
VERGE
The most privacy focused cryptocurrency
BLACKPAPER

1.0 Introduction

인터넷에서 일어나는 트랜잭션들의 내재된 결함을 해결하고자 2009년에 비트코인이 개발되고 출시되었다. Nakamoto는 그의 게시글에서 "온라인 전자 거래는 신뢰할 수 있는 제3자의 역할을 하는 금융기관에 거의 무조건 의존하는 상황까지 왔다. 대부분 트랜잭션에 대해서는 이 시스템이 잘 동작하지만, 그래도 신뢰기반 모델 특성상의 결함들로부터는 자유롭지 못하다." 라고 얘기했다. 2009년에 공개된 이후로, 비트코인은 여러 시장에 급속도로 퍼지고 있다. 비트코인의 급성장의 대표적인 이유는 여러가지 대용량 트랜잭션을 처리하기 위한 오리지널 블록체인의 수요 증가이다. 수요 증가는 트랜잭션 지연 시간의 증가로 이어졌고, 트랜잭션 확인 속도를 높이기 위해 더 높은 트랜잭션 비용으로 이어졌다.

비중앙집중화 구조는 비트코인의 주요 혁신점이다. 이전의 명목화폐와는 달리, 비트코인은 중앙 통제, 정보의 중앙집중화, 중앙 관리, 중앙 결점이 없다. 하지만, 비트코인을 기반으로 생겨난 대부분의 실제 온라인 서비스나 온라인 비즈니스는 중앙집중화되있다는 문제가 있다. 현재 시스템들의 중앙집중성 때문에 온라인 거래는 "취약한"() 컴퓨터 시스템을 사용하는 특정 지역의 사람들에 의해 돌아간다. Verge는 비트코인의 핵심을 충실히 반영하려고 노력했고, 또다른 새로운 익명성을 실현했다. Verge는 현재 사용 가능한 진정한 비중앙집중화된 화폐 중에 하나이다.

2.0 Tor Integration

Tor는 소프트웨어 프로젝트인 The Onion Router의 줄임말로서, 계층화 된 회로 기반 네트워크에서 익명 통신을 가능케 해주는 IP 암호화 서비스이다. Tor는 사용자의 위치와 사용 내역을 네트워크 감시 또는 트래픽 분석을 하는 사람으로부터 숨기기 위해, 인터넷 트래픽을 7천 개 이상의 relay를 가지는 무료 worldwide volunteer overlay network로 가게 한다. 이름이 Onion Router인 이유는, Tor이 데이터 패킷을 익명화할 때 사용되는 여러 암호화된 주소 정보의 레이어가 양파를 닮았기 때문이라고 한다. 이 레이어 때문에 Tor 네트워크를 지나는 데이터 패킷의 경로를 완벽히 추적하기 힘들다. Tor의 목적은 유저의 개인 정보를 보호하고, 온라인 활동 내역을 모니터링으로부터 지켜줌으로써 신뢰성 있는 통신의 자유와 능력을 보장해주는 것이다.

