О криптографии и валютах в криптовалютах

Г.Б. Маршалко,
Д.М. Дыгин,
И.В. Лавриков

РусКрипто 2016
24.03.2016г.

Содержание доклада

Дисклэймер:

- Представленные в настоящем докладе материалы являются частным мнением докладчика (и частично – соавторов доклада), их не стоит трактовать как мнение какой-либо организации или организованной группы людей.
- Все факты являются вымышленными, совпадения с реально существующими мнениями являются случайными совпадениями.

- *Политические*, *экономические*, *юридические* и прочие *-ические* аспекты оставлены за рамками доклада.
  Но забывать про них не сто́ит.

Перейдём к пункту

Что такое деньги? Это небо?

Ok.. Google!

- Деньги – специфический товар максимальной ликвидности, который воплощает в себе несколько свойств: является инструментом обмена для товаров или услуг, служит универсальным эквивалентом стоимости других товаров и услуг, а также является удостоверением общественного характера частного труда товаропроизводителя.

Денежная система – это сложившееся исторически и закреплённое законодательством устройство денежного обращения в стране. Денежная система определяет денежный знак, имеющий хождение в данном государстве.

Виды денег

- **Действительные** деньги (выражены золотом, серебром или другими драгоценными металлами) – деньги, номинал которой соответствует реальной стоимости, то есть стоимости металла, из которых они изготовлены.
- **Фиатные** деньги (знаки стоимости, заменители реальных денег) – в том числе, виртуальные и электронные.

Исторически:

- товарные;
- обеспеченные;
- фиатные;
- кредитные.

Функции денег

- инструмент обмена
- мера стоимости
- средство обращения
- средство платежа
- средство накопления
- мировые деньги (внешнеторговые связи, международные займы, оказание услуг внешним партнёрам)

+ средство формирования сокровищ
+ функции мировых денег (взаимоотношения между экономическими субъектами)

Какие деньги зачем нужны

В большинстве стран фиатные деньги (в том числе, их электронный вариант) широко используются для реализации всех указанных функций денег.
Виртуальные деньги используются ограниченным кругом субъектов и, с формальной точки зрения, не являются номинированными в денежных знаках.

При чём здесь криптография?

Криптографические методы используются для обеспечения безопасности при хранении и использовании электронных денег.

- *Вообще говоря, можно придумать как с помощью криптографических методов обеспечивать какой-то из аспектов безопасности физически существующих фиатных денег, например, при реализации механизмов защиты от подделок.*

Что можно сказать здесь про криптографию

Ввиду законодательного регулирования данной области деятельности, методы, которые используются для обеспечения безопасности, обычно использует стандартизированные (на национальном или международном уровне) криптографические примитивы и механизмы, которым уделяется большое внимание научного сообщества в области криптографии, поэтому они обладают высокой репутационной стойкостью, а иногда и теоретически доказуемыми (доказанными) свойствами.

Перейдём к пункту

Есть ли вообще такое понятие "криптовалюта"?

Hey.. Siri!

Криптовалюты – электронный механизм обмена (у.е.?), цифровой актив, эмиссия и учёт которого зачастую децентрализованы. Функционирование системы происходит в рамках распределённой компьютерной сети.

Термин закрепился после статьи «Crypto Currency», опубликованной в 2011 году в журнале Forbes.

- более содержательный термин, на самом деле, исходно использованный – «электронная наличность» (от англ. electronic cash).

Ключевая особенность

Большая часть современных систем криптовалют привлекает новых пользователей отсутствием (даже необходимости создания) регулирующих органов. Таким образом, обеспечивается отсутствие возможности воздействия на транзакции любых участников системы, в том числе, обеспечивается необратимость сделок.

Ключевая особенность –> ключевая проблема?

Нет контролирующего органа –> как разрешать конфликты? –> коллегиальные решение? –> как бороться с пользователями-«нарушителями» режима? –> задача *о византийских генералах*!

