БИТКОИН И ФИДУЦИАРНЫЕ ДЕНЬГИ

Буликов Сергей Николаевич

доктор экономических наук, доцент,
ФГОБУ ВО «Ярославский государственный технический университет»,
кафедра «Управление предприятием»,
г. Ярославль, Российская Федерация.
E-mail: sbulikov@ya.ru

JEL G 10; G 19

БИТКОИН И ФИДУЦИАРНЫЕ ДЕНЬГИ

Аннотация: Различные криптовалюты стремительно распространяются сегодня на мировом финансовом рынке. Однако, понимание механизма этого явления на уровне обыденного сознания остается весьма проблематичным. Цель данной работы – снижение возможных затруднений обычной аудитории в понимании такой экономической категории как криптовалюта – безналичные цифровые деньги. Побудительный мотив публикации – собственные затраты труда и времени на освоение названной категории с использованием общедоступных Интернет-ресурсов, а также приобретенный здесь опыт – «сын ошибок трудных». Автор надеется на полезность представленной информации для многих криптовалютных новичков – подобных ему самому «чайников» в этом вопросе.

Ключевые слова: криптовалюта и фидуциарные деньги; биткоин; асимметричное шифрование информации; технология эмиссии криптовалюты – майнинг в блокчейн(е); аксиома биткоин.

BITCOIN AND FIDUCIARY MONEY

Abstract: Various cryptocurrencies are spreading rapidly today in the world financial market. However, understanding the mechanism of this phenomenon at the level of everyday consciousness remains problematic. The purpose of this work is to decrease the possible difficulties of a General audience in the understanding of such economic categories as the cryptocurrency of non-cash digital money. Incentive publications – self labor costs and time on the development of named categories using the publicly available Internet resources, as well as acquired the experience – «the son of errors difficult» ©. The author hopes the usefulness of the information presented for many cryptocurrency novice like himself «dummies» in this issue.

Keywords: cryptocurrency and fiduciary money; bitcoin; asymmetric encryption of information; the emission technology of cryptocurrency – mining blockchain; axiom bitcoin.

Введение

Уверенное понимании такой экономической категории как криптовалюта – безналичные цифровые деньги становится жизненно необходимым на современном этапе развития общества. Действительно, криптовалюта, как современное направление развития мировой платежной системы, становится все более актуальной и популярной. Так, страница https://bitmakler.com/kriptovaluta показывает, что на валютном рынке сегодня торгуется 748 наименований криптовалют. Единицей любой криптовалюты является «coin» – «монета» [англ].

Самой ценной и популярной криптовалютной монетой является биткоин (btc) – см. таблицу 1. На примере btc рассмотрим далее характерные отличительные черты криптовалют и их соответствие традиционным фидуциарным деньгам.

Таблица 1 – Некоторые виды криптовалют

Крипто-валюта	Символ	Цена, BTC	Объём 24, BTC	Всего монет	Алгоритм	Год
Bitcoin	BTC	1	155186.4115	21000000	SHA-256	2009

Ethereum	ETH	0,0804	8964.1029	90000000	Dagger-Hashimoto	2015
Litecoin	LTC	0,0162	6643.0934	84000000	Scrypt	2011
Bitcoin Cash	BCH	0,135	3677.0236	21000000	SHA-256	2017
Ethereum Classic	ETC	0,0036	2217.6013	90000000	Dagger-Hashimoto	2015
Monero	XMR	0,0259	1932.4875	18446744	CPU mining, CryptoNight	2014
Ripple	XRP	0,0000494	1406.9979	100000000000	ECDSA	2013
Dashcoin	DSH	0,0771	1120.5333	184467440737	CPU mining, CryptoNight	2014
BitShares	BTS	0,00003108	881.2305	2000000000	Транзакционный сбор	2014

Что такое биткоин

Сатоси Накамото определил электронную монету как цифровую пиринговую наличность в виде определенной временной точки в последовательности цифровых подписей под транзакциями в блокчейн(е) [9]. Такой точкой выступает факт создания нового блока в блокчейн(е). Этому факту соответствует некоторый конечный объем цифровой информации. Этот объем информации принимается за 1 btc.

Блокчейн является оверлейным образованием поверх компьютерной сети пользователей btc в Интернет. В этой связи требуется четко отличать блокчейн от названной компьютерной сети. Последняя, с ее суммарной вычислительной мощностью, являются физической основой и носителем виртуальной цепочки блоков транзакций – блокчейн(а).

Эмиссия биткоинов

По аналогии с [10] нами был произведен расчет ограниченной эмиссии цифровых btc-монет. Результаты расчета, как расписания выпуска btc, представлены в таблице 2. Таблица показывает, что в протоколе и программном обеспечении btc С. Накамото четко прописал следующие условия-ограничения эмиссии btc:

а) первые 50 btc-монет принадлежат автору криптовалюты за создание первого блока транзакций, положившему начало блокчейн(у) – см. поле G в таблице 2;

б) дальнейшая эмиссия btc происходит в виде вознаграждения пользователей btc за их цифровые подписи под транзакциями с №1 в каждом новом блоке блокчейн(а): майнер , чья подпись стоит под транзакцией, случайным образом ставшей первой в новом блоке блокчейн(а), автоматически получает установленную награду в виде новых btc-монет;