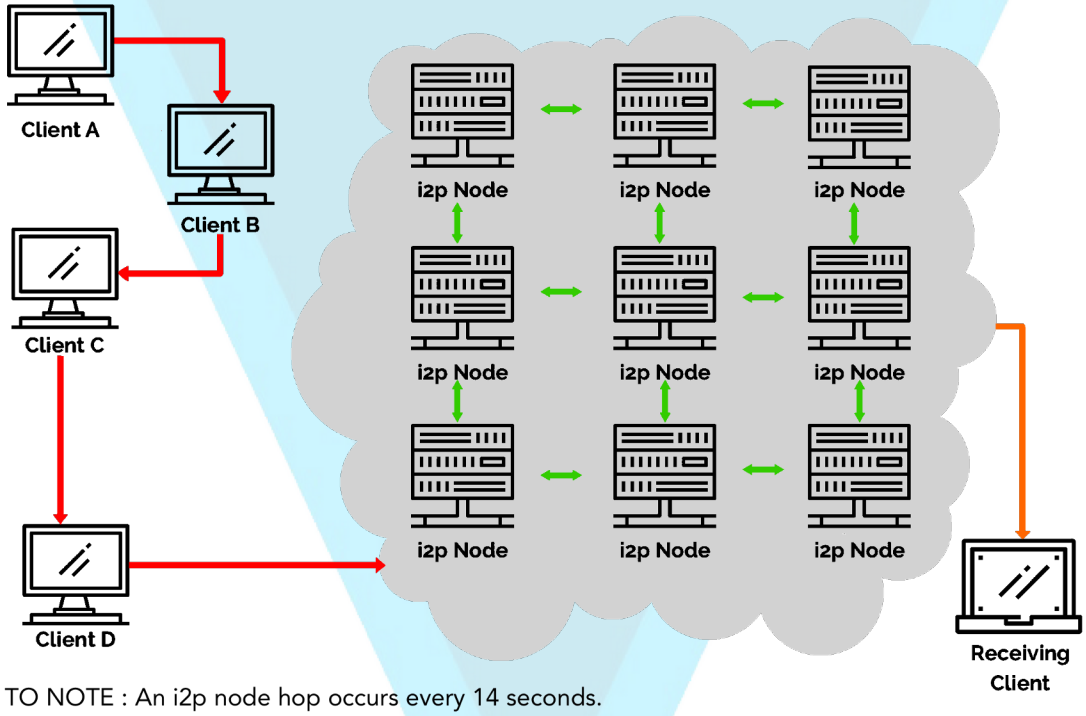
Onion 라우팅은 통신 프로토콜 레이어 중 application layer의 암호화를 통해 이루어지는데, 양파의 모양처럼 여러 레이어의 형태로 암호화한다. Tor은 다음 노드의 목적지 IP를 포함한 데이터를 여러번 암호화시킨 후, 연속적이면서 랜덤으로 선택된 Tor relay들을 가지는 가상 회로를 통과시킨다. 각 relay는 데이터 패킷 wrapper의 일부를 복호화시키는데, 이전 relay와 다음 relay만 알 수 있을 정도로만 복호화시킨다. 그 후 relay는 데이터를 새로운 wrapper로 묶고 다음 relay로 보낸다. 마지막 relay는 암호화 레이어 중 가장 밑단의 레이어를 복호화하고, 암호화되기 전 원래 데이터를 최종 목적지로 보낸다. 이 때 마지막 relay는 이 데이터의 소스 IP를 공개하지 못하며 심지어 알지도 못하는 채로 데이터를 전송하게 된다.

Tor 회로의 각 노드에서 라우팅 정보가 일부 숨겨지기 때문에, 소스와 목적지 정보에 의존하는 네트워크 감시를 통해 통신 peer를 알아낼 수 있는 지점은 존재하지 않게 된다.

3.0 I2P Integration

I2P는 알려지지 않은 지역에서 서버를 관리하기 위해 필요한 hidden service를 제공하기 위해 개발되었다. I2P도 Tor의 장점을 많이 가지고 있다. 둘 다 익명 접속을 가능하게 하고, P2P 형태의 라우팅 구조를 이용하며, 레이어 암호화를 통해 동작한다. 차이점은, I2P는 트래픽이 특정 경계선 안에서만 이동하는 "인터넷 안의 네트워크"를 구현하려고 했다는 것이다. 그리고 I2P는 Tor의 회로 기반 라우팅과 달리 패킷 기반 라우팅을 사용한다. 이것이 가져오는 장점은, 인터넷의 IP 라우팅과 유사하게 트래픽 정체나 서비스 중단을 dynamic하게 우회하는 라우팅이 가능해진다는 것이다. 이것은 I2P 네트워크에 더 높은 레벨의 신뢰도와 반복성을 제공한다.

