Raiden Network

Ethereum network payment channels

MESSARI

Raiden Network is an independent protocol layer that uses hash time-lock contracts to facilitate trustless payments over the Ethereum blockchain.

The Raiden Network utilizes the concept of payment channels to provide bi-directional monetary transfers focused on high speed, zero counterparty risk, and low fees. By taking transactions off-chain, the Raiden Network is ultimately designed to alleviate scalability concerns on the Ethereum platform.

Project Overview

Name	Raiden Network
Issuer	Brainbot Labs
Category	Utility Token
Sector	Payment Channel
Sale Start	10/18/2017
Sale End	11/01/2017

Token Overview

Name	Raiden Network Token
Symbol	RDN
Type	ERC-20 token
Initial Distribution	50,000,000
Current Supply	50,168,936
Max Supply	100,000,000
Emission Type	Fixed

Resource Links

- [Website](#)
- [GitHub](#)
- [Twitter](#)
- [Medium](#)
- [Reddit](#)
- [Whitepaper](#)

Project Background

Raiden Network is building a second-layer payment solution for the Ethereum blockchain. The project builds off the same technological innovations pioneered by the Bitcoin Lightning Network by facilitating transactions off-chain, but focuses on support for all ERC-20 complaint tokens. Participants will transact directly through payment channels without needing to settle transactions on the blockchain, helping to avoid bottlenecks related to processing numerous and often small payment transactions. Users hedge themselves against counterparty risk by swapping cryptographic "promissory notes" that can be pushed to the Ethereum blockchain if circumstances require. Invalidation of previous notes when new ones are created prevents any party from gaming the system.

At first, the system might not be very appealing unless two participants plan to remunerate very frequently, since opening a new channel requires locking up assets via an on-chain broadcasted transaction. To alleviate this, the team plans to integrate the ability to route channels deterministically through multiple parties. Users having unique channels with many participants means less money in their wallets for discretionary spending, significantly reducing the versatility of their funds. Raiden plans to alleviate these concerns by introducing an effective pathfinding algorithm between network participants. If the relationships between users is extremely isolated, the system can keep introducing more intermediaries to form a lineage robust enough to facilitate payments.

The network plans to use the Raiden Network token (RDN) to transmit payments more conveniently for end users, while simultaneously offering incentive structures for liquidity providers and full node operators. While the token is not a functional requirement for the system, the team hopes it can provide incentives for network participants. For example, light clients that don't want to run full stack nodes can send small fees in the form of RDN to full node operators as compensation for utilizing their infrastructure. Network users can pay liquidity providers and channel monitors in RDN as well. By design, participants are incentivized to relay these peripheral fees using RDN (compared to Ether or other ERC-20 tokens) due to lower transaction costs.

Technology

Raiden utilizes standard hash-lock time commitments, referred to as balance proofs, to achieve cryptographic security of transactions. The process starts when two parties initiate an opening transaction by depositing tokens to a multi-signature escrow. This process collateralizes the channel and once collateralized, the parties can transact infinitely in both directions, so long as the balance between the two parties at a given time sums to the balance of originating deposits.

Each new transaction in a payment channel is unique, and each message creates obligations the recipient must fulfill to redeem the funds. Transactions are always time-locked until a future date, ensuring the recipient cannot redeem the money arbitrarily. When the two parties advance the state of the channel by signing a new transaction, they also relinquish a secret key that invalidates the previous state. This procedure allows an honest participant to punish a dishonest participant. The punishment scheme allows the honest participant to leave with the entirety of the channel balance if wronged. The probability of the dishonest participant successfully cheating is theoretically impossible since the system is built on cryptographic properties. Thus, strong economic incentives exist for each party to act honestly.

Raiden builds off this escrow-like process by applying the rules to a chain of participants, introducing events called multihop transfers. Multihop transfers can create a network of payment channels, which connect any two parties looking to transact, without needing to have a direct channel established between the parties themselves. In this case, a payee will be required to send a "secret" hashed message to the payer before posting collateral. Inter-channel funds can then deposited in hash-locked smart contracts from the payee, through the chain of intermediaries, to the payer. Redemption of the funds occurs in the reverse direction with the payee identifying funds waiting in escrow after the last multihop transfer and releasing the secret message to the intermediary liquidity provider. Releasing the secret catalyzes two reactions. First, it allows the payee to claim the funds out of the escrow and second, the receipt allows the correspondent to claim the money sitting in escrow. This process continues down the line until every intermediary has been paid, ensuring security across each leg of the channel and an incentive for each intermediary to pass along the cryptographically secured package.

Distribution

Brainbot Labs completed a token sale between Oct. and Nov. 2017, raising 109,532 ether (ETH) worth $33.4 million at the time. Participants purchasing over 2.5 ETH worth of RDN were required to fill out KYC documentation to gain whitelist access to the auction.

A uniform Dutch auction model was used for the token sale in an attempt to ensure fair distribution of tokens. In the auction, a fixed amount of 50 million RDN were guaranteed to be sold to buyers, regardless of the final strike price. Bidding commenced at an artificially high value and continued to depreciate until buyers accepted an equilibrium point they were willing to bid at. Prices continued to decline until all tokens were sold, at which point the auction terminated. All buyers received a uniform price equivalent to the most recent bid price, regardless of what they previously bid at earlier in the auction.

At the launch of the network, 100 million RDN tokens were created. Token sale participants received 50% (50 million RDN) of total supply. The issuer, Brainbot Labs, retained 34% of tokens (24 million RDN) to compensate early developers and founders. The remaining 16% of supply (16 million RDN) was allocated to an external development fund to assist in security auditing and provide incentive models for future applications.

Team

Heiko Hees
CEO

- Previously founder of PediaPress

- Ethereum core developer

Oliver Bünting
Consultant & developer

- Previously Director at CryptoCoins Consulting

Lefteris Karapetsas
Senior software engineer

- Previously software engineer at Oracle

André Vitor De Lima Matos
Software engineer

- Previously founder at Link Solutions

Christopher Seifert
Marketing consultant

- Previously analyst at Deutsche Bank

|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||

AdditionalResources

- [YouTube: How Raiden Network Works](#)

- [Developer API](#)

- [RDN Token Page](#)