1				Создано блоков , шт.				Эмиссия btc, монет		
2	№ 4-летнего календарного периода	Дата начала периода	Дата окончания периода	на начало периода	за период (const.)	на конец периода	Награда за создание блока в текущем периоде, btc/блок	на начало периода	за период	на конец периода
3	1 (4 года)	01.01.2009	31.12.2012	0	210000	210000	50,00000000	0,00000000	10500000,00000000	10500000,00000000
4	2 (4 года)	01.01.2013	31.12.2016	210000	210000	420000	25,00000000	10500000,00000000	5250000,00000000	15750000,00000000
5	3 (4 года)	01.01.2017	31.12.2020	420000	210000	630000	12,50000000	15750000,00000000	2625000,00000000	18375000,00000000
6	4 (4 года)	01.01.2021	31.12.2024	630000	210000	840000	6,25000000	18375000,00000000	1312500,00000000	19687500,00000000
7	5 (4 года)	01.01.2025	31.12.2028	840000	210000	1050000	3,12500000	19687500,00000000	656250,00000000	20343750,00000000
8	6 (4 года)	01.01.2029	31.12.2032	1050000	210000	1260000	1,56250000	20343750,00000000	328125,00000000	20671875,00000000
9	7 (4 года)	01.01.2033	31.12.2036	1260000	210000	1470000	0,78125000	20671875,00000000	164062,50000000	20835937,50000000
10	8 (4 года)	01.01.2037	31.12.2040	1470000	210000	1680000	0,39062500	20835937,50000000	82031,25000000	20917968,75000000
11	9 (4 года)	01.01.2041	31.12.2044	1680000	210000	1890000	0,19531250	20917968,75000000	41015,62500000	20958984,37500000
12	10 (4 года)	01.01.2045	31.12.2048	1890000	210000	2100000	0,09765625	20958984,37500000	20507,81250000	20979492,18750000
13	11 (4 года)	01.01.2049	31.12.2052	2100000	210000	2310000	0,04882813	20979492,18750000	10253,90625000	20989746,09375000
14	12 (4 года)	01.01.2053	31.12.2056	2310000	210000	2520000	0,02441406	20989746,09375000	5126,95312500	20994873,04687500
15	13 (4 года)	01.01.2057	31.12.2060	2520000	210000	2730000	0,01220703	20994873,04687500	2563,47656250	20997436,52343750
16	14 (4 года)	01.01.2061	31.12.2064	2730000	210000	2940000	0,00610352	20997436,52343750	1281,73828125	20998718,26171870
17	15 (4 года)	01.01.2065	31.12.2068	2940000	210000	3150000	0,00305176	20998718,26171870	640,86914063	20999359,13085940

	A	B	C	D	E	F	G	H	I	J
21	№ 4-летнего календарного периода	Дата начала периода	Дата окончания периода	Создано блоков , шт.			Награда за создание блока в текущем периоде, btc/блок	Эмиссия btc, монет		
22				на начало периода	за период (const.)	на конец периода		на начало периода	за период	на конец периода
23	18 (4 года)	01.01.2077	31.12.2080	3570000	210000	3780000	0,00038147	20999839,78271480	80,10864258	20999919,89135740
24	19 (4 года)	01.01.2081	31.12.2084	3780000	210000	3990000	0,00019073	20999919,89135740	40,05432129	20999959,94567870
25	20 (4 года)	01.01.2085	31.12.2088	3990000	210000	4200000	0,00009537	20999959,94567870	20,02716064	20999979,97283940
26	21 (4 года)	01.01.2089	31.12.2092	4200000	210000	4410000	0,00004768	20999979,97283940	10,01358032	20999989,98641970
27	22 (4 года)	01.01.2093	31.12.2096	4410000	210000	4620000	0,00002384	20999989,98641970	5,00679016	20999994,99320980
28	23 (4 года)	01.01.2097	01.01.2101	4620000	210000	4830000	0,00001192	20999994,99320980	2,50339508	20999997,49660490
29	24 (4 года)	01.01.2101	31.12.2104	4830000	210000	5040000	0,00000596	20999997,49660490	1,25169754	20999998,74830250
30	25 (4 года)	01.01.2105	31.12.2108	5040000	210000	5250000	0,00000298	20999998,74830250	0,62584877	20999999,37415120
31	26 (4 года)	01.01.2109	31.12.2112	5250000	210000	5460000	0,00000149	20999999,37415120	0,31292439	20999999,68707560
32	27 (4 года)	01.01.2113	31.12.2116	5460000	210000	5670000	0,00000075	20999999,68707560	0,15646219	20999999,84353780
33	28 (4 года)	01.01.2117	31.12.2120	5670000	210000	5880000	0,00000037	20999999,84353780	0,07823110	20999999,92176890
34	29 (4 года)	01.01.2121	31.12.2124	5880000	210000	6090000	0,00000019	20999999,92176890	0,03911555	20999999,96088450
35	30 (4 года)	01.01.2125	31.12.2128	6090000	210000	6300000	0,00000009	20999999,96088450	0,01955777	20999999,98044220
36	31 (4 года)	01.01.2129	31.12.2132	6300000	210000	6510000	0,00000005	20999999,98044220	0,00977889	20999999,99022110
37	32 (4 года)	01.01.2133	31.12.2136	6510000	210000	6720000	0,00000002	20999999,99022110	0,00488944	20999999,99511060
38	33 (4 года)	01.01.2137	31.12.2140	6720000	210000	6930000	0,00000001	20999999,99511060	0,00244472	20999999,99755530