Figure 2.1
How an i2p Transaction Occurs



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

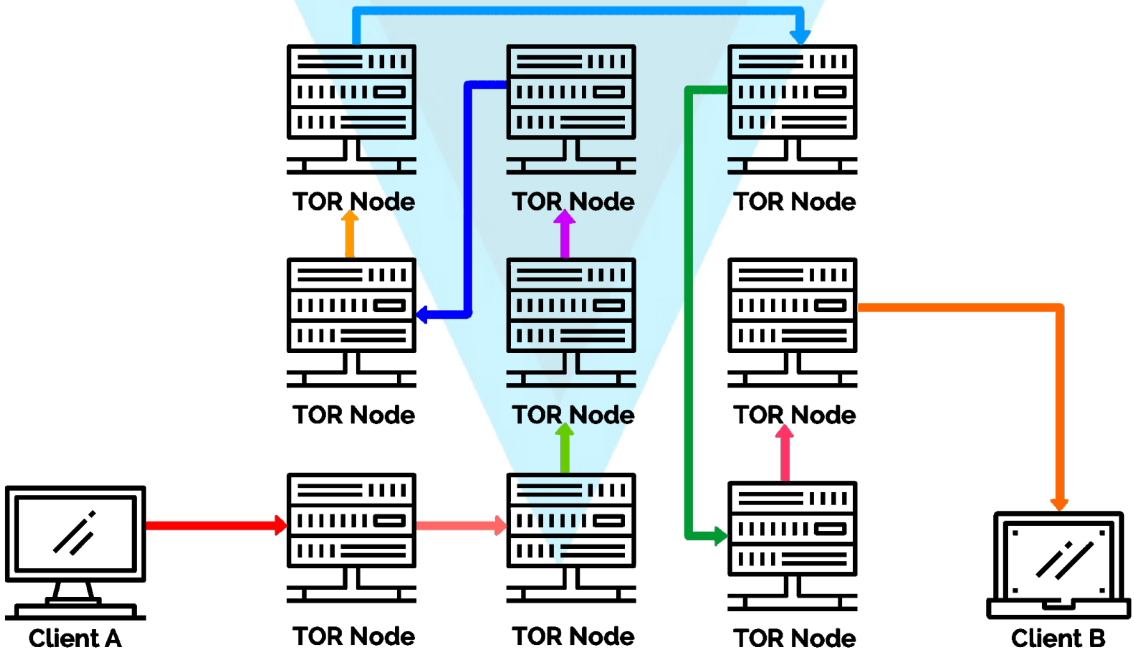
어떤 클라이언트가 다른 클라이언트와 첫 통신을 할 때, 완전히 분산된 "네트워크 데이베이스" (Kademlia 알고리즘에 기반한 DHT의 변형 형태)에 쿼리를 날리게 된다. 이것은 다른 클라이언트의 접촉점을 효율적으로 찾는 데 사용된다. 이후의 데이터 패킷에는 주로 그 정보가 포함돼있기 때문에 더 이상의 네트워크 데이베이스 lookup은 필요없게 된다.

3.1 I2P Integration

I2P는 자신의 네트워크를 통해 보내지는 모든 Verge 데이터를 익명화시키는, IPv6를 사용하는 높은 수준의 난독화 터널링 서비스이다. 각 클라이언트 애플리케이션은 각자의 I2P 라우터로 하여금 여러 개의 입구와 출구 "터널"을 만들게 한다. 여기서 터널은 peer의 배열을 뜻하는데, 이 peer들은 데이터를 보내거나 받을 때 중간에서 데이터를 받아 넘기는 역할을 해준다. 이렇게 되면 클라이언트가 다른 클라이언트에게 데이터를 보내고 싶을 때, 송신자의 애플리케이션이 데이터를 출구 터널 중 하나로 내보내게 되고 수신자의 입구 터널로 향하게 되어, 목적지에 결국 도착하게 된다.

I2P는 네트워크 state를 파악하기 위해, Tor처럼 중앙집중된 디렉토리 서버에 의존하기 보다는 두 개의 분산된 해쉬 테이블을 사용한다. DHT, 즉 분산 해쉬 테이블은 해쉬값: content 매핑을 위한 분산된, 비중앙집중화된 메커니즘이다. DHT의 최대 장점은 scalability이다. 좋은 비중앙집중화 P2P 네트워크는 자신의 서비스에 대한 scalability를 필요로 하는데, 이것은 content나 트랜잭션 sharing의 크기가 요구에 맞게 계속 늘어날 수 있음을 보장하기 위해서이다. 그리고 I2P는 루트 정보를 얻기 위해 신뢰된 디렉토리 서비스에 의존하지 않는다. 대신, 네트워크 루트들이 서로를 매순간 연산하며 dynamic하게 루트가 생성되고 업데이트된다. 마지막으로 I2P는 각 호스트 간의 데이터 전송을 위해, Tor의 단일 양방향 회로와 달리 두 개의 독립적인 단방향 터널을 사용한다. (figure 1.1 참고).

