

Прикладная эконометрика, 2016, т. 44, с. 5–24.  
Applied Econometrics, 2016, v. 44, pp. 5–24.

Д. Фантаццини, Э. М. Нигматуллин,  
В. Н. Сухановская, С. В. Ивлиев<sup>1</sup>

## Все, что вы хотели знать о моделировании биткойна, но боялись спросить. Часть I

*Биткойн — это децентрализованная цифровая валюта и платежная система с открытым кодом. Она привлекла к себе значительное внимание и глобальный интерес, возрастающее число статей посвящено вопросам ее операционной, экономической и финансовой жизнеспособности. Данная статья рассматривает эконометрические и математические инструменты, которые были предложены к настоящему времени для моделирования цены биткойна, и различные другие аспекты, включая преимущества и ограничения. Обсуждаются методы определения основных характеристик биткойн-пользователей, модели оценки фундаментальной стоимости биткойна, эконометрические подходы к моделированию динамики цены биткойна, тесты для выявления финансовых пузырей в ценах и методологии, предложенные для изучения ценообразования на биткойн-биржах.*

**Ключевые слова:** биткойн; криптовалюты; хэшрейт; майнинг; привлекательность инвесторов; социальное взаимодействие; денежное предложение; спрос на деньги; спекуляции; прогнозирование; алгоритмическая торговля; пузыри; ценообразование; LPPL.

**JEL classification:** C22; C32; C51; C53; E41; E42; E47; E51; G17.

### 1. Введение

**Б**иткойн — это онлайн-децентрализованная валюта, которая позволяет пользователям покупать товары и услуги и осуществлять транзакции без привлечения третьей стороны. Она была запущена в 2009 году человеком или (что более вероятно) группой людей, действовавшей под псевдонимом Сатоши Накамото. Биткойн заложил основу для развития так называемых «криптовалют», которые базируются на криптографических средствах защиты. Основным свойством криптовалют является их децентрализованная структура: для их функционирования не требуется центральный орган, который выпускает и регулирует валюту, а транзакции осуществляются с использованием пирингового протокола без каких-либо посредников. Обзоры биткойна с точки зрения структуры и операций приведены в (Becker et al., 2013; Segendorf, 2014; Dwyer, 2015; Böhme et al., 2015) и на сайте

<sup>1</sup> **Фантаццини Деан** — Московская школа экономики, МГУ, Москва; fantazzini@mse-msu.ru.

**Нигматуллин Эрик Маликович** — Bocconi University, Милан, Италия; nigmatullin.erik@gmail.com.

**Сухановская Вера Николаевна** — Пермский государственный национальный исследовательский университет, Пермь; vera-sukhanovskaya@yandex.ru.

**Ивлиев Сергей Владимирович** — Пермский государственный национальный исследовательский университет, Пермь; ivliev@gmail.com.

www.bitcoin.org. Несколько центральных банков также изучали биткойн, см. (Velde, 2013; Lo, Wang, 2014; Badev, Chen, 2014; Ali et al., 2014; ECB, 2012, 2015). Обсуждение биткойна как потенциальной альтернативы денежной системы приведено в работах (Rogojanu, Badea, 2014; Weber, 2016), а экономика так называемого майнинга изучается в (Kroll et al., 2013). Анализ правовых вопросов, связанных с биткойном, приведен в работах (Allen, 2016; Murphy et al., 2015).

Данная статья рассматривает эконометрические и математические инструменты, которые были предложены к настоящему времени для моделирования цены биткойна и некоторых других аспектов. Насколько известно авторам, подобный обзор отсутствует в финансовой литературе и может быть интересен как профессионалам рынка, так и исследователям, учитывая раннюю стадию развития эмпирической литературы, посвященной биткойну.

Статья организована следующим образом. Раздел 2 описывает принципы, на которых построено функционирование биткойна, и приводит краткую статистику сети. В разделе 3 приведен обзор исследований, посвященных анализу характеристик, свойственных пользователям биткойна. В разделе 4 обсуждаются основные модели, используемые для оценки фундаментальной стоимости биткойна, от моделей размера рынка до моделей предельных издержек майнинга, основанных на энергопотреблении. Раздел 5 описывает несколько эконометрических подходов, предложенных для моделирования ценовой динамики биткойна, начиная с кросс-секционных регрессионных моделей, включающих в себя большинство торгуемых цифровых валют, и заканчивая одномерными и многомерными моделями временных рядов и моделями частотного диапазона. В разделе 6 приводится обзор тестов, используемых для выявления наличия финансового пузыря в ценах биткойна, которые могут быть условно разделены на два класса в зависимости от того, направлены ли они на определение одного пузыря или (потенциально) множественных пузырей. В разделе 7 изучаются методики, предложенные для оценки информационной доли различных биткойн-бирж с точки зрения информации, генерируемой рынком в целом, что является важным как для краткосрочных трейдеров, так и для долгосрочных инвесторов, которые хотели бы понимать, какая из бирж наиболее быстро реагирует на новую информацию. В разделе 8 приводятся основные выводы и предлагаются несколько возможных направлений дальнейших исследований<sup>2</sup>.

## 2. Определение криптовалют и биткойна

### 2.1. Как устроен биткойн?

#### 2.1.1. Цифровые подписи и криптографическая хеш-функция

В процессе проведения платежей в сети Биткойн используется криптография для проверки транзакций и создания блоков транзакций. В частности, Биткойн опирается на две криптографические схемы: 1) цифровые подписи и 2) криптографические хэш-функции. Первая схема позволяет обмениваться платежными инструкциями между сторонами транзакции, а вторая используется для поддержания дисциплины внесения записей по транзакциям в публичный реестр (блокчейн). Следует заметить, что ни одна из этих схем не явля-

<sup>2</sup> Разделы 5–8 будут опубликованы в другом выпуске журнала.

ется уникальной для Биткойна — все они широко используются для защиты коммерческих и государственных коммуникаций. Приведем краткое описание ниже.

Цифровые подписи используются для удостоверения подлинности сообщения между отправителем и получателем и обеспечивают:

- (i) *удостоверение подлинности*: получатель может проверить, что сообщение пришло от отправителя;
- (ii) *невозможность отказа*: отправитель не может отказаться от отправки сообщения;
- (iii) *целостность*: сообщение не было подделано.

Применение цифровых подписей включает шифрование с открытым ключом, в котором пара ключей — открытый и закрытый — генерируются с определенными желаемыми свойствами. Цифровая подпись используется для подписания сообщений: транзакция подписывается с помощью закрытого ключа, а затем транслируется в сеть Биткойн. Все участники сети могут проверить, что эта транзакция пришла от владельца открытого ключа, взяв сообщение, подпись, открытый ключ и запустив алгоритм проверки.

Криптографическая хеш-функция принимает на входе строку произвольной длины (сообщение  $m$ ) и возвращает строку с заранее определенной длиной (хэш  $h$ ). Функция является детерминированной, это означает, что один и тот же  $m$  на входе всегда будет давать один и тот же  $h$  на выходе. Помимо этого, функция также должна обладать следующими свойствами.