1 сатоши =10^{-8}btc

в) каждые 4 года установленная сумма награды за новый блок уменьшается в два раза, пока не доходит до одного сатоши (10-8btc) – предел деления btc-монеты, названный по имени ее создателя; тогда весь отрезок времени btc- эмиссии делится на 33 4-летних периода в течение 2009-2140 гг., где 2009 г. – время появления в сети первых btc-монет – см. поля A,B,C,G в таблице 2;

г) по заданному btc-алгоритму, в течение каждого 4-летнего периода в блокчейн(е) автоматически создается (возникает) 210 тыс. новых блоков – см. поле E таблицы 2; со средней скоростью 1 блок / 10 мин. = 6 блоков / час = 144 блока /сутки = 52500 блоков / год; эмиссия btc заканчивается на блоке № 6930000 выпуском 1-го сатоши – см. ячейки F38 и G38 таблицы 2;

д) по заданному btc-алгоритму, весь объем эмиссии рассматриваемой криптовалюты составляет 21млн. btc-монет – см. ячейку J38 таблицы 2.

В заключение этого раздела представим график эмиссии btc-валюты из [13]. График хорошо коррелируется с нашими данными таблицы 2.

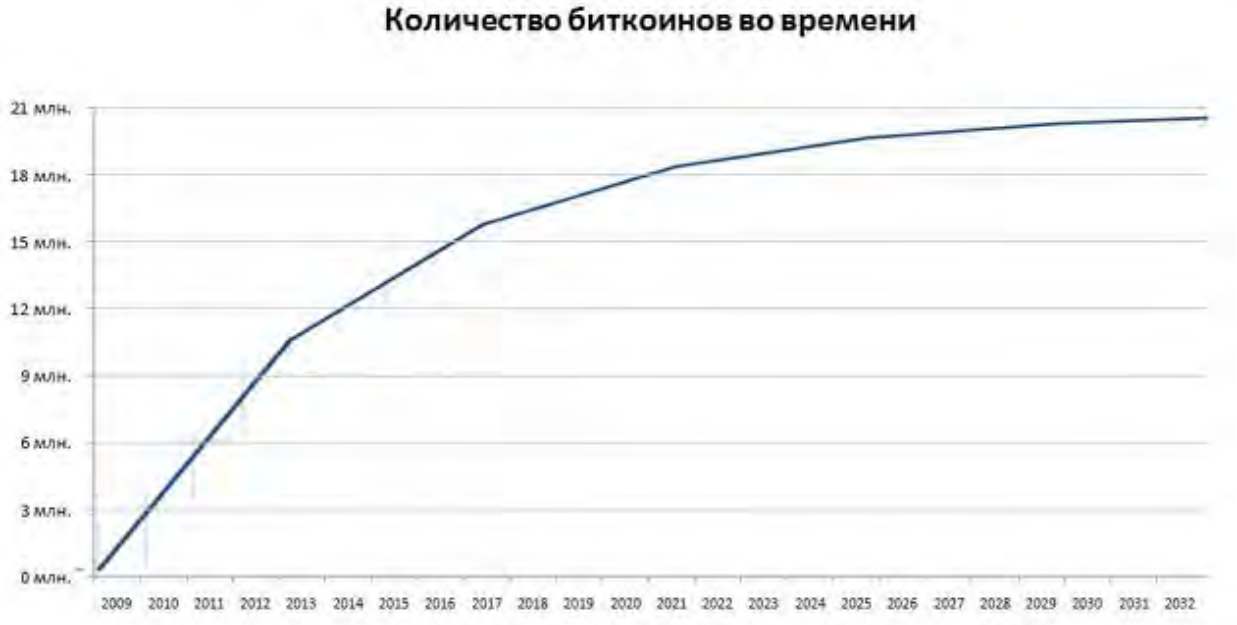

Рисунок 1 – Известный график эмиссии btc-валюты [13]

Основы технологии майнинга (блокчейн)

Майнинг осуществляется майнером путем совершения своих собственных транзакций в блокчейн(е) btc-платежной системы. В соответствии с п. б) в предыдущем разделе, майнер, чья подпись стоит под транзакцией, случайным образом ставшей первой в новом блоке блокчейн(а), автоматически получает установленную награду в виде определенной суммы новых btc-монет. Данное положение предопределяет нижеследующие требования к майнерам.

Характерные отличительные черты майнера и аксиома биткоин

Майнер это человек, занимающийся майнингом:

1. зарегистрированный участник криптовалютного рынка btc, имеющий собственную, уникальную цифровую подпись (логин, пароль), а также соответствующую уникальную цифровую ключевую пару – открытый и закрытый (секретный) ключи участника ; ключевая пара автоматически генерируется при регистрации участника;

2. участник облачных вычислений в публичном облаке ;

3. элемент сети параллельных вычислительных систем – субъект блокчейн(а) и провайдер вычислительных ресурсов.

