Soldo Ecosystem White Paper

MARCH '18 RELEASE
RUSSIAN EDITION

Оглавление отчёта о Сольдо

Что такое Сольдо?

Сольдо – это народные деньги, которые существуют в безналичной форме и обслуживают платежи через Интернет.

Они созданы по принципам, сходным с Биткоином, но используют усовершенствованные технологии.

Эти деньги истинно народные потому, что:

- даже обладая ограниченными компьютерными ресурсами, каждый может заработать их в благодарность за поддержку сети;
- никто не сможет помешать кому-либо осуществить платёж или принять его;
- средства доступны только владельцу, их никто не сможет заморозить или конфисковать.

В отличие от народных денег правительственные (фиатные) деньги имеют множество правил, ограничивающих их применение.

Заявляя, что всё делается в интересах людей, появилась масса инструкций о том, как нам дозволено использовать собственные, потом и кровью заработанные деньги.

Нахлебники запрещают и ограничивают использование правительственных денег – они могут так делать потому, что это их деньги, они ими управляют.

Попробуйте осуществлять регулярные переводы - на третий – пятый раз к вам применят санкции и заставят доказывать, что вы не занимаетесь незаконным предпринимательством.

Организациям не позволяется хранить наличные средства в кассе, заблокировать счета могут без решения суда, просто по телефонному звонку или решению сотрудников банка.

Простой человек не может открыть счёт в иностранном банке и копить там на пенсию или образование детей – новые законы ставят массу преград этому.

Регулярные разорения банков из-за воровства руководства также не добавляют стабильности.

Народные деньги позволяют обойти все эти преграды – тратьте или копите свои средства по своему усмотрению.

Рынок криптовалют 2018

- Биткоин и прочие монеты (коины)
- Токены – другой класс цифровых активов
- Криптоновые (Cryptonotes)
- Байткоин (Bytecoin) и потомки
- Группа Монеро (Monero)
- DigitalNote и потомки
- Брошенные создателями архаичные монеты
- Модифицированные Криптоновые

Биткоин и прочие монеты (коины)

- Биткоин.

Биткоин был первой цифровой валютой и прообразом для большинства современных криптовалют, он имеет самую большую капитализацию и объём торгов.

Новые монеты появляются при его добыче (майнинге).

Большая часть платежей проходит в Биткоинах, большинство иных активов торгуется в первую очередь именно к Биткоину.

Однако, будучи древней валютой Биткоин не лишён недостатков.

Биткоин очень дорогой и желанный, простому человеку практически невозможно его добыть.

Принцип равноправия, заложенный создателями в криптовалюты был нарушен – сейчас только гигантские предприятия способны его добывать (большая часть этих фабрик расположена в Китае или контролируется его гражданами) .

Платежи в Биткоинах очень дорогие и медленные – иногда за проведение платежа необходимо заплатить десятки долларов и ждать почти сутки, а платить за мелкие покупки и вовсе лишено смысла из-за стоимости перевода.

Переводы в сети Биткоин не содержат информацию о владельцах средств, но вся информация общедоступна и позволяет провести анализ переводов и вычислить владельцев.

- Прочие монеты.

Большинство прочих монет (*альткоины*) – копии биткоина с небольшими изменениями, они также позволяют добывать новые монеты майнингом.

Часть альткоинов использует собственные оригинальные технологии, не копируя биткоин.

Существуют монеты, которые уже при разработке были полностью добыты, но сейчас это редкость, такие монеты полностью заменены токенами.

Токены – другой класс цифровых активов

Монеты существуют сами по себе, токены основаны на базе монет.

Для создания токенов не нужны никакие затраты, просто желание создателей выпустить их.

Технологии стандартные, ничего нового изобретать не нужно.

К ним можно относиться как к акциям коллективов – разработчиков.

Иногда они обеспечены новыми технологиями или материальными ценностями, деньгами или акциями.

Но чаще всего – просто обещаниями, их ценность равна вере покупателей в них, не более.

Инвестиции в токены – удел профессионалов.

Зачастую целью создателей токенов является рекламная компания, во время которой создаётся шумиха в прессе.

Для презентации инвесторам изготавливаются красочные рекламные материалы, пишутся серьёзные научные труды с математическими выкладками, снимаются профессиональные видео, нанимаются известные актёры и знаменитости на их продвижение.

Сопровождается реклама радостными ожиданиями и восторгами нанятых агитаторов и экспертов.

В итоге, после проведения размещения токенов на рынке разработчики начинают тратить полученные средства на собственное потребление, иногда просто исчезают.

Инвесторы остаются с кучкой никому не нужных токенов, купленных по высокой, непонятно кем установленной цене.

Криптоновые (Cryptonotes)

Одной из групп монет, созданных по технологиям, отличным от Биткоин являются Криптоновые (Cryptonotes).

Из их преимуществ следует выделить:

- анонимность – информация о контрагентах хранится в зашифрованном виде и доступна только участникам перевода;
- защита от отслеживания платежей и анализа блокчейна;
- высокая скорость переводов и их невысокая стоимость;

Криптоновые используют более стойкое шифрование данных и в большем объёме, поэтому для обслуживания платежей требуется больший объём дискового пространства в сравнении с Биткоином, нагрузка на процессор также выше.

Современные криптоновые можно объединить в следующие группы по функциям, свойствам и происхождению:

- Байткоин и потомки;
- группа Монеро;
- ветвь DigitalNote;
- заброшенные создателями монеты;
- модифицированные Криптоновые.

Байткоин (Bytecoin) и потомки

- Байткоин (Bytecoin, BCN)

Является родоначальником всех криптоновых монет, большинство криптоновых монет базируется на его коде и заимствуют его технологии.

Недорогие и быстрые переводы.

Имеется информация о том, что более 85% монет были добыты тайно (премайн) до начала публичного майнинга.

Команда первоначальных разработчиков таинственно исчезла, квалификация новой команды спорна, будущее туманно.

Ошибки в коде позволили хакерам создать ещё около 700.000.000 монет из воздуха.

- Дашкоин (Dashkoin, DSH)

Прямая копия кода (клон) Байткоин, но без премайна в 80%, поэтому не имеет команды разработчиков.

Ошибки в коде позволили хакерам создать монеты из воздуха, после чего сеть монеты разделилась на 2 ветви – изначальную и пула Minergate.

Последнюю поддержала биржа Hitbtc, первая не прижилась на биржах и на сегодня монета нежизнеспособна.

- Forknote

Большая группа монет, построенная на коде оригинального Байткоин, позволяющая менять свойства и параметры монеты просто использованием файла конфигурации.

Группа Монеро (Monero)

- Монеро (Monero, XMR)

Самый популярный представитель Криптоновых, имеющий самую мощную команду разработчиков.

Число узлов в сети Монеро исчисляется десятками тысяч, сообщество очень многочисленно, торгуется на множестве бирж в том числе и к фиатным валютам.

