
VERGE
Самая конфиденциальная криптовалюта
BLACKPAPER

1.0 Вступление

Криптовалюта Bitcoin была разработана и выпущена в 2009 году с целью решить актуальную проблему обработки платежей в Интернете. В своей публикации «Биткоин: цифровая пиринговая наличность» автор под псевдонимом Сатоши Накамото утверждает, что интернет-коммерция зависима от финансовых институтов, которые при обработке платежей выступают как доверенные посредники. Несмотря на то, что система неплохо функционирует, слабым местом существующей модели остается проблема доверия.

С 2009 года Bitcoin используется в качестве платежного средства на многих торговых площадках. Увеличение спроса на Bitcoin и распространение этой криптовалюты привело к тому, что оригинальный блокчейн не может быстро обрабатывать большое количество транзакций. Чтобы увеличить скорость обработки платежных операций приходится увеличивать транзакционные сборы.

Особенность валюты Bitcoin – её децентрализованная структура. В отличие от традиционных фиатных валют Bitcoin не контролируется каким-либо центральным органом, а значит, не имеет центрального хранилища информации или пункта управления. Тем не менее, одним из главных недостатков Bitcoin является централизация большинства интернет-сервисов и компаний, формирующих экосистему. Это значит, что большинство операций в экосистеме совершается узким кругом лиц и компаний, которые используют уязвимые компьютерные системы и подвержены правовым трудностям и другим ньюансам.

Verge – одна из настоящих децентрализованных валют на сегодняшний день. Основанный на ценностях и видении Bitcoin проект Verge поднимает анонимность цифровой личности, конфиденциальность данных и децентрализацию на новый уровень.

2.0 Сеть Tor

Tor (сокр. от. англ. «The Onion Router») – система прокси-серверов, которая позволяет устанавливать анонимное сетевое соединение. Tor перенаправляет трафик в зашифрованном виде через анонимную сеть виртуальных туннелей, состоящую из более чем 7000 узлов, скрывая местоположение пользователя. Слои зашифрованной информации напоминают лук, что и дало название сервису. Задача Tor – защищать персональные данных пользователей, их свободу и сохранять анонимность коммуникации.

Маршрутизация Tor обеспечивается шифрованием на уровне приложения в стеке протоколов коммуникаций, составленных как слои лука. Tor несколько раз кодирует данные, включая IP-адрес следующего узла сети, и отсылает их через виртуальную сеть случайно выбранных последовательных узлов-зеркал. Каждый узел расшифровывает только ту часть пакета данных, которая позволяет понять, откуда и куда направляется весь пакет. После этого данные вновь зашифровываются и передаются далее по сети. Конечный узел расшифровывает внутренний слой и отсылает оригинальные данные получателю, не раскрывая адрес отправителя.

