

Технология блокчейн

Криптовалюты

Биткойн



Нимерницкая И.А.

2017

©

Криптовалюта

- ❑ Цифровая (виртуальная) валюта, единица которой – монета (англ. -coin).
- ❑ Монета защищена от подделки, т.к. представляет собой зашифрованную информацию, скопировать которую невозможно (пользование криптографии и определило приставку «крипто» в названии).



Технология блокчейн

- ❑ Криптовалюта, - виртуальные деньги, не имеют материального эквивалента и представляют из себя просто записи в специальной базе данных.
- ❑ База очень надежна, и та технология, по которой она построена, вполне возможно, представляет из себя даже большую ценность для человечества, чем сама валюта.





Биткоин

- Новое поколение децентрализованной цифровой валюты, созданной и работающей только в сети интернет.
- Никто не контролирует ее, эмиссия валюты происходит посредством работы миллионов компьютеров по всему миру, используя программу для вычисления математических алгоритмов.
- Это первые в современном мире частные деньги.

Возникновение

- ❑ Концепция биткойн:
- ❑ Это должны быть деньги, принадлежащие только вам, которые никак не подделать и которыми можно мгновенно рассчитаться с кем угодно в любой точке земного шара, где есть интернет.
- ❑ Bitcoin не обладает износом, который характерен для всех обычных монет.



Производство

- Необходимым и достаточным элементом этой платёжной системы является базовая программа-клиент (имеет открытый исходный код).
- Запущенные на множестве компьютеров программы-клиенты соединяются между собой в одноранговую сеть, каждый узел которой равноправен и самодостаточен.



Возникновение идеи

- В 1983 году Дэвид Чаум (Калифорнийского университет), задумался о том, как совместить анонимность платежей и их прозрачность для всех участников рынка.
- Ученый предложил использовать так называемый алгоритм «слепой подписи», позволявший провести секретную сделку между двумя анонимными участниками, но при этом сообщить о самом ее факте сторонним наблюдателям.



Создатель биткоина

- Разработчик программы зовет себя Satoshi Nakamoto (есть мнение, что это группа разработчиков-программистов); он предложил электронную платежную систему, основанную на математических вычислениях.
- Идея состояла в том, чтобы произвести обмен монетами без любой центральной власти.
- Идея реализована в 2009 году.



Сатоси Накамото

- ▣ Satoshi Nakamoto — псевдоним человека или группы людей, разработавших протокол криптовалюты биткойн и создавших первую версию программного обеспечения, в котором этот протокол был реализован.
- ▣ Было предпринято несколько попыток раскрыть реальную личность или группу, стоящую за этим именем, но ни одна из них не привела к успеху.



Первая покупка

- В феврале 2010 года в сети появился первый сервис для покупки биткоинов Bitcoin Market, а уже в мае пользователь форума о криптовалюте решил купить две пиццы за 10 тысяч биткоинов.



Рост стоимости

- В июле 2010 о биткоинах написали на популярном среди компьютерщиков портале Slashdot, и число пользователей виртуальных денег начало резко расти.
- В результате уже через месяц 10 тысяч биткоинов стоили 600 долларов, а многие пользователи сети начали активно майнить себе криптовалюту. Это привело к появлению первой биржи биткоинов



Производство биткоина

- Эмиссия биткоинов возможна только в цифровом виде и любой желающий может начать добывать или, как говорят, майнить биткоины в любое время.
- Майнинг биткоинов происходит посредством использования вычислительных мощностей компьютера в распределенной сети.





BlockChain

- ❑ Создана децентрализованная (не имеющую главного сервера) база данных, копии которой в зашифрованном виде будут храниться у всех участников систем.
- ❑ В случае Биткойна — это база транзакций, т. е. всех совершаемых с единицами этой криптовалюты операциями (ее добыча, передача, продажа, получение и т.д.).
- ❑ Все протоколируется и эта информация доступна всем участникам.

Безопасность

- Все новые записи в этой базе согласуются со всеми ее копиями у всех участников. Работают алгоритмы синхронизации и достижения консенсуса.
- Чтобы что-то украсть, нужно будет подменить данные как минимум у половины участников, а это при миллионной сети практически невозможно.



Гарантии



- Очередной блок в базе транзакций (цепочке блоков — блокчейне) содержит информацию о том блоке, что шел перед ним: используется его уникальный хеш, который служит гарантией целостности.
- Для подделки платежа нужно подделать всю цепочку блоков хранящуюся в распределенной базе (на тысячах компьютеров), что очень затратно, требует доступа к этим компьютерам и делает такие действия бессмысленными.

Количество биткоинов

- В коде биткоина стоит ограничение, «добыть» максимум можно 21 миллион биткоинов.
- Несмотря на это, биткоин может делиться на более мелкие части, это же цифровая валюта.
- Минимальная передаваемая величина (наименьшая величина дробления) — 10^{-8} биткойна — получила название «сатоши» в честь создателя.



