*УДК 003.26*

***Н.Н. Григорьева, Е.А. Горба***
*Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация*

# КРИПТОГРАФИЯ КАК СПОСОБ ПОЛУЧЕНИЯ ПРИБЫЛИ

***Аннотация***. *После появления криптографии с открытым ключом она превратилась в быстроразвивающуюся область вполне научных изысканий. В области исследования, в которой сейчас работают тысячи исследователей и проводятся сотни конференций. С ростом технологий выросла и потребность шифрования данных. Новые информационные технологии позволили лучше скрывать информацию от «глаз» потенциального противника. Но рост технологий ведет не только к улучшению возможностей шифрования, но и к растущей возможности дешифровки информации, что в свою очередь заставляет придумывать новые способы сохранить целостность и правдивость информации, например, такие как система блокчейн. В свою очередь основываясь на блокчейне появилась возможность коллективного заработка, которым активно пользуются тысячи участников системы.*

*В статье рассмотрена криптография как наука о шифрофровании и дешифровки информации и каким образом она применяется в современном финансовом мире. Как на ней зарабатывают тысячи участников системы блокчейн. Также в статье рассмотрена сама система блокчейн и каким образом происходит процесс получения дохода участников системы.*

***Ключевые слова:*** *майнинг, криптовалюта, криптография, блокчейн, шифрование.*

***N.N. Grigoryeva, E.A. Gorba***
*Irkutsk State Transport University, Irkutsk, the Russian Federation*

# CRYPTOGRAPHY AS A WAY TO MAKE A PROFIT

***Annotation.*** *After the advent of public key cryptography, it turned into a rapidly developing field of quite scientific research. In the field of research, which now employs thousands of researchers and hosts hundreds of conferences. With the growth of technology, the need for data encryption has also grown. New information technologies have made it possible to better hide information from the "eyes" of a potential enemy. But the growth of technology leads not only to the improvement of encryption capabilities, but also to the growing possibility of decrypting information, which in turn forces us to come up with new ways to preserve the integrity and truthfulness of information, such as the blockchain system. In turn, based on the blockchain, there is an opportunity for collective earnings, which is actively used by thousands of system participants. The article discusses cryptography as the science of encrypting and decrypting information and how it is used in the modern financial world. How thousands of blockchain system participants earn on it. The article also discusses the blockchain system itself and how the process of generating income for system participants takes place.*

***Keywords:*** *mining, crypto currency, cryptography, blockchain, encryption.*

## Введение

Появление первых попыток шифрования текстов принято относить к третьему тысячелетию до нашей эры. Как только письменность распространилась по миру, появилась задача защитить написанное от нежелательных глаз. Началось все с моноалфавитных шифров, при использовании которых изначальные буквы просто заменялись буквами из другого алфавита. В IX веке на Ближнем Востоке зародилась мода на полиалфавитные шифры, которые к XV веку благополучно добрались и до Европы.

Американский инженер, криптоаналитик и математик Клод Элвуд Шеннон в своих знаменитых работах «Теория связи в секретных системах» [5] и «Математическая теория связи» [6] заложил основы математической криптографии. Он вывел и доказал шесть теорем, описывающих фундаментальные принципы и законы передачи информации. Но это все еще была классическая криптография с секретным ключом.

С ростом технологий выросла и потребность шифрования данных. Новые информационные технологии позволили лучше скрывать информацию от «глаз» потенциального противника. Но рост технологий ведет не только к улучшению возможностей шифрования, но и к растущей возможности дешифровки информации, что в свою очередь заставляют приду-

мывать новые способы сохранить целостность и правдивость информации, в том числе такие как система блокчейн. В свою очередь, основываясь на блокчейне, появилась возможность коллективного заработка, которым активно пользуются тысячи участников системы [5].

На сегодняшний день криптография является одной из ведущих областей науки в сфере защиты информации. Современные криптографические средства давно перестали быть собственностью государств и даже бизнеса. Они широко и незаметно для пользователей используются в самых распространенных сферах жизни и быта. На базе же современной криптографии появилось новая система «блокчейн», которая в свою очередь легла в основу нового экономического направления заработка на основе добычи цифровой валюты – майнинга [1, 7].

**Основная часть**

Криптография применялась в шифровании информации еще в далекой древности и в течение многих поколений её единственная задача состояла в обеспечении секретности данных [4,8,9].

В последние годы, благодаря высокому подъему развития цифровых и информационных технологий, потребность в поиске способов защитить информацию сильно возросла. При этом, во многих областях жизни первостепенной задачей является обеспечение целостности информации, под которой понимается гарантия поступления информации пользователю из доверенного источника в подлинном и целостном виде.