Figure 1.1
How a TOR Transaction Occurs



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

4.0 Electrum

Electrum의 장점은 속도와 단순함, 그리고 적은 자원 사용량이다. Verge 네트워크의 가장 복잡한 부분을 다루기 위해 안전한 원격 서버를 사용하고, 유저들이 비밀 문구를 통해 지갑을 복구할 수 있게 해준다. 그리고, Electrum은 간단하면서 쓰기 쉬운 cold storage solution을 제공한다. 이것은 유저가 자신의 코인을 오프라인에서 일부 또는 전부 저장할 수 있게 해준다. 또, Electrum은 Tor와 I2P를 native하게 지원하는 유일한 지갑이다. Electrum을 Tor와 I2P와 결합함으로써 데스크탑 또는 모바일 지갑을 사용할 때 익명성을 보장할 수 있다. IP 주소 정보나 트랜잭션 정보가 클라이언트와 연결돼있는 서버에 노출되지 않기 때문에 개인 정보 보호가 향상된다.

Electrum은 다중서명 기능을 지원한다. 이것은 Electrum 트랜잭션을 허가시키기 위해서는 두 개 이상의 키가 필요하다는 것이다. Verge 네트워크 상의 일반 트랜잭션은 "단일서명 트랜잭션"이라 불릴 수 있다. 왜냐하면 Verge 주소 소유자의 비밀키만 필요하기 때문이다. 다중서명을 가지는 Electrum 트랜잭션은 코인이 전달되기 전에 여러 사람의 서명이 필요하다. 다중서명이 나오게 된 배경은, 여러 집단의 주소들이 제공되면서, 그 집단들과 어떠한 거래를 하기 위해서는 모든 집단의 협조가 필요하게 됐다는 것이다.

> 다음은 그 예시이다 : "하나의 Electrum 지갑은 컴퓨터에 있고, 다른 지갑은 스마트폰에 있다. 이 코인들은 두 개의 디바이스 모두에서 서명이 되어야 사용할 수 있다. 즉, 이 코인들을 훔치기 위해서는 두 디바이스에 모두 접근권이 있어야 한다."

Electrum 지갑의 주요 특징

Deterministic Key Generation
지갑을 잃어버리면, 그 seed로부터 복구할 수 있다. 자신의 실수로부터는 보호받을 수 있다.

Instant On
클라이언트는 blockchain을 다운받지 않고, 서버에 blockchain 정보를 요구해야한다. 딜레이가 없고, 항상 최신 상태로 업데이트 된다.

Locally signed Transactions
Electrum 서버는 유저 계정을 저장하지 않는다. 그리고 비밀키를 export할 수 있다. 즉, 유저마다 고유의 주소를 가진다.

Freedom and Privacy
Electrum 지갑은 어떠한 script도 내려받지 않는다. 중재 서버는 임의적인 코드를 보낼 수 없으며 당신의 코인을 훔칠 수 없다.

5.0 Multi-Algorithm Support

Verge는 다양한 마이닝 장비를 보유한 사람들이 코인 수입에 동등하게 액세스 할 수 있도록 설계된 multi-algorithm 암호화 화폐이다. 이것은 5개의 hash 함수를 하나의 blockchain에 결합하는 것을 지원하는 유일한 암호화 화폐이다. 그 결과 보안이 향상되고 다양한 사람들과 장비가 Verge를 마이닝할 수 있으므로 당연히 모든 사람에게 Verge의 균등 분배가 보장된다.

