

МОНОГРАФИЯ

ФИНАНСОВЫЙ  
УНИВЕРСИТЕТ  
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Г. О. Крылов  
В. М. Селезнев

# ПРОБЛЕМЫ БЕЗОПАСНОСТИ ОБОРОТА ЦИФРОВЫХ ФИНАНСОВЫХ АКТИВОВ В КРИПТОЭКОНОМИКЕ



УДК 330.88:004.738.5:336.747.5

ББК 65.26

К 85

**Рецензенты:**

*Ревенков П. В.* — доктор экон. наук, профессор, заместитель начальника Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности ЦБ РФ;

*Кубанков А. Н.* — доктор военных наук, кандидат технических наук, зав. кафедрой безопасности радиосвязи Московского технического университета связи и информатики, профессор, Заслуженный работник связи Российской Федерации;

*Леонов П. Ю.* — кандидат экономических наук, доцент, Генеральный директор ООО АУДИТ-УНИВЕРСАЛ.

**Крылов Г. О., Селезнев В. М.**

**К 85** Проблемы безопасности оборота цифровых финансовых активов в криптоэкономике: Монография / Г. О. Крылов, В. М. Селезнев. — М.: Прометей, 2020. — 348 с.

ISBN 978-5-907244-98-6

В монографии изложены проблемы безопасности оборота цифровых финансовых активов (криптовалюты) в криптоэкономике и международный опыт его регулирования.

Издание предназначено для бакалавров, магистрантов, аспирантов, а также для научных работников, преподавателей, сотрудников правоохранительных органов, изучающих проблемы информационной безопасности финансово-экономических систем.

© Крылов Г. О., Селезнев В. М.,  
2020

© Издательство «Прометей»,  
2020

ISBN 978-5-907244-98-6

# ОГЛАВЛЕНИЕ

|                                                                    |     |
|--------------------------------------------------------------------|-----|
| Определения, обозначения и сокращения.....                         | 5   |
| Предисловие .....                                                  | 8   |
| Введение.....                                                      | 9   |
| Глава 1. История и эволюция блокчейн-технологии .....              | 10  |
| 1.1. Генезис блокчейн-технологии и виртуальной валюты ..           | 11  |
| 1.2. Исследования и применения блокчейн-технологии ....            | 14  |
| 1.3. Предварительный прогноз внедрения блокчейн-технологии .....   | 18  |
| 1.4. Инновации в финансовых системах учета .....                   | 20  |
| 1.5. Возможные направления использования блокчейн-технологии ..... | 34  |
| <i>Выводы по главе 1</i> .....                                     | 47  |
| Глава 2. Анализ атак на блокчейн и защиты от них .....             | 49  |
| 2.1. Особенности транзакций и принципа работы блокчейн .....       | 49  |
| 2.2. Алгоритмы криптовалют .....                                   | 54  |
| 2.3. Обзор потенциальных кибератак на криптовалюты ....            | 59  |
| 2.4. Оценка стоимости атак .....                                   | 77  |
| 2.5. Возможные виды защиты.....                                    | 89  |
| <i>Выводы по главе 2</i> .....                                     | 102 |
| Глава 3. Сравнение волатильности криптовалют и фиатных денег ..... | 104 |
| 3.1. Выбор вида криптовалют для расчета волатильности .....        | 104 |
| 3.2. Выбор прогнозных методов и моделей .....                      | 105 |
| 3.3. Анализ методом простой исторической волатильности (SHV) ..... | 108 |
| 3.4. Анализ методом GARCH-модели .....                             | 127 |
| Итоговые оценки волатильности по GARCH(1,1) .....                  | 141 |
| 3.5. Сравнение аналитических значений волатильности .....          | 141 |
| <i>Выводы по главе 3</i> .....                                     | 143 |

