

КРИПТОВАЛЮТЫ ИХ ВИДЫ. КРИПТОВАЛЮТНЫЕ КОШЕЛЬКИ. СПОСОБЫ ЗАЩИТЫ КРИПТОВАЛЮТ.

Секацкая А.С.

Научный руководитель: Ковалькова И.А.

Белорусский национальный технический университет

Криптовалюта – это вид электронных денег, то есть математический код. Называется она так из-за того, что при обращении этих цифровых денег используются криптографические элементы, такие как электронная подпись. Но в отличие от таких систем, как Яндекс, Деньги или QIWI, криптовалюты неподконтрольны государству, а безопасность расчётов обеспечивается системой шифрования данных. Единицей измерения в этой системе считаются «койны» (буквально – «монеты»). Такие деньги существуют исключительно в цифровом виде.

«Выпуск» цифровых денег происходит различными способами: это и ICO (первичное размещение монет, система инвестирования), и майнинг (поддержание специальной платформы для создания новых криптовалют), и форжинг (образование новых блоков в уже имеющихся криптовалютах). То есть криптовалюта возникает буквально «из интернета».

Цифровые деньги впервые появились в 2008 году, а к настоящему времени их существует уже несколько тысяч разновидностей.

Их можно условно разделить на две категории:

1) Полностью основанные на исходном коде биткоина (например – Litecoin);

2) Имеющие исходный код, отличный от биткоина (например, Эфир).

Наиболее распространёнными видами криптовалют являются:

– *Биткоин* (BTC, bitcoin, на данный момент один биткоин эквивалентен примерно 6759 долларов США). Криптовалюта биткоин – это самая первая цифровая валюта, на основе которой разрабатывались все последующие. Разработчик биткоина (группа разработчиков) – Сатоши Накамото. Для этой валюты заявлен предел по количеству в 21 000 000 единиц, однако, в настоящее время он всё ещё не достигнут.

– *Эфириум* (ethereum, на данный момент равен примерно 400 долларов США). Это разработка российского программиста Виталия Бутерина. Появилась такая валюта сравнительно недавно – в 2015 году. Сейчас она довольно популярна наряду с биткоинами.

– *Лайткоин* (litecoin, LTC, на данный момент приравнивается примерно к 115 долларам США). Валюта разработана программистом Чарли Ли и выпускается с 2011 года. Лайткоин считается аналогом серебра среди криптовалюты (а биткоин – аналогом золота). Выпуск

лайткоинов, как и биткоинов, тоже лимитирован и составляет 84 000 000 единиц.

- *Зи-кэш*(Z-cash, эквивалентен примерно 182 долларам США).
- *Дэш*(dash, в эквиваленте составляет примерно 297 долларов США).
- *Риппл*(Ripple, 0,482 долларов США).

Кроме указанных наименований, в электронном обращении используются также *Даркоин, Праймкоин, Пиркоин, Нэймкоин* и многие другие.

Наиболее популярной из всех криптовалют является биткоин. Её название составлено из слов «бит» – наименьшая единица информации и «коин», что в переводе с английского означает «монета».

Для того, чтобы конвертировать свои сбережения в криптовалюту, необходимо выбрать надёжный криптовалютный кошелек для её хранения. Криптовалютные кошельки – это программы, которые хранят приватные и публичные ключи и взаимодействуют с различными блокчейнами, чтобы пользователь мог проверять баланс, отправлять деньги и выполнять другие операции. Чтобы иметь возможность тратить эти монеты и получить доступ к средствам, приватный ключ, хранящийся в вашем кошельке, должен соответствовать публичному ключу, к которому привязаны монеты. Если приватный и публичный ключи соответствуют друг другу, баланс вашего кошелька увеличивается, а кошелька отправителя, соответственно, уменьшается.

Существует несколько типов кошельков, которые предоставляют разные способы хранения и доступа к цифровым валютам. Кошельки можно разбить на 3 больших категории: программные, аппаратные и бумажные. Программные кошельки подразделяются ещё на 3 категории: для компьютера, для мобильных устройств и онлайн-кошельки.

Для компьютера: такие кошельки можно скачать и установить на личный компьютер. Доступ к ним можно получить только при помощи компьютера, на который они установлены. Однако, если компьютер будет взломан или заражён вирусом, есть вероятность потерять все деньги.

Для мобильных устройств: такие кошельки работают как приложения на вашем мобильном устройстве. Их можно использовать где угодно. Такие кошельки гораздо меньше и имеют более простую структуру, чем кошельки для компьютера.

Онлайн-кошельки: такие кошельки запускаются в облаке, а доступ к ним можно получить при помощи любого устройства с доступом в интернет. Хотя пользоваться такими кошельками и удобнее в некоторых ситуациях, они хранят ваши приватные ключи в сети и контролируются третьими лицами, а значит, риск взлома или кражи выше.

Аппаратные кошельки: эти кошельки хранят приватные ключи на физическом носителе. Хотя все транзакции происходят в сети, хранятся они вне сети, что повышает уровень безопасности. Аппаратные кошельки совместимы с несколькими веб-оболочками и могут поддерживать различные криптовалюты.

Бумажные кошельки: такие кошельки просты в использовании и предоставляют очень высокий уровень безопасности. Термин «бумажный кошелек» может означать либо приватные и публичные ключи в напечатанном виде, либо специальную программу, которая генерирует пару ключей, а затем печатает их. Передача биткоинов или любых других криптовалют на бумажный кошелек осуществляется путём отправки денег с вашего программного кошелька на публичный адрес, напечатанный на вашем бумажном кошельке.

Примерами криптовалютных кошельков являются: Blockchain, Cryptoray, Coinkite, Coinbase, Bitgo и многие другие.

Также криптовалюта может быть подвергнута угрозам. Одним из способов атак хакеров является фишинг криптовалют. **Фишинг** – это интернет атака, сутью которой является обман получателя с целью обретения таких его личных данных как: имени пользователя, паролей, банковских данных и тому подобного.

Существуют такие виды атак как:

- атака 51%;
- атака «чёрных дыр»;
- атака на узлы сети;
- вирусные атаки на кошельки пользователей;
- атака бирж;
- роутинговая атака и разделение сети;
- атака повторного воспроизведения и многие другие.

Чтобы обезопасить себя от кибератак, следует соблюдать следующие условия:

- 1) слежение за безопасностью ПК;
- 2) использование специально выделенного ПК или мобильного устройства, а также защищённой сети;
- 3) создание надёжных паролей;
- 4) шифрование данных;
- 5) создание резервных копии данных;
- 6) использование двух кошельков: основного и мультивалютного;
- 7) использование услуг сторонних компаний по кибербезопасности;
- 8) соблюдение мер предосторожности в сети и многие другие.

Несмотря на такое количество возможностей защиты от атак, всё же их вероятность существует, однако, даже если в какой-то момент биткоин

потеряет свою популярность и выйдет из оборота, существует множество других криптовалют, основанных на технологии блокчейн: Ethereum, Zcash и др.

Криптовалюты прочно вошли в систему онлайн бизнеса и заняли существенную часть финансового рынка. Кроме этого, сейчас есть даже особые банкоматы, в которых можно перевести биткоины в привычные бумажные деньги, а ряд торговых сетей и магазинов принимают эту валюту для расчёта наряду с обычными купюрами и монетами, поэтому нет сомнений, что эта сфера продолжит развиваться и приобретать всё большее влияние на нашу повседневную жизнь.