- создание и управление виртуальными дисплеями,
- создание групп дисплеев для более удобного управления,
- отправка нотификаций в случае неполадок,
- настройка параметров нотификации,
- просмотр истории дисплеев.

ЛИТЕРАТУРА

1. Wikipedia. Электронная энциклопедия [Электронный ресурс]: SAAS модель. – Режим доступа: https://ru.wikipedia.org. – Дата доступа: 23.04.2017.

2. ГОСТ Р 52870-2007 «Средства отображения информации коллективного пользования. Требования к визуальному отображению информации и способы измерения».

УДК 003.26

Студ. Е. С. Котик; студ. В. С. Хворост

Науч. рук. проф. П.П. Урбанович

(кафедра информационных систем и технологий, БГТУ)

КРИПТОВАЛЮТА БИТКОИН

Биткоин — это цифровая валюта, которую создали, чтобы решить все проблемы онлайн-платежей [1]. Может показаться, что существующая система и так хороша, но все наши нынешние покупки проходят через банки, которые берут себе долю транзакций и опираются на наше доверие их компетентности. Многие пытались придумать платёжную систему без такого посредника. Но есть проблема: как доказать, что ты оплатил покупку? Или что у тебя вообще есть нужная сумма, если нет поручителя? Проблема настолько серьёзная, что у неё даже есть название — проблема двойной траты.

В 2008 году анонимный программист, который представился как Сатоши Накамото нашёл решение этой проблемы. С. Накамото разместил на популярном криптографическом блоге статью с описанием платежной системы, являющейся валютой. Он предложил, чтобы вместо банка или кредитной компании, которые записывают все транзакции в одну общую книгу, нужно чтобы все пользователи записывали все транзакции одновременно. В результате любая попытка обмануть сеть будет замечена и платёж будет отменен. Ни один конкретный пользователь, государственный аппарат или банк не могут требовать комиссию за платежи или управлять их движением. Получается более дешевый, быстрый и простой метод

тратить деньги даже через государственные границы. Спустя несколько месяцев за биткоины уже продавали товары, их стали принимать интернет-магазины, за них стало возможным купить еду и даже оплатить учёбу в университете. Однако есть и проблемы. В то время, как одни подключились рано и получают прибыль, иные прогорают на этом молодом непостоянном рынке. Также люди открывают компании и скупают массы биткоинов, но поскольку по своей задумке биткоинов в обороте будет ограниченное количество, в будущем это может вызвать проблемы.

В своей основе биткоин — это цифровой файл, в котором записаны имена и балансы, как в регистре. Каждый компьютер в сети биткоин видит копию этого файла. Эти числа не имеют ничего физического, они ценны лишь потому, что люди готовы обменивать реальные товары и услуги ради большего числа напротив своего имени и уверены, что того же хотят остальные. Отправляя деньги, пользователь сообщает в сеть сумму, на которую уменьшится его баланс и увеличится баланс получателя, узлы или компьютеры в сети биткоин копируют эту транзакцию в свои регистры и передают транзакции следующим узлам. Если дополнить это цифровой защитой, получится система, позволяющая группе компьютеров вести регистр. И хотя по описанию она похожа на регистр, который ведет банк, тот факт, что регистр ведет группа, а не один владелец, создает ряд отличий. Во-первых, в отличие от банков, в которых каждый знает только о своих транзакциях, в биткоине все знают обо всех транзакциях. Также банку можно доверять или, как минимум, его «засудить», в случае махинаций. В биткоине же кругом незнакомцы, поэтому доверять нельзя никому. К счастью, система биткоина продумана таким образом, что доверие и не нужно. Особые математические функции защищают каждый аспект системы. Система биткоин работает следующим образом.

На базовом уровне, отправляя деньги Ивану, Алина распространяет сообщение с именами и суммой: «Отправить Ивану 5 биткоинов от Алины». Каждый узел, получая сообщение, обновляет свою копию регистра и передает сообщение о транзакции дальше.

Но откуда узлам знать, что этот запрос настоящий? Что реальный владелец счета отправил это сообщение?