|                                                                                  |            |
|----------------------------------------------------------------------------------|------------|
| <b>Глава 4. Блеск и нищета блокчейн-технологии .....</b>                         | <b>144</b> |
| 4.1. Декларируемые свойства блокчейна .....                                      | 145        |
| 4.2. Блокчейн как «базовая технология» .....                                     | 148        |
| 4.3. Внедрение блокчейна и теория диффузии инноваций ..                          | 150        |
| 4.4. Проблемы консенсуса, доверия и определения<br>блокчейна .....               | 151        |
| 4.5. Блокчейн и традиционные институты .....                                     | 160        |
| <i>Выводы по главе 4</i> .....                                                   | 161        |
| <b>Глава 5. Международный опыт правового регулирования<br/>криптовалют .....</b> | <b>163</b> |
| 5.1. Международный терминологический разнобой .....                              | 163        |
| 5.2. Существующие законодательные определения .....                              | 166        |
| 5.3. Основные нормативные правовые акты в разных<br>странах .....                | 169        |
| 5.4. Государственное регулирование криптовалют .....                             | 171        |
| 5.5. Международное правовое регулирование<br>криптовалют .....                   | 174        |
| <i>Выводы по главе 5</i> .....                                                   | 189        |
| <b>Глава 6. Рекомендации ФАТФ в сфере оборота<br/>криптовалют .....</b>          | <b>190</b> |
| 6.1. Разработки ФАТФ для провайдеров услуг<br>виртуальных активов .....          | 190        |
| 6.2. Сфера применения стандартов ФАТФ .....                                      | 204        |
| 6.3. Применение стандартов ФАТФ в странах<br>и в компетентных органах .....      | 224        |
| 6.4. Рекомендации ФАТФ провайдерам услуг<br>виртуальных активов .....            | 280        |
| 6.5. Риск-ориентированный подход к регулированию<br>оборота криптовалют .....    | 294        |
| <i>Выводы по главе 6</i> .....                                                   | 316        |
| <b>Заключение .....</b>                                                          | <b>318</b> |
| <b>Библиографический список .....</b>                                            | <b>322</b> |
| <b>Приложение .....</b>                                                          | <b>342</b> |

## ПРЕДИСЛОВИЕ

Монография подготовлена в соответствии с государственным образовательным стандартом с учетом достижений в области финансового мониторинга, на основе анализа действующего законодательства и международной практики.

В монографии исследуется история и эволюция блокчейн-технологии, проводится анализ атак на блокчейн и способы защиты от них, показаны результаты сравнения волатильности ведущих фиатных денег и цифровых финансовых активов, которые в международной практике получили сленговое название криптовалют. Далее проводится сравнение достоинств и недостатков блокчейн-технологий, оцениваются перспективы применения, анализируется международный опыт правового регулирования оборота криптовалют и приводятся Рекомендации ФАТФ провайдерам услуг виртуальных активов.

Монография может использоваться студентами высших учебных заведений, обучающихся по направлению «Информационная безопасность», равно как по направлению «Финансы и кредит».

Авторы выражают признательность рецензентам — Заместителю начальника Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России, доктору экономических наук Павлу Владимировичу Ревенкову и доктору военных наук, кандидату технических наук, профессору, заслуженному работнику связи РФ, заведующему кафедрой безопасности радиосвязи Московского технического университета связи и информатики Александру Николаевичу Кубанкову, а также кандидату экономических наук, доценту Генеральному директору ООО АУДИТ УНИВЕРСАЛ Павлу Юрьевичу Леонову — за ценные замечания, помощь и поддержку при подготовке монографии.

## **ВВЕДЕНИЕ**

Стремление бизнеса взаимодействовать без посредников привело к созданию блокчейн-технологии, реализующей децентрализованную инфраструктуру распределенных реестров, в которой достижение консенсуса участников потребовало применения криптографических протоколов и породило вознаграждение победителям состязательных процессов в виде программных кодов на материальных носителях, получившее название цифровых финансовых активов (криптовалюты).

С появлением криптовалюты вошло в практический оборот понятие криптоэкономики, которую можно определить как деятельность по проектированию и созданию децентрализованных систем, работа которых основана на экономических стимулах и криптографии.

Вместе с тем, оборот цифровых финансовых активов в криптоэкономике требует решения многих проблем информационной и экономической безопасности, связанных с атаками на распределенные реестры, и, особенно, с их волатильностью, анонимностью и трансграничностью. Последние, как показала практика, приводят к отмыванию преступных доходов и финансированию терроризма.