Принципиальная схема функционирования блокчейн(а) представлена на рисунке 2.

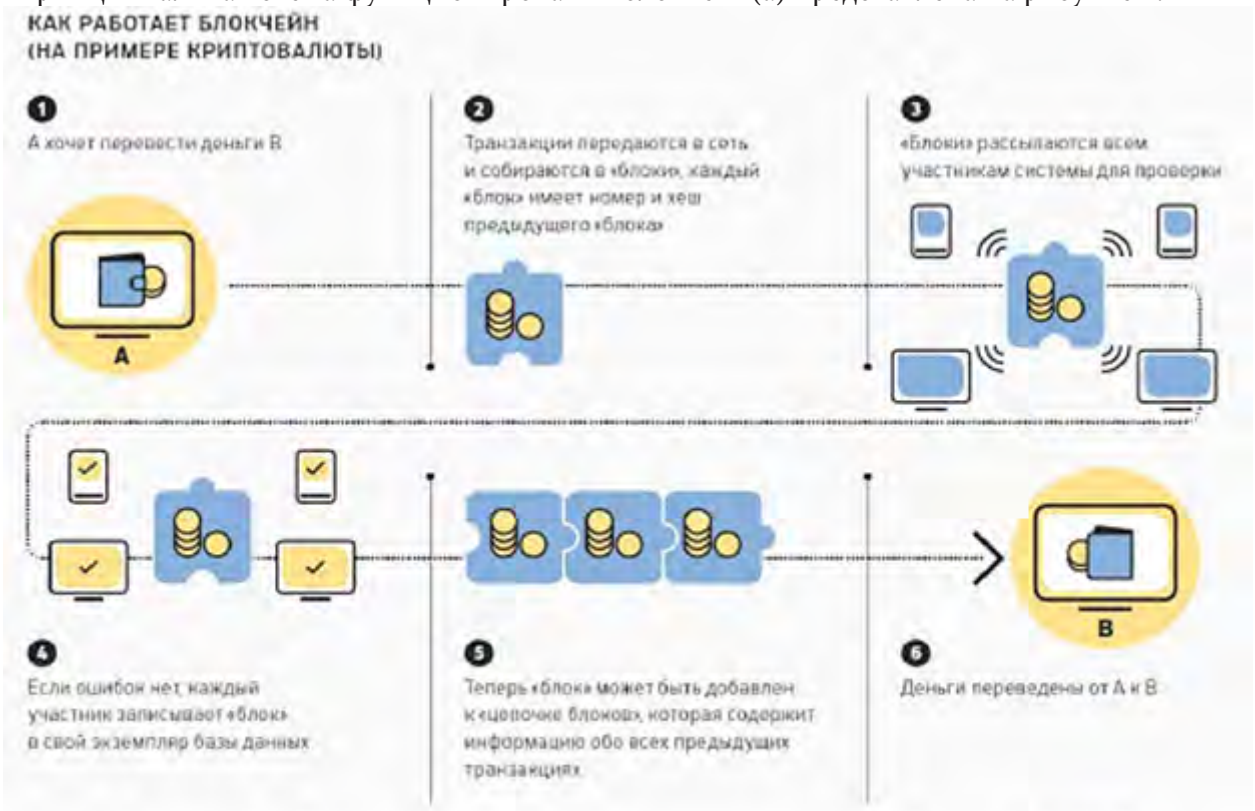

Рисунок 2 – Принципиальная схема функционирования блокчейн(а) [16]

Данные таблицы 2 и рисунка 2 показывают, что в btc-платежной системе технологии эмиссии, майнинга и валютных транзакций тесно взаимообусловлены. Эти технологии соответствует добропорядочному желанию их автора, честных майнеров и пользователей btc-платежной системы:

а) сделать жизненный путь каждой btc-монеты максимально открытым (прозрачным) и, за счет этого,

б) оградить эмиссию и транзакции от диктата третьих лиц, кем бы они ни были и, в первую очередь, различных государственных, банковских и силовых структур, а также валютных злоумышленников (мошенников и воров);

в) устранить двойные транзакции – двойную трату (расход) одной и той же btc-монеты (фальшивые деньги);

г) сделать транзакции необратимыми (только «туда»).

Условно обозначим эти четыре пункта (а-г) как «аксиома btc».

Аксиома btc обусловила отказ от доверительного осуществления транзакций при посредничестве банковских структур и переход к криптографическому их (транзакций) осуществлению в сети блокчейн. Как отмечал С. Накамото: «Необходима платежная система, основанная на криптографии, а не доверии, которая позволила бы любым двум участникам осуществить перевод средств напрямую, без участия посредника» [9].

Отказ от доверительного централизованного осуществления эмиссии и транзакций, а также необходимость эффективного решения проблемы двойной траты настоятельно потребовал использования в btc-платежной системе:

а) хеширования транзакций и их блоков с постановкой метки времени (календарная дата и суточное время хеширования);

б) криптографической системы с открытым ключом.

Хеширование транзакций и их блоков

Криптографическое осуществление каждой транзакции потребовало хеширования (цифрового свертывания – кодирования) формальных признаков транзакции: дата (время) отправления платежа; счет отправителя; валюта и сумма платежа; счет получателя; назначение платежа и т.п.