(i) *Стойкость к восстановлению прообраза*. При данном хэше  $h$  сложно найти такое сообщение  $m$ , при котором  $\text{хэш}(m) = h$ .

(ii) *Стойкость к коллизиям*. При заданном сообщении  $m1$  сложно найти другое сообщение  $m2$ , при котором  $\text{хэш}(m1) = \text{хэш}(m2)$ . Другими словами, изменение сообщения приводит к изменению хэша.

Выход хэш-функции выглядит так, как будто получен случайным образом, хотя и является детерминированным. Биткойн в основном использует алгоритм безопасного хеширования SHA-256 — тип Secure Hash Algorithm (SHA-2), разработанный Агентством национальной безопасности и опубликованный Национальным институтом стандартов и технологий, см. (Dang, 2012).

### 2.1.2. Владение биткойнами и биткойн-адреса

С технической точки зрения биткойны находятся в Биткойн сети по так называемым биткойн-адресам. Владение определенным количеством биткойнов сводится к возможности отправки платежей по сети Биткойн с биткойн-адресов, к которым эти биткойны привязаны. Возможность отправки платежей с биткойн-адресов контролируется с помощью цифровых подписей, которые включают пары открытого и закрытого ключей. В частности, каждый биткойн-адрес индексируется с помощью уникального открытого ID — буквенно-цифрового идентификатора, который, по сути, соответствует открытому ключу. Закрытый ключ контролирует биткойны, хранящиеся по этому адресу. Любой платеж (сообщение), где этот адрес задействован как адрес отправителя, должен быть подписан соответствующим действительным закрытым ключом. Проще говоря, владение биткойнами по указанному биткойн-адресу означает знание закрытого ключа, который соответствует этому адресу.

В любой момент времени каждый биткойн-адрес привязан к биткойн-балансу, который, по сути, является общественной информацией. Каждую существующую или предлагаемую (вновь транслируемую) транзакцию можно проверить на предмет соответствия предшеству-

ющей истории транзакций, т. е. проверить, что суммы по транзакциям действительно имеются в соответствующих биткойн-адресах.

### 2.1.3. Транзакция в цепочке блоков (блокчейне)

Субъекты участвуют в транзакциях в сети Биткойн посредством набора биткойн-адресов, называемых кошельком (набор биткойн-адресов, принадлежащих одному лицу). Каждая запись транзакции включает один или несколько адресов отправки (*входов*) и один или несколько адресов получения (*выходов*), а также сведения о том, сколько каждый из этих адресов отправил и получил. Пример транзакции представлен на рис. 1.



**Рис. 1.** Транзакция в сети Биткойн

В указанном примере Алиса отправляет Бобу транзакцию в размере 8 биткойнов (BTC). У данной транзакции имеется два входа (2 и 7 BTC) и два выхода (8 и 1 BTC), причем выход на 1 BTC является, по существу, сдачей и возвращается на кошелек Алисы. Поскольку у каждой транзакции может быть несколько адресов отправки и получения, часто невозможно привязать конкретный адрес отправки к средствам, отправляемым по конкретному адресу получения. Следствием этого наблюдения является то, что нельзя присвоить серийные номера биткойнам и проследить их пути в сети Биткойн.

Процесс ведения транзакции в сети Биткойн основан на механизмах, которые гарантируют, что:

- (а) проверка каждой транзакции распределяется между несколькими участниками сети;
- (б) запись каждой транзакции дискретизирована по времени, т. е. транзакции линейно упорядочены с последовательными временными отметками;
- (в) участники платежной сети соревнуются и получают вознаграждение за запись транзакции в блок;
- (г) несколько узлов ведут перекрестную проверку каждой записанной транзакции.

### 2.1.4. Инициирование транзакции

Допустим, Алиса хочет отправить Бобу 1 биткойн с использованием сети Биткойн. Для этого у Алисы и Боба должны быть биткойн-адреса. Назовем их ID\_Алиса и ID\_Боб. Затем Алисе нужно выслать и удостоверить (в цифровом виде) подлинность сообщения типа

*«ID\_Алиса отправляет ID\_Боб 1 биткойн».*

После того как Алиса подписывает сообщение транзакции с помощью своего закрытого ключа и транслирует его, любой участник сети Биткойн может проверить, что это именно Алиса отправила сообщение, и сообщение не было подделано. К тому же, как указывалось ранее, цифровые подписи гарантируют, что никто другой не мог подписать это сообщение, т. е. Алиса не может отрицать, что его подписала она.

#### 2.1.5. Проверка транзакции

Перед выполнением транзакции протокол Биткойн должен проверить два аспекта сообщения. Во-первых, именно ли Алиса транслировала сообщение транзакции? Схема цифровой подписи гарантирует, что на самом деле только владелец закрытого ключа для данного адреса мог подписать сообщение. Во-вторых, имеется ли на адресе отправки достаточно средств, чтобы гарантировать завершение транзакции?

Хотя ведение учета и проверка транзакций — основные функции всех электронных платежных систем, эти функции, как правило, осуществляются через частные реестры, поддерживаемые доверенными третьими сторонами. Децентрализованные системы, такие как Биткойн, заменяют сторонних посредников и хранящиеся у них записи общественным реестром, который ведется распределенной информационной системой.

#### 2.1.6. Обновление блокчейна

После первоначальной проверки подписанного сообщения транзакции группы участников сети Биткойн начинают состязаться за возможность записать транзакцию в блокчейн. Сначала в блоке транзакций конкурирующие узлы группируют транзакции, которые транслировались с момента последней записи в блокчейне. Затем блок используется для определения сложной для вычисления задачи. Победителем состязания становится узел, который *первым* решит эту задачу. После определения победителя запись транзакции завершается. Узел-победитель имеет право сделать запись и забрать вознаграждение.

Задача, в решении которой состязаются узлы, опирается на одну из описанных выше криптографических схем — хэш-функции. Сначала блок вновь транслируемых транзакций используется в качестве входных данных в криптографической хэш-функции для получения хэша под названием *дайджест*. Этот дайджест вместе с одноразовым случайным кодом *nonce* (буквенно-цифровой строкой) и хэшем предыдущего блока вводятся в другую хэш-функцию, которая выдает хэш блокчейна нового блока. Задача, которую необходимо решить узлам, включает нахождение такого случайного кода, при котором хэш блокчейна нового блока имеет определенные свойства (в данном случае имеет определенное количество начальных нулей). Первый из соревнующихся узлов, который найдет нужный случайный код, транслирует эту информацию остальным участникам сети, а блокчейн обновляется. В данной схеме реализован Hashcash — система *доказательства правильности работы* (*proof of work*), целью которой является обеспечить, чтобы компьютеры использовали определенное количество вычислительных ресурсов для выполнения какой-либо задачи, см. Bask (2002).

Узлы, которые осуществляют процесс доказательства правильности работы, в сети Биткойн именуется *майнерами*. Эти майнеры стимулируются на использование вычислительных ресурсов в этом процессе путем получения вознаграждения, встроенного в протокол Биткойн. Обычно вознаграждение — это заранее определенное количество вновь создан-

ных биткойнов. Остальная часть вознаграждения, которая в настоящее время гораздо меньше, — это добровольные операционные сборы (комиссии), уплачиваемые инициаторами транзакций майнерам за обработку их транзакций. Первоначальная идея состояла в том, чтобы эти добровольные взносы заменили вознаграждение в виде создания биткойнов для стимулирования майнеров в случаях, когда эта сумма стремится к нулю (Nakamoto, 2008).

