Международные процессы, Том 17, № 1 (56), сс. 22–37
DOI 10.17994/IT.2019.17.1.56.2

ЭКОСИСТЕМА ФИНТЕХА
*КРУПНЕЙШИЕ ЧАСТНЫЕ КРИПТОСИСТЕМЫ**

СТАНИСЛАВ ЖУКОВ
ИВАН КОПЫТИН
АЛЕКСАНДР МАСЛЕННИКОВ
Национальный исследовательский институт мировой экономики и международных отношений имени Е. М. Примакова РАН, Москва, Россия

Резюме

Кризис традиционной финансовой системы и волна технологических новаций способствовали опережающему становлению глобального криптокомплекса. Этот комплекс развивается быстрыми темпами, на конец июля 2018 г. в мире действовало около 1700 криптопроектов. Криптокомплекс включает в себя отдельные криптосистемы, которые связаны в единую сеть через торговлю криптовалютами. В статье раскрываются экономическая природа и бизнес-модели трёх самых крупных и наиболее известных криптосистем – *Bitcoin, Ethereum* и *Ripple*, на которые приходится около 70% совокупной капитализации глобального криптокомплекса. Если *Bitcoin* и *Ethereum* пытаются выстроить альтернативу традиционной финансовой системе, то *Ripple* предлагает новые высокотехнологичные и эффективные решения для сложившихся банковской и платёжных систем. Авторы показывают, что самая крупная глобальная частная криптосистема *Bitcoin*, цель которой заключается в замене фиатных денег одноимённой криптовалютой, в действительности очень далека от идеальной системы распределённых денег, автоматически поддерживающей сделки между равными партнёрами через нейтральный компьютерный код. *Bitcoin*, как и другим системам криптовалют, присуща своя иерархия, в ней ярко проявляются монопольные эффекты. Де-факто контроль над работой *Bitcoin* осуществляется крупными игроками, заменившими собой центральный банк. Эти игроки являются основными бенефициарами от периодического роста капитализации криптовалют. Стратегическая задача превращения bitcoin в альтернативу фиатным деньгам в качестве массово используемого платёжного средства потерпела неудачу. Из-за повышенной ценовой волатильности bitcoin не смог составить достойную альтернативу фиатным деньгам и традиционным активам в качестве средства сбережения для массового инвестора. Бизнес-модели *Ethereum* и *Ripple* слабо связаны с динамикой развития криптовалют, обслуживающих эти системы. Бизнес-модель *Ethereum* заключается в максимизации доходов, рент и любых выгод от экстенсивного развития системы для её создателей. *Ripple* делает экономическую ставку на продажу своих специальных программных решений традиционным игрокам финансового рынка. Авторы делают вывод, что криптовалюты эффективно обслуживают интересы двух клиентел. *Во-первых*, пионеров цифровизации финансового сектора в лице программистов, инженеров-компьютерщиков, специалистов по криптографии и теории игр и действующих параллельно с ними венчурных инвесторов. *Во-вторых*, экономических агентов, занимающихся различного рода нелегальной и криминальной деятельностью. Авторы дают прогноз, что с учётом

* Статья подготовлена в рамках НИР «Формирование полицентричного миропорядка: риски и возможности для России» программы Российской академии наук КП19-268 «Большие вызовы и научные основы прогнозирования и стратегического планирования».

Дата поступления рукописи в редакцию: 03.09.2018
Дата принятия к публикации: 11.03.2019

Для связи с авторами / Corresponding author:
Email: zhukov@imemo.ru

политики регуляторов финансовых рынков с псевдоанонимностью трансакций в секторе криптовалют уже в ближайшем будущем будет покончено.

Ключевые слова:
криптосистема; криптовалюта; Bitcoin; Ethereum; Ripple; bitcoin; ether; XRP; блокчейн.

Авторы анализируют новое для мировой экономики и финансов явление – становление современного глобального криптокомплекса на примере трёх самых крупных по капитализации, а потому и наиболее известных криптосистем – *Bitcoin*, *Ethereum* и *Ripple*. Исходный тезис авторов состоит в том, что криптокомплекс не сводится к обслуживающим его криптовалютам. Каждая из криптосистем посредством особой стратегии и специфической бизнес-модели пытается решать конкретную функциональную задачу. Проведённое авторами исследование свидетельствует о появлении на этапах стартапа и организации венчурного бизнеса новых тенденций, возможно тупиковых и преходящих.

1

В основе бурной динамики глобального комплекса криптосистем и криптовалют лежат три взаимосвязанные причины. *Во-первых*, мировой финансово-экономический кризис 2008–2009 годов, спровоцированный политикой центральных банков и правительств ведущих экономик мира, подорвал доверие инвесторов и населения к традиционной финансовой системе и институтам. *Во-вторых*, неконвенциональная монетарная политика, с помощью которой центральные банки попытались предотвратить системную катастрофу, накачав мировую экономику дешёвыми деньгами, имела следствием взрывной рост венчурных проектов и стартапов, в том числе в финансовой сфере. *В-третьих*, развитие компьютерных технологий и Интернета вышло на новый уровень, запустив волну цифровизации современной экономики, включая финансы.

В этих условиях в финансовой сфере начала формироваться новая система, получившая название финтех (FinTech). Она объединяет проекты и инициативы, которые, опираясь на прорывные и «подрывные» технологии, пытаются выстроить альтернативу традиционной финансовой системе или принципиально модернизировать последнюю. Глобальный комплекс криптосистем и криптовалют представляет собой одну из подсистем финтеха. Подавляющее большинство криптосистем организуются как открытые цифровые площадки, предназначенные для решения специфических технологических и экономических задач. Они объединяют комплекс компьютерных технологий, концептуальных идей, коллективов разработчиков и пользователей, которые составляют единую цифровую сеть. Вне зависимости от поставленных задач все криптовалюты используют технологию распределённого реестра, преимущественно блокчейна.

В основе криптосистем лежат положения теории игр, специальные компьютерные программы и Интернет. Децентрализованные криптосистемы позволяют их участникам равноправно взаимодействовать в соответствии с заданным протоколом без посредников. Встроенный в компьютерный код математический аппарат обеспечивает их работу в соответствии с заданными правилами и процедурами и позволяет осуществлять экономические трансакции. Компьютерный код заменяет собой закон, а также правила и процедуры, которые действуют в обычной финансовой системе.

Глобальный криптокомплекс развивается быстрыми темпами. Значительное число выходящих на рынок криптопроектов быстро прекращает своё существование, но постоянно запускается ещё большее количество новых проектов. На конец июля 2018 г. в мире действовало более 1670 криптопроектов[1]. Ниже подробно анализируют-

[1] Подсчитано по базе данных Cryptocurrency Market Capitalizations. URL: https://coinmarketcap.com (accessed 20.08.2018).

Таблица 1

Доля отдельных криптовалют в совокупной капитализации криптовалют, % на конец года

	2013	2014	2015	2016	2017	2018 (конец июля)
Bitcoin	88	78	91	88	39	47
Ether	0	0	1	4	12	16
XRP	2	13	3	1	14	6
Bitcoin Cash	0	0	0	0	7	5
Litecoin	5	2	2	1	2	2
Прочие	5	7	2	6	26	24
Всего	100	100	100	100	100	100

Составлено авторами по базе данных Cryptocurrency Market Capitalizations. URL: https://coinmarketcap.com (accessed 20.08.2018).