В таблице 3 представлены результаты хеширования двух массивов входных данных произвольной длины в выходную битовую строку фиксированной длины с помощью функции свертки по алгоритму SHA-256 из btc-платежной системы [15].

Таблица 3 показывает, что любое изменение входного массива информации (строка 1 - …btc; 1257; …; строка 2 - …btc; 1256; …;) вызывает изменение его хеш-кода.

Таблица 3 – Пример хеширования

Входной массив (ключ, сообщение)	Хеш (хеш-код, хеш-сумма, сводка сообщения)	Строка
Транзакция №XXXX; 28.09.2017; 08-58; счет отправителя 123456; btc; 1257; счет получателя 654321; Материалы	63cca91093cfd535d4c8391da6f8211bc9658ec2ba6d78263 0be576a0e985910	1
Транзакция №XXXX; 28.09.2017; 08-58; счет отправителя 123456; btc; 1256; счет получателя 654321; Материалы	0fd186bb3ca14e31b3ee72bfec984ac3e8874e228a46ca5a66 9a8b5ef0426d17	2

SHA-256 позиционируется автором как безопасный хеш-алгоритм, легко создающий контрольные суммы, один из ряда существующих криптографических хэш-функций. Этот алгоритм генерирует уникальный криптографический хеш (информационную сводную строку-свертку) фиксированного размера – 64 знака = 256 бит (32 байта). 1 знак = 4 бит информации. 1 байт = 8 бит – двоичная система счисления – основа работы компьютера.

Криптографический хеш является односторонней функцией – его нельзя расшифровать обратно. Это делает его подходящим для уникальной цифровой подписи текста или файла данных, хэш-аутентификации, проверки электронного пароля. SatoshiAlgorithm SHA-256 является сегодня одной из самых сильных хэш-функций.

Криптографическая система с открытым ключом [19]

Как было отмечено в предыдущем разделе, каждый зарегистрированный участник btc-платежной системы имеет собственную уникальную цифровую подпись в виде собственного логина и пароля, также собственную ключевую пару – открытый и закрытый (секретный) ключи.

Главное криптографическое свойство ключевой пары: по секретному ключу легко вычисляется открытый ключ, но по известному открытому ключу практически невозможно вычислить секретный.

Закрытый ключ (en:Private key) – ключ, известный только своему владельцу. Сохранение участником btc-платежной системы своего закрытого ключа в строгой тайне гарантирует НЕвозможность злоумышленной подделки транзакции и цифровой подписи участника [20].

Открытый ключ (en:Public key) – ключ, который публикуется участником btc-платежной системы и используется для:

- проверки подлинности подписанной кем-то транзакции, пришедшей на IP-адрес участника ;
- предупреждения мошенничества со стороны участника в виде его отказа от требуемой от него подписи этой транзакции.

Открытый ключ участника вычисляется, как значение некоторой заданной функции от его закрытого ключа, но знание открытого ключа участника не дает возможности определить его закрытый ключ [20].

Технологические этапы майнинга (блокчейн) – рисунок 2.

Этап 1. «А хочет перевести деньги В» будем понимать как очередной владелец btc (участник А) готовит транзакцию в виде отправки монеты ее следующему владельцу (участнику В).

С учетом принятой «аксиомы btc» А должен показать когда и откуда монета появилась в его btc-кошельке («пришла на его расчетный счет»):

- А получил монету в виде вознаграждения за свою цифровую подпись под какой-то транзакцией с №1 в новом блоке блокчейн(а);
- А получил монету в виде оплаты своих собственных работ или услуг.

В любом случае А всегда подписывает хеш предыдущей транзакции, где он выступает в роли получателя монеты.

Механизм btc-транзакций представлен на рисунке 3.

Рисунок 3 - Механизм btc-транзакций по данным [9]

Рисунок 3 показывает, что очередной владелец отправляет монету следующему посредством:

1. подписи хэш(а) предыдущей транзакции с ее меткой времени;
2. подписи открытого (публичного) ключа будущего владельца монеты;
3. присоединения этой информации к монете.

Чтобы удостовериться и подтвердить корректность всей цепочки предыдущих Владельцев

монеты каждый следующий ее Получатель проверяет каждую транзакционную подпись на всем жизненном пути (по меткам времени транзакций) пришедшей к нему монеты. Пунктирные стрелки на рисунке 3 обозначают автоматизированную проверку соответствия подписи и ключевой пары участников btc-платежной системы в их различных транзакциях.

Выполнение названного условия способствует соблюдению таких пунктов условной аксиомы btc, как:

а) сделать жизненный путь каждой btc-монеты максимально открытым (прозрачным) и, за счет этого,

б) оградить эмиссию и транзакции от диктата третьих лиц и, в первую очередь, различных государственных, банковских и силовых структур, а также валютных злоумышленников (мошенников и воров).

Обеспечение третьего и четвертого пунктов условной аксиомы btc – «устранить двойные транзакции – двойную трату (расход) одной и той же btc-монеты (фальшивые деньги), сделать транзакции необратимыми» начинается с Этапа 2 в числе технологических этапов майнинга (блокчейн) – «транзакции передаются в сеть и собираются в блоки; каждый блок имеет номер и хеш предыдущего блока» (рисунок 2).