Обеспечивают абсолютную анонимность, информация о транзакции шифруется полностью, включая суммы переводов.

Из-за тотального шифрования размер блоков в десятки и сотни раз больше прочих криптоновых.

Соответственно монета крайне тяжелая в использовании, подходит лишь для крупных сумм.

Размер блокчейна измеряется десятками гигабайт, сетевой траффик узлов очень высокий, первоначальная синхронизация может занимать несколько дней, даже с использованием предварительно загруженного архива блокчейна.

Стоимость переводов очень высока и сильно зависит от объёма передаваемой информации.

- Sumokoin

Базируется на коде Монеро, унаследовав все его недостатки и обещая сомнительные преимущества, не имеет мощной команды разработчиков и сообщества

- Electroneum

Обещают мобильные версии кошельков.

К недостаткам Electroneum добавляется отсутствие публично доступных исходных кодов.

DigitalNote и потомки

- DigitalNote (DuckNote, DarkNote, XDN)

изначально назывался утиной банкнотой – DuckNote.

На данный момент самый нетребовательный из Криптоновых к ресурсам – размер блокчейна на диске и памяти минимален.

Сетевой траффик узла также минимален.

Скорость распространения транзакций исчисляется секундами, подтверждения – минутами.

Позволяет передавать сообщения вместе с переводом.

Имеет функцию депозитов с начислением процентов на базе блокчейна.

Может добываться параллельно с другими монетами без дополнительных затрат ресурсов.

То есть технически монета наиболее сбалансирована, пригодна к ежедневному применению и при этом не перегружена.

Главная проблема – отсутствие сообщества и команды разработчиков.

Единственный разработчик исчез более 18 месяцев назад, с тех пор монета не обновлялась.

- Fantomcoin FCN

Копия XDN, лишенная функций депозитов и сообщений.

Брошенные создателями архаичные монеты

Существует достаточное количество Криптоновых монет, которые были заброшены создателями.

Они используют самые старые версии программного кода, потребляют в использовании массу ресурсов, особенно ценной оперативной памяти.

По этой причине на их основе не создаются новые монеты, а сами они удаляются с бирж и торговых площадок – использование таких монет очень накладно для инфраструктуры.

При этом сети этих монет функционируют исправно, приложения доступны для загрузки, отдельными энтузиастами даже осуществляется майнинг.

Примеры таких монет:

- Infinium INF8
- Moneta Verde MCN

Однако, недавно некоторые архаичные монеты энтузиасты смогли перевести на использование технологии Forknote.

С этого момента самые свежие версии кода Байткоин стали доступны для сетей этих монет и появилась возможность их возрождения.

Типичный пример – QuazarCoin QCN.

Модифицированные Криптоновые

Кроме четырёх вышеперечисленных канонических ветвей Криптоновых можно выделить ещё одну категорию, в которые входят монеты, базирующиеся на данной технологии, но имеющие изменённые алгоритмы.

Как правило, изменяется как минимум функция доказательства работы Proof-of-Work со стандартного алгоритма CryptoNight.

Такие монеты невозможно майнить программами майнерами, предназначенными для традиционных Криптоновых.

- Boolberry BBR

Основан на архаичном коде Байткоин.

Функция Pow работает по алгоритму Wild Keccak и использует данные из предыдущих блоков цепи.

В сообществе были неоднократные расколы, перебои в работе сети, что привело к постепенному закату популярности монеты и делистингу с некоторых бирж.

- AEON

Функция Pow работает по алгоритму Cryptonight-Light и имеет нацеленность на мобильных клиентов.

В алгоритме вдвое сокращён размер области данных массива для перестановок и количество итераций цикла перестановок.

Основан на архаичном коде Монеро, до сих пор имеет только консольные версии приложений, однако будущее проекта не вызывает опасений.

- Soldo SLD

Первая из серии монет с изменённым алгоритмом хэширования PoW.

Сочетает в себе стабильность и надёжность Криптновых с модифицированным CryptoNight алгоритмом SoftCrypton, обеспечивающим соло-майнинг даже на устаревших компьютерах и планшетах.

Предназначена для повседневного использования и пригодна для микроплатежей благодаря сверхбыстрому подтверждению транзакций и мизерной комиссии на перевод, а также минимальному расходу ресурсов – дисковой и оперативной памяти, сетевого трафика.

Позволяет передавать текстовые комментарии к транзакциям.

Создана на базе ветви кода DigitalNote, активно разрабатывается.

Преимущества Soldo

- Причины создания
- Миссия и реализация
- Характеристики
- Свойства
- Финансовые параметры
- Целевая аудитория
- Контакты, анонсы, продвижение
- Загрузка приложений
- Биржи, рейтинги, пресса

Причины создания

Сольдо – это народные деньги, существующие в безналичной форме и обслуживающие платежи через Интернет, созданные по принципам и правилам, сходным с Биткоином, но использующие усовершенствованные технологии.

Говоря более формально, Сольдо это современная криптовалюта, один из видов цифровых активов с уникальными характеристиками, созданная для повседневного использования.

Для осуществления перспективных проектов группе инвесторов была необходима криптовалюта, обладающая рядом свойств и подходящая по характеристикам.

После проведённых исследований выяснилось, что большинство существующих криптовалют не обеспечивают анонимности, а пригодные анонимные не годятся из-за того, что;

- требуют высокие комиссии за перевод;
- потребляют избыточное количество ресурсов при работе;
- транзакции происходят крайне медленно;
- сообщество не доверяет им из-за грязного прошлого или непрозрачной процедуры запуска;
- заброшены разработчиками или базируются на устаревшем программном коде;
- не умеют передавать текстовую информация вместе с платежом;
- не учитывают интересы майнеров из-за слишком быстрой добычи монет в начале майнинга;
- были изменены разработчиками так, чтобы ограничить вознаграждение майнерам и дать приоритет участникам первого года майнинга;
- не имеют новых характеристик в сравнении с предшественниками;
- изначально не предусматривают развития так как создаются только для быстрой продажи на бирже или имеют слишком большое вознаграждения для создателей и разработчиков монеты;
- имеют проблемы с реализацией из-за низкой квалификации команды или промахов в проектировании;

Потеряв месяцы в ожидании решения проблем существующими командами разработчиков, инвесторами проектов было принято решение о запуске новой монеты на базе наиболее подходящего программного кода.

При проектировании монеты было уделено максимальное внимание решению вышеупомянутых проблем.

Запуск был произведён публично под аудитом независимого гаранта.

Миссия и реализация

Сольдо был спроектирован на базе общего для всех Криптоновых кода CryptoNote для обеспечения анонимности переводов, вбирая лучшие идеи всех популярных монет.

Благодаря этому никто не может контролировать Сольдо и владеть им.