## 2.2. Статистика сети Биткойн

### 2.2.1. Капитализация сети

На сегодняшний день в обращении находится более 15 млн биткойнов. Цена одного биткойна за 4 месяца 2016 года колебалась в пределах 400–460 долларов США (см. рис. 2). Таким образом, совокупная стоимость всех выпущенных биткойнов составляет около 7 млрд долларов США.



**Рис. 2.** Динамика стоимости биткойна к доллару США, долл. США за 1 биткойн

Рыночная капитализация биткойна в 10 раз выше, чем у второй по этому показателю криптовалюты — Ethereum. Таким образом, биткойн, очевидно, является безусловным лидером.

Ценность валюты сильно зависит от числа участников, что, в свою очередь, привлекает еще больше участников, приводя в действие сетевой эффект. У биткойна есть существенное преимущество перед другими криптовалютами, которое имеет три аспекта:

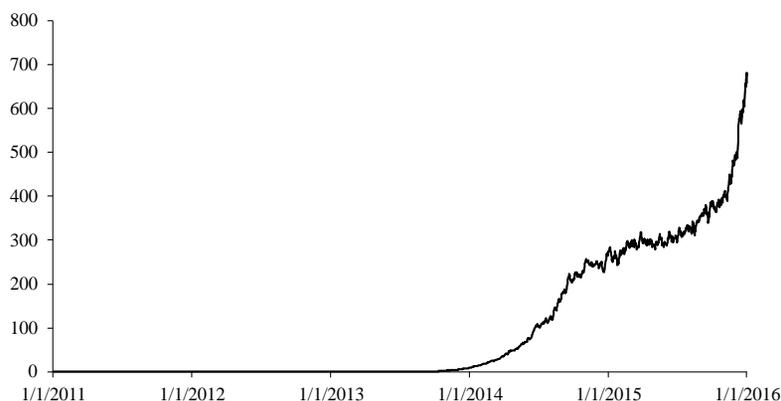
- чем больше пользователей, тем более полезным он становится: появляется больше мест, в которых можно потратить биткойны, и контрагентов, с которыми можно обменять биткойны — это привлекает еще больше пользователей;
- валюты требуют доверия, но оно может быть получено только с течением времени, таким образом, при прочих равных условиях, старейшая валюта получает естественное преимущество перед конкурентами;
- чем больше объем, тем больше комиссии за транзакции, это привлекает больше майнеров и делает сеть более безопасной, что, в свою очередь, снова привлекает дополнительных пользователей и объем средств.

Для валют, служащих средством накопления, есть еще одно препятствие: для перевода накоплений из одной валюты в другую требуются дополнительные усилия. Таким образом, действуют многочисленные эффекты, которые делают смещение биткойна с позиции криптовалюты номер один крайне маловероятным.

### 2.2.2. Мощность сети

Объем вычислительной мощности, поддерживающий сеть, сейчас приближается к 800 петахэшам/с (см. рис. 3)<sup>3</sup>. Оценка совокупной стоимости используемого оборудования превышает 300 млн долларов.

Ежедневная совокупная выручка майнеров от комиссий за запись транзакций и валидацию новых блоков составляет 1.2–1.5 млн долларов США. Число открытых биткойн-



**Рис. 3.** Динамика вычислительной мощности в сети Биткойн с 01.01.2011 по 31.12.2015, петахэш/с



**Рис. 4.** Динамика числа транзакций в сети Биткойн с 01.01.2011 по 31.12.2015, тыс. транзакций/день

<sup>3</sup> Петахэш = 1 млн гигахэшей.

кошельков превышает 15 млн. Ежедневно пользователями сети совершается более 200 тысяч транзакций (см. рис. 4).

Динамика транзакций имеет естественный предел, связанный с размером блока (1Мб или около 1500 транзакций). С учетом среднего времени, требуемого на майнинг нового блока (10 минут), теоретический предел Биткойн сети составляет на сегодня 7 транзакций в секунду или около 600 тыс. транзакций в день. Биткойн-сообщество находится в активном поиске оптимального решения по увеличению размера блока. Среди основных инициатив можно назвать программный протокол SegWit, который позволит в 1.5–2 раза поднять пропускную способность, а также LightningNetwork, предполагающий построение сети хабов ликвидности для проведения микроплатежей в защищенных P2P-каналах с возможностью значительного удешевления стоимости.

### 3. Кто использует биткойн? Эконометрический анализ пользователей биткойна

Биткойн привлек внимание людей по всему миру, и количество статей, посвященных ему, стабильно растет<sup>4</sup>. К сожалению, очень немного исследований посвящено анализу характеристик пользователей Биткойн сети. Такой анализ мог бы обеспечить лучшее понимание этого феномена и его перспектив в будущем. Относительный дефицит академического интереса к данной области не стоит воспринимать как сюрприз, с учетом того, что сбор данных о пользователях биткойна крайне сложен, т. к. они в своем большинстве желают оставаться анонимными. В паре работ авторы попытались преодолеть это препятствие, проведя интервью с десятком пользователей биткойна, см. (Baur et al., 2015; Huhtinen, 2014).

Bohr, Bashir (2014) были первыми, кто проанализировал более крупный структурированный набор данных, полученных на основе опроса, проведенного Lúí Smyth (на тот момент исследователем цифровой антропологии в University College London). Опрос состоит из 1193 ответов, собранных в период с 12 февраля 2013 г. по 4 апреля 2013 г. Bohr и Bashir попытались ответить на три исследовательских вопроса:

- 1) что предсказывает накопление богатства среди пользователей биткойна;
- 2) что предсказывает оптимизм относительно краткосрочной и долгосрочной стоимости биткойна;
- 3) что привлекает людей к биткойну.

Первый вопрос был исследован с помощью простой регрессии заявленного каждым респондентом количества биткойнов в его собственности (логарифмированного по основанию 2 во избежание асимметрии) на набор характеристик пользователей биткойна, извлеченный из опроса:

- возраст пользователя *Age* и возраст, возведенный в квадрат, для учета нелинейности;
- переменная *Installation*, которая отражает период первой загрузки клиента биткойн (программы, которая осуществляет подключение к сети Биткойн), она может принимать значения от 1 (первый квартал 2009 г.) до 17 (первый квартал 2013 г.) и центрирована по среднему значению;

<sup>4</sup> Более подробно см. Böhme et al. (2015) и сайт <https://en.bitcoin.it/wiki/Research>.

