What is the Raiden Network?

Summary

The Raiden Network is an off-chain scaling solution for performing ERC20-compliant token transfers on the Ethereum blockchain. It is Ethereum's version of Bitcoin's Lightning Network, enabling near-instant, low-fee, scalable, and privacy-preserving payments.

The Raiden Network allows secure transfers of tokens between participants without the need for global consensus. This is achieved using digitally signed and hash-locked (https://en.bitcoin.it/wiki/Hashlock) transfers, called **balance proofs**, fully collateralized by previously setup on-chain deposits. This concept, illustrated in figure 1, is known as **payment channel technology**. Payment channels allow for practically unlimited, bidirectional transfers between two participants, as long as the net sum of their transfers does not exceed the deposited tokens. These transfers can be performed instantaneously and without any involvement of the actual blockchain itself, except for an initial one-time on-chain creation and an eventual closing of the channel.

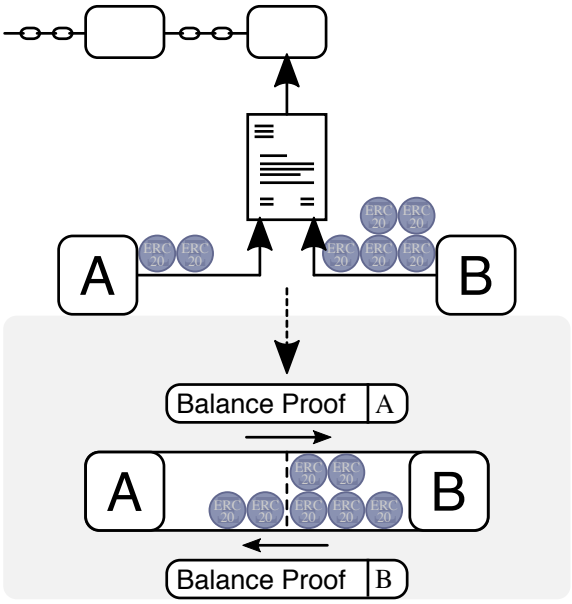

Figure 1: Simple Bidirectional Payment Channel

A Raiden balance proof is a binding agreement enforced by the Ethereum blockchain. Digital signatures make sure that neither party can back out of any of the value transfers contained therein, as long as at least one of the participants decides to present it to the blockchain. Since nobody else other than the two participants has access to the tokens deposited in the payment channel's smart contract, a Raiden balance proof is as binding as an on-chain transaction.

The true strength of Raiden lies in its network protocol. Since opening and closing a payment channel between two peers still requires on-chain transactions, creating channels between all possible peers becomes infeasible. As it turns out, however, you do not need a direct payment channel between a payer and a payee if there exists at least one route through a network of channels that connects the two parties, as shown in figure 2. This network and its associated protocol for routing and interlocking channel transfers is called the Raiden Network.

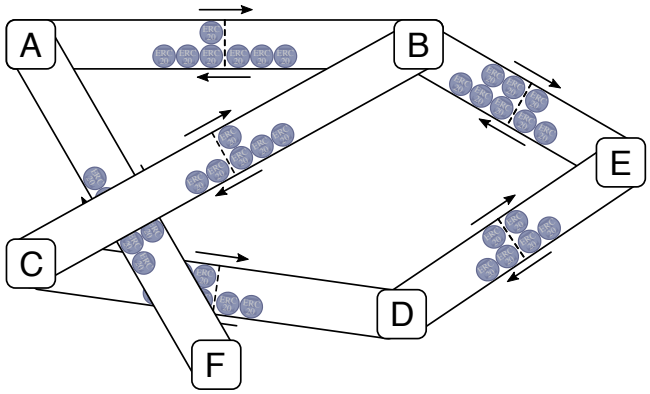

Figure 2: Payment Channel Network

In addition, payment channel transfers, in contrast to on-chain transactions, do not require any fees. Intermediaries within the greater network, however, will want to charge fees on a low percentage basis for providing their own channels to the network, leading to complex routing and a competitive channel fee market. The Raiden protocol aims to facilitate this market by using both protocol-level features and optional auxiliary services.