Однако, одна его составляющая, функция подтверждения работы PoW была изменена с CryptoNight на SoftCrypton для функционирования даже на маломощных компьютерах, включая планшеты и телефоны.

Это позволило выступить Сольдо в качестве легковесной альтернативы существующим Криптоновым монетам.

Транзакции и сообщения, передаваемые по сети Сольдо практически мгновенно могут осуществляться в любой точке мира сохраняя защищённость и приватность.

Наиболее строгая версия современной криптографии используется для защиты сети Сольдо от цензуры и наблюдения, позволяя лишь участникам операций быть в курсе финансовых транзакций и информационного обмена.

В сети Сольдо все равны, нет никаких различий кроме главного – приватного ключа, который и является единственным механизмом доступа к счету, его балансу, истории транзакций и сообщений.

Транзакции в сети Сольдо проходят практически моментально и с мизерной комиссией, благодаря этому можно осуществлять любые, даже самые мелкие переводы, например пожертвования в реальном времени.

Сольдо был создан на базе современного кода DigitalNote, позволяющем передавать текстовую информацию наряду с финансовой, в который был внесён ряд принципиальных изменений.

Для работы приложений Сольдо расходуется настолько мало ресурсов компьютера, насколько это возможно при сохранении анонимности приватности и защищённости, всех - и памяти, и траффика и хранилища.

Один из самых элегантных механизмов, встроенных в Сольдо – это лотерея на базе блокчейна для поддержки майнеров. Ведь в реальности заранее неизвестно, сколько золота будет в ведре, только промыв грунт становится виден результат.

Для долгосрочного инвестирования реализовано улучшенное управление ключами кошельков – их можно сохранять и восстанавливать как в виде шестнадцатеричного кода так и в виде мнемонического сида, для безопасного хранения активов возможно создание ключей холодного кошелька без подключения сети, в автономном режиме.

Запуск майнинга был произведён публично под аудитом независимого гаранта, разработчики не получили вознаграждения за создание монеты в виде премайна.

Всё было сделано максимально открыто и прозрачно, программный код общедоступен для исследования на Github, а разработчики готовы добавить новые функции и устранить проблемы в самые минимальные сроки.

Характеристики

Идентификация

- Название - Soldo
- Тикер – SLD

Конфигурация монеты

- Pow алгоритм - SoftCrypton
- Целевая сложность- 20 sec
- Подтверждение транзакций - 18 блоков

Сеть

- P2P порт - 33711
- RPC порт - 33712

Сокеты источников данных сети

- s1.soldo.in:33711
- s2.soldo.in:33711
- s3.soldo.in:33711
- s4.soldo.in:33711
- s5.soldo.in:33711
- s6.soldo.in:33711

Финансовые параметры

➢ **Эмиссия**

- общее количество технически возможных монет – неограниченно;
- фактическое количество эмитируемых монет – 10М (10.000.000);

➢ **Премайн**

- премайн отсутствует.

➢ **Этапы майнинга**

1. Первый блок содержит 50.000 монет (0,5% эмиссии) и переводится в Фонд Развития Проекта;
2. Следующие 1000 блоков имеют награду 100 SLD. Это премиальные блоки для ранних адептов монеты. Любой может получить данную премию, но необходимо помнить, что данная премия будет заблокирована для использования в течение 750.000 блоков, то есть примерно полгода.
3. До достижения максимума эмиссии - 10.000.000 SLD обычная награда за блок неизменна и равна 1 SLD.
4. После достижения максимума остаётся лишь техническая награда за блок в виде 1 атомарного юнита монеты.

➢ **Лотерея**

Для поддержки майнинга Сольдо использует встроенную в блокчейн лотерею.

Благодаря этому награда за блок может быть умножена на коэффициент удачи.

Майнер может выиграть коэффициенты x2, x100, x1.000, x10.000 и даже x100.000.

Вероятность выпадения выигрышей и их количество неизвестно – это реальная лотерея в прямом смысле этого слова.

➢ **Фонд Развития Проекта**

Каждый может купить любое количество монет из фонда по курсу 0.00025 к BTC.

Большая часть запасов фонда будет потрачена на оплату листинга на биржах.

Промо акции также будут оплачиваться в Сольдо из данного фонда.

Если фонд не будет истрачен по истечении 26 недель после запуска монеты оставшиеся активы будут проданы на аукционе.

Целевая аудитория

При создании Сольдо не вводилось каких-либо ограничений на область применения монеты.

Однако, наибольшие преимущество Сольдо будет иметь, используясь для:

- накоплений;
- микротранзакций;
- для покупок в локальных торговых точках, использующих методику членства в клубе потребителей;
- благотворительных взносов;
- межбиржевых переводов;
- создания закрытых частных платёжных систем на базе блокчейна;
- образовательных проектов;
- обучающих технологий;
- торговых и платёжных автоматов;
- частных переводов физических лиц;
- некоммерческих проектов, программ голосования и учёта, статистики;