Передача транзакции в сеть является результатом двух действий:

1. автоматизированное отнесение транзакции к текущему блоку (1 блок / 10 мин. = 6 блоков / час и т.д.). Если повезет – награда за эмиссию.

2. автоматизированная постановка метки времени на блок транзакций и хеширование этого блока.

3. открытой публикации этого хэш(а) в сети.

Обеспечение третьего и четвертого пунктов условной аксиомы btc продолжается на Этапе 3 технологии майнинга (блокчейн) – «Блок рассылается всем участникам системы для проверки» (рисунок 2). На этом этапе уже все участники (IP-адреса) в btc-платежной системе проверяют достоверность транзакций в составе блока по их хеш(ам), т.е. времени транзакций, их подписям (отправителям) и открытым ключам (получателям) – рисунок 3.

Этап 4 – «Если ошибок нет, каждый участник записывает проверенный блок в свой экземпляр базы данных» (рисунок 2). Таким образом все участники проекта имеют единую и достоверную (проверенную и принятую всеми IP-адресами) базу данных. После такой тотальной проверки можно приступать к следующему этапу.

Этап 5 – «Теперь блок может быть добавлен к цепочке блоков, которая содержит информацию обо всех предыдущих транзакциях» (рисунок 2). Этап 5 обеспечивает качество информации в блокчейн, т.е. ее (информации) достоверность, прозрачность, своевременность, полноту, однозначность и необратимость.

Этап 6 – «Деньги переведены от А к В» – со счета А на счет В в виде их btc-кошельков.

В резюме к этому разделу отметим, что основой технологии блокчейн является хеширование меток времени, тотальная проверка соответствия фактических отправителей и получателей информации их заданным IP-адресам, а также единство и достоверность общей базы данных. При этом метка времени в хэш(е) транзакций гарантирует, что в данный момент конкретные транзакции достоверно существовали и потому попали в хэш блока. Каждый хэш включает в себя предыдущую метку: так выстраивается блокчейн, где очередное звено (блок) укрепляет достоверность транзакций всех предыдущих блоков – рисунок 4.

Технология блокчейн подтверждает возможность отказа от доверительного осуществления транзакций при посредничестве банковских структур и переход к криптографическому их (транзакций) осуществлению в компьютерной сети. При этом обеспечивается принятая Аксиома btc, т.е. жизненный путь каждой btc-монеты становится максимально открытым (прозрачным) и, за счет этого, эмиссия

и транзакции становятся свободными от влияния третьих лиц, кем бы они ни были и, в первую очередь, различных государственных и банковских структур, а также валютных злоумышленников (мошенников и воров). Кроме того, устраняются фальшивые деньги в виде «двойных транзакций» т.е. двойной траты (расхода) одной и той же btc-монеты, что обеспечивает необратимость транзакций.

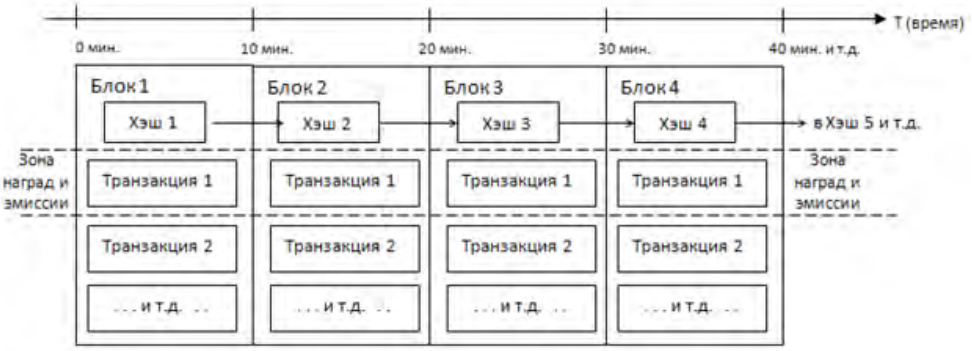

Рисунок 4 – Механизм формирования блокчейн(а)

Перспективы майнинга

Присутствие множества средств платежа на валютном рынке обусловливают его конкурентность и лишают валютного монополиста соответствующих диктаторских преимуществ. Эта рыночная аксиома предопределяет перспективы майнинга любой криптовалюты.

На протяжении всей истории денег валютным монополистом всегда выступали и продолжают выступать властные государственные структуры с их эмиссионными подразделениями. Общественные структуры, начиная с отдельных граждан, семей, домовладений и заканчивая сферами частного материального производства, медицины, образования, науки, искусства не имеют права совершать свои транзакции опосредованно, минуя меркантильное и алчное участие государства в лице иерархии госчиновников, банкиров и силовиков.

В таком аспекте перспективы развития любой криптовалюты обусловлены текущим правовым статусом государственных и общественных структур – регуляторов финансового рынка, законодательной и исполнительной ветвей государственной власти. При доминировании государства в экономике для криптовалют не просматривается позитивного будущего, что обусловлено монополистическими интересами госчиновников, банкиров и силовиков.