- фиктивная переменная *Miner* для учета того, добывал ли пользователь биткойны самостоятельно;
- переменная взаимодействия  $Installation \times Miner$  для проверки наличия преимущества в накоплении биткойнов у ранних майнеров над поздними;
- фиктивная переменная *Bitcoinsins*, которая равна 1, если респондент признал добычу биткойнов через чье-либо оборудование без разрешения владельца (с помощью вредоносных программ) или кражу биткойнов;
- фиктивная переменная *LivesinU.S.*, которая равна 1, если респондент живет в США;
- фиктивная переменная *Illicitgoods*, которая равна 1, если респондент признал покупку с помощью биткойнов наркотиков, услуг по азартным играм или других незаконных товаров;
- фиктивная переменная *Bitcointalk*, которая равна 1, если респондент обозначил, что он использует специализированные для биткойна платформы, чтобы общаться с другими людьми на тему биткойна;
- фиктивная переменная *Investor*, которая равна 1, если респондент описал свою роль в контексте биткойна как инвестора;
- целочисленные переменные *Profit* и *Community*, которые принимают значения от 1 (не мотивирует) до 5 (очень мотивирует) в зависимости от того, считает ли респондент прибыль или сообщество мотивирующими факторами для их изначального присоединения к Биткойну.

Bohr и Bashir (2014) обнаружили, что возраст является статистически значимым фактором для предсказания количества биткойнов, которыми обладал респондент: молодые респонденты обладали меньшим количеством биткойнов, но это количество примерно вдвое увеличивается каждые 10 лет, достигая максимума между 55 и 60 годами, аналогично накоплению других активов. Переменная взаимодействия  $Installation \times Miner$  значима, и это подтверждает, что майнинг биткойнов был проще в более ранние периоды действия сети, таким образом, ранние майнеры получили преимущество в накоплении биткойнов. Активные участники онлайн сообществ, посвященных биткойну, обладали вдвое большим количеством биткойнов по сравнению с теми, кто не участвовал в таких сообществах, в то время как определившие себя как *Investor* накопили вчетверо больше биткойнов по сравнению с теми, кто себя так не определил. При прочих равных условиях, превышение накоплений пользователей биткойна, приобретавших запрещенные товары, такие как наркотики, над накоплениями тех, кто покупал только легальные товары, достигало 45%.

Bohr и Bashir (2014) затем представили 2 дополнительные регрессии, в которых краткосрочные (4 месяца от времени опроса) и долгосрочные (6 лет после опроса) ожидаемые стоимости 1 биткойна в долларах США зависели от описанного выше набора данных. Старшие пользователи оказались менее оптимистичными по сравнению с молодыми, а пик оптимизма пришелся на возраст около 35 лет, в то же время, чем выше был уровень социальной вовлеченности в онлайн форумы, тем выше была предсказанная цена. Интересно, что те, кто позже установил биткойн, были более оптимистичны относительно краткосрочной стоимости, а майнеры были более пессимистичны относительно долгосрочной стоимости по сравнению с теми, кто не занимается майнингом биткойнов.

На втором этапе исследования Bohr и Bashir (2014) разделили пользователей на основе их (пользователей) описания биткойна относительно анонимности, свободы и банковской системы, и проанализировали эти три группы с помощью логистической регрессии. Они обнаружили, что политическая идентичность пользователей не являлась фактором, пред-

сказывающим ценность анонимности биткойна. Единственным значимым фактором, определяющим предпочтение биткойна за его анонимность, было осуществление пользователем добычи биткойнов, т. е. являлся пользователь майнером или нет. Пользователи, которые предпочитали биткойн за его потенциал подорвать банковскую систему, оказались старше 40, живущими за пределами США и политически определяющими себя как «зеленые». Наконец, пользователи, которым биткойн нравится за его качества, характеризующие свободу этой сети, политически определяли себя как «либертарианцы», жили за пределами США и были в возрасте от 30 до 39 лет. Интересно, что сами авторы хорошо осведомлены об ограничениях имевшегося набора данных и просят читателя воспринимать их результаты с осторожностью: выборка может не быть репрезентативной с точки зрения всей совокупности пользователей биткойна и принимает во внимание только англоговорящее биткойн-сообщество. Кроме того, опрос является довольно-таки устаревшим, т. к. он проводился до краха биржи Mt. Gox, которая потеряла сотни тысяч биткойнов и сейчас является банкротом. Несмотря на эти ограничения, это исследование, определенно, является перспективным направлением для будущих исследований.

Yelowitz и Wilson (2015) попытались решить проблему маленького набора данных путем использования данных Google Trends для исследования детерминант интереса к биткойну. Google Trends может быть использован для извлечения данных либо по точным условиям поиска, либо по общим темам, в последнем случае учитываются также связанные поисковые запросы. Исследователи построили прокси для четырех возможных классов пользователей биткойна (программисты-энтузиасты, спекулятивные инвесторы, либертарианцы и преступники) и для интереса к биткойну в каждом штате США. В категории «Валюта» они искали данные по общим темам, относящимся к биткойну; в категории «Дисциплина» — запросы на тему «Информатика»; а для оставшихся классов пользователей (преступники, либертарианцы и спекулятивные инвесторы) использовали точные условия поиска «SilkRoad», «Свободный рынок» и «Заработать деньги» соответственно. Отметим, что данные Google Trends представляют, как много веб-поисков было осуществлено по конкретному ключевому слову/словам в заданную неделю и в заданной географической области по отношению к общему числу веб-поисков за ту же неделю и в той же области. Полученный показатель затем масштабируется Google в пределах от 0 до 100 путем его деления на свое максимальное значение и умножения результата на 100. Для каждого штата США Yelowitz и Wilson (2015) изначально вычислили временной ряд с 31 наблюдением (от января 2011 г. до июля 2013 г.) относительной популярности биткойна для каждой группы клиентов. Затем они использовали Google Trends, чтобы измерить относительный уровень популярности в штате для каждого поискового условия для всего периода и масштабировали каждый ряд для штата относительно самого популярного штата. Этот тип анализа имеет два ограничения: Google дополняет выборку в своей базе данных каждый раз, когда выполняется запрос, поэтому точное копирование невозможно, хотя качественные результаты не изменяются (см. также раздел 4.4 в (Fantazzini, Toktamysova, 2015) для обсуждения данной проблемы); Google Trends подставляет значение 0, если число поисков слишком мало<sup>5</sup>. Из 1488 (48 штатов × 31 месяц) потенциальных наблюдений Yelowitz и Wilson (2015) использовали 794 с ненулевыми значениями. Вслед за Stephens-Davidowitz (2014) они нормализовали каждый уровень поиска к его z-баллу и оценили следующую панельную регрессию:

<sup>5</sup> [https://support.google.com/trends/answer/4355213?hl=en&ref\\_topic=4365599](https://support.google.com/trends/answer/4355213?hl=en&ref_topic=4365599).

$$BITCOIN_{jt} = \beta_0 + \beta_1 X_{jt} + \delta_j + \delta_t + \varepsilon_{jt},$$

где  $BITCOIN_{jt}$  — интерес к биткойну в штате  $j$  в месяц  $t$ ,  $X_{jt}$  — интерес клиентуры, а  $\delta_j$  и  $\delta_t$  — фиксированные эффекты штата и времени. Каждый штато-месяц взвешен по населению штата (в июле 2011 года), а стандартные ошибки скорректированы на невложенную двунаправленную кластеризацию по уровням штата и времени, см. (Cameron et al., 2011) для подробностей. Yelowitz и Wilson (2015) применили большой набор спецификаций, постепенно включая дополнительные регулирующие переменные для штата и времени, такие как уровень безработицы и несвязанные «плацебо-переменные», условия взаимодействия исходных переменных с ценами биткойна. Более того, некоторые спецификации были оценены с использованием данных от 2012 года и позже (когда биткойн был более популярен) или для 24 штатов США, для которых было как минимум 20 месячных наблюдений. Во всех случаях они обнаружили положительные связи между интересом к биткойну и двумя группами клиентов — программистами-энтузиастами и теми, кто, возможно, вовлечен в нелегальную деятельность — в то время как никакой значимой связи с теми, кто интересуется либертарианской идеологией или руководствуется инвестиционными мотивами, обнаружено не было.