ся крупнейшие криптосистемы *Bitcoin*, *Ethereum* и *Ripple*, на которые приходится около 70% совокупной капитализации глобального криптокомплекса (табл. 1).

2

Bitcoin – самая крупная глобальная частная криптосистема, цель которой заключается в замене обычных (фиатных) денег одноимённой криптовалютой. С некоторыми натяжками криптосистему *Bitcoin* можно отождествить с её криптовалютой. Концептуальные основы децентрализованных криптоденег были сформулированы мифическим персонажем Сатоши Накамото в «Белой книге»[2], опубликованной в октябре 2008 года. В соответствии с ней криптовалюта *bitcoin* и основанная на ней криптоденежная система *Bitcoin* принципиально отличаются от фиатных денег. Она базируется на частных, а не государственных деньгах, в системе отсутствует монопольный центр эмиссии, трансакции между равноправными экономическими агентами осуществляются напрямую, без участия посредников в лице банков (табл. 2). В этой идеальной системе *bitcoin* выполняет все функции денег: меры стоимости, средства обмена, сбережения и накопления.

Общее доверие в системе, её надёжность и эффективность автоматически обеспечиваются компьютерным кодом, заставляющим участников взаимодействия поступать таким образом, чтобы реализация личных целей и интересов не нарушала целостность системы. Компьютерный код гарантирует транспарентность работы и состоятельность трансакций, полностью заменяя центральный банк, коммерческие финансовые организации и регуляторов денежного рынка.

Криптосистема *Bitcoin* организована как глобальная открытая интернет-площадка. Её работу поддерживают майнеры – объединённые в пулы или действующие индивидуально владельцы компьютерных мощностей, которые решают постоянно усложняющиеся криптографические задачи, обеспечивая тем самым непрерывную эмиссию и трансакции *bitcoin*. Майнером может стать любой желающий, установив на компьютере специальную программу, которая свободно скачивается в Интернете. Объединение в пул обеспечивает агрегирование компьютерных мощностей, что позволяет ускорить решение криптографических задач, а значит, и получать эмитируемые *bitcoin* на счёт. Собственно, майнинг и представляет собой процесс эмиссии криптовалюты. Майнеры, решившие криптографическую задачу быстрее и успешнее других, получают на свои счета (кошельки) определённое количество криптовалюты.

[2] *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System. White Paper. URL: https://bitcoin.org/bitcoin.pdf (accessed 19.03.2019).

Таблица 2
Сравнение *Bitcoin* и фиатных денег

	Фиатные деньги (факт)	***Bitcoin*** (идеология)
общая организация денежной системы и денежной политики		
собственность	государственные деньги	частные деньги
централизованный регулятор	центральный банк	отсутствует
посредники трансакций	банки	прямые трансакции P2P
риск инфляции	высокий	отсутствует
риск дефляции	низкий	высокий
гибкий инструмент для проведения экономической политики	да	нет
предложение денег		
эмиссия	монополия государства	децентрализованные совместные действия майнеров
объём эмиссии	регулируется по потребности и в зависимости от задач денежной и кредитной политики	увеличивается со снижающимся темпом, заданным компьютерным алгоритмом. Максимальный объём эмиссии фиксирован
функции денег		
Мера стоимости	да	да
Средство платежа	да	да
Средство сбережения и накопления	да	да

Составлено авторами с привлечением [He, Habermeier et al. 2016].

Есть возможность присоединиться к системе в качестве пользователя денег, создав индивидуальный счёт или электронный кошелёк. Приобрести *bitcoin* можно, приняв его в качестве оплаты за поставленные товары и услуги, а также купив на бирже, на электронной торговой площадке или в специальном банковском автомате.

Бизнес-модель криптосистемы предельно проста: обеспечивая процесс эмиссии криптовалюты и трансакции пользователей, майнеры получают вознаграждение, покрывающее их издержки и обеспечивающее прибыль. Всего в обращение должно быть выпущено 21 млн *bitcoin*. Эмиссия идёт с заданной математическим алгоритмом скоростью, которая постепенно снижается и в долговременной перспективе асимптотически приближается к нулю. Предположительно, последние *bitcoin* будут эмитированы после 2140 года.

За почти десять лет с момента запуска системы в обращении находится 82% запланированной эмиссии криптовалюты. Уместно задаться вопросом, удалось ли *bitcoin* утвердиться в качестве альтернативы фиатных денег, а также насколько формирующаяся компьютерная денежная система отвечает принципам, которые были продекларированы её создателями.

По формальным количественным показателям система продемонстрировала впечатляющие успехи: число электронных кошельков достигло почти 28 млн (пользователь может поддерживать несколько кошельков), в среднем за день в системе совершается более 200 тыс. трансакций (табл. 3).

Тем не менее криптосистема не реализовала заявленную стратегическую цель. В ряде теоретических и аналитических работ, рассмотревших *Bitcoin* в логическом времени компьютерной сетевой игры, были вскрыты многие её дефекты, в том числе на уровне кода и алгоритмов работы сети. Реальные характеристики денежной криптосистемы принципиально отличны от заявленных. Рассмотрим наиболее важные характеристики, которые девальвируют первоначальные идеи её создателей.

Таблица 3
Характеристики развития экосистемы *Bitcoin*

	Число *bitcoin* в обращении, млн (на конец периода)	**Среднее число трансакций в день, тыс.**	**Число кошельков, млн (на конец года)**	**Расчётная среднегодовая цена *bitcoin*, тыс. долл.**	**Расчётная среднегодовая плата за трансакцию, долл.**
2009	1,62	0,09	...	...	...
2010	5,01	0,5	...	...	3,24
2011	8,00	5	0,0004	...	7,94
2012	10,61	23	0,077	...	3,52
2013	12,19	54	0,97	...	14,64
2014	13,67	69	2,72	527	32,87
2015	15,035	125	5,44	272	8,34
2016	16,07	227	10,98	568	7,11
2017	16,77	285	21,51	4 006	31,08
2018*	17,22	208	27,86	8 652	85,4

* 1 января – 20 августа 2018 г.

Составлено авторами по данным Cryptocurrency Market Capitalizations (URL: https://coinmarketcap.com); Bitcoin Block Explorer. URL: http://blockchain.info (accessed 20.08.2018).

Во-первых, быстро выяснилось, что *Bitcoin* на деле не является системой распределённых денег, поддерживающей сделки между равными партнёрами через изначально заданный компьютерный код. В системе действует своя иерархия, и ей присущи монопольные эффекты. Де-факто контроль над работой системы осуществляется крупными игроками, в число которых входят её создатели. Официального регулятора в лице центрального банка заместила не автоматическая криптосистема, а пионеры *Bitcoin* и крупные игроки. Они не только зарезервировали за собой значительные объёмы криптовалюты ещё до начала её эмиссии, но также обладают эксклюзивными правами на внесение изменений в протокол работы сети и при необходимости могут пересматривать решения, принятые в результате голосования майнеров, хотя последние могут и остаться работать в старом протоколе, неся при этом издержки по его поддержанию. Это свойство всех крупнейших криптосистем (табл. 4).