Контакты, анонсы, продвижение

Website - http://soldo.in

BT main topic - https://bitcointalk.org/index.php?topic=2332011

Ryver - https://zzl.ryver.com/application/signup/members/ho7SVMfFAvFRGiZ

Twitter - https://twitter.com/Soldo_SLD/

Telegram - https://t.me/SLD_Soldo

FB - https://www.facebook.com/sldcoin/

VK - https://vk.com/sld_soldo

Discord - https://discord.gg/Y8g6B4y

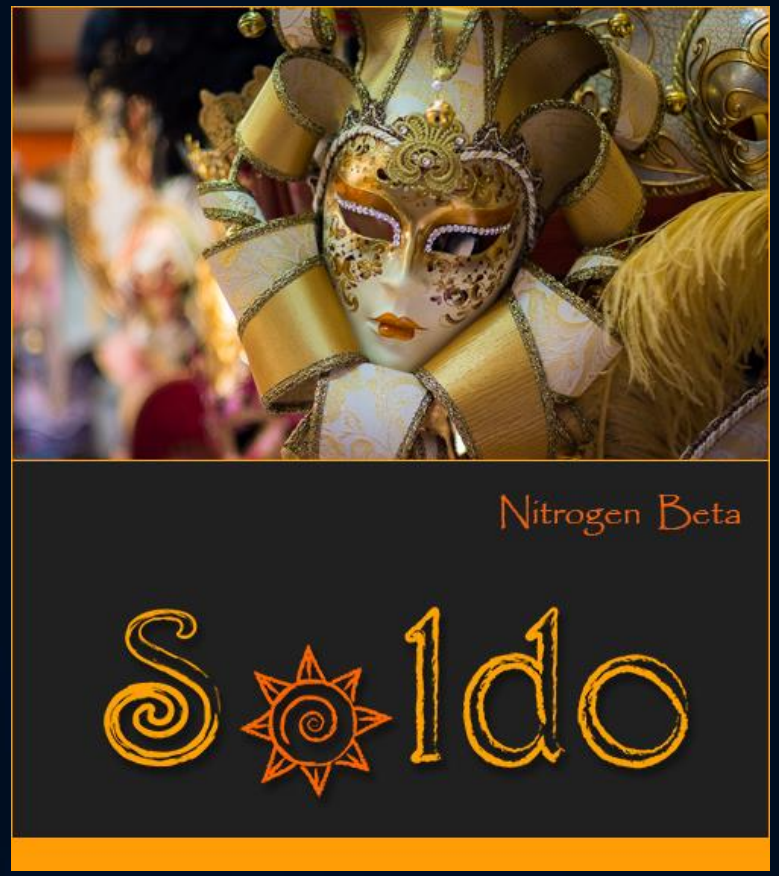
Загрузка приложений

Source codes @ Github -
https://github.com/monselice/sld

Windows binaries @ Github -
https://github.com/monselice/sld/releases/

Docker Container for Soldo @ Github -
https://github.com/awmyhr/docker-soldo/

Windows GUI Wallet Beta @ Github -
https://github.com/monselice/soldo/releases/



Биржи, рейтинги, пресса

Биржи

- CREX24 - https://crex24.com/exchange/SLD-BTC/
- BTC-Alpha - https://btc-alpha.com/exchange/SLD_BTC/

Рейтинги

- CoinLib - https://coinlib.io/coin/SLD/Soldo/
- CoinCodex - https://coincodex.com/crypto/soldo/
- Coinranker - https://www.coinranker.net/cryptocurrency/Soldo
- Altcoin Calendar - https://www.altcoincalendar.info/coins/3518-SLD

Дух сообщества Soldo

- Рождённая сообществом
- Рождение Клана
- Независимые Команды
- Почему доверяют Soldo

Рождённая сообществом

Проект Сольдо был первоначально задуман как частный цифровой актив закрытой группы инвесторов.

Однако, при дальнейшем рассмотрении было принято решение расширить возможности монеты и выпустить её как публичный актив, ограничив влияние инвесторов.

Для запуска монеты был приглашён независимый гарант проекта, на него также были возложены роли координатора проекта и аудитора.

На этом деятельность инвесторов в проекте Сольдо была завершена, более они не имеют влияния на решения, принимаемые координатором для поддержки существования монеты.

После консультаций с различными группами энтузиастов координатором был одобрен план и характеристики новой монеты, предложенные группой, состоящей из майнеров, модераторов и администраторов ряда пулов и бирж.

Коммьюнити интернационально, большинство так или иначе связано бывшим СССР и странами Восточной Европы – Россией, Украиной, Белоруссией, Латвией, Эстонией, Чехией и Словакией, а также Польшей.

Помимо изначального проектирования свойств и характеристик монеты коммьюнити принимало действенное участие в бета-тестировании прототипа и первоначальном запуске монеты.

Первые жизненно важные сервисы, такие как блокчейн-эксплорер и узлы-сиды также были созданы благодаря усилиям коммьюнити.

Некоторая часть информационных ресурсов и по сей день управляется решениями сообщества.

Рождение Клана

Однако, завершив этап первоначального запуска сети монеты и создания базовых сервисов, пришло осознание того, что коммьюнити многогранно, интересы его участников зачастую диаметрально противоположны и не всегда идут на пользу дальнейшему развитию Сольдо.

Положение усугубило желание некоторой части коммьюнити внести изменения в изначальные характеристики монеты и увеличить преимущество существующих владельцев монет путём ограничения эмиссии.

Во избежание дальнейшего раскола было принято решение, что только мнение участников коммьюнити, внесших вклад в проект Сольдо будет иметь вес.

Так родилась идея Клана.

Участником Клана признаётся каждый, кто внёс какой-либо вклад в развитие проекта Сольдо – не только финансовый, но и свои знания, своё время, свой труд, пусть даже и в самой незначительной степени.

В своём развитии проект Сольдо стал базироваться на идеях и предложениях Клана вместо коммьюнити.

Постепенно пришло видение того, что не технологии или программы, а именно люди участвующие в процессе, Клан – самое главное достижение, полученное в ходе реализации проекта Сольдо.

Чтобы подчеркнуть важность этого факта было принято решение, что дальнейшие проекты, создаваемые на базе Сольдо участниками Клана будут передавать часть своих активов для поддержки участников Клана и Фонда Развития Сольдо.

Любой участник Клана, имеющий 1000 SLD и более будет иметь долю от всех проектов, упомянутых выше.

Независимые Команды

Независимые Команды – один из механизмов поддержания баланса интересов в развитии Сольдо.

Каждая команда может работать в любом интересном для неё направлении, вектор приложения усилий выбирают участники команды, при этом Команда независима и неподконтрольна никому извне.

Команда может создать собственный визуальный образ – аватар – Сольдо, свои приложения для использования Сольдо, брендирование элементов, собственные сайты и прочие каналы коммуникаций.

До тех пор, пока используется единый блокчейн и программный код для работы с ним, визуальные изменения проходят в рамках проекта Сольдо.

В этой функциональности Сольдо похож на Евро, которое выпускается множеством банков из разных стран, различается изображениями на реверсах монет, сохраняя при этом неизменными изображение на лицевой части, вес, размер, состав металлов и прочие атрибуты.

Типичный пример – Команда, которая работает с региональным рынком, переводит информацию на язык данного региона и брендирует визуальные элементы исходя из своих потребностей.

Однако, изменение внешнего вида или каналов распространения информации не единственная сфера приложения усилий Команд, ряд Команд реализует проекты в инфраструктуре Сольдо, создаёт код для запуска новых сервисов, никак не влияя на внешнее представление монеты.

Единственное исключение из вышеупомянутых правил – Sole Team, обеспечивающая базовую функциональность проекта и подчиняющаяся Координатору проекта.

Почему доверяют Soldo

Проект Сольдо заслуживает доверия по ряду причин, наиболее значимые из которых:

- Полностью независимый проект.
- Нацелен на длительное развитие.
- Не обещает достижения невыполнимых результатов.
- Всегда выполняет обещанное и соблюдает оговоренные временные рамки.
- Имеет чёткие планы длительного развития.
- В первую очередь защищает интересы существующих инвесторов проектов.
- Обслуживается командой IT-профессионалов высочайшей квалификации с многолетним опытом работы.
- Способность разработчиков в минимальные сроки реагировать на фатальные проблемы, анализировать причины их возникновения и эффективно устранять последствия, не допуская в дальнейшем повторения произошедшего.

Экосистема Сольдо

- Грядущие проекты
- Гарантийное агентство
- Моментальные кошельки
- Биржа
- Книжный магазин
- Рулетка
- Платёжный центр с токенами монет из драгметаллов
- Запуск новых монет

Грядущие проекты

Ниже будут перечислены проекты в рамках инфраструктуры Soldo, которые будут реализованы Командами и Кланом.