Однако, технология блокчейн, как криптографическое оформление информационных связей участников одноранговых (пиринговых) проектных структур при тотальной цифровой проверке подлинности каждого документа и единой внутрипроектной базе данных, остается актуальной даже в условиях государственного монополизма. Иными словами, однозначное понимание, реализация и достоверное подтверждение соответствия плановых и фактических параметров проекта, в т.ч. любой госпрограммы, всегда востребовано в условиях корректных транзакций. Если условие корректных, в т.ч. финансовых, транзакций не обязательно, то и блокчейн становится не актуальным. А это значит, что остаются не востребованными приведенные ниже правила опосредованных и добросовестных системных связей (отношений) рыночных субъектов:

1. Никто не доверяет друг другу, но все доверяют бесстрастному и объективному автоматизированному цифровому подтверждению корректности транзакций.

2. Для такого подтверждения каждая транзакция обязательно имеет следующие электронные атрибуты: метку времени; хэш, связанный с хэш(ем) предшествующей транзакции; электронную подпись Отправителя; открытый ключ Получателя. Последний своим закрытым ключом подтверждает подпись Отправителя. С другой стороны, Отправитель, используя открытый ключ Получателя,

убеждается в достоверности его подписи (см. рис.3). Так осуществляется первый этап цифрового подтверждения корректности транзакций и страховки от фальшивых денег.

3. Затем, каждая финансовая транзакция, уже подтвержденная ее Сторонами, рассылаются всем участникам проекта – узлам информационной системы в виде ее отдельных IP-адресов. Это необходимо для отслеживания жизненного пути криптомонет, токенов и автоматизированного регулирования финансовых параметров проекта.

4. Каждый узел, по заданным признакам, объединяет пришедшие транзакции в блок.

5. Узлы принимают этот блок в блокчейн и свою базу данных, только если все транзакции в нем корректны и не используют уже потраченные средства;

6. Свое согласие с новыми данными узлы выражают, начиная работу над следующим блоком и используя хэш предыдущего в качестве новых исходных данных (см. рис.4).

Так осуществляется второй этап цифрового подтверждения корректности транзакций и страховки от фальшивых денег. Кроме того, данный этап необходим для безусловного соблюдения заданных финансовых параметров проекта.

Невостребованность данных правил опосредованных, свободных и добросовестных отношений рыночных субъектов говорит о сегодняшней неготовности государства и общества к честному, креативному взаимодействию.

Заключение

Криптовалюта это такие же фидуциарные деньги , как и любая другая валюта на земном шаре. Стоимость фидуциарных денег поддерживается за счёт веры людей в то, что они смогут обменять их на что-либо ценное. Очевидно, что феномен btc во многом обусловлен падением авторитета государственной власти и ее банковской системы. Люди просто устали от унизительной финансовой диктатуры госчиновников, банкиров и силовиков.

В таких условиях государство, как финансовый монополист, может только запрещать или, в лучшем случае, игнорировать криптовалюту. Ведь, как правило, никто и никогда не поддерживает своего конкурента.

Однако, криптовалюта имеет ряд привлекательных характеристик, которые выгодно отличают ее от традиционных валютных систем и повышают ее конкурентоспособность на валютном рынке:

- ограниченность, определенность, известность и децентрализация эмиссии;
- безналичность и тотальная автоматизированная проверка корректности транзакций;
- низкая вероятность использования фальшивых денег;
- слабое влияние чиновничьей и банкирской недобросовестности и злонамеренности;
- ничтожная внутрипроектная коррупционная емкость;
- глобальная унифицированность и доступность.

Названные преимущества криптовалюты, а также ее информационная защищенность оставляют возможность использования btc как фактора цивилизационного развития в XXI-м веке.

В настоящее время криптовалюта, как и любое другое новшество, находится на стадии общественного осмысления, слабого понимания и, как следствие, отторжения. Достаточно вспомнить восстание луддитов – «бунт против машин» в Англии в начале XIX века или такие «лженауки» как генетика и кибернетика – «продажные девки империализма» в России XX века. Первоначальное непонимание Интернета можно также добавить к этому списку.

Однако, в свете сегодняшнего состояния глобального валютного рынка и коррупционной проблематики разных стран, остается надежда, что технология блокчейн и криптовалюта получат достойное понимание и поспособствует позитивному развитию мировой финансовой системы и национальных экономик, а также соответствующей трансформации общественных и государственных институций.

В завершение считаю необходимым отметить, что положения и выводы, высказанные мною в данной работе, на мой взгляд, логично «вписываются» в русло поисков разработчиков концепции теоретической экономии [см., например: 28-31]. Прежде всего это, наверное, касается аспектов определения объективных тенденций сегодняшней экономики и прогнозирования путей перехода к будущему состоянию социума и его хозяйства через преодоление нынешней системной катастрофы в мировой и российской экономике.

СПИСОК ЛИТЕРАТУРЫ:

1. Значение слова Категория по Логическому словарю. - [Электрон. ресурс]. – Режим доступа: http://tolkslovar.ru/k2988.html (дата обращения 10.09.2017).

2. Крипто... в Энциклопедическом словаре. - [Электрон. ресурс]. – Режим доступа: http://tolkslovar.ru/k11416.html (дата обращения 10.09.2017).

3. Валюта. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Валюта (дата обращения 10.09.2017).

4. Сатоси Накамото. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Сатоси Накамото (дата обращения 10.09.2017).

5. Одноранговая сеть. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Одноранговая сеть (дата обращения 23.09.2017).