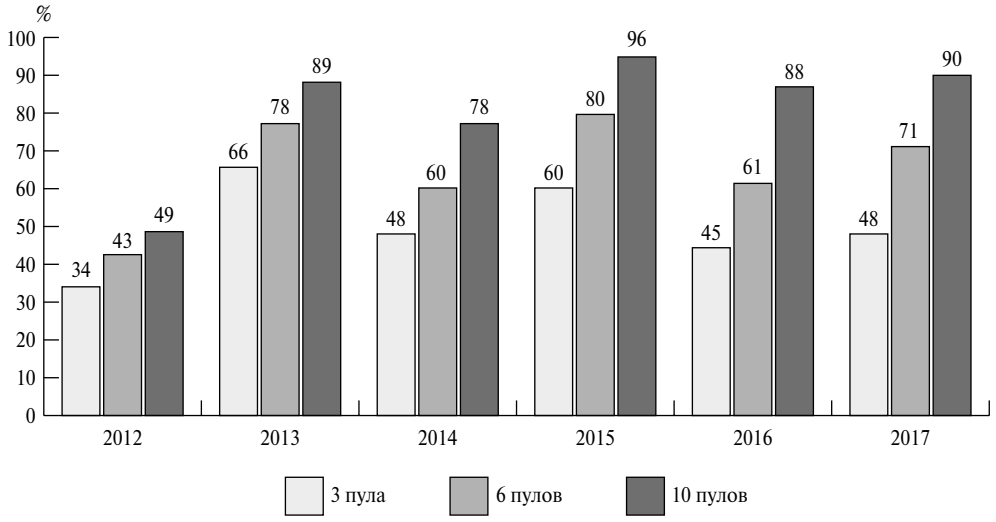
В настоящее время эмиссия *bitcoin* находится под контролем ограниченного числа майнинговых пулов. Начиная с 2014 г. три пула устойчиво контролируют около 50% процесса майнинга в *Bitcoin*, а 10 пулов – около 90% (рис. 1). Теоретически контроль над 51% майнинга позволяет остановить

Таблица 4
Влияние пионеров проекта на развитие систем криптовалюты

	bitcoin (Bitcoin)	***Ether (Ethereum)***	***XRP (Ripple)***
Объём эмиссии криптовалюты	21 млн	не ограничен	100 млрд
Объём криптовалюты, зарезервированной за пионерами до начала эмиссии	около 1 млн	72 млн	20% + 80% у компании
Механизм распределения новой эмиссии	конкурентный майнинг	конкурентный майнинг	покупка у компании *Ripple*
Эксклюзивные права пионеров на внесение изменений в протокол	да	да	да
Случаи пересмотра пионерами решений майнеров	да	да	...

Составлено авторами по материалам бизнес-периодики.

Рисунок 1
Концентрация компьютерной мощности в Bitcoin, доли крупнейших пулов майнеров (на декабрь соответствующего года), %



Составлено авторами по данным Pool Stats. URL: http://btc.com/stats/pool (accessed 20.08.2018).

работу остальных майнеров по формированию блока и верификацию трансакций, а главное – провести «атаку двойного платежа», то есть расплатиться одними и теми же *bitcoin* по разным трансакциям [Lin, Liao: 656].

Эмитированные *bitcoin* распределены среди владельцев крайне неравномерно (табл. 5), в первую очередь из-за того, что в первые годы работы криптосистемы её создатели смогли приобрести, причём в низкоконкурентном режиме и без больших издержек, значительный, если не подавляющий, объём эмиссии. По некоторым оценкам, около 40% *bitcoin* находятся в руках тысячи человек. Члены этого закрытого клуба хорошо знакомы друг с другом и способны координировать свою деятельность на рынке[3].

Во-вторых, по мере развития и усложнения *Bitcoin* вскрылись дефекты, которые ставят под вопрос устойчивость существующей бизнес-модели в долговременной перспективе. Увеличение числа пользователей и объёма трансакций спровоцировало конфликт между интересами майнеров и пользователей. Значительно выросли как продолжительность трансакций, так и плата за их проведение (рис. 2). Увеличение платежей за трансакции стало влиять на очерёдность обработки майнерами запросов пользователей [Gur Huberman G. et al. 2017: 7]. Заинтересованность майнеров в крупных трансакциях, за которые полагается более высокое вознаграждение, оборачивается дискриминацией небольших трансакций. В фундаментальном плане это ставит под вопрос возможности масштабирования *Bitcoin*.

В-третьих, потерпела неудачу идея добиться использования *bitcoin* как альтернативы фиатным деньгам в качестве массово используемого платёжного средства. Хотя агрегированной статистики на этот счёт не

[3] *Kharif O.* The Bitcoin Whales: 1,000 People Who Own 40 Percent of the Market. A few massive investors can rock it with a shrug. URL: https://www.bloomberg.com/news/articles/2017-12-08/the-bitcoin-whales-1-000-people-who-own-40-percent-of-the-market (accessed 11.04.2018).

существует, судя по разрозненным сообщениям, подобные трансакции ограничены по объёму и носят спорадический характер. Массовому потребителю неудобно использовать сложно зашифрованную систему компьютерных кошельков и частных ключей. Криптовалюте не добавляет популярности отсутствие возможности отменить ошибочный платёж и восстановить потерянные *bitcoin*. К тому же велик риск воровства хакерами криптовалюты из электронных кошельков бирж и индивидуальных пользователей, причём алгоритма отмены операции в случае кражи криптоденег из кошелька в системе не существует.

Также и в качестве средства сбережения и накопления *bitcoin* не смог составить достойную альтернативу фиатным деньгам и традиционным активам по причине высокой волатильности цены (см. табл. 3).

Таблица 5

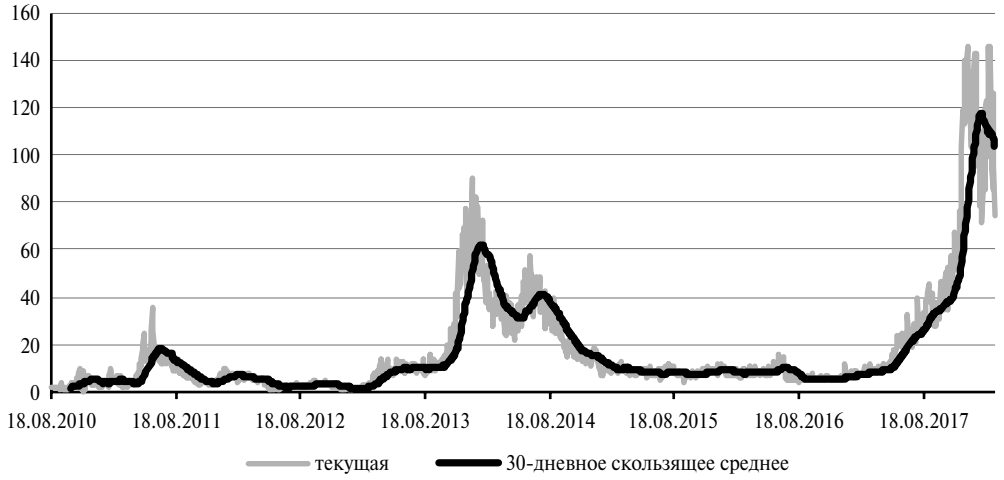
Характеристики концентрации владения *bitcoin* (балансов кошельков) по состоянию на август 2018 г.