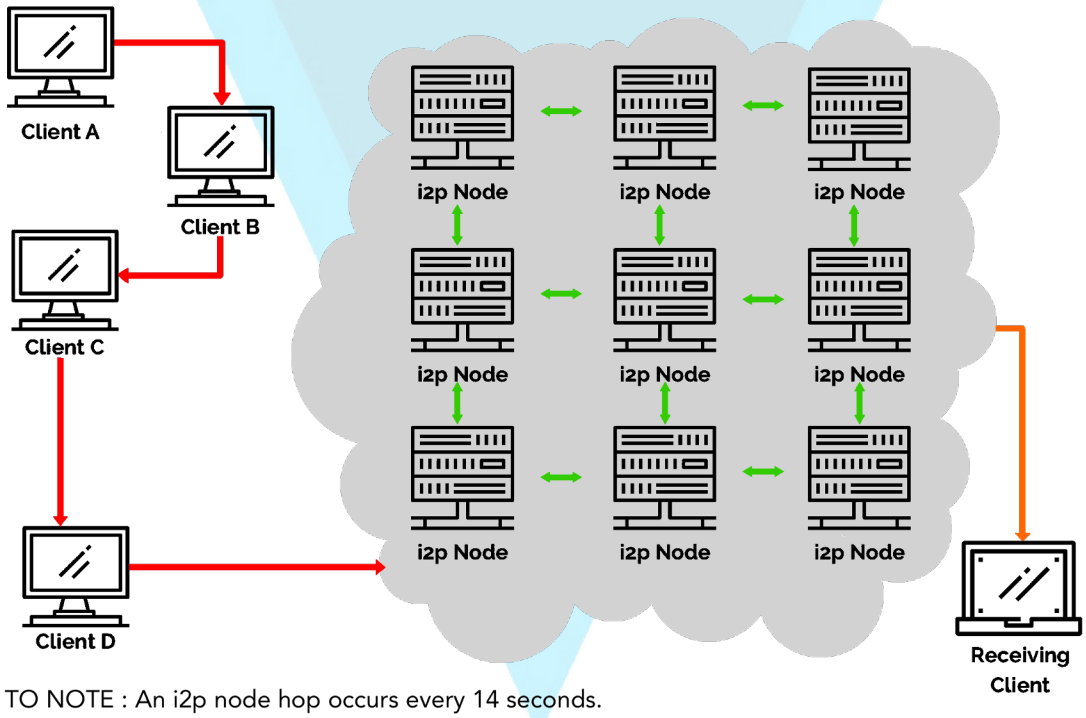
2.1 Интеграция Tor

Маршрутизация коммуникаций, при которой информация скрыта на каждом прыжке между узлами Tor, исключает возможность обнаружения связи между отправителем и получателем, поскольку для этого необходимо установить источник и конечный пункт доставки информации.

3.0 Интеграция I2P

Изначальная цель i2P – скрывать размещенные сервера в неизвестных локациях. i2P, как и сеть Tor, обладает многочисленными преимуществами. Оба сервиса предоставляют анонимный доступ к онлайн-контенту, используют маршрутную структуру P2P и многослойное шифрование данных. Тем не менее, сервис i2P был задуман как «сеть внутри интернета» (см. рисунок 2.1), которая не выпускает трафик за свои пределы. i2P, в отличие от Tor, работает по принципу пакетной, а не сетевой маршрутизации. Данная особенность позволяет i2P динамически обходить загруженные маршруты и сервисные разрывы и напоминает IP-маршрутизацию в Интернете. Это обеспечивает высокий уровень надежности и невысокую загруженность i2P-сети.

Figure 2.1
How an i2p Transaction Occurs



TO NOTE : An i2p node hop occurs every 14 seconds.

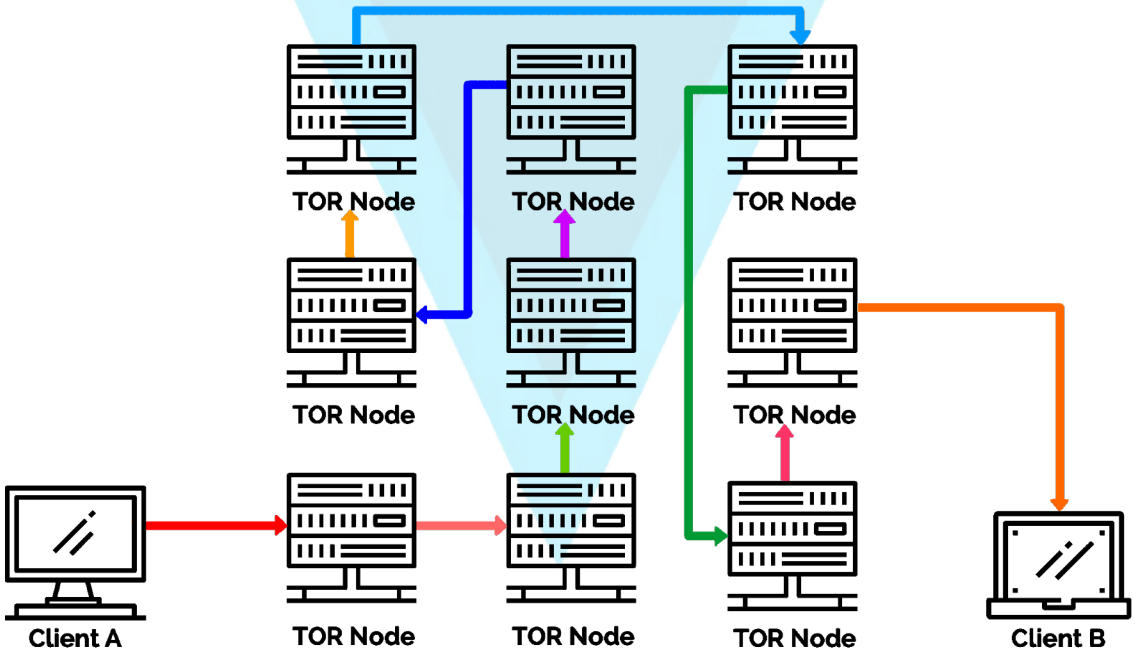
При первом коммуникации двух пользователей запрос отправляется в общую распределенную «сетевую базу». Эта структурированная распределенная хэш-таблица (DHT) на основе алгоритма Kademlia [2] позволяет эффективно находить внутренние туннели другого клиента. Последующий обмен данным между клиентами содержит эту информацию, что исключает необходимость повторных запросов.