Verge의 전체 공급은 165억개의 coins 이다. Verge가 다른 암호화 화폐에 비해 두드러지는 것은 Scrypt, X17, Lyra2rev2, myr-groestl, blake2s 와 같은 블록체인 위에서 돌아가는 5 Proof-of-Work(PoW) 알고리즘이다. 5개 알고리즘 모두 30초의 block target block time을 갖는다. 난이도는 오직 알고리즘의 hash rate에 영향을 받는다. 이로 인해 보안이 향상되고 51% 공격으로부터 보호가 가능하다.

6.0 Android Tor + I2P

Verge는 안드로이드 암호화 화폐에서 혁신의 선두주자이다. 우리는 두 종류의 독창적이고 최초격인 안드로이드 wallets을 개발했다. 하나는 The Onion Router Network(Tor)에서만 운영되고, 다른 하나는 The Invisible Internet Project(I2P)에서만 운영된다. Verge Tor, I2P는 익명성을 전제로 구축되었다. 즉 지갑에는 Clearnet을 통해 사용자 정보에 connect하거나 broadcast 할 수 있는 기능이 없다. 트랜잭션은 Simple Payment Verification(SVP)를 통해 완료된다. 이 기술은 Nakamoto Satoshi 논문에 나와있듯이 지갑이 전체 트랜잭션을 다운로드 하지 않고도 블록에 특정 트랜잭션이 포함되어 있는지 확인하는 방법인 proof of inclusion 을 통해 트랜잭션을 확인할 수 있게한다. Electrum wallet functions 이 동작하는 방식과 유사하다.

SVP는 거의 즉시 결제 확인이 가능하다. 왜냐하면 이것은 전체 블록에 비해 아주 작은 블록 헤더만 다운받으면 되는 thin client 처럼 동작하기 때문이다. Verge Tor와 I2P 지갑은 또한 보안을 위한 추가 레이어를 위해 4 자리 핀 코드와 생체 인식과 같은 보안 기능이 내장되어있다.

또한 Verge Tor와 I2P 지갑은 instant 검증을 통해 P2P QR 코드 스캔 트랜잭션을 처리 할수 있는 기능이 포함되어 있다. Clients는 필요하다면 종이 지갑에서 QR코드를 가져올수 있다.

7.0 Future Development: RSK Smart Contracts

Rootstock은 일반적으로 RSK로 불리며, 스마트 계약 기능을 Verge 네트워크에 접목시킨 양방향 안정형 개별블록체인(사이드체인)이다. 이것은 또한 인스턴트 결제를 위해 오프 체인(개별블록체인을 구성하여 사용하는) 프로토콜을 도입했다. RSK는 독립적인 블록 체인이지만 자체 토큰이 없으므로 이것의 통용를 위해 대신에 Verge를 사용한다. RSK는 pegging 또는 matching을 통해 이를 수행한다. 이것이 Verge의 스마트토큰이 된다. 그 결과 RSK 토큰값과 Verge의 토큰값이 일치하게된다. 사용자는 두 체인간에 토큰을 자유롭게 이동시킬수 있다.

Smart Contract는 사용자의 Verge를 고정된 예비 공간에 배치 한 후, smartXVG로 불리는 RSK 토큰을 backup하는데 사용한다. 당신의 Verge를 계좌에 넣고 RSK 네트워크를 이용하여 그 돈을 사용하는 것으로 생각하면된다. Bitcoin은 사용자가 'mutlisig'와 같은 simple contract을 작성하여 두 명 이상의 user가 지불을하기 전에 서명을해야만 공개 할 수있는 간단한 계약이 있음을 알아 두는 것이 중요하다. Verge에 RSK를 구현하면 단순한 스마트 계약이 완전히 새로운 차원으로 접어 들며 스마트 한 계약 기능이 제공되어 ethereum의 기능과 맞붙을수 있다.