Баланс кошелька, *bitcoin*	**Доля от всего числа кошельков (адресов), %**	**Доля *bitcoin* на балансе, % от всей эмиссии**	**Баланс усреднённого кошелька, долл.**
0 – 0,001	49,44	0,01	1,5
0,001 – 0,01	22,43	0,12	30
0,01 – 0,1	17,3	0,72	241
0,1 – 1	7,64	3,21	2,4 тыс.
1 – 10	2,51	8,63	19,8 тыс.
10 –100	0,6	25,68	248,6 тыс.
100 – 1 000	0,07	21,8	1,8 млн
1 000 – 10 000	0,01	19,75	16,5 млн
10 000 – 100 000	0	17,41	199,7 млн
100 000 – 1 000 000	0	2,67	1 130,8 млн
Всего	100	100	5 772

Источник: Bitinfocharts. URL: https://bitinfocharts.com/ru/top-100-richest-bitcoin-addresses.html (accessed 14.08.2018).

Рисунок 2

Динамика цены трансакции в системе Bitcoin, 18 августа 2010–20 августа 2018, долл.



Источник: Bitcoin Block Explorer. URL: http://blockchain.info (accessed 20.08.2019).

Мы разделяем позицию председателя Банка Англии, отметившего, что *bitcoin* не справился с задачей стать полноценными деньгами: он не является ни средством накопления, ни средством оплаты товаров и услуг[4].

Какие же секторы и виды экономической деятельности обслуживает *bitcoin*? В Китае, на который до введения в 2017 г. запрета на торговлю криптовалютами и их первичные размещения, по оценкам, приходилось более 95% мирового оборота этой платёжной единицы, операции с *bitcoin* обслуживали вывод капитала за границу[5]. В других странах они широко используются для отмывания денег и поддержки криминальной экономической активности. Например, в 2013 г. власти США закрыли площадку анонимной интернет-торговли наркотиками *Silk Road*, использовавшую для обеспечения анонимности браузер *Tor* и оттянувшую значительную часть оборота *bitcoin* [Conti M. et al. 2017]. Анализ сделок, проведённый эконометрическими методами с опорой на базу данных клиентов *Bitcoin*, которая была составлена регуляторами по информации о работе нелегальной площадки, показал, что четверть пользователей криптосистемы, почти половина трансакций и более половины накопленных *bitcoin* связаны с наркооборотом и секс-индустрией. Оборот криптовалюты в этих криминальных сегментах оценён в 72 млрд долларов в год [Foley et al. 2018].

К настоящему времени финансовые регуляторы не усматривают в *bitcoin* (и криптовалютах в целом) системного риска для действующей финансовой системы, поскольку криптовалюты используют лишь 0,5% потребителей – таковы данные опроса, который провёл Совет по надзору за финансовой стабильностью США[6]. Регуляторы признают, что *bitcoin* и даже лучше защищённые криптографическими методами криптоденьги *Monero* и *Zcash* абсолютно прозрачны для квалифицированного мониторинга[7].

3

Вторая после *Bitcoin* по капитализации глобальная частная криптосистема *Ethereum* поддерживает собственную криптовалюту *ether*. Её концептуальные основы были заложены в «Белой книге» 2013 года[8] и детализированы в «Жёлтой книге» 2014[9]. Официально система была запущена в середине 2015 года.

По ряду важнейших технико-экономических характеристик *Ethereum* близка *Bitcoin*. Обе криптосистемы основаны на блокчейне, в обеих – эмиссия криптовалюты реализуется через процесс майнинга, а консенсус по трансакциям основан на принципе *proof-of-work*. Как и в *Bitcoin*, в системе *Ethereum* майнинг находится под контролем ограниченного числа игроков: 85% счётной мощности контролируют 5 компаний[10]. Специальные исследования показывают, что в еженедельном режиме майнинг в *Ethereum* более монополизирован в сравнении с *Bitcoin* [Gencer et al. 2018].

[4] *Milliken D.* BoE's Carney says Bitcoin has "pretty much failed" as currency. URL: https://www.reuters.com/article/us-britain-boe-carney-currencies/boes-carney-says-bitcoin-has-pretty-much-failed-as-currency-idUSKCN1G320Z (accessed 11.04.2018).

[5] *Wong J.I.* Chinese money dominates bitcoin, now its companies are gunning for blockchain tech // Quartz, October 2, 2017. URL: https://qz.com/1072907/why-china-is-so-hot-on-bitcoin (accessed 19.03.2019).

[6] Financial Stability Oversight Council 2017 Annual Report. Wash. D.C. P. 99.

[7] *Russo C.* Bitcoin Speculators, Not Drug Dealers, Dominate Crypto Use Now. URL: https://www.bloomberg.com/news/articles/2018-08-07/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now?srnd=cryptocurriences (accessed 20.08.2018).

[8] *Buterin V.* Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. URL: http://ethereum.org/ethereum.html (accessed 20.08.2018).

[9] *Wood G.* Ethereum: A Secure Decentralised Generalised Transaction Ledger. EIP-150 REVISION. 2014. URL: http://gavwood.com/paper.pdf (accessed 20.08.2018).

[10] Ethereum Price. URL: http://www.bitcoinprice.com/ethereum (accessed 20.08.2018).

Многие аналитики отмечают высокую технологическую уязвимость этой криптосистемы и отдельных умных контрактов [Grishchenko et al. 2018]. Масштабные потери *ether* из-за ошибок в коде смарт-контрактов и в результате хакерских атак присущи *Ethereum* едва ли не в большей мере, чем криптосистеме *Bitcoin*[11].

В целом, несмотря на многие различия, по концентрированности майнинга, технологической уязвимости, потерям криптовалюты из-за атак и встроенных технологических дефектов, значительное число которых остаётся пока даже не выявленными, *Ethereum* и *Bitcoin* сопоставимы. Вместе с тем разработчики *Ethereum* учли проблемы *Bitcoin* и по ряду характеристик сделали свою систему более эффективной. Главное достижение заключается в ускорении работы благодаря тому, что в десятки раз сокращено время для генерации нового блока[12]. В ближайшее время *Ethereum* планирует перейти от принципа *proof-of-work* к принципу *proof-of-stake Caspers*[13], что дополнительно ускорит работу системы.

Стратегическая цель киберсистемы заключается в создании глобальной технологической площадки для реализации смарт-контрактов и распределённых прикладных приложений. Умный контракт – это криптоконтракт, позволяющий осуществлять сделки с деньгами, активами, собственностью, информацией, идеями, то есть со всем, что удалось переложить на компьютерный язык. На практике *Ethereum* формируется как глобальная платформа, которая, используя универсальный компьютерный язык и алгоритмы, позволяет представителям любых видов человеческой деятельности взаимодействовать в цифровом пространстве. Криптовалюта *ether* лишь средство для решения данной стратегической задачи. В идеале криптосистема *Ethereum* может бесконечно расширяться путём добавления новых умных контрактов. Центральный элемент в системе – виртуальная машина *Ethereum (EVM)* – обладает свойством полноты по Тьюрингу, иначе говоря, может работать с программой, написанной на любом компьютерном языке [Hirai 2017], что значительно упрощает процесс создания смарт-контрактов.