3.1 Интеграция I2P

i2P - это высокозащищенный туннельный сервис, который использует ipv6 для анонимизации всех данных Verge, передаваемых в сети. Каждый клиент имеет свой iP2-маршрутизатор, построенный на нескольких входящих и исходящих туннелях: последовательности пиров, которые передают данные в одном направлении (к или от клиента, соответственно). При отправке данных Verge приложение пропускает сообщение через один из исходящих туннелей.

В отличии от Tor, который полагается на централизованный набор служб каталогов, i2P использует две распределённые хэш-таблицы (DHTs) для функционирования сети. DHTs предназначены для привязки хэш-значений к контенту, используя распределенный и децентрализованный механизм. Главное преимущество DHTs состоит в масштабируемости, необходимой для качественной работы децентрализованной сети P2P, увеличения трафика и количества транзакций. i2P не полагается на доверенную службу каталогов, чтобы получить маршрутную информацию. Сетевые пути формируются и обновляются динамически. Каждый маршрутизатор сверяет данные с другими узлами сети. Наконец, i2P устанавливает два независимых симплексных туннеля для трафика, который проходит через сеть, в отличие от формирования одной дуплексной схемы, как это делает Tor (см. рисунок 1.1).

Figure 1.1
How a TOR Transaction Occurs



TO NOTE: A TOR nod hop occurs every 10 minutes.

4.0 Electrum

Сильные стороны Electrum – скорость, простота и оптимизация технологии. Electrum использует безопасные удаленные сервера, обрабатывающие компоненты Verge, и делает возможным восстановление кошельков при помощи секретной комбинации слов. Electrum предлагает удобный холодный кошелек, где пользователи могут хранить монеты оффлайн. Он также является одним из немногих кошельков, поддерживающих Tor и i2P. Интегрируя Electrum, Tor и i2P, Verge сохраняет конфиденциальность пользователей, использующих мобильный/ПК кошелек. IP-адрес и информация о транзакциях защищены и сокрыты для промежуточных серверов. Это повышает конфиденциальность данных пользователей.

Electrum поддерживает мультиподпись, которая требует несколько ключей для подтверждения транзакции. Стандартные транзакции в сети Verge можно назвать «транзакциями с одной подписью» [4], поскольку для подтверждения требуется всего одна подпись от владельца закрытого ключа соответствующего адреса Verge. Во время отправки монет транзакция Electrum запрашивает несколько подписей. В свою очередь, Verge требует адреса нескольких сторон для проверки данных.

Например:

> Один кошелек Electrum находится на Вашем ПК, а другой – на смартфоне. Монеты не могут быть потрачены без подписи на обоих девайсах, следовательно злоумышленник должен получить доступ к обоим устройствам, чтобы украсть монеты.

Главные особенности и преимущества кошелька Electrum:

Генерирование ключей

в случае утери кошелька, вы можете его восстановить, используя секретную комбинацию. Таким образом, вы защищены от случайных ошибок.

Моментальное использование

клиентское приложение не загружает весь блокчейн, а подкачивает необходимую информацию с сервера. Обновленный кошелек всегда готов к использованию.

Локальное подтверждение транзакций

ваши приватные ключи не передаются на сервер, и вам не нужно доверять серверу свои монеты.

Свобода и конфиденциальность

сервер Electrum не хранит учетные записи пользователей. Вы не привязаны к определенному серверу, а он не может вас распознать. Более того, серверы Verge и i2P Electrum даже не получают IP-адрес пользователя. Вы можете экспортировать свои личные ключи, потому что вы – полноценный хозяин своего кошелька.

