УДК 336.745

А. Д. Лукиных, студент
С. П. Сырыгин, кандидат технических наук
Ижевский государственный технический университет имени М. Т. Калашникова

РАЗВИТИЕ ПЛАТЕЖНЫХ СИСТЕМ В РАМКАХ VI ТЕХНОЛОГИЧЕСКОГО УКЛАДА

Технология блокчейн появилась в 2009 г., но с каждым годом набирает все большую популярность. Основная сфера ее применения – криптовалюта, в частности денежные переводы. В статье рассмотрены существующие платежные системы, их достоинства и недостатки. Описаны свойства и принцип работы технологии блокчейн. Проведено сравнение комиссий на переводы денежных средств с использованием существующих платежных систем и технологии блокчейн. После чего были представлены перспективы применения технологии блокчейн как платежной системы.

Ключевые слова: блокчейн; платежная система; VI технологический уклад.

В настоящее время мир стоит на пороге VI технологического уклада. Его контуры только начинают складываться в развитых странах мира и характеризуются нацеленностью на развитие и применение наукоемких технологий. В их числе: нанотехнологии, генная инженерия, квантовые технологии, микромеханика и термоядерная энергетика. Одним из основных двигателей развития новых технологий являются денежные расчеты, обеспечиваемые платежными системами. Существующие платежные системы имеют ярко выраженные недостатки, которые будут тормозить развитие новых технологий.

В современной России существует большое количество как локальных, так и международных электронных платежных систем. К международным системам можно отнести *ApplePay*, *GoogleWallet*, *AndroidPay*, *WesternUnion*. На отечественном рынке услуги по обеспечению платежей кроме банков осуществляют специализированные платежные системы. Наиболее популярными являются Яндекс.Деньги, *WebMoney*, *QIWI*, Сбербанк Онлайн. Безусловно, эти платежные системы имеют ряд достоинств, в числе которых можно отметить: мобильные приложения, через которое пользователь может проверить состояние счета и производить различные переводы. При переводе денежных средств между счетами клиентов в одной платежной системе не возникает комиссий и задержек с момента списания денежных средств до момента получения их другим пользователем.

Основные затруднения возникают у пользователя, который хочет перевести средства на счет клиента другой платежной системы. Такие переводы сопровождаются высокой комиссией. Например, в системе *QIWI* берется комиссия в размере 2 % от суммы перевода плюс 50 рублей, Яндекс.Деньги взимают 3 % от суммы перевода плюс 15 рублей, в системе Сбербанка – 1,5 %, но не менее 30 рублей, и наименее затратной является платежная система *WebMoney*, в которой установлены тарифы в размере 0,8 % от суммы перевода плюс 15 рублей. (табл. 1). Важным недостатком является длительное время перевода – в среднем операция занимает от 1 до 3 суток.

Таблица 1. **Сравнение величины комиссии, взимаемой в различных платежных системах**

Сумма перевода, руб	Комиссии платежных систем			
	QIWI	Яндекс.Деньги	Сбербанк Онлайн	*WebMoney*
10000	250	315	150	73,16
100000	2050	3015	1500	596,6
1000000	20050	30015	15000	5831
10000000	200050	300015	150000	58175
100000000	2000050	3000015	1500000	581615

Кроме того, в этих платежных системах существуют лимиты по операциям. Например, в системе *WebMoney* с псевдонимным аттестатом существует лимит на максимальную сумму, которая составляет 45 000 рублей. Конечно, для большинства пользователей такой лимит не создаст ограничений. Если же пользователю необходимо увеличить лимиты по операциям, он должен представить документы для подтверждения личности (паспорт, водительское удостоверение). После получения необходимых документов кошелек верифицируется, и лимиты могут быть увеличены. В свою очередь, документы и личные данные клиентов попадают в централизованные базы данных платежной системы, что может привести к хищению личных данных клиента после взлома базы данных или сотрудником платежной системы.

Сформируем основные недостатки действующих платежных систем:
– высокие комиссии;
– длительное время перевода;
– наличие различных лимитов по операциям;
– возможность взлома или человеческой ошибки.

Представленные недостатки обусловливают появление в 2009 г. криптовалюты биткоин и платежной системы, обеспечивающей перевод денежных средств от одного собственника к другому, базирующейся на технологии блокчейн.

Технологию *блокчейн* можно представить, как распределенную одноранговую систему подтвержденных и связанных между собой записей, которые могут быть проверены в любой момент. Такие записи могут описывать любые явления. Все записи в такой системе должны быть проверенными и подтвержденными, а сама система надежной.