Хотя работа Yelowitz и Wilson (2015) решила некоторые проблемы анализа в (Bohr, Bashir, 2014), но она относится только к американскому сообществу биткойна, а данные собраны до банкротства биржи Mt. Gox. Тем не менее, в ней предложены некоторые идеи по использованию данных Google Trends, которые впоследствии (в разделе 5) будут включены в более сложные модели, предложенные для моделирования динамики цены биткойна.

#### 4. Сколько стоит биткойн? Обзор финансовых и экономических подходов

Стоимость биткойна была крайне подвержена волатильности в течение последних нескольких лет, в связи с чем был поднят вопрос, не является ли он пузырьем. Одним из способов ответа на этот вопрос является проведение тестов на определение финансовых пузырей, которые будут рассмотрены в разделе 6. Другой вариант — попробовать оценить внутреннюю (фундаментальную) стоимость валюты. В этом направлении к настоящему времени были предложены два подхода, базирующиеся на определении емкости рынка и предельных издержек производства, зависящих от потребления электроэнергии.

##### 4.1. Верхняя граница: оценка емкости рынка

Метод, основанный на оценке емкости рынка, широко используется компаниями, намеревающимися запустить новый продукт или услугу. Данный подход может быть использован и для получения ориентира оценки справедливой стоимости биткойна.

Woo et al. (2013) в отчете Банка Америки Мерилл Линч оценили отдельно стоимость биткойна как средства обмена и как средства накопления и затем просуммировали их, чтобы получить грубую оценку справедливой стоимости биткойна. Для того чтобы вычислить стоимость биткойна как средства обмена, они рассмотрели два варианта его использования: *электронную коммерцию* и денежные переводы. В первом варианте авторы оценили скорость

обращения денег в экономике США, поделив расходы на личное потребление ( $C_{US}$ ) на размер наличных денежных средств и чековых депозитов домашних хозяйств ( $HD_{US}$ ). Полученная скорость обращения денег, усредненная за последние 10 лет, умножалась далее на совокупный объем продаж в розничной электронной торговле за предыдущий год в предположении, что для онлайн-продаж и расходов домашних хозяйств США скорость обращения в целом одинакова. Woo et al. (2013) предположили, что биткойн станет средством платежа в 10% всех онлайн-покупок ( $Bitcoin_{share}$ ), что дает оценку необходимого объема биткойнов в обращении на сумму 1 млрд долларов США. Наконец, с учетом того, что ВВП США составляет около 20% мирового ВВП, была получена оценка совокупной стоимости биткойнов в 5 млрд долларов, необходимых для онлайн-покупок. Полученная в результате формула имеет вид:

$$V_{e-commerce_t} = \frac{1}{10} \left( \sum_{i=1}^{10} \frac{C_{US_{t-i}}}{HD_{US_{t-i}}} \right) \cdot B2C_{t-1} \cdot Bitcoin_{share} \cdot \frac{GDP_{world_{t-1}}}{GDP_{US_{t-1}}}$$

Woo et al. (2013) подчеркнули, что, помимо роли биткойна как средства платежа в онлайн-покупках, возможно его использование для *денежных переводов*. Они рассмотрели трех основных игроков в индустрии денежных переводов: Western Union, MoneyGram и Euronet, обладающих примерно 20% рынка, и предположили, что биткойн мог бы стать одним из трех крупнейших игроков в этой индустрии. Затем, в предположении, что капитализация биткойна является эквивалентом стоимости компании, они добавили среднюю рыночную капитализацию Western Union, MoneyGram и Euronet (приблизительно 4.5 млрд долларов) к максимальной рыночной капитализации биткойнов как средства обмена:

$$V_{money\ transfer_t} = \frac{1}{3} (MK_{WU_t} + MK_{MG_t} + MK_{E_t})$$

Woo et al. (2013) предположили, что активами, наиболее близкими к биткойну как к средству накопления, являются, по всей видимости, драгоценные металлы и наличные денежные средства. В частности, у биткойна и золота есть три общих характеристики: 1) они не подразумевают уплаты процента, 2) предложение обоих ограничено, и 3) их сложнее отслеживать, чем большинство финансовых активов (кроме наличных денег). Принимая во внимание то, что общая стоимость выпущенных золотых слитков/монет/ETF в 2013 году составляла приблизительно 1.3 трлн долларов, и что биткойн по сравнению с золотом гораздо более волатилен, Woo et al. (2013) предположили, что рыночная капитализация биткойна не может превзойти 300 млрд долларов. Более того, допуская, что биткойн со временем может приобрести репутацию серебра, и цена золота в 2013 году была примерно в 60 раз выше цены на серебро, они предположили, что рыночная капитализация биткойна как средства накопления могла бы достичь 5 млрд долларов. Примечательно, что они обратили внимание на то, что эта величина близка к стоимости всех отчеканенных с 1986 г. серебряных орлов США (около 8 млрд долларов — 12 тысяч тонн). Следовательно, простой грубый способ получить рыночную капитализацию биткойна как средства накопления:

$$V_{store\ of\ value_t} = 0.6 \cdot TSM_t \cdot P_{silver,t}$$

где  $TSM_t$  — общий объем отчеканенных с 1986 г. до момента  $t$  серебряных орлов США, а  $P_{silver,t}$  — цена 1 тройской унции серебра в момент времени  $t$ .

Наконец, Woo et al. (2013) рассчитали потенциальную справедливую стоимость биткойна как сумму максимальной рыночной капитализации биткойна как средства обмена и накопления, деленную на общее число биткойнов в обращении ( $TB_t$ ), таким образом, получая максимальную справедливую стоимость биткойна приблизительно равной 1300 долларам:

$$P_{\text{bitcoin}_t} = \frac{V_{e\text{-commerce}_t} + V_{\text{money transfer}_t} + V_{\text{store of value}_t}}{TB_t}.$$

Другой подход к определению размера рынка применили Bergstra, de Leeuw (2013), которые, следуя идее, предложенной Yermack (2013), сравнили биткойн с высокотехнологичным стартапом, который либо будет доминировать на рынке, либо провалится. Они предположили, что если биткойн будет успешным и просуществует до 2040 года, то он будет представлять половину всех денег в мире. С учетом технической новизны системы биткойна они присвоили данному событию очень низкую вероятность ( $p$ ): один шанс из 100 000. Предполагая, что общая денежная масса ( $MM$ ) в 2040 году будет  $10^{14}$  евро (всего лишь предположение!), они оценивают биткойн в 50 евро:

$$P_{\text{bitcoin}_t} = \frac{MM_{2040}}{TB_{2040}} \cdot p_t = \frac{10^{14}}{2 \cdot 10^7} \cdot 10^{-5} = 50 \text{ euro}.$$

Аналогичный подход также исследуется Huhtinen (2014), рассмотревшим текущие денежные агрегаты M2 для доллара США, евро и японской иены и альтернативные сценарии, касающиеся доли денежного предложения, которое могло бы быть замещено биткойном. Он утверждает, что наиболее реалистичным уровнем замещения для трех мировых валют является уровень 0.1%, который мог бы быть достигнут при оценке стоимости биткойна в 1573 евро.