Внешние проекты, которые ведутся изначальными инвесторами проекта и независимыми разработчиками не входят в данный документ, т.к. нет возможности проверить, насколько достоверна полученная информация и будут ли данные проекты реализованы.

Большая часть проектов – независимые коммерческие, однако некоторая часть – образовательные и имиджевые, направленные на популяризацию Сольдо и повышение биржевого курса, не подразумевающие получение значительной прибыли.

Все проекты, упомянутые ниже, после запуска передадут часть (от 10% до 50%) своих активов в общий фонд Клана, для вознаграждения инвесторов и повышения биржевого курса Сольдо.

Большинство новых проектов будет базироваться на сервисах, предоставляемых гарантийным агентством.

Гарантийное агентство

Гарантийное агентство – краеугольный элемент будущей экосистемы.

Большинство иных сервисов будет базироваться на его функционале.

Гарантийное агентство будет устроено по принципу мультивалютного хранилища активов, позволяющего:

- депонировать активы;
- выводить активы;
- выписывать цифровые чеки в валютах активов;
- погашать цифровые чеки;
- осуществлять переводы между счетами;
- вести учёт долей участников Клана.

Для обслуживания интересов Клана 25 раз в год каждые 2 недели будет осуществляться моментальный снимок состояния SLD-счетов.

Для каждого участника будет вычисляться Индекс, равный целой части от среднего за последние 25 периодов, делённого на 1000.

На каждую единицу индекса будет выплачиваться 0.01% активов, передаваемых новыми проектами в фонд Клана.

Данные активы можно сравнить с привилегированными акциями без права голоса в классической экономике.

Существует 5 уровней привилегий участников, в зависимости от величины вычисленного индекса:

- 1 – bronze – получение активов
- 10 – silver – доступ ко внутренним документам
- 100 – golden – доступ к данным аудита
- 200 – platinum – право голоса в проектах

В случае изменения максимальной эмиссии Сольдо данные величины могут быть пересчитаны с использованием коэффициентов.

Моментальные кошельки

Данный проект – логическое продолжение гарантийного агентства.

Суть проекта в предоставлении защищённого доступа к счетам гарантийного агентства для:

- проверки балансов;
- осуществления переводов;
- информационного обмена;

Доступ к сервису будет осуществлять путём использования множества механизмов для исключения единой точки отказа, в том числе:

- онлайн GUI-приложение;
- отправка ордеров через сайт;
- передача ордеров по сети Сольдо;
- использование чат-ботов типа Telegram;
- передача ордеров через e-mail;
- резервный вариант – приём ордеров на бумажных носителях через почту;

Главная цель данного проекта – дать возможность распоряжения средствами даже в случае самого неблагоприятного развития событий на отдельных территориях, включая полную изоляцию регионов от сетей передачи данных.

В сочетании с использованием токенов, номинированных в монетах из драгметаллов, данный проект предоставит возможность долгосрочного накопления средств и надежность, не уступающую швейцарским банкам.

Возможность анонимного использования сервиса в настоящее время простыми гражданами ставит его на ступень выше традиционных банковских сервисов.

Биржа

Данный проект состоит из двух этапов.

Первый этап ограничивается созданием рабочего прототипа, обеспечивающего обмен лишь некоторого количества крипто-активов.

Второй подразумевает получение лицензии в Еврозоне, для проведения обмена крипто-активов на Евро.

Суть проекта в предоставлении площадки для обмена одних цифровых активов на другие.

Обслуживание платёжных операций осуществляется на базе гарантийного агентства.

Таким образом биржа не отвечает за средства клиентов, что повышает доверие к ней и минимизирует затраты.

Модульность сервисов позволяет разместить каждый из них в наиболее благоприятной юрисдикции и быстро заменить или дополнить любой модуль при необходимости.

Так, при получении фиатной лицензии просто добавится ещё одно гарантийное агентство, которое занимается только приёмом средств, их хранением и выплатой, а на бирже торгуются токены, выпущенные гарантом на сумму имеющихся средств.

Следующим преимуществом является возможность дублирование сервиса биржи с минимальными расходами средств и времени для последующего брендирования, раскрутки и продажи.

Типовое решение можно предложить рынку в виде готовых к использованию виртуальных машин, аппаратных решений, преинсталлированных в датацентрах или даже в виде аренды сервиса.

Помимо продажи типовых биржевых решений данный проект будет получать прибыль с обменных операций и листинга новых активов.

Долю в проекте, не принадлежащую Клану также можно будет частично продать внешним инвесторам для финансирования приобретения фиатной лицензии.

Фонду Клана первоначально планируется передать долю в размере 10% данного проекта, однако, в дальнейшем данная величина может быть пересмотрена в сторону увеличения.

Все торги на собственной бирже будут проходить через Сольдо, оплата всех комиссий также планируется в Сольдо.

Книжный магазин

Данный проект разрабатывается отдельной командой, является демонстрационным, непрофитным, нацеленным на повышение биржевого курса Сольдо и его капитализации.

Задача проекта состоит в создании готового набора базовых программных компонент для быстрого запуска интернет-магазина с обслуживанием платежей в Сольдо, а также образца такого магазина.

При обслуживании платежей в Сольдо необходимо будет реализовать следующие методы оплаты:

- прямой перевод с кошелька покупателя на кошелёк магазина / web;
- моментальная онлайн-оплата мобильным клиентом платёжного требования через гарантийное агентство / касса;
- моментальная офлайн-оплата платёжного требования через гарантийное агентство посредством резервных офлайн-кодов оплаты / касса;
- оплата через схему клуба потребителей и финансовый депозит.

Данный проект может иметь прибыль в случае реализации сервиса установки типовых решений под ключ.

В Фонд Клана первоначально планируется передать долю в 50% активов данного проекта.

Рулетка на базе блокчейна

Классическая европейская рулетка, сервис, работающий в автоматическом режиме.

Выпавший номер вычисляется посредством алгоритма, генерирующего данные на базе блокчейна, что защищает от мошенничества, присущего многим современным игровым схемам.

Обработка ставок возможна как в режиме прямых переводов через сеть Сольдо, так и в режиме работы через гарантийное агентство.

Во избежание единой точки отказа планируется реализация через:

- онлайн GUI-приложение;
- асинхронные транзакции напрямую через сеть Сольдо;
- приём ставок в асинхронном режиме через сайт;

В фонд Клана планируется выделить долю в 10% данного проекта.

В дальнейшем можно дополнить данный сервис другими типами игры.

Базовый фреймфорк можно использовать и со ставками на событие, однако это требует наличия персонала и не может работать в автоматическом режиме.

Платёжный центр с токенами монет из драгметаллов

Суть проекта состоит в выпуске гарантийным агентством цифровых активов на базе имеющихся в наличии физических активов.