Ethereum продемонстрировала успехи в реализации заявленной стратегической цели. При всех отмеченных выше встроенных недостатках, открытость и удобство *Ethereum* подогревают интерес к этой площадке банков и компаний реального сектора, нацеленных на развитие смарт-контрактов. В сети действует множество открытых рабочих групп, развивающих на основе киберсистемы бизнес-направления в области рекламы, банков, массмедиа, аналитических приложений, энергетики, здравоохранения, формирования цепочек поставщиков[14].

В феврале 2017 г. был организован предпринимательский альянс *Ethereum (EEA)*, в который вошли 30 крупнейших мировых банков и корпораций, а также технологические и научно-исследовательские центры, заинтересованные в изучении и продвижении концепции умных контрактов на единой технологической платформе. В марте 2018 г. *EEA* объединял уже более 400 организаций[15]. Цель данной инициативы – помочь участникам альянса создавать специализированные блокчейны *Ethereum* для решения частных специфических задач

[11] *Chang S.* Ethereum Smart Contracts Vulnerable to Hacks: $4 Million in Ether at Risk. URL: https://www.investopedia.com/news/ethereum-smart-contracts-vulnerable-hacks-4-million-ether-risk (accessed 19.03.2019).

[12] Ethereum differs from Bitcoin in 7 main ways. URL: https://www.cryptocompare.com/coins/guides/why-is-ethereum-different-to-bitcoin (accessed 19.03.2019).

[13] *Shome A.* Ethereum is Actually Bigger than Bitcoin and All Altcoins Combined. URL: https://www.financemagnates.com/cryptocurrency/ethereum-actually-bigger-bitcoin-altcoins-combined (accessed 24.08.2018).

[14] Working Groups. https://entethalliance.org/working-groups/

[15] *Adriano L.* Marsh joins open source blockchain initiative. URL: https://www.insurancebusinessmag.com/us/news/technology/marsh-joins-open-source-blockchain-initiative-94961.aspx (accessed 20.08.2018).

Таблица 6

Первичное распределение *ether* по типам собственников (без учёта вторичных сделок)

	Число *ether*, млн	**Доля в общем объёме выпуска, %**
Создатели и первичные инвесторы (до запуска системы)	72,01	72,7
Майнеры блоков	27,109	27,3
Всего	99,120	100

Источник: Ethereum Market Capitalization and Supply Statistics. URL: https://etherscan.io/stat/supply (accessed 24.08.2018).

и выстраивания устойчивых индивидуальных бизнес-моделей. Общая технологическая платформа позволяет координировать работы, привлекать специалистов и без промедления распространять частные новации среди участников альянса. Возникает синергетический эффект параллельного движения как частных блокчейнов, так и публичной блокчейн-площадки[16].

Экономика и управление криптосистемой *Ethereum* принципиально отличны от *Bitcoin*. Первоначально её развитием занималась Децентрализованная автономная организация (*DAO*), затем её функции перенял специализированный фонд (*Ethereum Foundation*). Управляющее ядро обеих структур представлено пионерами проекта, которые строго следуют политике специфической, хотя и не обнародованной бизнес-модели, в рамках которой развитие криптосистемы выстраивается в соответствии с их текущими экономическими и стратегическими интересами. Фактически первичные разработчики создали «вечный двигатель по мобилизации инвестиций» в свои проекты. Он будет работать до тех пор, пока мировое сообщество поддерживает криптоманию и блокчейнманию.

В *Ethereum* отсутствует предел эмиссии криптовалюты. При этом изначально в системе был заложен практически абсолютный контроль первичных разработчиков и инвесторов над распределением криптовалюты и процессом развития системы. При первичном (до майнинга) размещении криптовалюты они получили 72 млн *ether* (табл. 6). Даже после трёхлетнего функционирования системы пионеры продолжают контролировать подавляющую часть эмиссии. Учитывая, что в 2014 г. они достигли соглашения эмитировать в год не более 18 млн *ether*[17], этот контроль ещё долго будет оставаться абсолютным.

Характер ключевых решений по изменению кода, как и способы урегулирования конфликтных ситуаций, подтверждает определяющую роль в управлении системой её разработчиков и редакторов. Самый известный пример – решение о восстановлении украденных в 2016 г. у Децентрализованной автономной организации (*DAO*) 50 млн долларов. По мнению многих участников криптосистемы, решение о восстановлении похищенных средств через «жёсткую вилку» было принято только потому, что эту организацию возглавляли создатели криптосистемы[18]. Некоторые наблюдатели сравнили принятое решение с типичной для системы фиатных денег операцией по спасению обанкротившегося банка[19]. Не все участники системы согласились с ним и после проведения «жёсткой вилки» продолжили поддерживать изначальный блокчейн под именем *Ethereum Classic*.

Бизнес-модель создателей криптосистемы заключается в максимизации доходов, рент и любых выгод от её развития. Быстрорастущее число пользователей системы повышает спрос на *ether*, в связи с чем усилия создателей системы направлены на

[16] *Khatwani S.* Enterprise Ethereum Alliance: Everything You Need To Know. URL: https://coinsutra.com/enterprise-ethereum-alliance/ (accessed 24.08.2018).

[17] Is the ether supply infinite? URL: https://www.ethereum.org/ether (accessed 24.08.2018).

[18] *Madeira A.* The DAO, The Hack, The Soft Fork and The Hard Fork. URL: https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/ (accessed 20.08.2018).

[19] *O'Leary R.R.* High Stakes: Ethereum's Fight Over Lost Funds Explained. URL: https://www.coindesk.com/high-stakes-ethereums-fight-lost-funds-explained (accessed 20.08.2018).

обеспечение её экстенсивного роста. Эти цели реализуются, невзирая на издержки, причём создателей системы не заботит проблема состоятельности криптоденег. Как отметил сооснователь *Ethereum* Дж. Любин: «Конечно, это пузырь. Надеюсь, пузырь в серии нарастающих ещё бóльших пузырей. Эти пузыри привлекают внимание, они приносят стоимость в экосистему. Эту стоимость осознают разработчики компьютерных программ и бизнес-девелоперы, они и создают фундаментальную стоимость и проекты, которые выращивают новую архитектуру»[20].

19 августа 2018 г. на площадке *Ethereum* было зарегистрировано 111,4 тыс. верифицированных кодов умных контрактов. Для сравнения: на конец апреля 2018 г. таковых было всего 24,2 тысячи, а в середине 2016 – всего 545 кодов[21]. Криптосистема переполнена контрактами и приложениями самого разного свойства и качества. Самый популярный способ получения прибыли – запуск новых умных контрактов или распределённых прикладных приложений на своём блокчейне, выполненный по облегчённому стандарту *ERC20*, который система предложила в 2015 году. Токены *ERC20*, на создание которых требуется не более 20–30 минут[22], привязаны к сети *Ethereum*, используют принятый внутри неё формат адресов и пересылаются при помощи *Ethereum*-трансакций. Примечательно, что пользователи быстро обнаружили встроенные ошибки в коде контракта *ERC20*, однако криптосистема продолжает его использовать[23].