5.0 Поддержка мульти-алгоритмов майнинга

Verge – это криптовалюта с поддержкой многих алгоритмов. Пользователи с разными типами майнинг-девайсов имеют равные возможности заработать монеты. Verge одна из немногих криптовалют с поддержкой пяти хэш-функций на одном блокчейне. Такая особенность повышает безопасность, а также делает Verge более доступной для тех, кто хотел бы майнить монеты XVG. Это способствует более равномерному распределению монет среди пользователей.

Общий объем эмиссии Verge составляет 16,5 млрд. монет. Наличие пяти Proof-of-Work алгоритмов (Scrypt, X17, Lyra2rev2, myr-groestl и blake2s), поддерживаемых блокчейном Verge – то, что отличает Verge от других криптовалют. Время формирования блока во всех алгоритмах – около 30 секунд. Сложность майнинга зависит только от хэшрейта того или иного алгоритма. Данная структура майнинга защищает от «51-процентных атак».

6.0 Android Tor + I2P

Verge – лидер в мобильном крипто-пространстве. Именно разработчики Verge создали два уникальных и первых в своем роде кошелька Android, один из которых работает через сеть Tor, а второй использует сервис i2P. Кошельки Verge Tor и Verge i2P построены по принципу анонимности и не могут устанавливать соединение или передавать информацию через Clearnet. Транзакции выполняются при помощи Simple Payment Verification (SPV) – технологии, описанной в публикации Сатоши Накамото. Кошельки подтверждают транзакции по принципу включения (Proof of Inclusion: транзакции в блоке подтверждаются без необходимости загружать полный блок, как и в случае Electrum).

С SPV подтверждение транзакций происходит почти моментально, поскольку облегченное приложение загружает только шапки блоков, которые весят намного меньше, чем цельные блоки. Для обеспечения дополнительного уровня защиты кошельки Verge Tor & i2P обладают встроенными функциями, такими как 4-значный пин-код и блокировка по отпечатку пальца. Более того, кошельки Verge Tor & i2P позволяют сканировать P2P QR-код и моментально подтверждать транзакции. Пользователи могут импортировать QR-код из бумажного кошелька и при необходимости восстанавливать баланс «холодного кошелька».

7.0 Будущее развитие: RSK

Rootstock (известный как RSK) - это двухсторонний привязанный «боковой» (sidechain) блокчейн, который добавляет функцию умных контрактов в сети Verge. RSK представляет собой внесетевой протокол для моментальных платежей и является независимым блокчейном без собственного токена. RSK использует уже существующие токены (например, Verge), привязывая цены умного токена RSK к токену Verge в пропорции 1:1. Таким образом, цена RSK токена абсолютно соответствует Verge, и пользователи могут без труда обменивать токены между двумя цепями.

Смарт-контракт RSK работает следующим образом: пользователь помещает Verge в резерв, удерживающий токены, который используется, чтобы подкрепить RSK токен – smartXVG. Представьте себе дебетовый счет, на который перечисляются монеты Verge, после чего счет используется для транзакций в сети RSK. Простые контракты для Bitcoin существуют уже некоторое время и позволяют пользователям создавать контракты с мультиподписью, что требует подтверждения транзакции несколькими пользователями. Благодаря интеграции RSK на Verge, простые контракты выходят на совершенно новый уровень и получают функции смарт-контрактов (аналог – платформа Ethereum).

Еще одно из преимуществ RSK – это масштабируемость. На сегодняшний день RSK обрабатывает 400 транзакций в секунду. Это намного больше аналогичного показателя Verge (100 тр/с). Команда разработчиков RSK намерена увеличить пропускную способность до 2000 тр/с, благодаря новой технологии Lumino. Согласно публикации LCTP, Lumino является дополнительной платежной системой, основанной на протоколе Lumino Transaction Compression Protocol. LTCP сравним с Lightning Network – решением для масштабируемости, которые было разработано для Bitcoin и используется Litecoin.

8.0 Будущее развитие : Discord & Telegram P2P

Осуществление транзакций Peer-to-Peer(P2P) в Discord доступна с августа 2017 года. Осуществление транзакций в Telegram находится в разработке (ожидаемая дата релиза – конец августа 2017).