По правилам биткоина, чтобы передать средства, нужен своеобразный пароль. Он называется *цифровой подписью*. Как и обычная подпись, цифровая заверяет сообщение, но делает это с помощью математического алгоритма, который предотвращает

копирование и подделку в цифровом пространстве. В противоположность постоянному паролю для каждой транзакции необходима новая уникальная цифровая подпись. Раскрывать пароль, который может скопировать и использовать кто-то чужой, крайне нежелательно. Цифровая подпись работает на основе 2 разных, но связанных ключей: приватного, который создает подпись, и публичного, с помощью которого её проверяют другие люди. Можно провести аналогию, что приватный ключ – это истинный пароль, а подпись – это посредник, который заверяет, что вы знаете пароль без необходимости его раскрывать. Публичный ключ служит адресом для получения биткоинов, т.е. отправляя человеку деньги пользователь отправляет их на его публичный ключ. Чтобы потратить деньги, необходимо доказать, что он реальный владелец публичного ключа, на который деньги отправлялись. Для этого генерируется цифровая подпись сообщения о транзакции и его приватного ключа.. С помощью привязанных к цифровой подписи вычислений, люди могут убедиться, что отправитель владеет приватным ключом, не видя сам приватный ключ. Важным аспектом является тот факт, что подпись зависит от сообщения, т.е. она новая для каждой транзакции и поэтому вор не сможет использовать её для другой транзакции. Эта зависимость от сообщения также означает, что никто не сможет изменить сообщение, передавая его по сети, поскольку изменения в сообщении сделают недействительной подпись.

Самые необыкновенные и интересные факты о биткоинах [2]:

С. Накамото — псевдоним создателя биткоинов, весь мир теряется в догадках о его настоящей личности. Сатоши создал биткоин в 2008 году. Предпринималось большое количество попыток раскрыть личность Сатоши, но пока без результатов. За 5 лет цена биткоинов выросла с нуля до 1000 долларов, а каждый день возникает примерно 3600 новых биткоинов. Монеты появляются в результате процесса, называемого майнингом.

В 2140 году будет добыт последний биткоин. 21 млн – именно таково максимальное количество биткоинов, которые будут когда-либо добыты. На сегодняшний день добыто около 12 млн. Алгоритм добычи уменьшает количество найденных монет в 2 раза каждые несколько лет, поэтому процесс неравномерен.

Житель Великобритании по имени Джеймс Хоулс по неосторожности выбросил жёсткий диск с ключом от кошелька, на котором находилось и до сих пор находится 7500 биткоинов, это примерно 5 млн долларов по текущему курсу

Исследователь из Норвегии по имени Кристофер Кох 2009 году купил биткоинов на сумму 27 долларов и забыл про них, а когда вспомнил, его инвестиция подорожала до 887 тысяч долларов, а покупал он те биткоины для своей дипломной работы по криптографии.

Таким образом, биткоин — это электронная валюта нового поколения, созданная по подобию золота и обеспечивающая достаточный уровень надежности и безопасности.

ЛИТЕРАТУРА

1. Bitcoin – что это такое? [Электронный ресурс] / Great-World.ru. – 2017. / Режим доступа: http://great-world.ru/bitcoin-chto-eto-zarabotat. – Дата доступа 01.04.2017.

2. Удивительные факты о "криптовалюте" Bitcoin [Электронный ресурс] / HiTech.ru. – 2017. / Режим доступа: http://hitech.vesti.ru/news/view/id/3771/ Дата доступа: 01.04.2017.

Студ. Н. Н. Чобот

Науч. рук. проф., д. т. н. П. П. Урбанович
(кафедра информационных система и технологий, БГТУ)

АЛАН ТЬЮРИНГ И ЕГО СИСТЕМА ВЗЛОМА МАШИНЫ «ЭНИГМА»

Алан Тьюринг — математик, логик, криптограф. Знаменит исследованиями в области вычислимости, занимался расшифровкой машины «Энигмы». Тьюринг является одним из основоположников информатики [1].

Во время Второй мировой войны Тьюринг работал в Блетчли-парке — британском криптографическом центре, где возглавлял одну из 5 групп, Hut 8, занимавшихся в рамках проекта «Ультра» расшифровкой закодированных немецкой шифровальной машиной «Энигма» сообщений. Историк и ветеран Блетчли-парка однажды сказал: «Блетчли-парку был нужен исключительный талант, исключительная гениальность, и гениальность Тьюринга была именно такой».

Польские коллеги накануне Второй мировой войны пытались пробить брешь в кодировке и создать «свою криптологическую бомбу», используя ошибки немецких шифровальщиков, пробуя