Реализация проекта состоит в закупке за фиат физических активов, хранении их в защищённом хранилище и продаже цифровых активов с премией за хранение.

Обратный выкуп цифровых активов за фиат не предусматривается, только обмен цифровых активов на физические.

Запланировано несколько центров хранения активов в юрисдикциях, допускающих хранение драгметаллов без лицензии под аудитом.

В качестве физических активов выбраны инвестиционные монеты из золота 900-920 пробы.

В отличие от слитков и коллекционных монет продажа инвестиционных монет не облагается НДС в большинстве стран.

Спрэд на покупку-продажу монет всегда меньше слитков, соответственно монеты более ликвидные.

Хранение монет из чистого золота требует дополнительной защиты в виде футляров, что увеличивает расходы на хранение в 3-4 раза, монеты 900-920 пробы такого недостатка лишены.

Для хранения выбираются монеты стандартного веса в 1 тройскую унцию, выпущенные до 2000 года в развитых странах, страны бывшего СССР и третьего мира не соответствуют критериям приемлемости.

В данный момент рассматриваемые кандидаты состоят из Южноафриканского Крюгеррэнда и Американского Орла, в дальнейшем возможен вариант добавления других золотых монет как самостоятельных активов, например Английский Соверен.

Серебряные монеты не рассматриваются, так как требуют гораздо больших затрат на хранение, единственный вариант – выпуск с повышенной премией скорее всего не поддержит рынок.

Монеты из платины слабо представлены на рынке и потому также не соответствуют критериям приемлемости.

Спрэд на покупку-продажу монет составляет 4-6%, за обслуживание хранения и эмиссию цифровых активов разумная премия составляет 6%, поэтому можно ориентироваться на стоимость актива как цена скупки монет * 1.12, стоимость продажи зачастую зависит и от спекулятивной составляющей.

Таким образом данный проект нацелен скорее на возможность создания актива для долговременного инвестирования и не несёт высокой прибыли, как впрочем и все активы, связанные с физическими драгметаллами.

Фонду Клана планируется передать долю в размере 10% данного проекта.

Торговля цифровыми активами планируется на базе собственной биржи.

Запуск новых монет

При достижении исходного кода Сольдо стадии зрелости на его базе будут выпускаться новые экспериментальные монеты, сочетающие надёжность технологии CryptoNote с самыми современными алгоритмами хэширования для подтверждение выполненной работы.

В фонд Клана планируется выделять долю от 10% до 50% новых монет, в зависимости от используемых алгоритмов хэширования и предполагаемой цели использования монет.

Если в будущем возникнет разделение монет, базирующихся на блокчейне Сольдо в виде форка, то все новые монеты, доступные после форка также будут зачислены на счета Фонда Клана.

Такой вариант развития событий вполне прогнозируем, если часть сообщества не поддержит каких-либо изменений в технологии Сольдо и решит развивать собственную ветку монеты.

При подобном развитии ситуации команда Сольдо готова помочь в создании программного кода форка монеты, а также поддерживать программный код новой монеты в течение года после осуществления форка.

Дорожная карта 2017

- Post-launch fixes
- Full key management
- Recovery seed
- Paper wallet for cold storage
- Transaction comments
- Blockchain Explorer
- Logo
- Basic website
- Attacks preventing fixes

Дорожная карта 2018

- Code change for public nodes
- Fusion transactions
- GUI Wallet
- Public nodes
- Blockchain Explorer
- Knowledge center / Wiki / Library
- Payment gateway implementation
- Exchange listing

Дорожная карта 2019-2021

- Code refactoring
- Escrow payments
- Lightweight wallets
- Exchange working prototype
- Advanced multilingual website
- Internet and POS sales solution software prototype
- Real silver/golden tokens payment
- Roulette

Дорожная карта 2022-2023

- Fiat currency license in EUR
- Exchange with cryptocurrencies and fiat trades

Финансовый прогноз

Монета запущена 30.10.2017, выход на биржу – февраль 2018.

- 1 SLD = 0.0004 XMR.

Предполагаемый рост курса:

2019

- 1 SLD = 0.001 XMR

2020

- 1 SLD = 0.01 XMR

2021

- 1 SLD = 0.1 XMR

После 2022

- 1 SLD – от 0.25 до 0.4 XMR.

Основы CryptoNote

- CryptoNote Philosophy
- Ring signatures: Untraceable payments
- One-time keys: Unlinkable transactions
- Double-spending proof
- CryptoNote blockchain analysis resistance
- Standard CryptoNote transaction
- Adaptive limits
- Smooth emission
- Egalitarian proof of work

CryptoNote Philosophy

Check https://cryptonote.org/inside/ for details.

CryptoNote is the technology that allows the creation of completely anonymous egalitarian cryptocurrencies.

A number of our community members have been focused on research and development for more than a decade.

We aim to promote the derived principles to influence the contemporary economic paradigm.

The current power distribution on our planet is the legacy of the world where the economy is controlled by the few.

The status quo was shaped throughout centuries, making human beings engage in rat races, detrimental rivalry, and bloodshed.

In spite of humanity's hope to overcome local crises through education and internationalization, we still fail to have full control over our lives.

However, state-of-the-art advancements in technology, mathematics, and cryptography may become the key to subvert this paradigm.

The advent of cryptocurrencies is the first sign that the new world is coming.

It is marked with a hope that the economy will interlace with the technology, that communities will set new transparent principles, and impartial cryptographic algorithms will control its implementation.

It is in our philosophy to encourage enlightenment through breakthrough innovations.

Emancipation begins with laymen getting access to financial resources that will give the oppressed the hope for quality education, drinking water, and a better life.

CryptoNote is not about creating yet another digital currency.

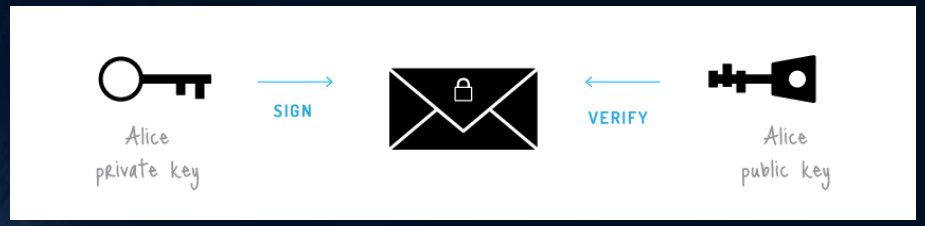
It is the mindset and concepts that represent the first small step to regain the power over ourselves in order to live peacefully and prosper.

Ring signatures: Untraceable payments

The ordinary digital signature (e.g. (EC)DSA, Schnorr, etc...) verification process involves the public key of the signer.

It is a necessary condition, because the signature actually proves that the author possesses the corresponding secret key.

But it is not always a sufficient condition.