또한 RSK의 또 다른 이점은 확장이 가능하다는 것이다. RSK는 현재 초당 400개의 지불 거래를 수행한다. 이는 현재 정상 거래 속도(초당 100개의 지불 거래)와 비교했을 때 엄청난 향상이다. RSK 개발팀은 Lumino라고 하는 second layer 기술을 사용하여 초당 2000개의 거래를 지원하는 것이 최종 목표라고 말했다. LCTP 백서에 명시된 것처럼 Lumino 네트워크는 Lumino Transaction Compression Protocol(LTCP) 을 사용하는 오프 체인 지불 시스템이다. LTCP는 현재 Litecoin에서 테스트중인 Bitcoin 용으로 설계된 scaling solution 인 Lightning Network와 비교할 수 있다.

8.0 Future Development: Discord & Telegram P2P

Telegram 및 Discord에 대한 P2P (Peer-to-Peer) 트랜잭션 지원은 현재 개발 중이며 8 월에 공개 될 예정이다. Telegram은 여러가지 OS(Android, iOS, Windows Phone, Windows NT, macOS 및 Linux)를 지원하는 무료 클라우드 기반 인스턴트 메시징 서비스이다. Telegram은 MTProto라는 대칭 암호화 체계를 사용한다. 이 프로토콜은 Nikolai Durov 개발팀이 Telegram에서 개발했으며 256 bit 대칭 AES 암호화, RSA 2048 암호화 및 Diffie-Hellman 키 교환을 기반으로한다. Discord는 여러 암호 커뮤니티에서 사용되고 있는 독점적인 VoIP 응용 프로그램(Freeware)이다. Telegram과 마찬가지로 Discord는 Windows, macOS, Android, iOS에서 지원되며 브라우저에서 액세스 할 수있는 웹 클라이언트를 지원한다. 이러한 플랫폼에서 Verge P2P 를 구현하면 actual 지갑을 설치했는지 여부에 관계없이 사용자가 어디서나 기금을 주고 받을 수 있다.

P2P는 사용자가 인터넷이나 모바일 장치를 통해 coin 을 전송할 수있는 온라인 기술이다. 이를 위해 사용자는 온라인 응용 프로그램 또는 봇 (bot)을 사용하여 전송할 coin의 양을 지정한다. 받는 사람은 사용자 이름으로 지정되며, 보낸 사람이 전송을 시작하면 받는 사람은 온라인 봇을 사용하라는 알림을 받는다. 즉 그는 새로 만들어진 입금 주소에서 payment를 받게된다. 그런 다음 사용자는 "! withdraw"와 같은 간단한 명령을 봇에 메시지를 보내거나 트윗한다. 그러면 새로 획득한 Verge를 받는 방법에 대한 방법을 표시해준다. 이 서비스는 사용자가 송금 할 금액과 송금 할 대상 외에 다른 추가 정보를 필요로 하지 않는다. 이 과정에서 IP주소, 위치, 이름과 같은 개인 정보는 유지되지 않는다. 거래 시작 외의 개인 정보는 완전히 익명이 보장된다.

Verge는 트위터뿐만 아니라 Reddit, IRC (Internet Relay Chat), Slack 및 Steam을 포함하여 여러 플랫폼에서 간단하고 사용하기 쉬운 P2P 전송을 위해 이미 이러한 기능을 제공하고 있는 유일한 암호화 화폐 중 하나이다. 이 기능을 사용하면 누구든지 동일한 소셜 플랫폼을 사용하는 한 어디서나 누구에게나 Verge 를 전송할 수 있다.

9.0 References

[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/

Additional References:

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 Contributors

As an open source project we find it very important to thank our contributors who have given us a helping hand in order for us to get to where we are today.

To that we say

Thank you

Korean Translators

SungJun, Kim (Verge Korea)
JongHyeon, Min

The Author

CryptoRekt

O.G Verge Development Team

Sunerok

Gfranko

CryptoRekt

Contributors

Core Marketing Team

@Spookykid
@CryptoRekt
@gfranko
@Crypto_K1NG
@JtheLizzard
@lucklight
@Cryptonator92
@feyziozsahin
@Slemicek
@Trilla6six6
@Dabbie USA
@Cyrus7at
@Thehunter9 Netherlands
@GGWeLost
@Jeanralphio69
@Crypth
@deheerlen
@Twomanytimes
@ScagFX
@TraderNILW

Github Contributors

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

Contact Info

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