

## Криптовалюта что это и с чем его едят

В общем, криптовалюта - это сеть пользователей с кошельками (с какими объясню ниже). Сами пользователи имеют равные права соблюдение этих прав контролирует алгоритм кошелька, базовый кошелек - это Sibcoin QT На с++

JS кошелек тоже опен-сорс , он более простой. Коды обоих продуктаов лежат на гитхабе.

Майнинг - это часть алгоритма кошелька, точнее, это часть протокола сети, другими словами это API

Майнинг представляет собой программку (маинер), которая решает вероятностную мат.задачку. Эта задача и есть алгоритм добычи.

Дальше сеть признает по API результаты и начисляет награду в червонцах за найденные верные решения. Расчет награды тоже часть алгоритма и таким образом эмитируются червонцы

База данных всех транзакций сети публична, называется - Блокчейн, она хранится у каждого пользователя Sibcoin QT на устройстве и синхронизируется с другими.

Браузерный JS кошелек не имеет блокчейн, он обращается за ним по API к внешнему web сервису, который называется обозреватель сети, Explorer который в нашем случае это <http://chain.sibcoin.net> Обозревателей может быть сколько угодно. Он просто отображает блокчейн и дает по нему возможность поиска.

В браузерных JS-кошельках самое важное - это ключи. Ими можно подписать транзакцию и отправить ее в сеть. Построено все на асимметричном шифровании.

Чтобы отправить червонцы надо знать публичный ключ получателя и иметь свой приватный ключ. При создании транзакции кошелек шифрует публичным ключом получателя. В свою очередь получатель расшифрует приватным ключом который генерируется на девайсе получателя при помощи джава скрипта котелком. Зашифрованная транзакция вещается по сети

Все могут проверить валидность подписи. Майнеры добавляют транзакцию в блок и подтверждают только после проверки. Таким образом транзакция набирает все больше и больше подтверждени и одновременно распространяется по сети.

Внести изменения в многократно подтвержденную транзакцию нельзя. Это распределенная база без возможности редактирования. Записать можно, но изменить нельзя. Изменения не будут приняты другими кошельками (sibcoin QT например)

Раз в 2.6 мин в сети Червонца находится новый блок. Транзакция добавляется в блок и после этого блок скачивают кошельки

Блок - это запись в блокчейн, содержащая хеш нового блока цепи (искомый результат майнинг) и прикрепленными всеми транзакциями, накопленными к этому времени

У сети биткоина это происходит раз в 10 мин

Майнеры нашли хеш, после этого к нему можно добавить транзакцию Это и есть структура блокчейн

В отличие от биткоина, сеть червонца двухранговая

У биткоина есть только один уровень - кошельки, а в сети червонца есть еще суперузлы, которые называются мастерноды. Их может завести любой участник. Мастерноды должны иметь IPv4 и набор запущенных приложений в числе которых Sibcoin QT. Они должны быть в онлайн все время и обрабатывать трафик. За это они получают 50% добычи майнеров. Но, чтобы создать мастерноду нужно иметь 1000 Ч, их надо купить на рынке за деньги

Червонцы добываются майнерами и они в свободной продаже. Каждый сам распоряжается своими червонцами

Заблокировать действия юзеров нельзя

Это как раз то качество, которое не очень нравится государствам, но им приходится мириться с тем что деньги добывают сами пользователи и бесконтрольно ими платят друг другу, и с этим сложно что-либо поделать, закон издать можно, но исполнить не получится.

В общем, двухранговая архитектура позволяет строить сервисы:

а) Первый сервис Ч - скоростные транзакции, мгновенные, через голосование мастернод.

б) Второй сервис - анонимайзеры позволяющий запутать транзакцию, скрывая отправителя и получателя так, что снаружи не распутать еще 10 лет

в) Третий сервис сейчас в разработке. Для него нужны C++ разработчики  
Сервис - децентрализованный обмен червонцев на биткоины через сеть мастернод. Мастерноды выступают посредниками. Клиринг.  
Но украсть деньги не могут технически. Таким образом обмен гарантируется сторонам протоколом, а не конторой, или биржей. Доверие не требуется третьей стороне.

Это очень сильная фишка для всего крипто рынка. потому что транзакции децентрализованы, а обмен - нет

У всех обычных валют и биржи (это точки контроля и отказа спама) и гос регулирования, а здесь биржи не нужны и при этом, обмен нельзя контролировать с третьей стороны

Но он гарантирован тем, кто меняет

Это прорывная тема для всех валют, если коротко

Ч может стоить 500\$ после релиза

Бесконтрольный обмен черных червонцев на белые битки - это круто

Биткоин сильно зарегулирован и контролируется, Скоро он будет как евро или доллар, белый.

Есть еще ряд сервисов, которые нужно интегрировать, адаптировать под ядро Ч, Например кошельки Electrum и HD Браузерный другой, более крутой и платформу OpenBazar Это типа e-bay на блокчейне, Децентрализованная система выпуска токенов для ICO, Например, эту <http://www.omnilayer.org>

Это все нужно понять и попользоваться.

Кроме этого будут и обычные веб сервисы типа sib.cards. Но большинство все же связано с блокчейн, а это иная архитектура, Не похожая на клиент-сервер, или не всегда похожая

Например, один из требуемых веб сервисов: Таск менеджер на базе блокчейн и браузерного кошелька. Тут серверная часть отсутствует. Таск менеджер на базе блокчейн и браузерного кошелька. Можно сделать для затравки ))

Да, Понятно что народу нужны простые инструменты. А здесь все иначе и дофига работы, чтобы это все причесать