Внедрение цифровых финансовых активов существенно сдерживается несовершенством национальных и международных нормативных правовых актов, регулирующих их оборот в разных юрисдикциях. Единственное, что объединяет разные юрисдикции, это стремление противодействовать отмыванию денег и финансированию терроризма в соответствии с Рекомендациями Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ).

Рассмотрению этих проблем в монографии посвящены соответствующие главы.

## Глава 1

# ИСТОРИЯ И ЭВОЛЮЦИЯ БЛОКЧЕЙН-ТЕХНОЛОГИИ

---

В 2000 году Окинавская хартия глобального информационного общества провозгласила наступление нового этапа развития социума и биосферы. Человечество вступило в эпоху информационного общества, в котором господствующей социальной группой становятся производители и владельцы информации и новых информационных технологий - инициаторы промышленных революций. Создана всемирная информационная паутина. Мир неуклонно приближается к формированию ноосферы, которую гениально предвосхитил Владимир Иванович Вернадский. Четвертая промышленная революция стремительно меняет человеческое общество. Нано- и биотехнологии, искусственный интеллект, робототехника, интернет вещей, виртуальная и дополненная реальность на протяжении жизни одного поколения на глазах трансформируют общество. Феноменальный взлет и падение первой и ведущей криптовалюты биткоин стал возможен в результате действия доверившихся новым информационным технологиям миллионов людей, стремящихся избавиться от посредников и комиссионных издержек при взаимных расчетах.

В связи с интенсивным развитием информационных технологий, государствам необходимо адекватно реагировать на изменения в инфосфере и связанные с ними новые общественные отношения. Такие криптосистемы как Биткоин являются общепланетарными децентрализованными системами и не подконтрольны государствам в силу анонимного и трансграничного характера своего функционирования. Поэтому работа правоохранительных органов

и связанных с ними структур существенно осложнилась. Несмотря на то, что биткойн существует уже более 10 лет, на сегодняшний день отсутствуют инструменты, позволяющие отделить законные операции от незаконных, прежде всего от незаконных операций по наркобизнесу, отмыванию преступных доходов, подготовке заказных убийств, финансированию терроризма.

Виртуальные валюты и схожие с ними технологии способны создать более быстрые и дешёвые финансовые услуги, а также могут стать мощным инструментом для распространения финансовых услуг в развивающихся странах, равно как реализовать противодействие неправомерным и политически ангажированным санкциям, как, например, в Венесуэле во взаимоотношениях с США.

Проблема состоит в том, как воспользоваться всеми известными преимуществами и при этом не допустить их незаконное использование, включая наркобизнес, отмывание денег, финансирование терроризма, а также уклонение от уплаты налогов и от контроля за оборотом капитала.

Для исследования этой проблемы следует обратиться к истории и эволюции блокчейн-технологий, породивших криптовалюту и другие виртуальные валюты, провести анализ социальных предпосылок успехов и неудач их применения.

## **1.1. Генезис блокчейн-технологии и виртуальной валюты**

Первые объекты, которые принято относить к виртуальным деньгам, появились, как суррогат для внутренних расчетов в закрытых и удаленных сообществах, а впоследствии как система лояльности, в виде бумажных талонов и купонов ещё в середине XIX века. Дальнейшее развитие концепция получила в контексте постепенной цифровизации человеческой деятельности. В частности, внедрение цифровых электронно-вычислительных машин в банковской деятельности началась на самой заре компьютерной эры, в 1965 году, привела к тому, что большинство традиционных финансовых активов с 80-х годов хранятся в цифровом виде.

Следующим шагом в развитии виртуальных денег стало изобретение цифрового кошелька, изначально связанного с носителем, чиповой картой, что позволило создать системы с локальным хранением средств. Пик популярности электронных кошельков на базе чиповой карты пришелся на середину 90-х и был связан с системой Mondex. В 1982 году признанный ученый-криптограф Дэвид Чаум впервые предложил схему анонимных платежей, основанных на публичной криптографии и, в 1989 году, основал на базе своих научных разработок, платежную схему eGold, не достигшую, впрочем, большого успеха. Значительный вклад в популяризацию денежных суррогатов и виртуальных валют, внесли онлайн игры.