До появления первых автоматизированных систем банков, единственный способ, позволявший защитить информацию от кражи, который могла предложить криптография — это разработанные средства шифрования данных. По этой причине, все способы защиты банков сводились именно к шифрованию [3]. В конечном итоге, люди пришли к выводу, что для обеспечения целостности информации требуются иные средства чем для обеспечения конфиденциальности. Так появилось новые методы шифрования данных – криптографические протоколы.

Под криптографическим протоколом подразумевается алгоритм, позволяющий шифровать информацию для большого количества участников (более 2-х). Такие протоколы рассчитаны на определенных злоумышленников. В стандартных криптосистемах это внешний противник, пытающийся получить засекреченную информацию, передаваемую между двумя доверенными участниками общения (атака – человек посередине). В протоколах злоумышленником может являться не только внешний противник, но и любой из участников общения. Таким образом, криптографические протоколы защищают информацию от других участников общения.

Несмотря на развитие систем шифрования данных, в одиночной системе банка возможны множество проблем: хакерские атаки, мошенники или ошибки сотрудников могут вызвать сбой и проблемы на любом из этапов передачи денег от одного участника другому. Тогда записи о транзакциях (передачах денег) могут исчезнуть или быть изменены.

Возможность этих проблем неизбежна, если контроль над транзакцией осуществляют конкретные организации и записи об операциях хранятся только в одном месте.

Для уменьшения таких рисков была придумана технология блокчейн (непрерывная цепочка блоков), осуществляющая системный контроля на основе распределенных реестров, что в свою очередь, серьезно уменьшает саму возможность потери данных (рис.1) [1].

Блокчейн так же называют технологией распределенных реестров, так как вся цепочка операций и актуальный список владельцев хранят на своих устройствах множество независимых пользователей системы. Даже если один или несколько компьютеров дадут сбой, информация не исчезнет [1, 3].