Основная идея блокчейна в том, что это большая распределенная база данных, доступ к которой имеет любой пользователь. У такой базы данных нет централизованного руководства и места хранения, а обеспечением работоспособности занимаются специализированные компьютеры – узлы. На узлы возложена проверка подлинности совершенных транзакций и формирование из них блоков, выстраиваемых в цепочки. Устройство блока определенно таким образом, что в каждом новом блоке существует информация о предыдущем [1].

Последовательность формирования блоков и их запись в блокчейн можно представить следующим образом:

1) транзакция отсылается всем узлам в пиринговой сети и попадает в пул необработанных заявок;

2) узлы переводят транзакции из пула необработанных заявок в блок;

3) каждый узел занимается подбором хеша блока по установленным разработчиками условиям;

4) после того, как узел нашел правильный хеш блока, блок рассылается всем участникам сети, а сам узел получает вознаграждение за находку блока;

5) далее начинается проверка блока на корректность и возможное наличие повторного списания средств; если в процессе проверки будут найдены нарушения, то такой блок не принимается;

6) если в блоке не находят нарушений, такой блок принимается, и начинается работа над следующим блоком, основанном на информации о предыдущем блоке.

Важно отметить, что осуществление транзакций проходит с криптографическим подтверждением.

При регистрации в сети и установке соответствующего программного обеспечения каждый участник получает пару криптографических ключей: открытого – для подтверждения транзакции, и закрытого – для шифрования транзакции.

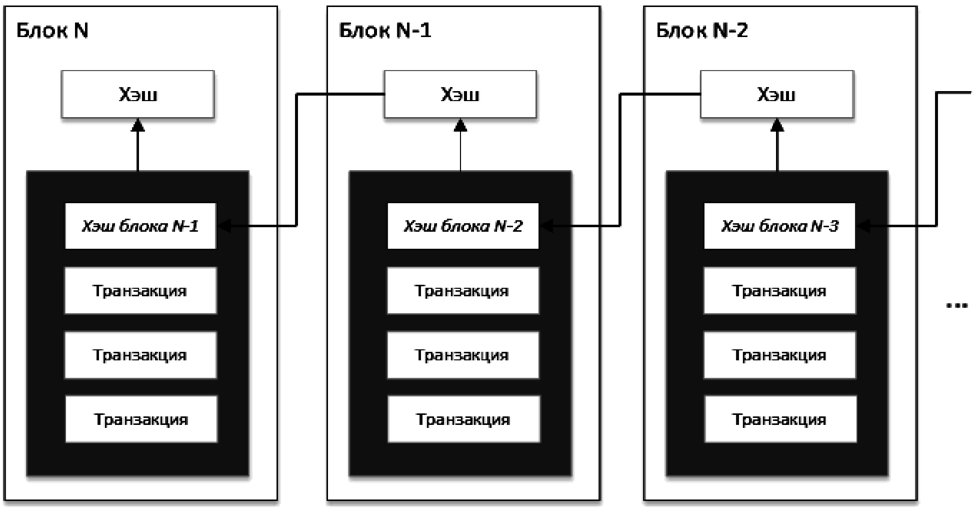
Любой участник, желающий произвести транзакцию, должен использовать открытый ключ другого участника как адрес, по которому нужно осуществить перевод, и при помощи закрытого ключа подтвердить эту транзакцию. Вся информация добавляется в конец блока. Поэтому получатель может увидеть всю цепочку транзакций, просмотрев все подписи прошлых участников транзакции.

Использование связки открытого и закрытого ключа одновременно с хешированием делает блокчейн-технологию более надежной [2].

Под хешем понимается массив данных, преобразованный с помощью хеш-функции. В случае криптовалют это информация о транзакциях. При использовании хеширования мы получаем уникальную буквенно-числовую строку, которая характеризует исходные данные, однако из хешированных данных невозможно воссоздать исходные.

Каждый новый блок включает в себя хеш предыдущего блока, поэтому если узел попытается добавить блок, который не соответствует этому правилу, то блок будет признан недействительным и отклонен другими узлами. Добавление невалидного блока возможно лишь при изменении всех предыдущих блоков, вплоть до самого первого блока в системе. Из этого возникает одно из основных свойств блокчейна – данные, попавшие в цепочку блоков, являются неизменяемыми.

Последовательность формирования блоков представлена на рисунке.



Последовательность формирования блоков в блокчейне

Для увеличения безопасности блокчейна при добавлении нового блока используются в основном два принципа: это принцип подтверждения проделанной работы (*Proof-of-Work*, *PoW*) и подтверждения доли (*Proof-of-Stake*, *PoS*).