Первая виртуальная валюта в онлайн играх появилась в 1999 году, соответственно, одновременно с этим появились и сервисы, которые позволяли обменивать реальные денежные средства на игровую валюту, и наоборот обналичивать игровую виртуальную валюту, тем самым придав ей квазиправомерный вид в форме реальных денежных средств [1]. Несмотря на многолетнее развитие виртуальных игровых валют, тем не менее, наиболее сильным рынком к середине 2000-х стал не рынок внутриигровых валют, а внешний, по отношению к разработчикам, рынок «артефактов» иначе «цифровых товаров» для таких игр, как например, World of Warcraft. По мере технологического развития понятия «цифровой валюты» и «электронных денег» создавались элементы и предпосылки для технологического подхода блокчейна, криптовалют и распределенных реестров. Следует отметить, впрочем, что в равной степени на изобретение блокчейна повлияли успехи распределенной анонимной сети хранения и обмена файлов bittorrent.

В 2008 году 18 августа было зарегистрировано доменное имя bitcoin.org, а уже 31 октября был опубликован документ «Bitcoin P2P e-cash paper», который представил миру первый современный цифровой товар Биткойн (англ. *bit* — единица измерения количества информации, *coin* — монета), получивший сленговое названия вир-

туальной валюты (криптовалюты). Вслед за ним стали бурно развиваться и другие криптовалюты.

Биткойн [2] одноранговая пиринговая система цифровой виртуальной валюты (**криптовалюты**), в которой **блокчейн** (англ. *Blockchain* — цепочка блоков) **является ключевой инновацией**. По сути, блокчейн представляет собой специализированную распределенную базу данных, предназначенную для обработки упорядоченных во времени данных, таких как финансовые транзакции. Основной элемент блокчейнов встроенная безопасность отличает их от обыкновенных горизонтально масштабируемых баз данных, таких как MySQL Cluster, MongoDB и Apache HBase. Безопасность блокчейна означает практическую невозможность удалить или изменить записи в базе данных; более того, безопасность обеспечивается не за счет централизованной проверки (что возможно для перечисленных выше баз данных), а за счет самого протокола блокчейна. Распределенность и децентрализация блокчейнов делает их привлекательной заменой для существующих решений, используемых, например, в финансовом секторе. Недостатки блокчейнов, такие как сравнительно медленное подтверждение транзакций и меньший уровень масштабируемости, для многих приложений не настолько важны, как возрастающий уровень безопасности и отсутствие точек отказа (англ. *single point of failure*). По словам Ника Сабо (Nick Szabo), изобретателя идеи смарт-контрактов, «настоящие финансовые инструменты уже в некоторой степени децентрализованы благодаря “человеческому блокчейну”, состоящему из бухгалтеров, аудиторов и т. п., проверяющих работу друг друга» [3]. Таким образом, автоматизация операций, производимых этой цепочкой при условии сохранения децентрализации, может стать шагом в правильном направлении. Финансовые учреждения и другие организации, работающие с реестрами данных, не спешат пользоваться блокчейном биткойна (самым развитым публичным блокчейном) или другими общественно доступ-

ными блокчейнами. Этому существует несколько причин, например, соответствие законам.

Авторы технологии утверждают, что решения на основе Blockchain (блокчейнов) одно из ключевых современных направлений исследований для финансовых и государственных учреждений. Нет сомнений в том, что костяк технологий, используемых в настоящее время в таких учреждениях, морально устарел и требует реорганизации для соответствия текущим требованиям. Децентрализованные и распределенные реестры в виде блокчейнов на данный момент являются одними из наиболее обсуждаемых решений описанной проблемы. В данной работе описываются системы на основе блокчейнов с эксклюзивным доступом к обработке транзакций (англ. *permissioned*), которые могут послужить основой для создания надежных финансовых баз данных или временно упорядоченных реестров документов. В работе рассматриваются варианты обоснования доступности протокола и данных блокчейн-систем для конечных пользователей; такой доступ позволяет достичь более высокого уровня децентрализации и прозрачности.

