Raiden Overview

What is Raiden?

What is the Raiden Network?

Which problems does the Raiden Network solve?

▸ Scalability

▸ Latency

▸ Transaction fees

▸ Improving privacy

What is µRaiden?

What is Raidos?

ELI5, how does the Raiden Network work?

What is a payment channel?

Why is the Raiden Network a network?

State & Vision

What is the status of the Raiden project?

Will the Raiden Network actually work?

▸ "Routing cannot be performed efficiently."

▸ "Intermediate transfers create a bottleneck on liquidity due to locked up tokens."

▸ "The Raiden Network cannot support large transfers."

▸ "Natural wealth distribution will cause a centralized network."

▸ "Channels degrade over time."

▸ "Nodes may become unresponsive."

Fees

Other Questions

Comparison to other projects

Raiden Overview

What is Raiden?

Raiden is an open source project that aims to scale Ethereum by using state channel technology.

What is the Raiden Network?

The Raiden Network is an off-chain transfer network for Ethereum ERC20 tokens. It provides a fast, scalable, and cheap alternative to on-chain token transfers. At the same time, the Raiden Network transfers provide users with guarantees of finality, security, and decentralization similar to those known from blockchains.

Which problems does the Raiden Network solve?

The Raiden Network is a technology that leverages off-chain payment channel networks to address these substantial issues on the Ethereum blockchain:

Scalability

Blockchains do not scale well. Current public, permissionless blockchains are unable to achieve more than a low, fixed number of transactions per second. Ethereum has been shown to reach its cap at about 10 transactions per second. Short-term scaling solutions, like raising maximum computation performed per block by a constant factor, will not be able to support continued mainstream adoption.

The Raiden Network will provide a payment system based on payment channel technology that scales with the number of its users. This means that the bigger the Raiden Network becomes, the higher its maximum throughput will be, with practically no upper limit in sight.

Latency

Blockchains are slow. At the moment, Ethereum mines a new block approximately every 15 to 30 seconds. To reach practical finality of a transaction, confirmation times of several minutes have to be endured. This significantly degrades user experience and hinders mainstream adoption.

Raiden Network transfers are as fast as text messages. The moment you receive a signed Raiden transfer, you can be certain that you now hold the amount included in the transfer. There is no need to wait for any confirmations.

Transaction fees

Using blockchains is expensive. Once a blockchain hits its limit, paying high enough fees to be included in a block becomes a competitive endeavor, as is the case with Bitcoin today. Ethereum will be no different, eventually leading to even higher confirmation times and transaction fees on the order of a few dollars per transaction. For the vision of a global, decentralized, and dependable computer this is highly detrimental.

Raiden Network transfer fees will be several orders of magnitude lower than on-chain transaction fees. Instead of paying for global consensus, you only pay for forwarding peer-to-peer consensus. Low fees allow for a long tail of new use cases which have not been practical before due to high transaction costs. Especially IoT and the Machine-to-Machine economy depend on being able to transfer tiny values. Raiden aims to be the predominant payment layer for these applications.

Improving privacy

Ethereum transactions are public, whereas Raiden transfers will be private between the payer, the payee, and the nodes forwarding the transfer. When channels are settled, only the sum of transactions will become visible to the entire world.

What is µRaiden?

µRaiden (Micro Raiden) shares some properties with the Raiden Network. It can provide trustless, instant and free transfers between two parties. It is intended for many-to-one payment setups, like users interacting with a Dapp. However, it is not suitable for many-to-many payment setups as it requires users to lock up tokens upfront for every potential payee. This limitation comes with reduced technological complexity, allowing μRaiden to be used on the mainnet today.

What is Raidos?

Raidos (or Raiden 2.0, “dos” is spanish for "two") is a proposed sidechain technology to generalize state channels. While the Raiden Network is limited to ERC20 token transfers, Raidos aims to scale Ethereum’s generalized computation capabilities through a network of satellite chains, which can host any smart contract. This technology is similar and complementary to Ethereum's sharding.

ELI5, how does the Raiden Network work?