#### 4.2. Нижняя граница: предельная стоимость производства биткойна

Оценка размера рынка может дать представление о потенциале биткойна в долгосрочном периоде, но данный подход определенно неудовлетворителен для объяснения краткосрочной динамики цены биткойна. В связи с этим Garcia et al. (2014) первыми предположили, что фундаментальная стоимость биткойна должна быть как минимум равна стоимости энергии, затраченной на его производство путем майнинга (добычи), и что эта стоимость должна использоваться в качестве нижней границы оценки фундаментальной стоимости биткойна. А именно, они разделили накопленную вычислительную мощность добычи в день на число добытых биткойнов, чтобы получить число хэшей (по алгоритму SHA-256), необходимых для майнинга одного биткойна. Затем они использовали приближение энергетических потребностей для добычи в размере 500 ватт за гигахэш/секунду (гх/с, GH/s) — это была средняя эффективность большинства графических процессоров, использованных для майнинга биткойнов в 2010–2013 годах<sup>6</sup>, и примерные издержки на электричество в размере 0.15 долларов за квт·час, что являлось средним значением американских и британских цен.

<sup>6</sup> На конец 2015 года потребности гораздо ниже.

Позднее в работах Hayes (2015, 2016) была разработана более изящная модель стоимости производства биткойна, которая детально обсуждается ниже. Hayes обращает внимание на то, что рациональные агенты не стали бы заниматься майнингом биткойнов, если из-за этого они бы понесли реальные убытки, и переменными, влияющими на решение о майнинге, по-существу, являются 5 показателей:

- 1) стоимость электричества в центах за киловатт·час;
- 2) потребление энергии на добывающую единицу в ваттах на гигахэш/секунду (1 Вт/гигахэш/сек = 1 джоуль/гигахэш), которое является функцией стоимости электричества и энергетической эффективности;
- 3) рыночная цена биткойна;
- 4) сложность алгоритма биткойна;
- 5) награда за блок (на текущий момент — 25 биткойнов), которая уменьшается вдвое примерно каждые 4 года.

На конкурентном товарном рынке агент предпринял бы майнинг, если предельные издержки в день (потребление электричества) были бы меньше или равны предельному продукту (среднее количество добытых в день биткойнов, умноженное на цену биткойна в долларах). Hayes (2015, 2016) утверждает, что спекулятивные свойства биткойна, а также свойства, уподобляющие его деньгам (т. е. как средства обмена и накопления) могут, несомненно, добавлять порцию субъективности в любые объективные попытки оценить внутреннюю стоимость биткойна. Как бы то ни было, предельная стоимость производства, определенная потреблением энергии, может служить нижней границей величины, вблизи которой майнеры будут принимать решение о производстве.

Hayes (2015, 2016) развивает свою модель, предполагая, что дневное производство майнером биткойнов зависит от его собственного уровня доходности, измеренного в ожидаемых биткойнах в день на единицу добывающих мощностей.

Ожидаемое количество биткойнов, которые будут добыты за день, может быть рассчитано следующим образом:

$$\text{BTC/day}^* = [(\beta \cdot \rho) / (\delta \cdot 2^{32})] \cdot \text{sec}_{\text{hr}} \cdot \text{hr}_{\text{day}}, \quad (1)$$

где  $\beta$  — награда за блок (на текущий момент — 25 биткойнов/блок),  $\rho$  — мощность хеширования, используемая майнером,  $\delta$  — сложность (которая выражается в единицах гигахэшей/блок). Константа  $\text{sec}_{\text{hr}}$  — количество секунд в часе (3600),  $\text{hr}_{\text{day}}$  — количество часов в дне (24). Константа  $2^{32}$  относится к нормализованной вероятности решения блока отдельно взятым хэшем в секунду и определяется сложностью задачи 256-битного шифрования в ядре алгоритма SHA-256, которую майнеры пытаются решить. Эти константы, нормализующие пространство для дневной периодичности и алгоритма добычи, могут быть записаны в виде одной переменной  $\theta = \text{sec}_{\text{hr}} \cdot \text{hr}_{\text{day}} / 2^{32} = 0.0000201165676116943$ . Уравнение (1), таким образом, может быть переписано в более компактном виде:

$$\text{BTC/day}^* = \theta \cdot (\beta \cdot \rho) / \delta. \quad (2)$$

Hayes (2015, 2016) устанавливает  $\rho=1000$  гх/с, несмотря на то что реальная мощность хеширования майнера, скорее всего, значительно отклоняется от этой величины. Как бы то ни было, Hayes (2015, 2016) утверждает, что этот уровень обычно является хорошим эта-

лоном измерения при текущих обстоятельствах. Стоимость майнинга в день  $E_{\text{day}}$  может быть выражена следующим образом:

$$E_{\text{day}} = (\text{price\_per\_kWh}) \cdot 24 \cdot (W_{\text{per\_GH/s}}) \cdot (\rho / 1000 \text{ GH/s}). \quad (3)$$

В предположении, что рынок биткойнов конкурентен, предельный продукт майнинга должен быть равным предельным издержкам, так чтобы равновесная цена (долларов/биткойн) задавалась коэффициентом «издержки в день / биткойнов в день»:

$$p^* = E_{\text{day}} / (\text{BTC/day}^*). \quad (4)$$

Эта цена может, однако, быть нижней границей для цены, ниже которой майнер будет работать с убытками и, вероятно, прекратит производство. Наоборот, имея рыночную цену биткойна, можно инвертировать уравнение (4), чтобы найти нижние границы (точки безубыточности, как определено Hayes (2015, 2016)) для других переменных, определяющих прибыльность биткойна. Например, при наличии наблюдаемой рыночной цены ( $p$ ) и сложности майнинга, точка безубыточности для издержек на электричество (в квт·часах) определяется формулой:

$$\text{price\_per\_kWh}^* = [p(\text{BTC/day}^*)/24] / W_{\text{per\_GH/s}}. \quad (5)$$

Аналогично, имея известную стоимость производства и наблюдаемую рыночную цену, можно решить уравнение для точки безубыточности для сложности майнинга:

$$\delta^* = (\beta \cdot \rho \cdot \text{sec}_{\text{hr}} \cdot \text{hr}_{\text{day}}) / [(E_{\text{day}}/p) \cdot 2^{32}]. \quad (6)$$