По ряду признаков, мировой бизнес очень узко смотрит на Bitcoin. Видит его как набирающего обороты конкурента, не понимая, что это всего лишь воплощение варианта новой, более совершенной информационной технологии для финансового сегмента всего мира.

Bitcoin — это сеть выполняющая роль финансовой системы, основой которой является технология blockchain (децентрализованная база данных о транзакциях в сети). В основе лежит технология так называемой несимметричной криптографии. Это уже опробованная в рабочем режиме финансовая система с объемами транзакций в миллиарды долларов США. Её код открыт и за 7 лет никто так и не смог её взломать (по утверждениям специалистов из США). По информации разработчиков, использование готового и опробованного в работе инструмента существенно сэкономит время и средства для успешного

старта вашей финансовой системы/финансовой модели предприятия/электронной валюты.

## **1.2. Исследования и применения блокчейн-технологии**

Начало активного применения технологии Blockchain (блокчейнов) совпадает с развитием несимметричной криптографии, как публичного сервиса, обеспечивающего идентификацию, авторизацию, принцип «неотказуемости» и другие необходимые для развития публичных электронных услуг, в т. ч. электронных и мобильных банковских технологий в информационном пространстве и глобальных информационных сетях (в т. ч. Интернет).

В 2013 году отдельная команда российских специалистов-энтузиастов занялась исследованиями технологии blockchain (основы существования сети Bitcoin). Цель исследования: проверка применимости технологий, лежащих в основе Bitcoin, и формирование решений для финансового сегмента бизнеса.

Начали с изучения следующих данных: открытого исходного кода криптовалюты на github, затем наблюдения за развитием Bitcoin с зимы 2012 года, следующий шаг — изучение теоретических данных. Информация, собранная группой, позволила увидеть огромный потенциал Blockchain не как противника имеющейся финансовой системы, а как новой эволюционной вехи финансовой системы мира.

С 2014 года тема баз данных на основе блокчейнов стала популярной среди банков и других финансовых учреждений. Было анонсировано несколько прототипов и моделей с использованием технологии блокчейна. В некоторых случаях, блокчейн биткойна используется напрямую:

- Эстонский LHV Bank тестирует Cuber (Cryptographic Universal Blockchain Entered Receivables), систему платежей, основанную на окрашенных монетах (англ. colored coins), организованных поверх биткойновского блокчейна [4].

- Аналогично, биржа NASDAQ планирует [5] использовать один из протоколов покраски биткойнов Open

Assets Protocol для обеспечения полного цикла управления ценными бумагами [6].

- Крупнейший французский банк BNP Paribas, по некоторым сведениям, исследуют возможные способы интегрировать биткойн в валютные запасы банка [7].

- Британский банк Barclays заключил партнерство с биткойновской биржей Safello для исследования возможных приложений блокчейн-технологии в финансовом секторе [8].

- Goldman Sachs опубликовал отчет «Будущее финансов: революция способов оплаты в грядущем десятилетии», в котором подразумевается, что биткойн и криптовалюты в целом могут изменить платежную экосистему [9]. Goldman Sachs также принял участие в финансировании общим объемом 50 млн долларов биткойновского стартапа Circle [10].

- Компания UBS, базирующаяся в Швейцарии, считает производные биткойна потенциально привлекательными, при условии принятия соответствующей юридической базы [11].

В некоторых других прототипах задействованы системы Ripple или Ethereum:

- Протокол Ripple был интегрирован с немецким банком Fidor, а также с CBW Bank из Канзаса и банком Cross River из Нью-Джерси [12]. Согласно словам Giles Gade, CEO и президента Cross River, одной из главных мотиваций использовать именно Ripple стало соответствие системы законам США.