Майнинг

- Все майнеры (виртуальные шахтеры) на своих ПК или на специально собранных под это дело системах (фермах) проводят очень трудоемкие расчеты — перебирают числа, у которых хеш (вычисляется по специальной формуле) будет соответствовать заданному шаблону.





Частота появления

- ❑ Шаблон выбирается с таким расчетом, чтобы при любом числе майнеров **новая единица биткоина появлялась не чаще, чем раз в десять минут.**
- ❑ Тому, кто добавит очередную новую единицу криптовалюты, выплачивается комиссия на покрытие расходов.
- ❑ Каждый пользователь системы получает специальный адрес (криптографический счет) и секретный ключ – кошелек и ключ к нему.

Контроль биткоинов

- ❑ Центрального органа контроля сети не существует, сеть распределена на всех участников, каждый компьютер, добывающий биткоины является участником этой системы.
- ❑ Это означает, что никакой центральный орган не имеет возможности диктовать правила владельцам биткоинов.



Цена биткойна

- Котировка биткойна формируется исключительно балансом спроса и предложения, не привязана к какой-либо валюте или другому активу.
- На 02.09. 2017 стоимость биткойна превысила 5. 000 долларов США,



Особенности биткойна

- Независимость
- Ограниченность
- Полная анонимность
- Отсутствие посредников
- Отсутствие обеспеченности
- Нелегализованность
- Недостаточная популярность



Независимость

- Система абсолютно автономна и не нуждается ни в чьем руководстве.
- Она не приемлет никаких воздействий извне.
- Все могут видеть, что кто-то кому-то что-то перевел, но не могут ни запретить, ни отменить, ни заблокировать транзакцию.





Ограниченность

- Запас биткоинов ограничен (по определению), его добыча сложна и трудозатратна (ее ведут майнеры), и его нельзя просто так взять и напечатать в нужном количестве, как обыкновенные деньги.
- Согласно алгоритму, который обеспечивает жизнеспособность криптовалюты, можно добыть не более 21 000 000 биткоинов, после чего их добыча прекратится.

Полная анонимность

- ❑ По номерам Bitcoin-кошельков нельзя определить, кто является или не является их владельцем.
- ❑ Иногда это хорошо.
- ❑ Однако открывается возможность незаконно отмывать деньги или мошенничать.
- ❑ И восстановить утраченный к своим деньгам доступ уже невозможно, некуда прийти с паспортом (в отличие от тех же банков)



Отсутствие посредников

- ❑ Перевод биткойнов происходит без участия третьей стороны (например, банка).
- ❑ Это упрощает, удешевляет и ускоряет сделки.
- ❑ Но делает их менее безопасными, ибо отозвать платеж уже невозможно.



Отсутствие обеспеченности

- ❑ В отличие от реальных денег, никакая криптовалюта не обеспечена золотыми резервами или уровнем ВВП.
- ❑ Поэтому текущий (высокий) курс биткоина может легко обвалиться до полного нуля, фундаментальных экономических факторов, которые могли бы его поддерживать, нет.
- ❑ Поэтому криптовалюты многие считают финансовыми пирамидами.





Нелегализованность

- В разных странах отношение к системе «Биткойн» сильно различается. В ряде стран официально разрешены операции с биткойнами.
- В Японии (с апреля 2017) Bitcoin является законным платёжным средством с налогом на их покупку.
- В других странах (например, в Китае) операции с биткойнами запрещены для банков, но разрешены для физических лиц
- В РФ был подготовлен законопроект об уголовном наказании за добычу Bitcoin, но пока что он не реализован.

Недостаточная популярность

- Пока что далеко не все экономические учреждения, интернет-магазины или сервисы, принимающие платежи, доверяют биткоинам. и продают товары взамен на криптовалюту.
- Ограниченная популярность мешает использовать Bitcoin на полную мощность.



От \$1 к \$2700: История биткоина

KtoNaNovenkogo.ru



1	3 января 2009	Создание первого блока Bitcoin	
2	22 мая 2010	Первая онлайн-покупка за биткоины (две пиццы)	
3	18 июля 2010	Открытие биржи Mt. Gox	\$0,07
4	9 февраля 2011	Стоимость биткоина достигла \$1	\$0,96
5	19 июня 2011	Взлом базы данных MtGox	\$17,77
6	1 марта 2012	Самая крупная кража биткоинов (более 46 000 BTC) на веб-хосте Linode	\$4,92
7	15 ноября 2012	Wordpress.com начал принимать биткоины	\$11,04
8	28 ноября 2012	Первое уменьшение эмиссионной награды с 50 до 25 BTC	\$12,25
9	20 ноября 2013	Народный банк Китая разрешил использование биткоина	\$641,23
10	29 ноября 2013	Стоимость биткоина на бирже Mt. Gox достигла \$1242	\$1132,26
11	24 февраля 2014	Заккрытие биржи Mt. Gox	\$547,09
12	26 марта 2014	Налоговое управление США постановило, что биткоин должен облагаться налогом как собственность	\$581,52
13	18 июля 2014	Dell начал принимать биткоины	\$624,1
14	11 декабря 2014	Microsoft начал принимать биткоины	\$352,56
15	18 сентября 2015	Регулятор сырьевых рынков США приравнял биткоины к биржевым товарам	\$234,65
16	27 апреля 2016	Steam начал принимать биткоины	\$461,08
17	9 ноября 2016	Дональд Трамп избран президентом, рынок резко упал	\$726,36
18	3 января 2017	Биткоин превысил \$1000 впервые за три года	\$1020,47
19	20 мая 2017	Биткоин впервые достиг отметки \$2000	\$2051,73
20	22 мая 2017	Биткоин пробил \$2100 и \$2200	\$2139,03
	24 мая 2017	Биткоин пробил \$2300 и \$2400	\$2476,3
	25 мая 2017	Биткоин пробил \$2500, \$2600 и \$2700	\$2745,94