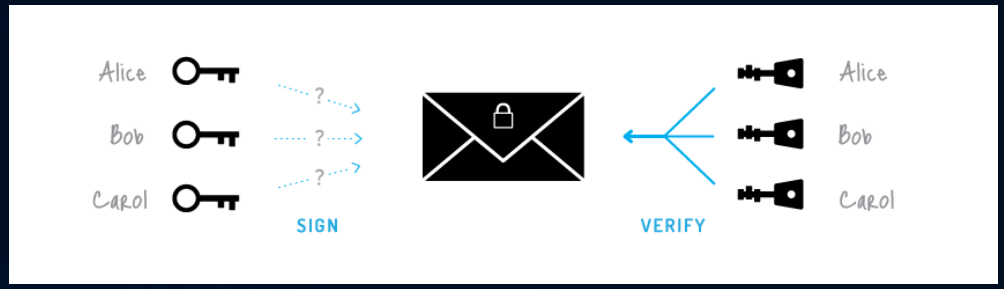
Ring signature is a more sophisticated scheme, which in fact may demand several different public keys for verification.

In the case of ring signature, we have a group of individuals, each with their own secret and public key.

The statement proved by ring signatures is that the signer of a given message is a member of the group.

The main distinction with the ordinary digital signature schemes is that the signer needs a single secret key, but a verifier cannot establish the exact identity of the signer.

Therefore, if you encounter a ring signature with the public keys of Alice, Bob and Carol, you can only claim that one of these individuals was the signer but you will not be able to pinpoint him or her.



Ring signatures: Untraceable payments

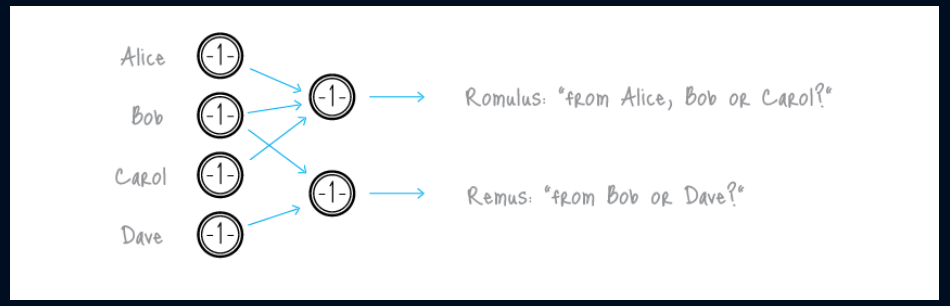
This concept can be used to make digital transactions sent to the network untraceable by using the public keys of other members in the ring signature one will apply to the transaction.

This approach proves that the creator of the transaction is eligible to spend the amount specified in the transaction but his identity will be indistinguishable from the users whose public keys he used in his ring signatures.

It should be noted that foreign transactions do not restrict you from spending your own money.

Your public key may appear in dozens of others' ring signatures but only as a muddling factor (even if you already used the corresponding secret key for signing your own transaction).

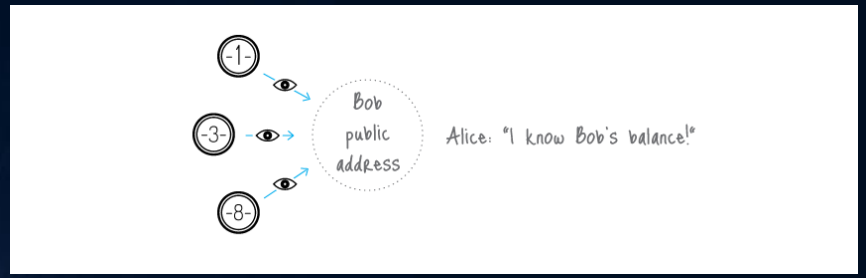
Moreover, if two users create ring signatures with the same set of public keys, the signatures will be different (unless they use the same private key).



One-time keys: Unlinkable transactions

Normally, when you post your public address, anyone can check all your incoming transactions even if they are hidden behind a ring signature.

To avoid linking you can create hundreds of keys and send them to your payers privately, but that deprives you of the convenience of having a single public address.



CryptoNote solves this dilemma by an automatic creation of multiple unique one-time keys, derived from the single public key, for each p2p payment.

The solution lies in a clever modification of the Diffie-Hellman exchange protocol.

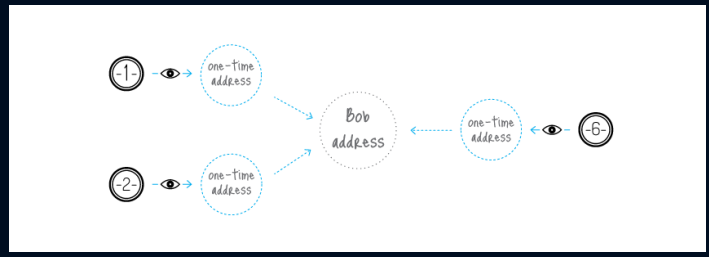
Originally it allows two parties to produce a common secret key derived from their public keys.

In our version the sender uses the receiver's public address and his own random data to compute a one-time key for the payment.

The sender can produce only the public part of the key, whereas only the receiver can compute the private part; hence the receiver is the only one who can release the funds after the transaction is committed.

He only needs to perform a single-formula check on each transactions to establish if it belongs to him.

his process involves his private key, therefore no third party can perform this check and discover the link between the one-time key generated by the sender and the receiver's unique public address.



An important part of our protocol is usage of random data by the sender.

It always results in a different one-time key even if the sender and the receiver both remain the same for all transactions (that is why the key is called "one-time").

Moreover, even if they are both the same person, all the one-time keys will also be absolutely unique.

Double-spending proof

Fully anonymous signatures would allow spending the same funds many times which, of course, is incompatible with any payment system's principles.

The problem can be fixed as follows.

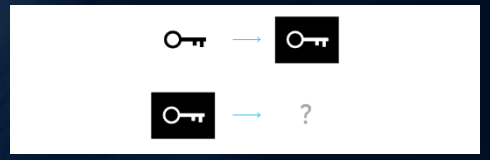
A ring signature is actually a class of crypto-algorithms with different features.

The one CryptoNote uses is the modified version of the "Traceable ring signature".

In fact we transformed traceability into linkability.

This property restricts a signer's anonymity as follows: if he creates more than one ring signature using the same private key (the set of foreign public keys is irrelevant), these signatures will be linked together which indicates a double-spending attempt.

To support linkability CryptoNote introduced a special marker being created by a user while signing, which we called a key image.



It is the value of a cryptographic one-way function of the secret key, so in math terms it is actually an image of this key.

One-wayness means that given only the key image it is impossible to recover the private key.

