения блокчейн-технологии для автоматизации расчетов по ценным бумагам. Данными организациями планируется разработка экспериментальной интегрированной платформы для расчетов по ценным бумагам и платежам, использующей распределенный реестр [8]. Такой процесс сделает более совершенным процесс управления ценными бумагами, что не только позволит удешевить расчетные транзакции по ценным бумагам, но и повысит надежность финансовой системы, особенно в кризисные периоды, за счет сокращения времени и уровня риска расчетов.

Механизмы обеспечения информационной безопасности при использовании технологии блокчейна

Сочетание свойств распределенного реестра с блочной структурой данных, основанной на криптографической связанности, позволяет блокчейну эффективно реализовывать два из трех ключевых аспектов информационной безопасности – целостность и доступность информации. В силу децентрализованной топологии и криптографических механизмов, злоумышленные манипуляции информацией становятся крайне дорогостоящими и затруднительными, а сама информация остается доступной для всех участников при значительных изменениях в размерах блокчейн-сети. Однако традиционная модель децентрализованной публичной блокчейн-сети, обеспечивающей прозрачность и устойчивость к цензуре, в силу своей архитектуры и идеологии не позволяет обеспечить третий аспект ИБ – конфиденциальность данных. По этой причине, а также из-за проблем масштабируемости, появилась модель приватного блокчейна.

Приватный или частный блокчейн в первую очередь отличается моделью обеспечения доступа к сети, при которой право вносить изменения в реестр есть у строго определенных участников. Кроме того, обычно ограничен доступ на чтение записей реестра. Приватный блокчейн идеологически отличается от публичного. В такой сети появляется оператор, и она уже не может быть децентрализованной, только распределенной. Тем не менее приватный блокчейн позволяет обеспечивать конфиденциальность записей, так как теперь доступ предоставляется согласно

политикам безопасности. Такие сети получают все большее распространение как инфраструктура для корпоративных и государственных задач.

Существует модель гибридного блокчейна, совмещающая оба подхода. При ней записи из приватной сети или их метаданные могут дополнительно храниться в публичном блокчейне, обеспечивая дополнительную отказоустойчивость всего реестра.

Безопасное хранение приватного ключа как основа защиты цифровых активов. Каждая транзакция (например, перевод криптовалюты из одного кошелька в другой) внутри блока подписывается ассиметричной электронной подписью (далее — ЭП). Этот дополнительный криптографический слой необходим в публичной сети, где участники анонимны и не доверяют друг другу.

Использование асимметричного механизма в цифровой подписи отличается от традиционного асимметричного шифрования. Подписание производится закрытым или приватным ключом, а проверка подписи — открытым или публичным ключом (проверить подпись транзакции может любой участник). Значение открытого ключа вычисляется на основе закрытого ключа, а вот обратное преобразование требует пока практически неосуществимого объема вычислений.

Блокчейн-сеть	Объем рынка валюты сети (доллары США)	Криптографический алгоритм	Хешрейт	Стоимость 1 часа проведения атаки 51% (доллары США)
Bitcoin	200 млрд	SHA-256	127,624 Петахеш/сек	460,783
Ethereum	41 млрд	Ethash	241 Терахеш/сек	378,047

Стоимость атаки 51% в час на популярные блокчейн-сети Bitcoin и Ethereum, сентябрь 2020 г. Источник: https://www.crypto51.app/

Взлом подписей и хеш-функций. В блокчейн-сетях используются различные криптографические механизмы, многие из них (например, алгоритмы SHA-256 и ECDSA) считаются крайне стойкими ко взлому текущим поколением вычислительных мощностей. Но появление квантовых компьютеров позволит преодолевать нынешнюю стойкость, и в результате взламывать механизмы, лежащие в основе блокчейна, в первую очередь, ЭП. К слову, уже начинает разрабатываться постквантовая криптография. Например, команда Quantum Resistant Ledger создает блокчейн-систему, криптостойкую к квантовым атакам.

Пути решения обеспечения информационной безопасности технологии блокчейна в банковские операции

Определение транзакции. Отправитель создает транзакцию, в которой содержится информация об адресе получателя, предмете транзакции (сумма средств,

товар и т.д.) и криптографическая цифровая подпись, верифицирующая валидность транзакции и ее правомочность.

Аутентификация транзакции. Узлы сети оповещаются о транзакции и проверяют валидность транзакции путем дешифрования электронной подписи. Если транзакция проходит проверку, то она встает в режим ожидания на включение в блок.

Создание блока. Один из узлов сети один раз за определенный интервал времени (10 минут в случае Биткоина) собирает находящиеся в режиме ожидания транзакции, формирует из них блок и отправляет на подтверждение другим участникам сети на предмет проверки и присоединения к цепочке.

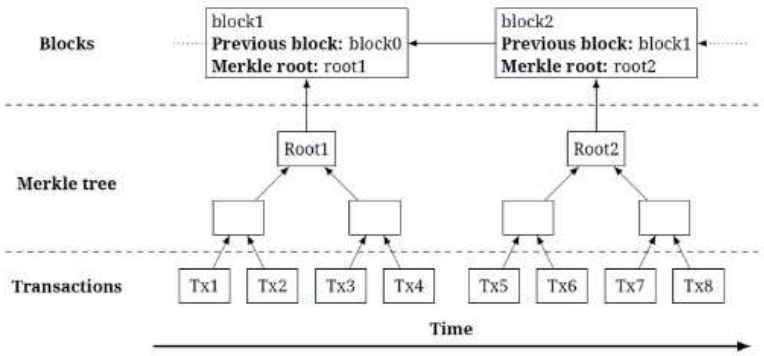
Валидация блока. Узлы, ответственные за валидацию блоков, получают просьбу свалидировать созданный блок. Они запускают повторяющийся процесс, который требует одобрения от других узлов-операторов для того, чтобы признать блок действительным.