Telegram – это бесплатный облачный мессенджер для Android, iOS, Windows Phone, Windows NT, macOS и Linux. Telegram использует симметричную систему шифрования, известную как MTProto. Протокол был разработан Павлом Дуровым и другими разработчиками Telegram и использует 256-битное симметричное AES-шифрование, RSA 2048 шифрование и протокол Диффи-Хеллмана.

P2P – онлайн-технология, позволяющая пользователям отправлять криптовалюты через интернет и мобильные устройства. Для этого потребитель использует онлайн-приложение (в данном случае бота). Получатель указывается по имени пользователя. Когда монеты отправляются получателю, ему приходит оповещение от онлайн-бота, которое сообщает, что сумма была доставлена на сгенерированный адрес. Пользователь может управлять ботом с помощью простой команды “!withdraw”, после чего он получает инструкции по выдаче монет Verge. Сервис не требует никакой информации помимо суммы для отправки и имени пользователя-получателя. Конфиденциальная информация: IP-адрес, местоположение и имя скрываются. Ваша цифровая личность за пределами транзакции остается полностью анонимной.

Verge – одна из немногих криптовалют с уже существующими P2P-решениями для Twitter, Reddit, Internet Relay Chat (IRC), Slack и Steam. Благодаря этому можно легко отправить Verge любому пользователю этих социальных платформ.

9.0 Ссылки и источники

[1] Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

[2] I2P: A scalable framework for anonymous communication - I2P. (n.d.). Retrieved from https://geti2p.net/en/docs/how/tech-intro

[3] Multisignature - Bitcoin Wiki. (n.d.). Retrieved August 8, 2017, from https://en.bitcoin.it/wiki/Multisignature

[4] Voegtlin, T. (n.d.). Welcome to the Electrum Documentation! — Electrum 2.5 documentation. Retrieved August 8, 2017, from http://docs.electrum.org/en/latest/

Дополнительные ссылки

Gribble, S., Brewer, E., Hellerstein, J., & Culler, D. (2000, October 23). Scalable, Distributed Data Structures for Internet Service Construction. Retrieved from https://www.usenix.org/legacy/events/osdi2000/full_papers/gribble/gribble_html/index.html

Anonymity and the Block Chain • IHB News™. (2014, November 18). Retrieved August 08, 2017, from https://ihb.io/2014-11-17/news/anonymity-block-chain-13570

Holden, E. (2017, July 18). An Introduction to Tor vs I2P. Retrieved August 08, 2017, from https://www.ivpn.net/privacy-guides/an-introduction-to-tor-vs-i2p

Distributed hash table. (n.d.). Retrieved August 08, 2017, from http://infoanarchy.org/Distributed_hash_table

Scharr, J. (2013, October 23). What Is Tor - How Does Tor Work - How to Use Tor. Retrieved August 08, 2017, from https://www.tomsguide.com/us/what-is-tor-faq,news-17754.html

Durumeric, Z., Wustrow, E., & Halderman, J. (2013). ZMap: Fast Internet-Wide Scanning and its Security Applications. Retrieved from https://zmap.io/paper.pdf

Voegtlin, T. (2015). Simple Payment Verification — Electrum 2.5 documentation. Retrieved from http://docs.electrum.org/en/latest/spv.html