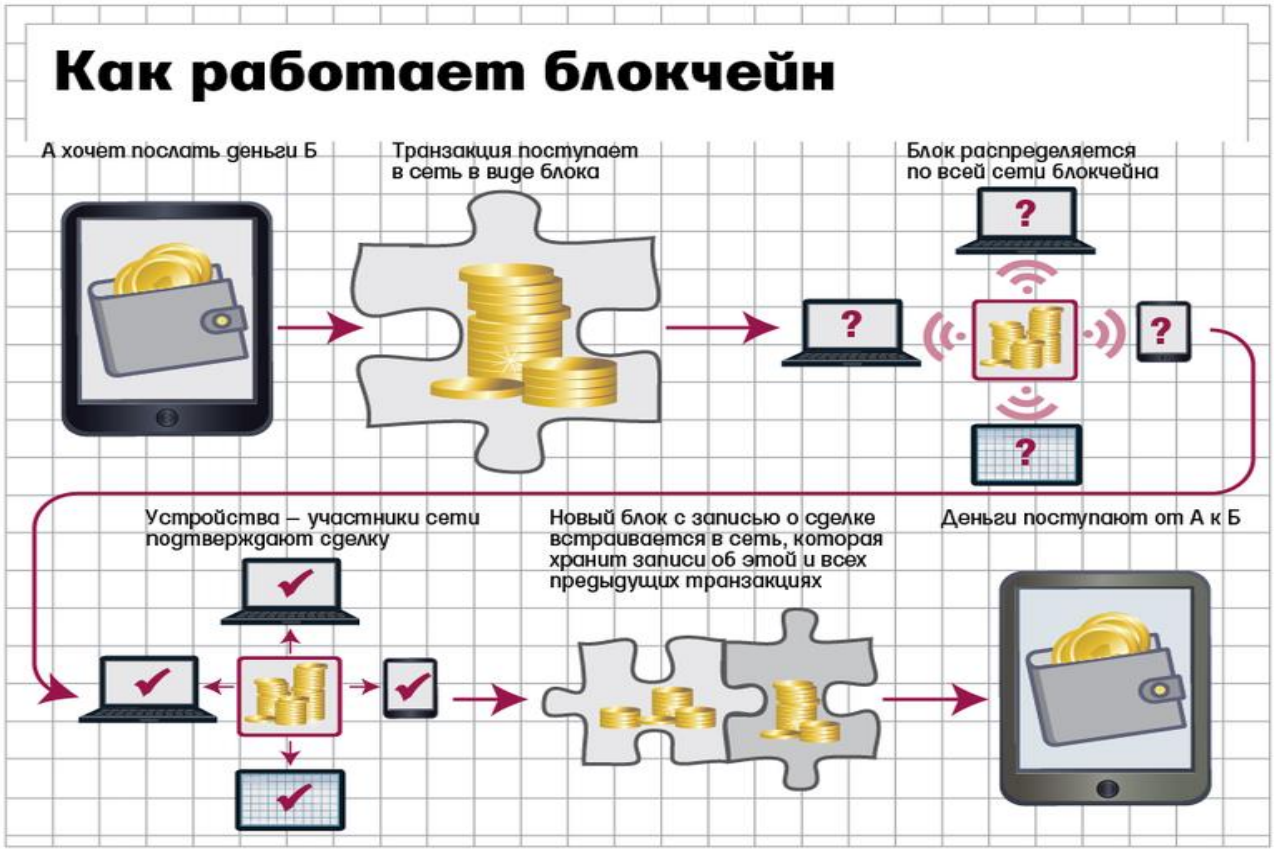


**Рис.1. Принцип работы блокчейна**

В блокчейне реестр владельцев не хранится на едином сервере одной организации. Его копии одновременно обновляются на множестве независимых компьютеров, объединенных через интернет.

Поэтому, в блокчейне реестры с данными о владельцах активов невозможно подделать. Для того, чтобы информация у всех участников была единой, полной и верной, в блокчейне ввели понятие консенсус. Если некоторые участники сети отключат свои устройства, или их записи окажутся ложными, это не повлияет на работу системы в целом. Процедура консенсуса – это достижение согласия, позволяющее восстановить единую верную информацию.

В блокчейн-сетях, за определенный период, времени происходит множество операций, записи о которых включаются в один блок.

Блок – это запись в распределенном реестре о нескольких транзакциях, отражающим информацию о последовательностях и объемах переводимых активов [8].

Все блоки последовательно соединяют в одну последовательную цепь. Цепь блокчейна непрерывна, так как каждый следующий блок содержит ссылку на предыдущий. Блоки нельзя изменить и удалить, можно только добавлять новые. Так, всегда можно детально узнать историю транзакций актива и определить актуального на сегодняшний день владельца.

Благодаря алгоритмам, по которым происходит создание блоков, следующих друг за другом, обеспечивается прозрачность и неизменяемость данных.

Для того, чтобы блокчейн работал и появлялись новые последующие блоки, необходима вычислительная мощность. Людей, которые предоставляют такие мощности и получают за эти процессы вознаграждение в виде криптовалюты, называют майнерами.

Майнеры выполняют в блокчейне следующие функций:

– сохранение блокчейна в виде аналогичных копий друг друга, что требуется для защиты информации от потери или фальсификации одним из участников системы;

– подтверждение операций по переводу, снятию и т.д.;

– проверка различных операций, которые регистрируют или совершают другие участники блокчейна – майнеры.

Обычно количество участников майнинга не имеет каких-либо ограничений. Чем больше устройств участвуют в процессе, тем надёжнее такая система. Участниками майнига может быть любой желающий имеющий специализированные компьютеры и программное обеспечение.

Награда, которую майнеры получают за участие в системе называется «криптовалюта» изначально она была цифровым аналогом денег с децентрализованной системой управления. Сейчас существует множество криптовалют, созданных для разных целей разными организациями, но их основой всегда останется технология блокчейн.

Весь процесс участия в системе и получение прибыли на основе системы блокчейн называется майнинг. Полученные награды в виде криптовалюты хранятся на специальных электронных кошельках. Распоряжаться ей можно, как и любыми другими ценными активами, если они имеют какую-то ценность и разыгрываются на торговых площадках. Принцип не отличается от классической биржи.

В процесс добычи «криптовалюты» используют компьютер или специализированные устройства, созданные для максимально быстрой обработки информации.

Алгоритмы криптовалют – это набор собственных правил, которые зашифровывают цифровую валюту. Майнеры при помощи специального компьютерного оборудования расшифровывают алгоритмы конкретной криптовалюты – этот процесс заключается в поиске хеша. Как только будет найден хеш, то в блокчейне создается новый блок, в котором хранится информация о транзакциях и хеше блока, который стоит до этого. Процесс расшифровки превращает набор случайных данных в упорядоченную систематизированную информацию, которая, впоследствии, записывается в блокчейн (рис.2).