Присоединения блока к цепочке. Когда все транзакции в блоке одобряются, новый блок становится присоединенным к общей цепочке.

Уполномоченные пользователи. Блокчейн дает пользователям возможность контролировать информацию, а также транзакции, частью которых они являются.

За счет использования хешей общее состояние блокчейна можно выразить одним-единственным числом: хешем самого нового блока. Поэтому свойство неизменности хеша одного блока гарантирует неизменность всего блокчейна.

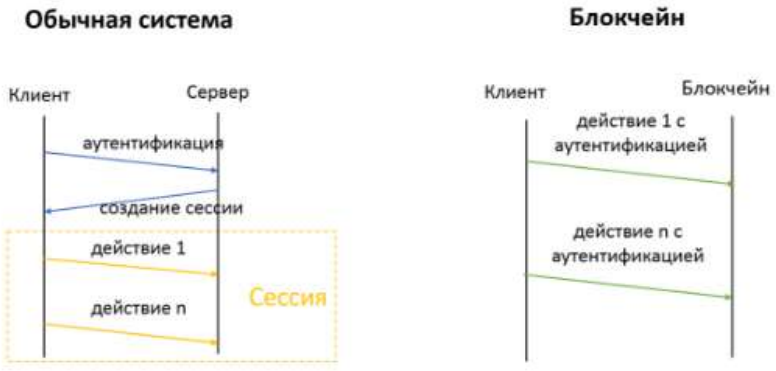
Структура блокчейна и формирование хеша[53]



В цифровых подписях в блокчейнах используются два ключа – закрытый и открытый. Первый используется для формирования цифровой подписи и является засекреченным. Второй – для проверки подлинности подписи. Открытый ключ можно вычислить на основании закрытого, а вот обратное действие на практике нереализуемо из-за слишком большого объема вычислений.*Различие в обращении к системе через электронную подпись в блокчейне и в обычных случаях*[54]

[53] «Криптография в блокчейнах»: о хеш-функциях, ключах и цифровых подписях. Код доступа: https://habrahabr.ru/company/bitfury/blog/327272/

[54]«Криптография в блокчейнах»: о хеш-функциях, ключах и цифровых подписях. Код доступа: https://habrahabr.ru/company/bitfury/blog/327272/



Разработка программного обеспечения блокчейна с применением хэш-функции

```
public class Agent {

    private String name;
    private String address;
    private int port;
    private List<Agent> peers;
    private List<Block> blockchain = new ArrayList<>();
    private ServerSocket serverSocket;
    private ScheduledThreadPoolExecutor executor = new ScheduledThreadPoolExecutor(10);
    private boolean listening = true;

    Block createBlock() {
        if (blockchain.isEmpty()) {
            return null;
        }

        Block previousBlock = getLatestBlock();
        if (previousBlock == null) {
            return null;
        }

        final int index = previousBlock.getIndex() + 1;
        final Block block = new Block(index, previousBlock.getHash(), name);
        System.out.println(String.format("%s created new block %s", name, block.toString()));
        broadcast(INFO_NEW_BLOCK, block);
        return block;
    }

    void addBlock(Block block) {
        if (isBlockValid(block)) {
            blockchain.add(block);
        }
    }
}
```

. Дата классы агент

Заключение

Блокчейн дает результаты, превосходящие другие по обеспечению безопасности. Во-первых, за счет электронной подписи однозначно проводится идентификация

пользователя – скомпрометировать ее можно, только украв ключ. Во-вторых, управление доступом и экранирование в блокчейне тоже на высоком уровне – технология позволяет разделять роли в системе (оператор, аудитор, рядовой пользователь) таким образом, чтобы не позволять всем участвовать, например, в подтверждении транзакций. В-третьих, у блокчейна высокий уровень криптографической защиты, поскольку блоки состоят из хеш-сумм, а по хеш сумме нельзя однозначно определить предмет транзакции и другие входные данные.

Четвертое преимущество блокчейна самое важное по сравнению с обычными базами данных и SWIFT – транзакции формируются в блоки, которые практически невозможно изменить. Это позволяет обеспечить близкое к идеальному протоколирование, поскольку без санкционированных действий никто не сможет удалить транзакции, что обеспечивает высокий уровень прозрачности и значительно облегчает аудит, поскольку ничто невозможно спрятать.

ЛИТЕРАТУРА:

1. "Editorial: Blockchain" Chris McPhee, Editor-in-Chief Anton Ljutic, Guest Editor "Technology Innovation Management Review"
2. October 2017 Melanie Swan "Anticipating the Economic Benefits of Blockchain"
3. Anderson, C. 2008. The Long Tail: Why the Future of Business is Selling Less of More. New York: Hachette Books.
4. Antonopoulos, A. 2017. Advanced Bitcoin Scripting. SF Bitcoin Developers Seminar, April 20, 2017. Accessed October 18, 2017: https://www.youtube.com/watch?v=MiS8-4uIOYo
5. Brandom, R. 2015. In the Silk Road Trial, Bitcoin is a Cop's Best Friend. The Verge, January 14, 2015. Accessed October 18, 2017: https://www.theverge.com/2015/1/14/7546669/silk-road-trialbitcoin-tracking
6. Brynjolfsson, E., Hu, Y. J., & Smith, M. D. 2010. The Longer Tail: The Changing Shape of Amazon's Sales Distribution Curve. SSRN, September 20, 2010. Accessed October 18, 2017: http://dx.doi.org/10.2139/ssrn.1679991
7. Chen, T. 2017. China Mobile Payment Report 2017. WalktheChat, June 25, 2017. Accessed October 18, 2017: https://walkthechat.com/china-mobile-payment-report-2017/