- Три австралийских банка Commonwealth Bank of Australia (CBA), Westpac Banking Corporation [13], а также Australia and New Zealand Banking Group экспериментируют с платежами через протокол Ripple [14]. David Whiteing, CIO банка CBA, назвал отсутствие встроенных токенов в Ripple как ключевую причину, по которой система была выбрана вместо биткойна.

- Компания UBS анонсировала эксперименты с блокчейном Ethereum с целью построения полностью автоматизированных бондов [15]. Alex Batlin, директор по инно-

ваниям и исследованиям UBS, не исключил возможности использования биткойновского блокчейна для схожих задач. Однако в большинстве случаев финансовые учреждения готовы строить свои собственные закрытые блокчейны или исследуют блокчейн-технологии без указания конкретной реализации:

- Три крупных нидерландских банка ABN Amro, ING и Rabobank исследуют использование блокчейна для платежных систем [16].

- Компания Citigroup построила три закрытых блокчейна и внутреннюю валюту на их основе, фокусируясь на платежах и исключении рисков при сделках с мелкими местными банками [17]. Помимо этого, Citigroup заключила партнерство с Safaricom, мобильным оператором из Кении, для того чтобы обеспечить денежные переводы без необходимости открытия счета в банке.

- Santander, один из крупнейших банков мира согласно рейтингу Форбс [18], выделил от 20 до 25 возможных применений блокчейн-технологии в банковском деле, включая международные денежные переводы, синдицированные займы и управление залогами обязательствами [19].

- Аналогично, Deutsche Bank заявил, что у распределенные систем учета и у блокчейнов есть применения в работе с фиатными валютами и ценными бумагами; они подходят для создания прозрачных систем и упрощения наблюдения согласно системам противодействия, отмыванию денег / Know Your Customer [20].

- Финансовое управление Сингапура назвало блокчейны одним из главных трендов технологий, которые могут затронуть финансовые сервисы. Низкая стоимость, более высокая скорость разработки и отказоустойчивость были названы главными преимуществами блокчейн-систем по сравнению с традиционными подходами [21].

Решения на основе блокчейнов используются не только для построения распределенных систем финансового учета. Схожее приложение Интернет вещей (англ. Internet of

Things) разрабатывается компаниями IBM и Samsung [22]. Проект под названием ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) использует протокол Ethereum для создания смарт-контрактов. Другой проект IBM также нацелен на создание платформы для смарт-контрактов и рассчитан в первую очередь для людей без доступа к традиционной банковской инфраструктуре [23].

Блокчейн достаточно часто упоминается в финансовой среде как технология, способная преобразить будущее платежей:

- Блокчейн упоминается в двух глобальных сдвигах, которые произойдут в ближайшем будущем, согласно исследованию Всемирного экономического форума [24].

### **1.3. Предварительный прогноз внедрения блокчейн-технологии**

Первый сдвиг — первый государственный налог, собранный с использованием блокчейнов, предположительно произойдет в 2023 году. Второй сдвиг — хранение более чем 10 % мирового ВВП на блокчейнах состоится до 2027 года.

- Банк Англии опубликовал отчет, в котором утверждается, что технологии распределенных финансовых систем учета представляет собой фундаментальное изменение правил работы платежных систем [25].

- Blythe Masters, CEO компании Digital Asset Holdings, сравнила блокчейн с электронной почтой для денег [26].

- Согласно словам, CIO Standard Chartered Anju Patwardhan, инфраструктура на основе блокчейна может сделать финансовые транзакции более надежными и отслеживаемыми, в то же время уменьшив их стоимость для конечных потребителей и упростив противодействие отмыванию денег [27].

- Usama Fayyad, chief data officer банка Barclays, назвал блокчейн революционной технологией для финансового сектора [28].

Общее отношение финансовых учреждений к биткойну и прочим общедоступным блокчейнам остается достаточно скептическим, в то время как мнения насчет закрытых блокчейнов или блокчейнов с регулируемым доступом в целом намного теплее. Основные причины сомнений в целесообразности использования общедоступных блокчейнов в финансовой среде заключаются в следующем:

- Невозможность контролировать обработку транзакций (т. е. майнеров в случае биткойна). В соответствии со многими юрисдикциями, личности обработчиков транзакций должны быть известными, что прямо противоречит декларируемой биткойном открытости (любой человек может быть майнером, достаточно иметь вычислительные ресурсы). Согласно CEO Metro Bank Craig Donaldson, отсутствие четко определенных правил для сервисов, работающих с биткойном, замедляет их потенциал развития.