Benefits of the Raiden Network

Any transaction on the Ethereum blockchain comes at a cost depending on the transaction's required computational resources. Accordingly, fees are largely independent of the actual amount of value transferred, be it ERC20 tokens or Ether itself. This makes on-chain transactions best-suited for medium to large value transfers, but less so for transactions on the scale of a few dollars or even fractions of a cent.

It does not matter whether a transfer is sent in one piece or split over thousands of micropayments. Hardly any transfer is too small to be sent efficiently over the Raiden Network.

Raiden transfers are also instant, in the sense that as soon as you receive an off-chain Raiden transfer, you can rest assured that the transferred value now belongs to you. In contrast, confirmation of on-chain transfers depends on block time and the time it takes miners to pick your transaction from the pool of pending transactions. Instead of waiting for the next blocks to confirm a transaction, with Raiden transfers you can send, receive, and confirm transfers as fast as sending a chat message over the internet.

Next to fees, blockchains also have another inherent problem that Raiden helps to solve: scalability. Capacity of most of the current blockchains is capped at a fixed or semi-fixed limit, regardless of the size of the userbase. In stark contrast, capacity of the Raiden Network scales linearly with the number of users, leading to an efficient and future-proof, decentralized transfer network.

Limitations of the Raiden Network

The answer to the question of whether you should use a Raiden token transfer rather than an on-chain transaction is actually just this: "why not?". There are, however, use cases where an on-chain transaction is a significantly better choice than a Raiden transfer.

Raiden transfers require some of your tokens to be locked up in a smart contract for the lifetime of the payment channel. Similarly to only withdrawing small amounts of money from an ATM, you would not want to lock up too much value in a payment channel. Once you withdraw money from an ATM, you cannot use it for anything else, like online payments or wire transfers. Likewise, and since each participant in the network will likely have multiple channels open at the same time, payment channel deposits are expected to be comparatively small, making it difficult to transfer large amounts of tokens over the network of channels.

Large value transfers should still be performed on the blockchain itself to save the extra cost of channel lifetime management and to avoid the need for routing through mostly inadequately equipped payment channels.

How it works

Lifecycle of a Raiden channel

In order to ensure that participants pay their debts, tokens have to be locked up as security in a smart contract for the lifetime of the payment channel. This deposit ensures that tokens can only be used to send and receive tokens to and from the channel partner until the channel is finally closed by either participant, preventing both from double-spending their tokens to other peers. The process of managing a Raiden channel is shown in figure 3.

Once a channel is created, participants may issue what can be considered certified checks (https://en.wikipedia.org/wiki/Certified_check) freely back and forth. Instead of keeping track of all checks, however, each peer only keeps a copy of the latest one. The balance proof contains the final sum of all Raiden transfers sent to a participant up to a certain point, digitally signed by the sender. Since each channel has two participants, it always maintains two of those and together they are essentially the channel's bar tab if you will. Multiple credits are exchanged back and forth, changing the total amount owed between the participants, possibly even rebalancing the channel many times in the process.