6. Оверлейная сеть. - [Электрон. ресурс]. – Режим доступа: https://traditio.wiki/Оверлейная сеть (дата обращения 23.09.2017).

7. Транзакция. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Транзакция (значения) (дата обращения 17.09.2017).

8. Блокчейн. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Блокчейн (дата обращения 23.09.2017).

9. Биткоин: цифровая пиринговая наличность. - [Электрон. ресурс]. – Режим доступа: https://coinspot.io/technology/bitcoin/perevod-stati-satoshi-nakamoto/ (дата обращения 23.09.2017).

10.Ограниченная эмиссия. - [Электрон. ресурс]. – Режим доступа: https://ru.bitcoin.it/wiki/Ограниченная эмиссия (дата обращения 23.09.2017).

11. Майнинг. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Майнинг (дата обращения 16.09.2017).

12. Словари и энциклопедии на Академике. - [Электрон. ресурс]. – Режим доступа: https://dic.academic.ru/dic.nsf/ruwiki/88479Параллельные вычислительные системы (дата обращения 17.09.2017).

13. Эмиссия биткоинов. - [Электрон. ресурс]. – Режим доступа: https://yandex.ru/images/График выпуска биткоинов (дата обращения 23.09.2017).

14. Хэширование. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Хэширование (дата обращения 28.09.2017).

15.Хэшкалькулятор. - [Электрон. ресурс]. – Режим доступа: http://www.xorbin.com/tools/sha256-hash-calculator (дата обращения 28.09.2017).

16. Криптовалюта Биткоин - определение и как работает, где купить и как заработать. - [Электрон. ресурс]. – Режим доступа: http://sovets.net/13628-bitkoin-chto-eto-takoe-prostymi-slovami (дата обращения 29.09.2017).

17. Открытый и закрытый ключ: для чего они применяются? - [Электрон. ресурс]. – Режим доступа: https://www.emaro-ssl.ru/blog/public-and-private-key/ (дата обращения 03.10.2017).

18.Облачные вычисления. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Облачные вычисления (дата обращения 18.09.2017).

19.Криптосистема с открытым ключом. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Криптосистема с открытым ключом (дата обращения 03.10.2017)

20. Закрытый ключ. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Закрытый ключ (дата обращения 04.10.2017)

21.IP-адрес. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/IP-адрес (дата обращения 04.10.2017)

22. Биткойн решает проблему «двойной траты». - [Электрон. ресурс]. – Режим доступа: https://bitnovosti.com/2014/05/01/double-spending-problem/ (дата обращения 07.10.2017)

23. Меркантилизм. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Меркантилизм (дата обращения 12.10.2017)

24. Токен. - [Электрон. ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Токен (дата обращения 14.10.2017)

25. Фидуциарные деньги. - [Электрон. ресурс]. – Режим доступа: https://yandex.ru/search/?text=фидуциарные деньги (дата обращения 14.09.2017)

26. Простой способ инвестировать в технологии blockchain. Инвестиционный фонд NakamotoCapital. - [Электрон. ресурс]. – Режим доступа: https://nakamoto.capital/?lang=ru (дата обращения 20.11.2017).

27. Простой способ инвестировать в технологии blockchain. Школа криптоэкономики. - [Электрон. ресурс]. – Режим доступа: http://bituniversity.ru (дата обращения 20.11.2017).

28. Гордеев В.А. Категория конкурентоспособности в зеркале теоретической экономии как нового парадигмального мейнстрима. Повышение конкурентоспособности экономики РФ в условиях западных санкций: Монография / под ред. В.А. Гордеева, М.А. Угрюмовой, С.В. Шкиотова. – Ярославль: Издательский дом ЯГТУ, 2015. - 364 с. – Глава 1. - С. 9-85.

29. Гордеев В.А. Категория новой индустриализации в зеркале теоретической экономии как нового парадигмального мейнстрима. Новая индустриализация как фактор повышения конкурентоспособности экономики Российской Федерации: теоретико-методологические аспекты: Монография / В.А. Гордеев [и др.]; под ред. В.А. Гордеева, М.А. Угрюмовой, С.В. Шкиотова, М.И. Маркина. – Ярославль: Издат. дом ЯГТУ, 2016. - 168 с. – Раздел 1. - С. 11-54.

30. Гордеев В.А. Новая индустриализация в РФ как фактор обгоняющего развития, её первые итоги. Новая индустриализация в РФ как фактор обгоняющего развития: первые итоги, причины торможения и пути их преодоления: коллективная монография / В.А. Гордеев [и др.]; под ред. В.А. Гордеева, М.А. Угрюмовой, С.В. Шкиотова. – Ярославль: Издат. дом ЯГТУ, 2017. - 220 с. – Раздел 1. - С. 18-25.

31. Гордеев В.А. Теоретическая экономия как новый парадигмальный мейнстрим в исследовании современных проблем экономической науки и практики [Текст] // Современные проблемы экономической науки и практики в зеркале теоретической экономии: Монография / В.А. Гордеев [и др.]; под ред. В.А. Гордеева, М.А. Угрюмовой, С.В. Шкиотова. – Ярославль: Издат. дом ЯГТУ, 2017. - 187 с. – Раздел 1. - С. 18-30.