Решение ключевой проблемы

- Задача византийских генералов обычно решается с использованием технологии блокчейн. Транзакции объединяются в блоки, из которых формируется цепочка блоков. Непрерывность цепочки обеспечивается включением в текущий блок значения хэш-кода предыдущего блока.

Можно ли выделить свойства криптовалют?

- отсутствие регулирующих или надзорных органов (автономность);
  - *при наличии некоторой воли – можно (нужно?) вводить регулирование в данной области..*
- обеспечение анонимности/псевдонимности пользователей;
- низкие издержки при проведении транзакций (если не учитывать средства, затраченные для процедуры майнинга);
- ?

Криптография в криптовалютах

Логичный вопрос:

Где же криптография то?!

Нелогичный ответ:

Криптография она повсюду в современном информационном пространстве.

- тогда причём тут крипто и прочие валюты?

Криптография ли в криптовалютах?

- С точки зрения обеспечения безопасности – используются классические механизмы: шифрование, протоколы, ключи, тунели, другие страшные слова.

~~В чём отличие от обычных электронных и виртуальных денег – история умалчивает~~

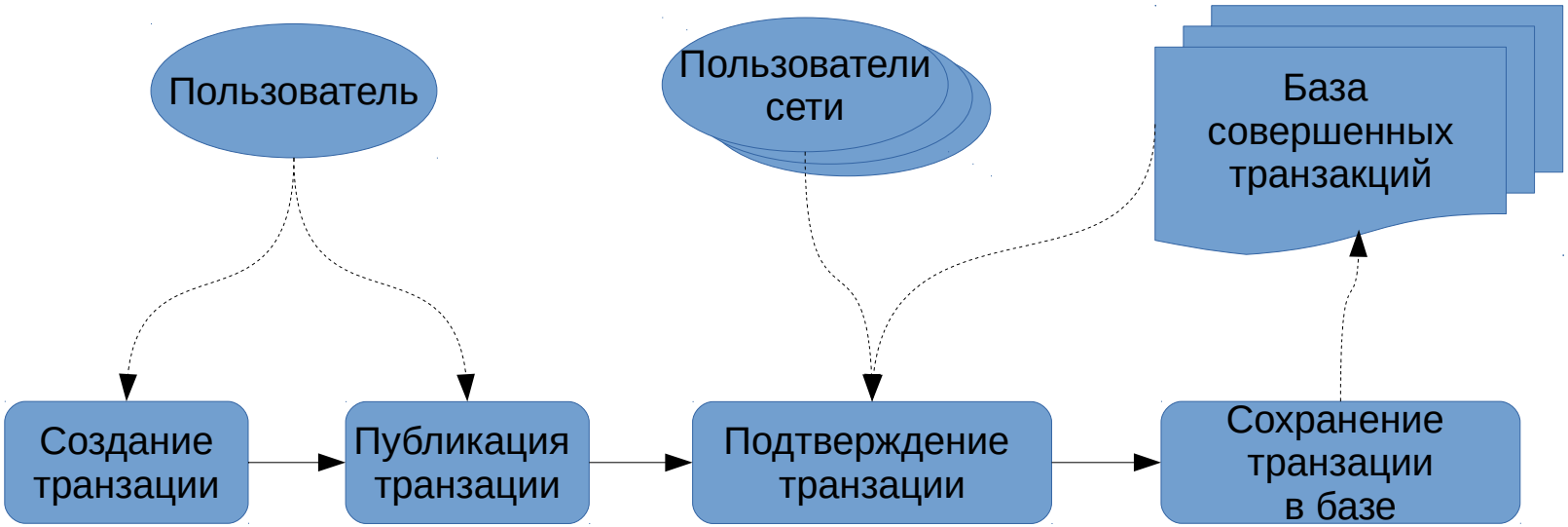
- Задача, на которой основывается процесс подтверждения транзакции (и иногда эмиссии), вообще говоря, может быть совершенно не криптографической.
- Вопросы голосования – сугубо алгоритмические, в основе решения – предположение о надёжности каналов передачи данных.