Помимо этого, площадка *Ethereum* используется для поддержания казино, схем понци, финансовых пирамид и других спекуляций[24]. В августе 2018 г. *Ethereum* объявил о скором предложении пользователям, совершающим операции с *ether*, возможность привязывать свои адреса к доменам верхнего уровня в сети Интернет, что упростит запоминание идентификаторов, связанных с кошельками, активами и другими услугами. Если до сих пор для работы с криптовалютами и для обычной деятельности в Интернете (таких, как использование электронной почты или посещения сайтов) требовались разные адреса, то новый сервис объединит Интернет с криптосистемами[25]. С запуском нового сервиса *Ethereum* станет выполнять функцию главного медиатора развития всего глобального криптокомплекса.

Фактически криптосистема *Ethereum* имеет двухуровневую структуру. На первом уровне хорошо осознающие риски квалифицированные инвесторы (банки и крупные компании реального сектора) в сотрудничестве с создателями системы тестируют бизнес-возможности блокчейна. На втором функционируют десятки тысяч контрактов, подавляющая часть которых

[20] *Gershgorn D.* «Of course it's a bubble»: Ethereum cofounder Joe Lubin isn't worried about a crash. URL: https://qz.com/1111123/of-course-its-a-bubble-ethereum-cofounder-joe-lubin-isnt-worried-about-a-crash/ (accessed 20.08.2018).

[21] How many contracts are currently deployed on the Ethereum blockchain? URL: https://ethereum.stackexchange.com/questions/8648/how-many-contract-are-currently-deployed-on-the-ethereum-blockchain (accessed 20.08.2018); Verified Contracts. URL: https://etherscan.io/contractsVerified (accessed 20.08.2018).

[22] *Neto M.* How to issue your own token on Ethereum in less than 20 minutes. URL: https://medium.com/bitfwd/how-to-issue-your-own-token-on-ethereum-in-less-than-20-minutes-ac1f8f022793 (accessed 24.08.2018); Redman J. Launching an ICO Token on Ethereum in Less Than Thirty Minutes. URL: https://news.bitcoin.com/launching-an-ico-token-on-ethereum-in-less-than-thirty-minutes/ (accessed 24.08.2018).

[23] *Mulders M.* A comparison between ERC20, ERC223, and the new Ethereum ERC777 token standard. URL: https://www.cointelligence.com/content/comparison-erc20-erc223-new-ethereum-erc777-token-standard/ (accessed 24.08.2018).

[24] Ethereum is full of ponzis, is that a problem? URL: http://jpkoning.blogspot.com/2018/05/ethereum-is-full-of-ponzis-is-that.html (accessed 24.08.2018).

[25] *Milano A.* Ethereum Is Getting Its First Top-Level Domain Name. URL: https://www.coindesk.com/ethereum-is-getting-its-first-top-level-domain-name/ (accessed 24.08.2018).

нацелена на получение прибыли в краткосрочном периоде любыми способами. Термин «контракт» в данном случае не должен вводить в заблуждение. Речь идёт не более чем о компьютерной программе, которая, ко всему прочему, может содержать встроенные ошибки. Взаимная ответственность сторон в умных контрактах криптосистемы предусмотрена только идеологически и идеалистически.

4

Основанная в 2005 г. система *Ripple* прошла в своём развитии несколько этапов. Криптовалюта системы *XRP*, иногда ошибочно называемая *ripple*, была запущена в 2012 году. В 2014, 2015 и 2017 годах она оставалась второй по капитализации крупнейшей криптовалютой после *bitcoin*, в конце июля 2018 г. – третьей, пропустив вперёд также и *ether*. Эта криптосистема принципиально отличается от *Bitcoin* и *Ethereum*. Она полностью централизована и развивается частной компанией *Ripple* (ранее *Ripple Labs*). В системе параллельно действуют два элемента: система платежей и переводов *RippleNet* и криптовалюта *XRP*.

Последняя функционирует на собственном блокчейне[26] и, по уверениям *Ripple*, представляет собой абсолютно децентрализованную площадку, которая не зависит от компании. С этим трудно согласиться, поскольку 100% *XRP* (100 млрд единиц) эмитированы до запуска системы, в которой отсутствует майнинг валюты. Компания *Ripple* зарезервировала за собой почти 62% эмиссии криптовалюты, причём 7% оставили за собой создатели компании. Оставшиеся 55%, принадлежащие фирме, размещены на специальных криптосчетах эскроу в реестре *XRP*, с которых, согласно политике компании, каждый месяц вводится в оборот около 1% эмиссии. Теоретически через 55 месяцев счета должны обнулиться, но при отсутствии спроса невостребованная валюта возвращается обратно на счета эскроу. Криптовалюту *XRP* участники системы могут купить напрямую у компании *Ripple* либо на криптобиржах *Bitstamp*, *Kraken*, *Gatehub*, *CoinOne*, *Bitflip*, *EXMO* и использовать для проведения трансакций.

О механизме продажи *XRP* компанией *Ripple* и со счетов эскроу известно мало, неизвестны и реальные цены сделок. Зафиксированы случаи проведения спланированных контрагентами сделок с целью раздувания стоимости криптовалюты[27]. После проведения трансакций объём первоначальной эмиссии уменьшается на сумму, эквивалентную плате за трансакции. Для проведения трансакций клиенты должны поддерживать на своих электронных счетах определённый минимум *XRP*.

Консенсус в протоколе *XRP* опирается не на принцип *proof-of-work*, а на консенсусное голосование подтверждённых, то есть заранее отобранных компанией *Ripple*, узлов. Консенсус достигается при подтверждении сделки 80% узлов. Их операторами в большинстве своём выступают банки, маркет-мейкеры и сама *Ripple*[28]. Они поддерживают компьютерный протокол «Система всеобщего осуществления платежей в режиме реального времени» (*Real Time Gross settlement System – RTGS*).

Система платежей и переводов *RippleNet* стремится перевести свою работу на протокол *Interledger*, не являющийся блокчейном. Он интегрирует работу многих компьютерных протоколов и обеспечивает высокую скорость трансакций, что должно способствовать реализации стратегической цели компании. Данный протокол распределённого реестра ближе к традиционным интернет-протоколам, обеспечивающим связь между веб-сайтами и адресами электронной почты. К *Interledger* через специ-

[26] *O'Leary R.R.* How XRP Fits Into Ripple's Payments Products Explained. URL: https://www.coindesk.com/xrp-fits-ripples-payments-products-explained/ (accessed 24.08.2018).

[27] The Ripple story. URL: https://blog.bitmex.com/the-ripple-story/ (accessed 20.08.2018).

[28] *Redman J.* Is the Centralized Ripple Database With the Biggest Pre-Mine Really a Bitcoin Competitor? URL: https://news.bitcoin.com/is-the-centralized-ripple-database-with-the-biggest-pre-mine-really-a-bitcoin-competitor/ (accessed 24.08.2018).