**Рис.2. Схема получения прибыли для участников системы блокчейн (майнеров)**

Чтобы участвовать в добыче криптовалюты, необходимо пройти несколько этапов:

1. Высчитать наиболее выгодный и актуальный на сегодняшний день токен для добычи;

2. Настроить необходимое программное обеспечение на устройствах, которые будут обрабатывать информацию под ваш электронный адрес;

3. Подключиться к одному из возможных пулов (объединению компьютеров в систему для более эффективной работы);

4. Следить за тем, чтобы устройство работало в приемлемых условиях и вовремя проводить техническое обслуживание и смену комплектующих, вышедших из строя.

На указанный адрес приходит вознаграждение согласно доле мощности участника системы от общего пула устройств. Со временем, сложность добычи возрастает, и устройства приносят меньше прибыли, поэтому необходимо следить за рентабельностью всего процесса. Немаловажен и текущий курс криптовалюты.

Криптовалюту нельзя прировнять к привычной денежной системе, по причине очень существенных отличий, таких как: анонимность проводимых операций и полная децентрализация системы.

Блокчейн – это длинная цепочка блоков или транзакций. Эта цепочка будет расти неограниченно долго – столько, сколько будет функционировать сама система. Создавая последовательность перечислений с фиксацией времени каждого из них, система контролирует состояние счета участника в любой момент, а также идентифицирует прикрепленную к цифровой валюте или его части информацию, о том, когда она был создана, израсходована или получена.

Майнинг является процессом добавления информационного блока, посредством которого производится выпуск новой криптовалюты [7]. Само назначение криптовалюты – это отказ от посредника и поддержание сложной системы взаимоотношений между участниками, в которой незнакомые люди могут вести деловые отношения друг с другом.

**Заключение**

На сегодняшний день криптография как наука является наиболее надежным средством обеспечения конфиденциальности и контроля целостности данных. Во многих отношениях она занимает ведущее место среди программно-технических способов обеспечения безопасности. А в связи с увеличивающимся влиянием электронно-цифровых денежных средств в мировой экономике и постепенным внедрением технологий распределённого реестра в различные сферы жизни общества, нельзя не сказать об актуальности детального изучения технологии блокчейн.

Предсказать дальнейшее развитие криптовалют невозможно, но мнение большинства аналитиков мира сошлось на том, что возможность краха системы цифровой криптовалюты вполне возможена, но технология блокчейна, изобретенная С. Накамото, будет жить еще долго и неоднократно послужит обществу.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Аграновский А.В., Хади Р.А. Практическая криптография: 2009 г. С. 56-59.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А. В. Основы криптографии. 2001 г. С. 470-479.
3. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. 2007 г. С. 546-551.
4. Ефишов И. Таинственные страницы. Занимательная криптография. 2016 г. С. 73-85.
5. Клод Элвуд. Теория связи в секретных системах. 1945 г.
6. Клод Элвуд. Математическая теория связи. 1948 г.
7. Равал С. Децентрализованные приложения. Технология Blockchain в действии. 2017 г. С. 131-137.
8. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. 2003 г. С. 800-807.
9. Фергюсон Н., Шнайер Б. Практическая криптография. 2005 г. С. 367-378.


## REFERENCES


1. Agranovsky A.V., Hadi R.A. "Practical cryptography". Year: 2009, pp. 56-59.
2. Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V. Fundamentals of cryptography. 2001, pp. 470-479.
3. Bauer F. Deciphered secrets. Methods and principles of cryptology. 2007, pp. 546-551.
4. Efishov I. Mysterious pages. Entertaining cryptography. 2016, pp. 73-85.
5. Claude Elwood. Communication theory in secret systems. 1945.
6. Claude Elwood. Mathematical theory of communication. 1948.

7. Raval S. Decentralized applications. Blockchain technology in action. 2017 p. 131-137.
8. Schneier B. Applied Cryptography. Protocols, algorithms, source texts in C. 2003 pp. 800-807.
9. Ferguson N., Schneier B. Practical Cryptography. 2005, pp. 367-378.

**Информация об авторах**

*Горба Евгений Александрович* – магистрант, Иркутский государственный университет путей сообщения, г. Иркутск, E-mail: dreik94@mail.ru

*Григорьева Наталья Николаевна* – кандидат экономических наук, доцент кафедры «Экономика и управление на железнодорожном транспорте», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: zolotkina@mail.ru.

**Information about the authors**

*Gorba Evgeny Aleksandrovich* – master student, Irkutsk State Transport University, Irkutsk E-mail: dreik94@mail.ru.

*Grigorieva Natalya Nikolaevna* – candidate of economic Sciences, Associate Professor of the Department of Economics and Management of Railway Transport, Irkutsk State Transport University, Irkutsk, e-mail: zolotkina@mail.ru.