- Учреждения видят угрозу конфиденциальности клиентов в публичной среде.

- Системы с ограниченным доступом могут быть эффективнее в плане тестирования, для быстрого внесения изменений в протокол блокчейна и т. п.

- Доказательство работы, фундаментальное для биткойна, в случае закрытых блокчейнов является в большой степени избыточным; избавление от него позволяет повысить поток обрабатываемых транзакций и сократить расходы на функционирование.

В финансовой среде существуют биткойн-оптимисты, например один из основателей LinkedIn, миллиардер Reid Hoffman [29]: «По крайней мере одна глобальная криптовалюта достигнет массового рынка. Этой валютой будет либо биткойн, либо производная валюта, вдохновленная биткойном». Аналогично, Richard Gendal Brown, СТО компании R3 CEV, которая занимается блокчейн-инновациями, предупреждает насчет игнорирования биткойна в пользу распределенных систем с ограниченным доступом: «Основная цель, заложенная в дизайн биткойна

быть цифровыми наличными деньгами с устойчивостью к цензуре имеет огромный потенциал, хороший и плохой; уже из-за одной этой возможности не стоит сбрасывать биткойн со счетов» [30].

#### **1.4. Инновации в финансовых системах учета**

В последние годы формируется тренд блокчейн-инноваций в системы, предназначенные специально для обеспечения финансовых сервисов нового поколения. Указанный ниже список компаний не является полным; для более детального анализа существующих решений, мы отсылаем читателя к отчету «Распределенные системы учета с ограниченным доступом» за авторством Tim Swanson [31].

- Digital Asset Holdings ([digitalasset.com](http://digitalasset.com)) строит распределенную многослойную систему для обработки трейдинга ценных бумаг. Наличие промежуточного уровня системы позволит использовать как блокчейн-решения, так и старую инфраструктуру вроде FedWire.

Фирма планирует использовать как открытые блокчейны (например, биткойн), так и закрытые, построенные на основе технологии Hyperledger [32].

- Компания Chain ([chain.com](http://chain.com)) предлагает коммерческую платформу на основе блокчейна с фокусом на передачу активов. Компания провела успешный раунд финансирования размером 30 млн долларов при поддержке крупных финансовых организаций, включая Visa, Nasdaq, Citi Ventures и Orange [33].

- R3 CEV ([r3cev.com](http://r3cev.com)) компания, специализирующаяся на инновациях в области построения глобальных финансовых сервисов нового поколения. R3 возглавляет партнерство между глобальными банками (включая Barclays, Credit Suisse, JP Morgan, UBS, BBVA, и Commonwealth Bank of Australia), целью которого является создание общей распределенной архитектуры финансовых систем учета [34].

- Компания Clearmatics ([clearmatics.com](http://clearmatics.com)) строит децентрализованную клиринговую сеть, которая позво-

лит пользователям производить обмен ценных бумаг и автоматизировать финансовые контракты при помощи технологии смарт-контрактов.

- Eris Industries ([erisindustries.com](http://erisindustries.com)) предоставляет решения с открытым исходным кодом, позволяющие финансовым учреждениям строить дешевую и качественную инфраструктуру, которая использует блокчейн и смарт-контракты.

- Компания Tembusu ([tembusu.sg](http://tembusu.sg)) разработала TRUST (Tembusu Reputation-based Universally Secure Transaction System) платформу для управления активами на основе блокчейна.

- Проект Enigma ([enigma.media.mit.edu](http://enigma.media.mit.edu)) создает облачную платформу с гарантированной безопасностью с использованием разделения секретов.