Наконец, имея рыночную цену, издержки на электричество (в квт·часах) и сложность добычи, можно найти точку безубыточности для энергетической эффективности:

$$W_{\text{per\_GH/s}}^* = p(\text{BTC/day}^*) / (\text{price\_per\_kWh} \cdot 24). \quad (7)$$

Уравнение (4) показывает, что если практическая эффективность майнинга увеличится (что и ожидается многими ввиду более эффективного оборудования), то безубыточная цена для производителей биткойна будет иметь тенденцию к снижению. Например, Garcia et al. (2014) обнаружили, что средняя эффективность майнинга за период с 2010 по 2013 г. составила приблизительно 500 ватт на гх/с. В то же время, используя уравнение (7) или взглянув на лучшее доступное оборудование для майнинга<sup>7</sup>, можно увидеть, что на текущий момент средняя эффективность окажется близкой к 0.50–0.90 ватт на гх/с. Более того, уравнения (2) и (4) показывают, что меньшая награда за блок  $\beta$ , при неизменных остальных параметрах, повысит цену биткойна. С учетом того, что в 2016 г. ожидается снижение награды за блок вдвое, т. е. до 12.5 биткойнов, если цена биткойна не вырастет, это будет свидетельствовать о том, что энергетическая эффективность майнинга должна будет компенсировать сниженную награду за блок.

<sup>7</sup> [https://en.bitcoin.it/wiki/Mining\\_hardware\\_comparison](https://en.bitcoin.it/wiki/Mining_hardware_comparison).

Приведем небольшой числовой пример. Предположим, что средняя мировая стоимость электричества составляет приблизительно 13.5 центов за киловатт·час (как в (Hayes, 2016)) и средняя энергетическая эффективность оборудования для майнинга составляет 0.75 дж/гх. Тогда, следуя формуле (3), средние издержки в день на оборудование мощностью 1000 гх/с составили бы примерно  $(0.135 \cdot 24 \cdot 0.75) \cdot (1000 / 1000) = 2.43$  доллара в день. Количество биткойнов, которое оборудование с мощностью 1000 ГХ/с может добыть в день, с текущей сложностью 60 883 825 480 равно 0.0082602265269544 биткойна в день. Учитывая, что предельные издержки теоретически должны быть равны предельному продукту, получим цену биткойна из уравнения (4):

$$(2.43 \text{ доллара в день}) / (0.0082602265269544 \text{ биткойна в день}) \approx \$294.18/\text{BTC},$$

что незначительно отличается от рыночного курса в 290–300 долларов/биткойн на момент написания настоящей статьи (декабрь 2015 года).

Интересно, что при прочих равных условиях при уменьшении награды за блок вдвое до 12.5 биткойнов<sup>8</sup>, справедливая цена биткойна должна быть в районе \$588.36/BTC. Увидим ли мы дальнейший рост цены в ближайшее время?

### Список литературы

- Ali R., Barrdear J., Clews R., Southgate J. (2014). The economics of digital currencies. *Bank of England Quarterly Bulletin*, Q3, 276–287.
- Allen H. J. (2016). \$=€=Bitcoin? *Suffolk University Legal Studies Research Paper Series, Research Paper*, No. 15–33.
- Back A. (2002). Hashcash — a denial of service counter-measure. <http://www.hashcash.org/papers/hashcash.pdf>.
- Badev A., Chen M. (2014). Bitcoin: Technical background and data analysis. *Finance and Economics Discussion Series 2014–104*. Divisions of Research and Statistics and Monetary Affairs, Federal Reserve Board, Washington, D.C.
- Baur A. W., Bühler J., Bick M., Bonorden C. S. (2015). Cryptocurrencies as a disruption? Empirical findings on user adoption and future potential of Bitcoin and Co. In: *Open and Big Data Management and Innovation*, 63–80. Springer International Publishing.
- Becker J., Breuker D., Heide T., Holler J., Rauer H. P., Böhme R. (2013). Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. In: *The Economics of Information Security and Privacy*, 135–156. Springer.
- Bergstra J. A., de Leeuw K. (2013). Bitcoin and beyond: Exclusively informational monies. *arXiv preprint*, arXiv: 1304.4758.
- Böhme R., Christin N., Edelman B., Moore T. (2015). Bitcoin: Economics, technology, and governance. *The Journal of Economic Perspectives*, 29 (2), 213–238.
- Bohr J., Bashir M. (2014). Who uses bitcoin? An exploration of the bitcoin community. In: *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference*, 94–101.
- Cameron A. C., Gelbach J. B., Miller D. L. (2011). Robust inference with multiway clustering. *Journal of Business and Economic Statistics*, 29 (2), 238–249.

<sup>8</sup> Ожидаемая дата изменения награды за блок — 23.07.2016, см. <http://www.bitcoinblockhalf.com/>.

Dang Q. (2012). Recommendation for applications using approved hash algorithms. *Technical Report*, National Institute of Standards and Technology.

Dwyer G. P. (2015). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, 17, 81–91.

ECB. (2012). Virtual currency schemes. *ECB report*, October 2012. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>.

ECB. (2015). Virtual currency schemes — a further analysis. *ECB report*, February 2015. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>.

Fantazzini D., Toktamysova Z. (2015). Forecasting German car sales using Google data and multivariate models. *International Journal of Production Economics*, 170, 97–135.

Garcia D., Tessone C. J., Mavrodiev P., Perony N. (2014). The digital traces of bubbles: Feedback cycles between socio-economic signals in the Bitcoin economy. *Journal of the Royal Society Interface*, 11 (99), 20140623.

Hayes A. (2015). A cost of production model for bitcoin. *Working Paper 05/2015*. Department of Economics, The New School for Social Research.

Hayes A. (2016). Cryptocurrency value formation: An empirical analysis leading to a cost of production model for valuing bitcoin. *Telematics and Informatics*, dx.doi.org/10.1016/j.tele.2016.05.005.

Huhtinen T. P. (2014). Bitcoin as a monetary system: Examining attention and attendance. Master's thesis. Department of Finance, Aalto University School of Business. [http://epub.lib.aalto.fi/fi/ethesis/pdf/13626/hse\\_ethesis\\_13626.pdf](http://epub.lib.aalto.fi/fi/ethesis/pdf/13626/hse_ethesis_13626.pdf).

Kroll J. A., Davey I. C., Felten E. W. (2013). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In: *Proceedings of WEIS 2013*.

Lo S., Wang J. C. (2014). Bitcoin as money? *Current Policy Perspectives*, 14–4, Federal Reserve Bank of Boston.

Murphy E. V., Murphy M. M., Seitzinger M. V. (2015). *Bitcoin: questions, answers, and analysis of legal issues*. US Congressional Research Service 7–5700, R43339. <https://www.fas.org/sgp/crs/misc/R43339.pdf>.

Nakamoto S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>.

Rogojanu A., Badea L. (2014). The issue of competing currencies. Case study — Bitcoin. *Theoretical and Applied Economics*, 21 (1), 103–114.

Segendorf B. (2014). What is Bitcoin. *Sveriges Riksbank Economic Review*, 2, 71–87.

Stephens-Davidowitz S. (2014). The cost of racial animus on a black candidate: Evidence using Google search data. *Journal of Public Economics*, 118, 26–40.