If you think of a blockchain as a universally trusted but very slow bank that charges you for wire transfers, then the Raiden Network offers checks that will never bounce back when cashed at that bank. Once you receive a Raiden check from someone, you can be absolutely certain that this check is real and that you are now richer than you were moments ago. But neither you nor your payer had to stand in line at the bank or wait for the clerk to perform a wire transfer. You can decide to cash this check at the bank at any time, potentially with hundreds and thousands of other checks simultaneously and you only need to pay fees once when turning all of these checks in. If your payer had instead made a single wire transfer per payment, he would have paid a lot more in fees and both of you would have waited a lot longer for a confirmation. As a side-effect, the bank is happy too because this system significantly reduces internal workload.

What's more, you don't even need to be in contact with the person that wants to give you a check. It is entirely sufficient if you know someone who knows someone who eventually knows someone that knows this other person. They all pass checks on to each other until one finally reaches you. But all of them are only valid if you confirm to everyone that you have received yours in the end.

The Raiden Network will take care of connecting you and your partner through this network of bank customers and will make sure that all checks are as binding as actually visiting the blockchain bank for a transfer.

What is a payment channel?

Payment channels are a technology that enables off-chain transfers of on-chain tokens. This works by first depositing the tokens in a payment channel contract. Then, transfers can be performed by sending signed messages directly between two parties without any involvement of the blockchain itself. Therefore, transaction frequency is only limited by the hardware of sender and receiver. But best of all, there are literally no transaction fees, other than for a one-time on-chain deposit and eventual settlement.

Since only the two participants have access to the deposit in the payment channel's smart contract, payment channel transfers are immune to double-spending attacks, **making them as secure as on-chain transactions**.

Why is the Raiden Network a network?

For every payment channel, tokens have to be deposited and are subsequently locked for the lifetime of the channel. It is easy to see that this makes opening payment channels with everyone infeasible: A huge amount of tokens would be required.

Instead, Raiden creates a network connecting all participants transitively through routes of payment channels. As long as there exists a route connecting payer and payee, the Raiden Network will enable token transfers just as if they were directly connected. This way, every participant only has to open a few channels, but will still able to transfer to any other peer.

State & Vision

What is the status of the Raiden project?

Raiden currently consists of three independent projects: µRaiden, Raiden Network, and Raidos.

There is a working implementation of ***µ*****Raiden**, which will be deployed on the Ethereum main net shortly.

The **Raiden Network** is still in development. A developer preview will be released soon and allow Dapp developers to get a first impression of the API and the properties of the system, also enabling them to build prototypes that interact with the Raiden Ropsten-based test network. In its current state the technology is not ready for production use. Significant tooling and even changes to the core protocol still need to be developed.

Raidos is currently only in its planning phase and development has not been kicked off yet.

On a more general note, you can always check the current state of development at our GitHub: https://github.com/raiden-network/raiden (https://github.com/raiden-network/raiden)

Will the Raiden Network actually work?

The Raiden Network already works in its current state. Transfers can be sent instantly to any participant in the network using a simple routing mechanism and intermediate transfers.

We are, however, aware of criticism surrounding the idea of networks like Lightning and Raiden. We want to address some of the most common ones here.

"Routing cannot be performed efficiently."

Scalable Routing is indeed one of the biggest issues of payment channel networks. There is a trade-off between centralization, privacy, and efficiency. Simulations have shown that our approach of combining a Kademlia-like structured network with a federation of path finding helpers allows for efficient and scalable path finding while preserving decentralization and privacy.

"Intermediate transfers create a bottleneck on liquidity due to locked up tokens."

This is not the case. While it is true that for the duration of a Raiden transfer, intermediate tokens are locked up and cannot be used elsewhere, this has no noticeable effect on network liquidity. The time it takes for a transfer to be completed is on the order of tenths of a second with configurable timeouts to account for failing nodes. When you decide to forward a transfer, it will be a matter of at most a few seconds to regain control over your locked up tokens.