Поскольку технология блокчейн не полагается на единый подтверждающий центр, такой, например, как платежная система с ее инфраструктурой безопасности, то каждый из узлов блокчейна не может располагать полной информацией о действительной версии базы данных.

Надежность биткоина в сети блокчейн основывается на алгоритме доказательства работы (*Proof-of-Work*) в процессе формирования блоков. Каждый узел, формирующий блок, должен решить сложную задачу, чтобы гарантировать корректность блока. За правильное решение узел получает вознаграждение в виде новых биткоинов. Для преднамеренного взлома и возможного повторного списания средств со счета хакеру необходимо располагать бóльшей частью вычислительных ресурсов сети.

Функционирование протокола биткоин таково, что безопасность сети поддерживается следующими ресурсами:

– специальные компьютеры, которые занимаются проведением вычислений;

– электроэнергия, которая необходима для работы компьютеров.

Эти два фактора делают биткоин неэффективным с точки зрения потребления ресурсов. Для увеличения своей доли вознаграждения в сети биткоин узлам необходимо постоянно наращивать свои вычислительные мощности, так называемая «гонка вооружений». Постоянное наращение вычислительной мощности сети и огромное количество потребляемой электроэнергии делает стоимость эксплуатации сети и вероятность хакерской атаки невероятно высокими, что привело к возникновению предложений построить подобные системы, которые требуют намного меньше ресурсов.

Для решения этих проблем стал применяться метод, основанный на алгоритме подтверждения доли (*Proof-of-Stake*). Основной смысл этого алгоритма состоит в том, что вознаграждение за найденный новый блок будет делиться между пользователями пропорционально их доли расчетов в общих вычислениях. Логическим обоснованием работоспособности алгоритма подтверждения доли заключается в следующем: узлы с наибольшими долями в системе имеют максимальный стимул в поддержании безопасности сети, потому что они больше других пострадают от падения стоимости и репутации криптовалют в результате различных атак.

Подводя итог, можно выделить следующие характеристики технологии распределенного реестра:

– децентрализация;

– открытость внесенных данных;

– математико-криптографическая защита информации;

– невозможность изменения уже внесенных данных.

В настоящее время ведутся переговоры о внесении поправок в законодательство о применении технологии блокчейн в Российской Федерации. Данная технология позволит обычным людям или организациям производить переводы денежных средств напрямую между собой. При помощи блокчейна мы можем избавиться от посредника в виде платежной системы и тем самым повысить прозрачность и скорость совершения переводов как внутри страны, так и международных платежей, существенно снизив их стоимость. Сравним стоимость перевода в существующих платежных системах (табл. 1) и перевода биткоин в сети блокчейн (табл. 2).

Таблица 2. **Комиссии при переводе в системе блокчейн**

Сумма перевода, BTC	0,01	0,1	1	10	100
Комиссия, BTC	0,0003	0,0003	0,0003	0,0003	0,0003
Комиссия, %	3	0,30	0,0300	0,0030	0,0003

Можно заметить, что использование биткоина, при переводах менее 0,1 BTC или 100 000 рублей (по курсу на 7.12.2017 г.) невыгодно относительно представленных платежных систем. Потому что при использовании биткоина значение комиссии фиксировано, а это значит, что при увеличении суммы перевода доля комиссии уменьшается. Данное свойство будет полезно клиентам, которым нужно перевести больше 100 000 р.

В заключение следует констатировать, что применение технологии блокчейн может устранить ряд недостатков, характерных для уже существующих платежных систем, а дальнейшее ее развитие приведет к возможному изменению всей индустрии финансовых услуг в VI технологическом укладе.

Библиографические ссылки

1. *Мащенко П. Л., Пилипенко М. О.* Технология блокчейн и ее практическое применение // Наука, техника и образование. – 2017. – №. 2 (32). – С. 61–64

2. *Пряников М. М., Чугунов А. В.* Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы // International Journal of Open Information Technologies. – 2017. – №. 6 (5). – С. 49–55.

A. D. Lukinykh, Student
S. P. Seregin, PhD in Engineering
Kalashnikov Izhevsk State Technical University

DEVELOPMENT OF PAYMENT SYSTEMS WITHIN THE FRAMEWORK OF THE SIXTH TECHNOLOGICAL SCHEME

The technology of the blockchain appeared in 2009, but every year is gaining popularity. The main field of its application is a cryptocurrency, particularly remittances. The article considers the existing payment systems, their advantages and disadvantages. Describes the properties and the working principle of blockchain technology. Comparisons were made commissions on remittances using existing payment systems and blockchain technology. Then was presented the prospects of applying the blockchain technology as the payment system.

Keywords: blockchain; payment system; sixth technological order.