Зачем же криптография в криптовалютах?

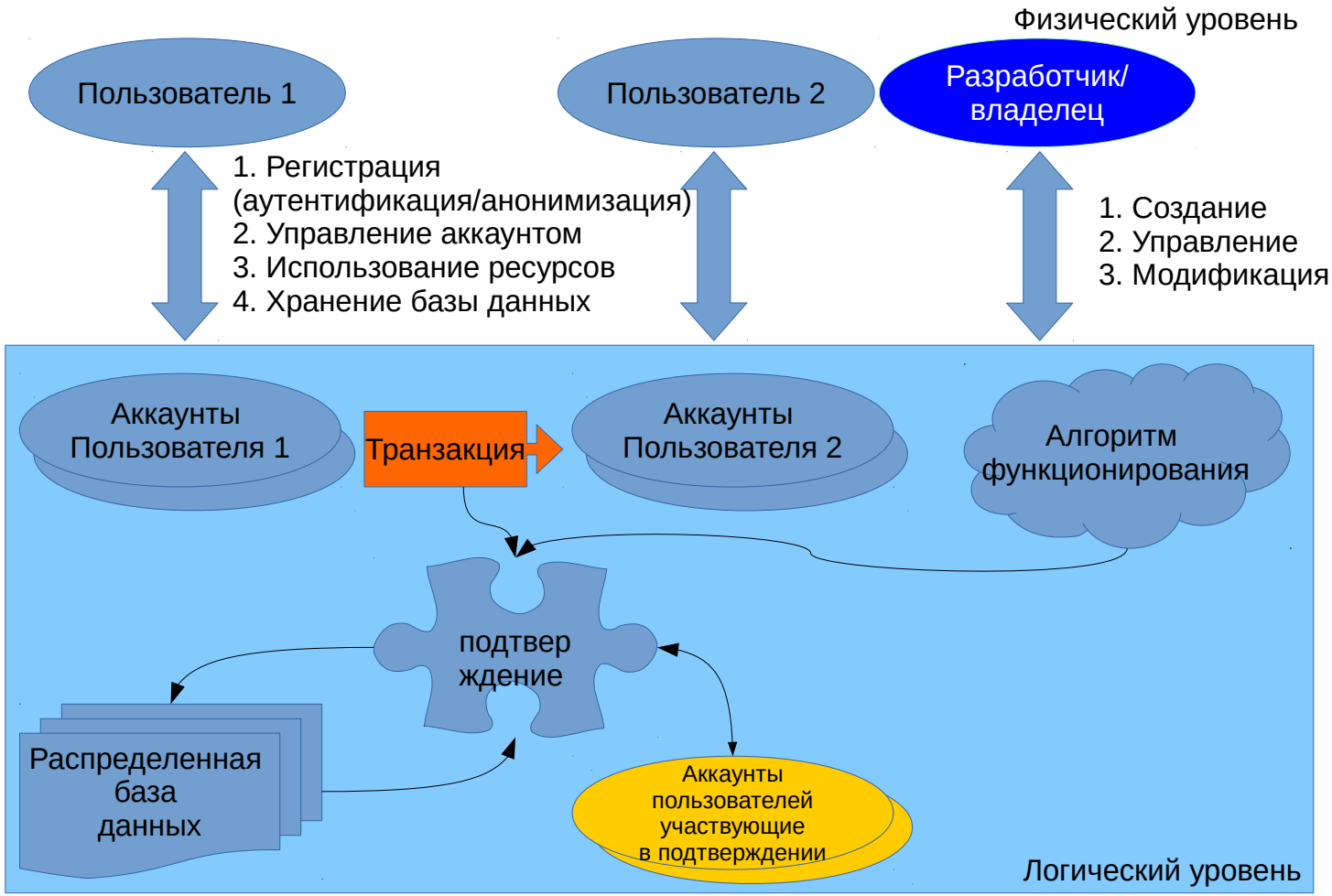
По всей видимости, всё дело в вере и заинтересованности людей:

- Драгоценные металлы редкие –> сложно добывать –> можно измерить необходимые трудозатраты –> ценность.
  Техника добычи развивается, а золото не дешевеет, удивительно...
- Криптографические задачи –> сложно решать –> математически оценить необходимые трудозатраты –> ценность (?).
  СВТ улучшаются, задачи усложняются, что будет с ценами...