альные соединения – шлюзы – могут легко подключаться любые компьютерные системы, протоколы, включая блокчейны, платёжные системы и активы. Фактически он должен выполнять в *Ripple* функции сетевой платёжной системы, которая интегрирует другие платёжные системы. Подключившись через шлюз к общей сети, её участники могут сохранить для себя автономный режим работы в закрытом режиме.

Система *Ripple* работает не только с *XRP*, но и с другими криптовалютами, а также с фиатными деньгами. Компания *Ripple* поставила перед собой стратегическую цель превратиться в глобальную цифровую площадку по осуществлению трансграничных мультивалютных межбанковских платежей – иными словами, стать аналогом *SWIFT* эпохи цифровизации за счёт повышения скорости трансакций и упрощения торговли низколиквидными активами. Она осуществляет обмены любых валютных пар, включая криптовалюты, по ценам, соответствующим ставкам оптового межбанковского рынка на текущий момент времени, без посредников в виде кредитных карт, расчётных организаций, валютных бирж и банков[29].

Используемые компьютерные алгоритмы должны обеспечить *Ripple* три конкурентных преимущества: *во-первых*, возможность трансакций между любыми валютами и активами; *во-вторых*, высокую скорость трансакций; *в-третьих*, неограниченную масштабируемость. В настоящее время система обрабатывает тысячу трансакций в секунду, но в дальнейшем ожидается увеличение скорости до пятидесяти тысяч трансакций в секунду, что сопоставимо с возможностями платёжной системы *Visa*[30]. Для продвижения своего бизнеса компания активно выстраивает партнёрства с ведущими мировыми банками и финансовыми организациями. В развитие компании *Ripple* инвестировали крупные рыночные игроки *Google*, *Goldman Sachs* и другие. Компания вышла на рынки стран Азиатско-Тихоокеанского региона.

Компания предлагает на рынке три программных продукта: *xCurrent*, *xRapid* и *xVia*. *xCurrent* – действующая компьютерная программа, позволяющая банкам непрерывно осуществлять трансграничные платежи, контролируя начало и завершение сделки. Используя *xCurrent*, банки перед проведением сделки в режиме реального времени согласуют детали трансакций и подтверждают их совершение. Взаимодействие между банками, операционная состоятельность и юридические вопросы регулируются сводом правил, который разработал консультативный совет *RippleNet Committee*[31].

Задача *xCurrent*, опирающейся на распределённый протокол *Interledger*, заключается в том, чтобы обеспечить трансакции между любыми парами денег, фиатных и крипто. В таких трансакциях *XRP* может использоваться наряду с другими деньгами, но в этом случае система в пилотном режиме использует программу *xRapid*. Эта компьютерная программа управления банковской ликвидностью должна проводить трансграничные межбанковские платежи, используя *XRP* в качестве валюты-посредника. Если эта цель будет достигнута, криптовалюта органично интегрируется в криптосистему *Ripple*. Вероятен и вариант, при котором *xRapid* сможет функционировать без использования *XRP*, аналогично тому, как это происходит в программах *xCurrent* и *xVia*. Программа *xVia* предназначена для осуществления трансграничных переводов платёжных требований (инвойсов). *xVia* находится в ранней стадии разработки.

[29] First Bitcoin, now Google-backed OpenCoin: a new disintermediation threat for banks. URL: https://www.euromoney.com/article/b12kjtsrxy09mk/first-bitcoin-now-googlebacked-opencoin-a-new-disintermediation-threat-for-banks (accessed 24.08.2018).

[30] Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal? URL: https://howmuch.net/articles/crypto-transaction-speeds-compared (accessed 24.08.2018).

[31] Instant and Certain Settlement. URL: https://ripple.com/solutions/process-payments/ (accessed 24.08.2018).

Компания *Ripple* пытается создать новые технологические решения для современной финансовой системы. Она предлагает не альтернативу сложившейся системе традиционных банков и систем платежей, а новые высокотехнологичные и эффективные решения. Многие примеры свидетельствуют о принципиальном стремлении компании выстроить долгосрочные отношения с регуляторами. Например, в мае 2015 г. Сеть по борьбе с финансовыми преступлениями Министерства финансов США (*FinCEN*) оштрафовала *Ripple* на 700 тыс. долларов за нарушения закона о банковской тайне, оборот денег и продажу криптовалюты без регистрации, а также за невыполнение требований по противодействию отмыванию денег. *Ripple* не просто уплатила штраф, но и пошла на тесное сотрудничество с регулятором. Она зарегистрировалась в *FinCEN*, новые партии *XRP* распределяет только между пользователями с зарегистрировавшими свои счета и предоставившими о себе информацию. Компания также согласилась соответствовать требованиям по противодействию отмыванию денег и ввела позицию работника по мониторингу соответствия этим требованиям (*compliance*). Она также допустила внешний аудит и стала предоставлять данные о трансакциях регуляторам с целью их анализа[32].

В июне 2016 г. *Ripple* получила от Департамента финансовой службы Нью-Йорка, одного из самых сильных финансовых регуляторов в США, лицензию на продажу криптовалюты *XRP* институциональным инвесторам и финансовым институтам в этом штате. Годом ранее Нью-Йорк ввёл обязательное лицензирование цифровых активов.

Платёжную систему *Ripple* по всему миру тестируют около 90 банков, включая ведущие глобальные финансовые организации *Santander*, *Bank of America* и *Axis Bank*. Весной 2017 г. 47 крупнейших банков и финансовых компаний Японии протестировали пилотное использование технологии *Ripple* на базе облачной платформы *RC Cloud*. Эта платформа использует алгоритмы *Ripple* для денежных трансакций внутри национальной платёжной системы и для трансграничных трансакций. Ряд совместных с банками проектов компании из тестовой фазы перешёл в фазу коммерциализации. Весной 2018 г. южнокорейский банк *Woori Bank* протестировал возможности технологий *Ripple* для осуществления денежных переводов мигрантов.

* * *

Как следует из проведённого анализа, к настоящему времени ни одна из крупнейших криптосистем не достигла заявленных целей. Криптовалюта *bitcoin* не стала полноценными деньгами: она практически не используется для оплаты товаров и услуг, а высокая волатильность лишает её привлекательности для массового инвестора. Перспективы криптосистем *Ethereum* и *Ripple* слабо связаны с динамикой развития криптовалют.

Криптовалюты эффективно обслуживают интересы двух принципиально разных клиентел. Первую образует узкая прослойка пионеров цифровизации финансового сектора в лице программистов, инженеров-компьютерщиков, специалистов по криптографии и теории игр и действующих вместе с ними венчурных инвесторов, которые не только заметно повысили своё личное благосостояние, но и создали алгоритм постоянного притока в свои проекты инвестиционных ресурсов. Их интересы заключаются в поддержании максимально возможного информационного напряжения вокруг проблемы криптовалют, криптосистем и блокчейна.

Вторая клиентела сформирована из числа экономических агентов, занимающихся различного рода нелегальной и криминальной деятельностью. Они быстро воспользовались специфическими возможностями, поначалу преимущественно *bitcoin*, но в возрастающей степени и прочих криптовалют. С учётом возрастающего внимания

[32] The Ripple story. URL: https://blog.bitmex.com/the-ripple-story/ (accessed 20.08.2018).