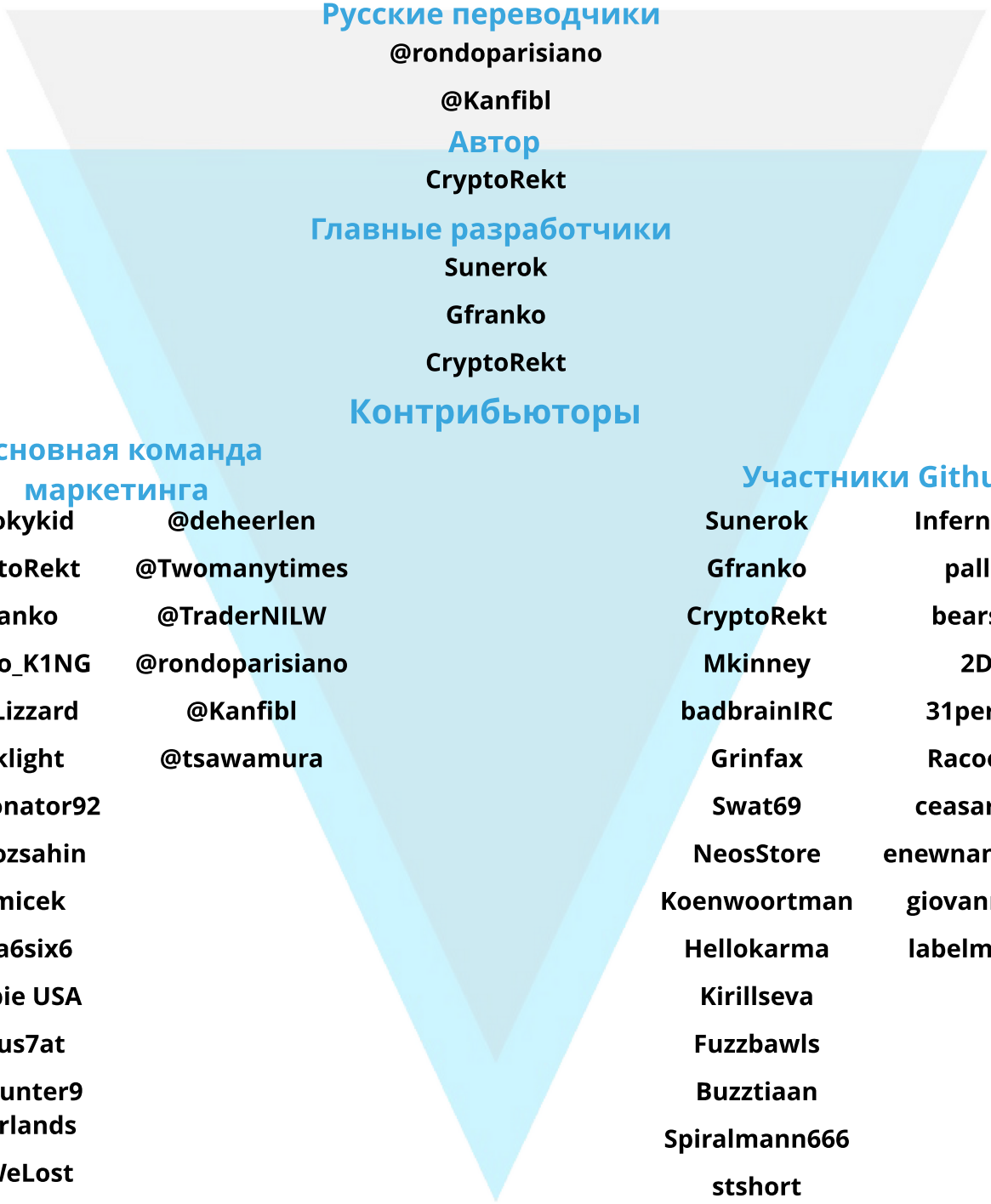
SPV, Simplified Payment Verification - Bitcoin Glossary. (2017). Retrieved from https://bitcoin.org/en/glossary/simplified-payment-verification

https://atlas.torproject.org/#search/flag:authority

http://torstatus.blutmagie.de/

10.0 Контрибьюторы

Мы хотели бы поблагодарить всех, кто помогает развивать проект, но в особенности этих людей:



Русские переводчики

@rondoparisiano

@Kanfibl

Автор

CryptoRekt

Главные разработчики

Sunerok

Gfranko

CryptoRekt

Контрибьюторы

Основная команда маркетинга

@Spookykid

@CryptoRekt

@gfranko

@Crypto_K1NG

@JtheLizzard

@lucklight

@Cryptonator92

@feyziozsahin

@Slemicek

@Trilla6six6

@Dabbie USA

@Cyrus7at

@Thehunter9 Netherlands

@GGWeLost

@Jeanralphio69

@Crypth

@deheerlen

@Twomanytimes

@TraderNILW

@rondoparisiano

@Kanfibl

@tsawamura

Участники Github

Sunerok

Gfranko

CryptoRekt

Mkinney

badbrainIRC

Grinfax

Swat69

NeosStore

Koenwoortman

Hellokarma

Kirillseva

Fuzzbawls

Buzztiaan

Spiralmann666

stshort

alcy0ne

chisustation

ShapeShifter499

Infernoman

pallas1

bearsylla

2Dai

31percent

Racoooon

ceasarpolar

enewnanwebdev

giovanni1186

labelmeagod

Контакты

Twitter Telegram Slack Facebook IRC Reddit Steam Verge Discord BitCoinTalk Radio Station