Velde F. (2013). *Bitcoin: A primer*. Chicago Fed Letter, 317, December.

Woo D., Gordon I., Iaralov V. (2013). Bitcoin: A first assessment. *FX and Rates*, December 2013, Bank of America Merrill Lynch.

Yelowitz A., Wilson, M. (2015). Characteristics of bitcoin users: An analysis of Google search data. *Applied Economics Letters*, 22 (13), 1030–1036.

Yermack D. (2013). Is bitcoin a real currency? An economic appraisal. *National Bureau of Economic Research working paper* No 19747.

Поступила в редакцию 01.06.2016;  
принята в печать 25.09.2016.

---

Fantazzini D., Nigmatullin E., Sukhanovskaya V., Ivliev S. *Applied Econometrics*, 2016, v. 44, pp. 5–24.

---

**Dean Fantazzini**

Moscow School of Economics, Moscow State University, Russian Federation;  
fantazzini@mse-msu.ru

**Erik Nigmatullin**

Bocconi University, Milan, Italy; nigmatullin.erik@gmail.com

**Vera Sukhanovskaya**

Perm State National Research University, Russian Federation;  
vera-sukhanovskaya@yandex.ru

**Sergey Ivliev**

Perm State National Research University, Russian Federation;  
ivliev@gmail.com

**Everything you always wanted to know about bitcoin modelling but were afraid to ask. Part I**

Bitcoin is an open source decentralized digital currency and a payment system. It has raised a lot of attention and interest worldwide and an increasing number of articles are devoted to its operation, economics and financial viability. This article reviews the econometric and mathematical tools which have been proposed so far to model the bitcoin price and several related issues, highlighting advantages and limits. We discuss the methods employed to determine the main characteristics of bitcoin users, the models proposed to assess the bitcoin fundamental value, the econometric approaches suggested to model bitcoin price dynamics, the tests used for detecting the existence of financial bubbles in bitcoin prices and the methodologies suggested to study the price discovery at bitcoin exchanges.

**Keywords:** crypto-currencies; hash rate; investors' attractiveness; social interactions; money supply; money demand; speculation; forecasting; algorithmic trading; bubble; price discovery.

**JEL classification:** C22; C32; C51; C53; E41; E42; E47; E51; G17.

**References**

Ali R., Barrdear J., Clews R., Southgate J. (2014). The economics of digital currencies. *Bank of England Quarterly Bulletin*, Q3, 276–287.

Allen H. J. (2016). \$=€=Bitcoin? *Suffolk University Legal Studies Research Paper Series, Research Paper*, No. 15–33.

Back A. (2002). Hashcash — a denial of service counter-measure. <http://www.hashcash.org/papers/hashcash.pdf>.

Badev A., Chen M. (2014). Bitcoin: Technical background and data analysis. *Finance and Economics Discussion Series 2014–104*. Divisions of Research and Statistics and Monetary Affairs, Federal Reserve Board, Washington, D.C.

Baur A. W., Bühler J., Bick M., Bonorden C. S. (2015). Cryptocurrencies as a disruption? Empirical findings on user adoption and future potential of Bitcoin and Co. In: *Open and Big Data Management and Innovation*, 63–80. Springer International Publishing.

Becker J., Breuker D., Heide T., Holler J., Rauer H. P., Böhme R. (2013). Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. In: *The Economics of Information Security and Privacy*, 135–156. Springer.

Bergstra J. A., de Leeuw K. (2013). Bitcoin and beyond: Exclusively informational monies. *arXiv preprint*, arXiv: 1304.4758.

Böhme R., Christin N., Edelman B., Moore T. (2015). Bitcoin: Economics, technology, and governance. *The Journal of Economic Perspectives*, 29 (2), 213–238.

Bohr J., Bashir M. (2014). Who uses bitcoin? An exploration of the bitcoin community. In: *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference*, 94–101.

Cameron A. C., Gelbach J. B., Miller D. L. (2011). Robust inference with multiway clustering. *Journal of Business and Economic Statistics*, 29 (2), 238–249.

Dang Q. (2012). Recommendation for applications using approved hash algorithms. *Technical Report*, National Institute of Standards and Technology.

Dwyer G. P. (2015). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, 17, 81–91.

ECB. (2012). Virtual currency schemes. *ECB report*, October 2012. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>.

ECB. (2015). Virtual currency schemes — a further analysis. *ECB report*, February 2015. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>.

Fantazzini D., Toktamysova Z. (2015). Forecasting German car sales using Google data and multivariate models. *International Journal of Production Economics*, 170, 97–135.

Garcia D., Tessone C. J., Mavrodiev P., Perony N. (2014). The digital traces of bubbles: Feedback cycles between socio-economic signals in the Bitcoin economy. *Journal of the Royal Society Interface*, 11 (99), 20140623.

Hayes A. (2015). A cost of production model for bitcoin. *Working Paper 05/2015*. Department of Economics, The New School for Social Research.

Hayes A. (2016). Cryptocurrency value formation: An empirical analysis leading to a cost of production model for valuing bitcoin. *Telematics and Informatics*, [dx.doi.org/10.1016/j.tele.2016.05.005](https://doi.org/10.1016/j.tele.2016.05.005).

Huhtinen T. P. (2014). Bitcoin as a monetary system: Examining attention and attendance. Master's thesis. Department of Finance, Aalto University School of Business. [http://epub.lib.aalto.fi/thesis/pdf/13626/hse\\_thesis\\_13626.pdf](http://epub.lib.aalto.fi/thesis/pdf/13626/hse_thesis_13626.pdf).

Kroll J. A., Davey I. C., Felten E. W. (2013). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In: *Proceedings of WEIS 2013*.

Lo S., Wang J. C. (2014). Bitcoin as money? *Current Policy Perspectives*, 14–4, Federal Reserve Bank of Boston.

Murphy E. V., Murphy M. M., Seitzinger M. V. (2015). *Bitcoin: questions, answers, and analysis of legal issues*. US Congressional Research Service 7–5700, R43339. <https://www.fas.org/sgp/crs/misc/R43339.pdf>.

Nakamoto S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>.

Rogojanu A., Badea L. (2014). The issue of competing currencies. Case study — Bitcoin. *Theoretical and Applied Economics*, 21 (1), 103–114.

Segendorf B. (2014). What is Bitcoin. *Sveriges Riksbank Economic Review*, 2, 71–87.

Stephens-Davidowitz S. (2014). The cost of racial animus on a black candidate: Evidence using Google search data. *Journal of Public Economics*, 118, 26–40.

Velde F. (2013). *Bitcoin: A primer*. Chicago Fed Letter, 317, December.

Woo D., Gordon I., Iaralov V. (2013). Bitcoin: A first assessment. *FX and Rates*, December 2013, Bank of America Merrill Lynch.

Yelowitz A., Wilson, M. (2015). Characteristics of bitcoin users: An analysis of Google search data. *Applied Economics Letters*, 22 (13), 1030–1036.

Yermack D. (2013). Is bitcoin a real currency? An economic appraisal. *National Bureau of Economic Research working paper* No 19747.

*Received 01.06.2016; accepted 25.09.2016.*