регуляторов финансовых рынков к возникшему сектору криптовалют и псевдоанонимности последних интерес криминального бизнеса к их использованию может ослабнуть. Если это произойдёт, цена эмитированных средств может обрушиться, что нанесёт ущерб значительному числу неквалифицированных случайных инвесторов, инвестировавших в сектор на волне разогнанной в 2014–2018 годах криптомании. Такой сценарий не представляет значимого риска для финансовой системы в целом, тем не менее следует ожидать усиления надзора и контроля над развитием экосистемы криптоактивов со стороны регуляторов.

Список литературы

Buterin V. Introducing Ripple. A Detailed Look at Cryptocurrency's New Kid on the Block // Bitcoin Market Journal. 2013. URL: https://bitcoinmagazine.com/articles/introducing-ripple/ (accessed 24.08.2018).

Conti M., Kumar S., Lal C., Ruj S. A Survey on Security and Privacy Issues of Bitcoin // IEEE Communications Surveys & Tutorials. 2018. Vol. 20. No. 4. P. 3416–3452.

Foley S., Karlsen J. R., Putnins, Talis J. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? // Review of Financial Studies. 2019. Vol. 32. No. 5. P. 1798–1853. DOI: 10.2139/ssrn.3102645

Gencer A.E., Basu S., Eyal I., van Renesse R., Sirer E.G. Decentralization in Bitcoin and Ethereum Networks. 2018. URL: arXiv:1801.03998v2

Grishchenko I., Maffei M., Schneidewind C. A Semantic Framework for the Security Analysis of Ethereum smart contracts // International Conference on Principles of Security and Trust. Springer, Cham, 2018. P. 243–269.

He D., Habermeier K., Leckow R., Vikram H., Almeida Y., Kashima M., Kyriakos-Saad N., Oura H., Saadi Sedik T., Stetsenko N., Verdugo-Yepes C. Virtual Currencies and Beyond: Initial Considerations. IMF Staff Discussion Note, January 2016. 42 p.

Hirai Y. Defining the Ethereum Virtual Machine for Interactive Theorem Provers // Financial Cryptography and Data Security. FC 2017. Lecture Notes in Computer Science / ed. by M. Brenner et al. Springer, Cham, 2017. P. 520–535.

Huberman G., Leshno J.D., Moallemi C.C. Monopoly without a monopolist: An Economic analysis of the bitcoin payment system. Bank of Finland Research Discussion Paper. 2017. No. 27/2017. 53 p.

Lin I., Liao T. A Survey of Blockchain Security Issues and Challenges // International Journal of Network Security. 2017. Vol. 19. No. 5. P. 653–659.

Silk Road and Bitcoin. GDPO Situation Analysis. Swansea University, December 2013. 4 p.

FINTECH ECOSYSTEM
THE LARGEST PRIVATE CRYPTOSYSTEMS

STANISLAV ZHUKOV
IVAN KOPYTIN
ALEXANDER MASLENNIKOV
Primakov Institute of World Economy and International Relations, Russian Academy of Sciences, Moscow, 117997, Russian Federation

Abstract

Crisis of traditional financial system and the wave of technological innovations supported the accelerated formation of the global cryptocomplex. The complex is rapidly evolving, by the end of July 2018 there were about 1700 cryptoprojects globally. The cryptocomplex includes separate cryptosystems linked into a

single network via cryptocurrencies trade. The article reveals economic nature and business models of the three largest and most famous cryptosystems – Bitcoin, Ethereum и Ripple, which are responsible for about 70% of the global cryptocomplex capitalization. Though Bitcoin and Ethereum try to create the alternative to the traditional financial system, Ripple proposes new cutting edge technological and effective decisions for the existing banking and payments systems. The authors show that the largest global private cryptosystem Bitcoin, whose goal is substitution of fiat money with bitcoin cryptocurrency, in reality is far away from the ideal system of distributed money, which automatically maintains deals between peers via the neutral computer code. Bitcoin, as well as other systems of cryptocurrencies, has inherent hierarchy and vivid monopoly effects. De-facto control over the Bitcoin functioning rests with the largest players, who replaced the central bank. These players are the main beneficiaries of recurrent rise in capitalization of cryptocurrencies. The strategic task of making bitcoin an alternative to fiat money as a mean of payments has failed. Due to the excessive price volatility bitcoin failed to become a worthy alternative to fiat money and traditional assets as a mean of saving for broad categories of investors. Ethereum and Ripple business models are weakly linked to the dynamics of cryptocurrencies development, serving these systems. Ethereum business model provides for maximization of incomes, rents and other benefits for the system creators from its extensive development. Ripple made an economic bet on selling its special digital solutions to traditional players in financial markets. The authors make a conclusion that cryptocurrencies effectively serve interests of the two clienteles. First are the pioneers of financial sector digitalization, including computer programmers, computer engineers, cryptography and game theory experts as well as venture investors working in parallel. Second are economic agents engaged into various illegal and criminal activities. The authors forecast that given the policies of financial markets regulators the pseudo anonymity of transactions in the sector of cryptocurrencies will cease to exist in the nearest future.

Keywords:

cryptosystem; cryptocurrency; Bitcoin; Ethereum; Ripple; bitcoin; ether; XRP; blockchain.

References

(2013). Silk Road and Bitcoin. GDPO Situation Analysis. Swansea University. 4 p.

Buterin V. (2013). Introducing Ripple. A Detailed Look at Cryptocurrency's New Kid on the Block. *Bitcoin Market Journal*. URL: https://bitcoinmagazine.com/articles/introducing-ripple/ (accessed 24.08.2018).

Conti M., Kumar S., Lal C., Ruj S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*. Vol. 20. No. 4. P. 3416–3452.

Foley S., Karlsen J. R., Putnins, Talis J. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? *Review of Financial Studies*. Vol. 32. No. 5. P. 1798–1853. DOI: 10.2139/ssrn.3102645

Gencer A.E., Basu S., Eyal I., van Renesse R., Sirer E.G. (2018). Decentralization in Bitcoin and Ethereum Networks. URL: arXiv:1801.03998v2

Grishchenko I., Maffei M., Schneidewind C. (2018). A Semantic Framework for the Security Analysis of Ethereum smart contracts. In: *International Conference on Principles of Security and Trust*. Springer, Cham. P. 243–269.

He D., Habermeier K., Leckow R., Vikram H., Almeida Y., Kashima M., Kyriakos-Saad N., Oura H., Saadi Sedik T., Stetsenko N., Verdugo-Yepes C. (2016). *Virtual Currencies and Beyond: Initial Considerations*. IMF Staff Discussion Note. 42 p.

Hirai Y. (2017). Defining the Ethereum Virtual Machine for Interactive Theorem Provers. In: Brenner M. et al. (eds) *Financial Cryptography and Data Security. FC 2017. Lecture Notes in Computer Science*. Springer, Cham. P. 520–535.

Huberman G., Leshno J.D., Moallemi C.C. (2017). *Monopoly without a monopolist: An Economic analysis of the bitcoin payment system*. Bank of Finland Research Discussion Paper. No. 27/2017. 53 p.

Lin I., Liao T. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*. Vol. 19. No. 5. P. 653–659.