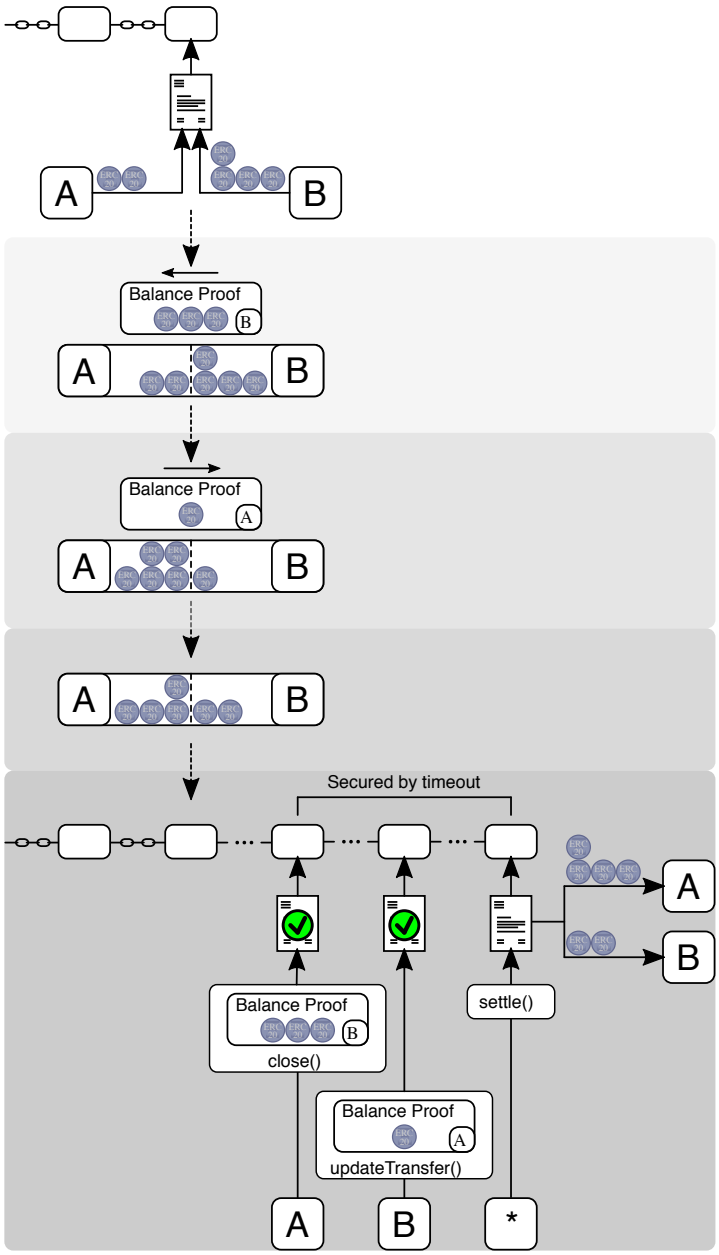

Figure 3: Lifecycle of a Raiden Payment Channel

Finally, when one party decides to settle the balance on the blockchain, either to claim or pay their outstanding balance, they can close the channel at any time by presenting their balance proof of choice to the smart contract. The other participant -- the one that did not choose to close the channel -- must now present a balance proof of their own or do nothing if they received no transfers. After both parties have submitted their balance proofs, they may now withdraw their deposits. This withdrawal may be triggered by anyone, including addresses other than the two participants.

If the second participant fails to present their balance proof in time, balances will be distributed according to the closing participant's proof, assuming that the other participant has not received any transfers. This way, Raiden asserts that each payment channel participant always has access to their funds.

Need for a network

As mentioned in the introduction, creation and settlement of payment channels have to be performed on the blockchain. Accordingly, it would be unreasonable, infeasible even, to create a new channel per potential target. Instead, Raiden creates a network of channels in which each participant is transitively connected to everybody else through a web of payment channels.

Let us say Alice wants to send tokens to David, as illustrated in figure 4. She first has to find a route through the network that connects her to David. Then, each participant along that path has to cooperate in order to funnel the payment through the route from Alice to David. Participants lend their own channels to Alice by forwarding the payment to the next hop in the path. A cryptographic hash lock prevents all of these intermediate transfers to be credited until David confirms to Alice that he received the payment. Once Alice decides to unlock the payments, she gives the key to the lock to David. If David now wants to claim the payment without closing the channel, he has to pass the key on to the last mediating peer in the route who in turn needs to pass it on to claim their own payment.