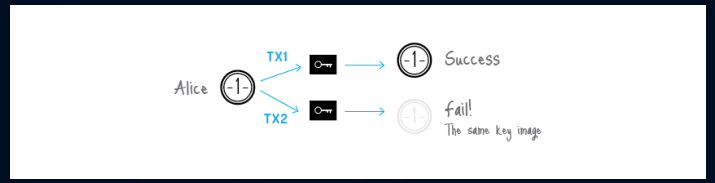
On the other hand, it is computationally impossible to find a collision (two different private keys, which have the same image).

Using any formula, except for the specified one, will result in an unverifiable signature.

All things considered, the key image is unavoidable, unambiguous and yet an anonymous marker of the private key.

All users keep the list of the used key images (compared with the history of all valid transactions it requires an insignificant amount of storage) and immediately reject any new ring signature with a duplicate key image.

It will not identify the misbehaving user, but it does prevent any double-spending attempts, caused by malicious intentions or software errors.



Standard CryptoNote transaction

A standard CryptoNote transaction is generated by the following sequence covered in the white paper.

Bob decides to spend an output, which was sent to the one-time public key.

He needs Extra (1), TxOutNumber (2), and his Account private key (3) to recover his one-time private key (4).

When sending a transaction to Carol, Bob generates its Extra value by random (5).

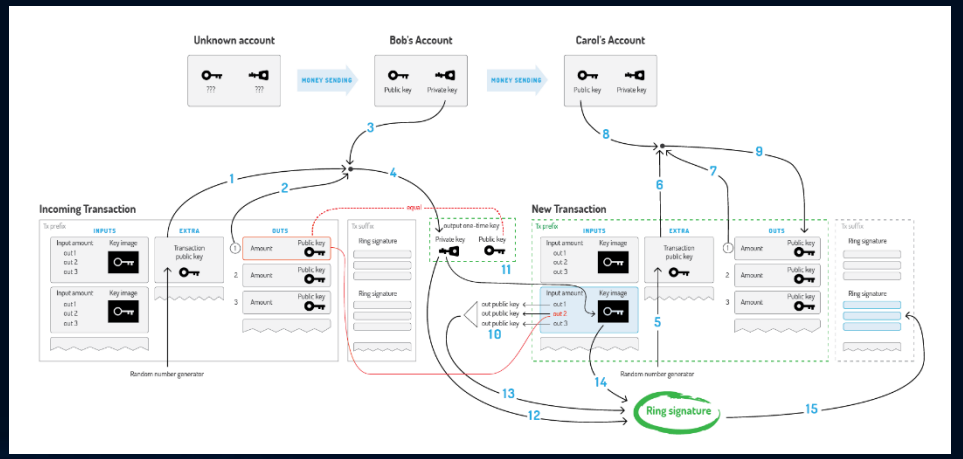
He uses Extra (6), TxOutNumber (7) and Carol's Account public key (8) to get her Output public key (9).

In the input Bob hides the link to his output among the foreign keys (10).

To prevent double-spending he also packs the Key image, derived from his One-time private key (11).

Finally, Bob signs the transaction, using his One-time private key (12), all the public keys (13) and Key Image (14).

He appends the resulting Ring Signature to the end of the transaction (15).



Adaptive limits

A decentralized payment system must not depend on a single person's decisions, even if this person is a core developer.

Hard constants and magic numbers in the code deter the system's evolution and therefore should be eliminated (or at least be cut down to the minimum).

Every crucial limit (like max block size or min fee amount) should be re-calculated based on the system's previous state.

Therefore, it always changes adaptively and independently, allowing the network to develop on it's own.

CryptoNote has the following parameters which adjust automatically for each new block:

- Difficulty.
- Max block size

Difficulty.

The general idea of our algorithm is to sum all the work that nodes have performed during the last 720 blocks and divide it by the time they have spent to accomplish it.

The measure of the work is the corresponding difficulty value for each of the blocks.

The time is calculated as follows: sort all the 720 timestamps and cut-off 20% of the outliers.

The range of the rest 600 values is the time which was spent for 80% of the corresponding blocks.

Max block size.

Let MN be the median value of the last N blocks sizes.

Then the "hard-limit" for the size of accepting blocks is 2*MN.

It averts blockchain bloating but still allows the limit to slowly grow with the time if necessary.

Transaction size does not need to be limited explicitly.

It is bounded by the size of the block.

Smooth emission

The upper bound for the overall amount of all digital coins is also digital:

- *MSupply = 2^{64} – 1 atomic units*

This is a natural restriction based only on the implementation limits, not on intuition like "N coins ought to be enough for everybody".

To make the emission process smoother CryptoNote uses the following formula for block rewards:

- *BaseReward = (MSupply – A) >> 18*

where A is amount of previously generated coins.

It gives a predictable growth of the money supply without any breakpoints.

Egalitarian proof of work

The proof of work mechanism is actually a voting system.

Users vote for the right order of the transactions, for enabling new features in the protocol and for the honest money supply distribution.

Therefore, it is important that during the voting process all participant have equal voting rights.

CryptoNote brings the equality with an egalitarian proof-of-work pricing function, which is perfectly suitable for ordinary PCs.

It utilizes built-in CPU instructions, which are very hard and too expensive to implement in special purpose devices or fast memory-on-chip devices with low latency.

We propose a new memory-bound algorithm for the proof-of-work pricing function.

It relies on random access to a slow memory and emphasizes latency dependence.

As opposed to scrypt, every new block (64 bytes in length) depends on all the previous blocks.

As a result a hypothetical "memory-saver" should increase his calculation speed exponentially.

Our algorithm requires about 2 Mb per instance for the following reasons:

1. It fits in the L3 cache (per core) of modern processors, which should become mainstream in a few years;

2. A megabyte of internal memory is an almost unacceptable size for a modern ASIC pipeline;

3. GPUs may run hundreds of concurrent instances, but they are limited in other ways: GDDR5 memory is slower than the CPU L3 cache and remarkable for its bandwidth, not random access speed.

4. Significant expansion of the scratchpad would require an increase in iterations, which in turn implies an overall time increase.

"Heavy" calls in a trust-less p2p network may lead to serious vulnerabilities, because nodes are obliged to check every new block's proof-of-work.

If a node spends a considerable amount of time on each hash evaluation, it can be easily DDoSed by a flood of fake objects with arbitrary work data (nonce values).

One of the proof-of-work algorithms that is in line with our propositions is CryptoNight, created by Bytecoin developers in a cooperation with our team.

It is designed to make CPU and GPU mining roughly equally efficient and restrict ASIC mining.

Заключение

Представленный путь развития Сольдо в громадной мере зависит от изменения курса монеты.

Запланированные проекты на базе Сольдо требуют инвестиций, если рынок не заинтересуется проектами, запланированными на базе Сольдо, Команда проекта не сможет получить достаточного финансирования и часть проектов так и останется проектами.

Так что, как бы не банально это звучало – будущее зависит от вас.

2018