Высокий уровень абстракции – транзакция в системе



Высокий уровень абстракции – уровни системы



Можно ли выделить функции криптовалют?

Hey, Cortana!

+ инструмент обмена
+ мера стоимости
+ средство обращения
+ средство платежа
+ средство накопления
? мировые деньги (внешнеторговые связи, международные займы, оказание услуг внешним партнёрам)
? средство формирования сокровищ
? функции мировых денег (взаимоотношения между экономическими субъектами)

Какие задачи и цели у криптовалют?

- Создание удобного децентрализованного средства создания, накопления и обмена vs. личная заинтересованность в накоплениях участников системы;
- Удешевление процесса осуществления транзакций vs. накопление “высвободившихся” средств у заинтересованных лиц;
- Добровольное привлечение ресурсов для решения сложных/интересных задач vs. создание распределённой сети взаимосвязанных узлов, которые теоретически можно использовать для противоправных действий;
- ?

Какие задачи могут решать криптовалюты?

- В первую очередь, те задачи, под которые данные системы разрабатывались: распределённые системы, неподконтрольные (частично подконтрольные) надзорным органам (в т.ч. администраторам системы), с увеличением их медийной поддержки всё чаще используются и принимаются в качестве средства платежа.
- Привлекаемые вычислительные ресурсы, вообще говоря, могут использоваться на благо человечества.
- В перспективе, построенные на идейных основах криптовалют системы вероятно могут заменить современные деньги (закон Коперника-Грешена?).

Что из всего этого следует?

- Криптовалюты в нынешнем виде дают больше вопросов, чем ответов.
- Закрывать глаза на их существование – нельзя, запретить их использование в условиях современного состояния информатизации всех сфер общественной жизни – крайне сложно (по крайней мере, в качестве средства накопления).
- Используемые технологии требуют интенсивного изучения и опробации, прежде чем можно будет говорить о возможности и целесообразности их использования при решении тех или иных задач.

Перейдём к пункту

На основании всего вышеизложенного...

Криптовалюты целесообразно разделять на две с половиной составляющие:

- финансовые вопросы;
- вопросы обеспечения безопасности;
- \+ криптографические вопросы.

С точки зрения финансов – они представляют собой почти законченную денежную систему. Вопросы принятия или неприятия её использования – за рамками.

С точки зрения обеспечения вопросов безопасности – все вопросы более менее решены, непонятно как в условиях децентрализации воплощать решения в жизнь.

С точки зрения криптографии – можно её использовать, а можно и не использовать.

Открытые вопросы:

- будут ли существующие криптовалюты долгожителями или «лопнут» в случае переключения внимания альтруистов на менее сомнительные вычисления?
- будет ли уровень комиссии за проведение транзакций достаточным для участия пользователей, не приведёт ли использование комиссии к «перекосам» в работе системы?
- будут ли пользователи привлекаться в системы, если в них не будут обеспечены исходные принципы (анонимность, децентрализованность и др.)?

Закрытые вопросы:

- криптовалюты существуют;
- криптовалюты широко используются;
- создать «новую» криптовалюту и даже привлечь в неё новых пользователей – представляется нетрудной задачей;
- законодательное регулирование работ с криптовалютами в процессе формирования и решения;
- \+ используемые механизмы могут быть применены при решении широкого класса, в том числе, криптографических задач.

Спасибо за внимание

Вопросы?