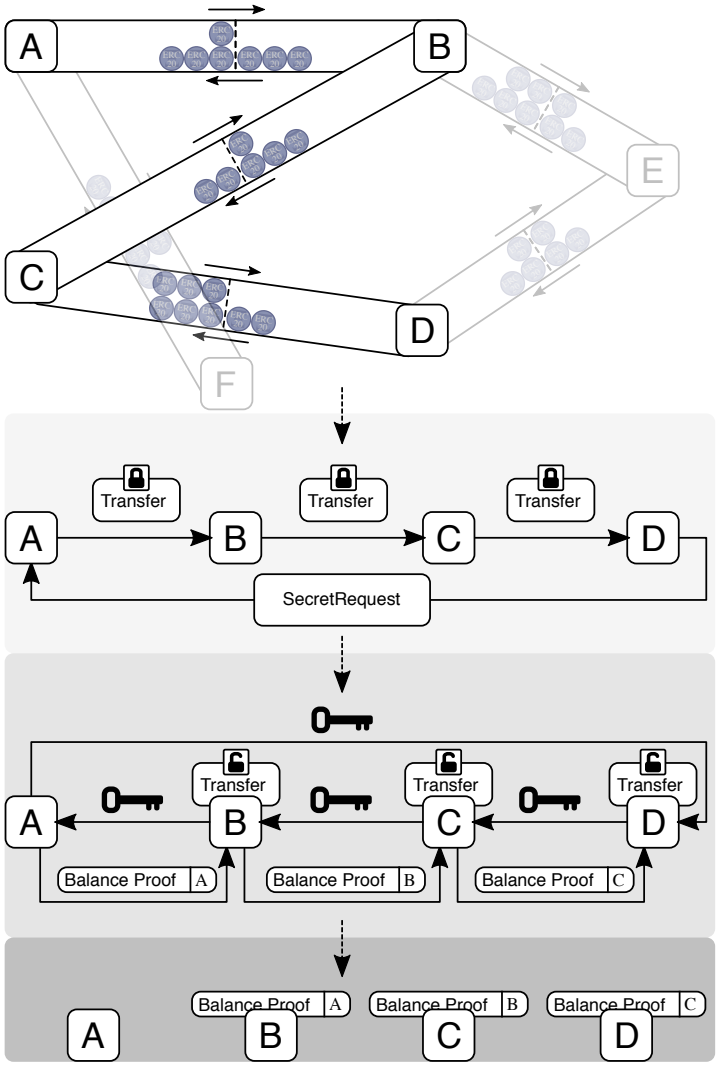

Figure 4: Multihop Transfer

Since each participant on that route has an incentive to unlock their incoming payment immediately, the key naturally propagates backward through the channel route, back to Alice. All locked transfers are redeemable on-chain using Alice's secret. It is, however, preferable for the participants to consolidate the locked transfers' values into a standard balance proof. Accordingly, after receiving the secret, each sender of an intermediate transfer signs a new balance proof that includes the locked transfer's value and invalidates the lock itself, cleanly synchronizing the channel state. The multihop transfer is now complete.

Likely, peers in the network will not provide their channels to be used as intermediaries for free. After all, transfers will cause additional network traffic and imbalances in their payment channels. To that effect, participants in the Raiden network are expected to demand fees to be compensated for lending their channels to the network. These fees may also be used to incentivize rebalancing of unbalanced payment channels, enabling long-lived payment channels.

Since the resulting fee market will be competitive and actual processing costs will be rather low, fees are expected to be orders of magnitude lower than those of on-chain transactions.

Privacy

Since most of the Raiden protocol is performed off-chain, transfers are largely private. Channel balances are hidden from the public until participants settle and withdraw their funds and the net channel balance is revealed. When they do however, channel balances may have already been obfuscated by other intermediary transfers that passed through this and other channels connected to the same nodes, making it extremely difficult to trace back on-chain transactions to off-chain Raiden transfers. Users might even offer paid services to artificially rebalance and obfuscate channel balances in order to increase the level of privacy. On the messaging layer, Raiden will make sure to protect traffic and sensitive data transmitted over the network. The messaging service will hide participants' IP addresses from the public, preventing arbitrary nodes from being subject to DoS attacks. Additionally, pre-computed routes may use an onion routing protocol where intermediary nodes participating in a transfer have no way of knowing the target address of a Raiden transfer. The protocol only reveals the next channel in the route to each participant.

Conclusion

The Raiden Network uses bidirectional token payment channels to connect participants directly with each other. On top of that, it provides a protocol to relay token transfers through routes of channels to make use of the natural channel network topology, rather than attempt to connect each and every participant directly. Multihop transfers are secured using cryptographic hash locks to ensure that a mediated transfer either succeeds, or is rejected entirely by all participants.

The Raiden Network aims to use the above technology to provide near-instant, low-fee, scalable, and privacy-preserving payments based on Ethereum ERC20 tokens and to extend current on-chain limitations.