Помимо этого, компании, например, Factom ([factom.org](http://factom.org)), разрабатывают инфраструктуру для финансовых сервисов на основе биткойна. В отличие от блокчейнов, используемых в криптовалютах, компании, перечисленные выше, предлагают решения, которые соответствуют пожеланиям финансовых учреждений:

- Предложенные решения в целом используют группы известных сервисов для создания блоков транзакций. В большинстве случаев, интеграция блоков в цепь не использует доказательство работы, используемое в биткойне и других криптовалютах. По этой причине предложенные дизайны блокчейнов не используют встроенные в протокол монеты для вознаграждения создателей блоков.

- Доступ к блокчейну ограничен кругом финансовых учреждений, создавших его, и регулируемыми учреждениями.

- Алгоритм определения корректных транзакций более сложный по сравнению с используемым в биткойне; он в общем случае отображает особенности конкретных типов финансовых услуг. Часто, в блокчейн интегрируется язык сценариев, полный по Тьюрингу [35], с целью

реализации комплексных контрактов. Отметим, что язык сценариев в биткойне является намеренно неполным по Тьюрингу, так как язык с большим количеством ограничений предотвращает использование уязвимостей в процессе проверки транзакций.

**Технология и объекты блокчейна.** Адрес кошелька в блокчейн-технологии, уникальный идентификатор внутри системы для получения и отправки средств представляет собой 160-битный хэш от открытого ключа ECDSA ключевой пары. Пример адреса в сети Bitcoin: «1BitforkXSxd1JpPwq4NzNwN47Ags1voYK».

Всего 34 символа. Допускаются цифры, буквы нижнего и верхнего регистра. Первый символ внутри сети Bitcoin всегда равен «1». Оставшиеся 33 символа тот самый хэш от открытого ключа клиента.

Кстати первый символ кошельков задается в конфигурационном файле `./src/base58.h` в параметре: «PUBKEY\_ADDRESS». В примере адреса кошелька всегда просматривается название компании. Это настоящий адрес кошелька (есть специальные программы, которые могут позволить сгенерировать адрес кошелька с красивой фразой внутри).

Адреса кошельков не попадают в Blockchain до тех пор, пока на данный адрес не происходит поступление. Можно создавать неограниченное количество адресов кошелька локально, в систему попадет только адрес, через который была проведена хотя бы одна транзакция.

**Транзакция в технологии Blockchain.** Транзакция в технологии Blockchain — это основа системы, которая представляется в виде записи во встроенное в кошелек NoSQL хранилище.

Технология Blockchain использует NoSQL хранилище вместо обычной реляционной базы. Наименование СУБД «Berkeley db» (названа в честь университета Беркли, на базе которого была разработана первая версия данной СУБД). Важная особенность Berkeley db в том, что это встраиваемая БД реализованная в виде библиотеки. Тем

самым не требуется отдельное поднятие сервера СУБД для её работы.

Так как Berkeley db является NoSQL хранилищем (хранит записи вида: ключ — значение) достигается высокая производительность при работе с данными, которые можно вытащить по ключу.

Каждая транзакция содержит в себе следующие значения:

- Уникальный идентификатор транзакции (txid).

- Количество средств, пересылаемых в транзакции (amount).

- Размер комиссии за транзакцию (Fee).

- Количество подтверждений сетью транзакции (confirmations).

- Время создания транзакции в формате timestamp (time).

- Адрес отправителя.

- Адрес получателя.

- Тип транзакции: отправка средств, генерация новых средств (эмиссия).

Блок представляет из себя контейнер, в который производится запись новых транзакций в системе и заголовка содержащего основную информацию о блоке: хэш блока, хэш предыдущего блока, хэш транзакций (вошедших в данный блок). Именно появление такого объекта как блок составляет основу технологии Blockchain.

Blockchain в переводе — цепочка блоков, именно как написано в названиее, так и реализована технология. Блоки хранят транзакции, а также информацию, которая позволяет создавать цепочку. Достигается это наличием информации о хэше предыдущего блока в заголовке нового генерируемого блока.

Блокчейн — распределенная база данных для обработки транзакций. Хотя в настоящее время большинство блокчейнов обрабатывают финансовые транзакции, в общем случае транзакции можно рассматривать просто как атомарные изменения состояния некоторой системы.