Разделение биткоина



- Первого августа 2017 года от классического биткоина (BTC) отделился Bitcoin Cash (BCC).
- Произошло это потому, что с приближением к граничному количеству скорость транзакций резко замедлилась.
- Поэтому выпустили новую программу, которая позволяет проводить в восемь раз больше транзакций за блок.
- Договориться сообщество между собой не смогло и сейчас мы имеем две валюты, которые очень отличаются в цене

Стоимость биткойна

- По данным на 13 августа, курс биткойна перевалил за 4 тысячи долларов.
- Что касается Bitcoin Cash, то он 13 августа на биржах стоил чуть более 307 долларов.



Реализация биткойн

- Биткойн — единственная виртуальная валюта, которая может использоваться как средство платежа.
- Его принимают в качестве оплаты во многих интернет-магазинах и даже кафе.
- Amazon работает с биткойном не напрямую, а через посредника. Но работает.



Реализация прочих криптовалют

- ❑ Остальные криптовалюты правильнее называть «квазивалютами», т.е. временными валютами с ограниченными свойствами.
- ❑ Их практически невозможно потратить. Поэтому это можно считать финансовым инструментом, но не деньгами в принятом смысле.



Прочие криптовалюты

- Количество разновидностей криптоденег регулярно растет. Основной причиной этой динамики стала популярность Bitcoin, его стоимость.
- Многие поддерживают криптоденьги, на их создание разработчики направили весьма солидные суммы.
- Каждая криптовалюта отличается от прочих своими преимуществами, степенью сложности майнинга, ценой и сервисами.



Лайткоин (Litecoin)

- По сравнению с прародителем всех криптовалют, Litecoin стоит около 35 долларов за одну монету.
- Он был создан как аналог серебра на рынке криптовалют, если биткойн это «золото».
- Максимальное количество «криптомонет» 84 млн., что в четыре раза больше чем в Bitcoin



Ethereum

- Курс Этериума — 137 долларов. Эту валюту придумал всего один программист — гражданин России Виталий Бутерин в 2005.
- Пока что, она не сумела зарекомендовать себя на рынке электронных валют, однако с самого первого месяца существования, приобрела большую стоимость



И еще...

- NMC Namecoin,
- Dogecoin,
- Peercoin,
- Ripple,
- Feathercoin,
- PPC
- PPcoin и многие другие.



Отношение к криптовалютам в мире



- ❑ Криптовалюта полностью запрещена во Вьетнаме, Боливии, Бангладеш, Эквадоре, Исландии.
- ❑ В США криптовалюта считается полноценным инвестиционным инструментом. Под налогообложение попадает эмиссия биткоинов, доход от её роста и т.д
- ❑ Криптовалюта в России запрещена для использования в качестве платежного средства, но приравнивается к биржевому инструменту. Налогообложение сделок неоднозначно.



Криптовалюты хайпы

- ❑ В ноябре 2015-го года в нескольких странах (в том числе и России) стартовал новый проект — E-Dinar, который обещал всем своим клиентам стабильный доход в месяц (20%).
- ❑ Уже в марте 2016-го года в соцсетях появились первые сообщения о том, что проект не выплачивает деньги. Логично, что инвесторы старались вывести деньги с получением первой прибыли (вывод денег).

Вложение в криптовалюты

- На сегодняшний день стоимость всех криптовалют (и биткойна в том числе) не гарантированы никакими финансовыми инструментами и не имеют правовой поддержки.
- Поэтому все операции с ними пользователь проводит на свой страх и риск.



Список использованных материалов

- <https://coinspot.io/beginners/что-такое-bitcoin>
- <https://bitcoin.org/ru/how-it-works>
- <http://www.amic.ru/voprosdnya/393777/>
- <http://bitcoinpaw.com/что-такое-bitcoin/>
- <https://ru.insider.pro/investment/2017-06-29/bitcoin-dlya-nachinayushih-polnoe-rukovodstvo/>
- <https://bitnovosti.com/что-такое-bitcoin/>
- <http://ideaman.ru/criptovalyut-krome-bitcoin.html>