Additionally, as long as you have enough tokens deposited in your channel, you can forward multiple transfers at the same time. Each node can forward many transfers per second, depending on their deposits.

"The Raiden Network cannot support large transfers."

This is partially true. The Raiden Network is not intended to support large value transfers. A Raiden transfer requires each channel on a route through the network to be able to relay the desired amount. The bigger a transfer, the lower the probability that there is a route of channels, each of which is able to support the transfer. Currently, we recommend to perform large-scale transfers on-chain. In the future, large transfers might simply be split up over multiple channels.

"Natural wealth distribution will cause a centralized network."

It is true that larger nodes will relay significantly more transfers than smaller nodes, having more channels and higher deposits. However, intermediary nodes cannot cheat, no matter how big they are. Nor do bigger nodes prevent smaller ones from participating in the network. The moment nodes stop accepting or forwarding transfers is the moment they stop being nodes to the rest of the network. It might very well be possible that wealthy institutions provide large transfer hubs to make a profit on transfer fees but this will only support the network with liquidity and competitive fees, not endanger its decentralization.

"Channels degrade over time."

This is only true in a naive system design. Without further systems in place, channels will become imbalanced over time. However, channels can be automatically rebalanced through proper incentivization. Nodes can adjust their forwarding fees in such a way that their channels remain balanced. Our simulations show that this alone helps to prolong channel longevity by a great deal.

"Nodes may become unresponsive."

This is entirely expected and is an issue that is handled gracefully in just about any modern peer-to-peer protocol. The Raiden Network is no exception. Nodes going offline will cause the Raiden Network to route transfers around that node within milliseconds.

While the network itself is resilient against unresponsive nodes, individual participants could be attacked if they go offline: Their channels may be closed fraudulently, requiring challenges that they would be unable to submit. For this reason, payment channels have challenge periods, meaning that down times would not directly allow for an attack. Additionally, third parties providing a challenging service will ensure that participants can safely go offline.

Fees

Are there fees in the Raiden Network?

Yes, there are two kinds of fees in the Raiden Network:

- Protocol level fees
- Peripheral fees

Protocol level fees are necessary to keep the payment channel network balanced. Nodes will use fees to prevent their channels from being depleted over time. These fees will be comparatively small and be denominated in the token that is transferred in the channel.

Peripheral fees will be payable to services in the network that, for example, assist with finding a path with sufficient capacity or services that provide channel monitoring services for offline users. Users running these services themselves will not need to pay these fees but can earn them instead. It is assumed that >95% of all nodes on the network will be light-clients happy to pay tiny fees for the convenience of not having to run the full stack of services.

Will there be a Raiden Network token?

Yes, peripheral services will be paid for in RDN tokens, a virtual currency dedicated to pay for services within the Raiden Network. Note that this token is not at the core of the protocol and only used by participants who opt to pay for the convenience of not having to run a full node.

Is the Raiden Network spam-resistant?

Yes, spamming a single node does not harm the network as a whole. Nodes throttle their connections and will disconnect spammers.

Other Questions

Can ETH be transferred over the Raiden Network?

Yes. While ETH currently does not qualify as an ERC20 token, simple wrapper contracts exist that allow ETH to be treated just like an ERC20 token.

Is there a white paper?

Unfortunately not yet. We have been busy researching and developing the software. But a protocol specification is in the making and at some point the final design will be presented in a white paper.

Who is developing Raiden?

Raiden is developed by brainbot, a company deeply committed to the Ethereum ecosystem.

Comparison to other projects

How is it different from the Lightning Network?

The Raiden Network is very similar to the Lightning Network (https://lightning.network/). In contrast to the Lightning Network, the Raiden Network supports all ERC20 tokens instead of being limited to the transfer of BTCs.

How is it different from Sharding?

Sharding (https://github.com/ethereum/wiki/wiki/Sharding-FAQ) will allow Ethereum to significantly scale overall transaction capacity, basically by partitioning state over multiple chains. It’s a very important and needed improvement which is complementary to the Raiden Network. While sharding helps to scale, it will still have suboptimal latency, cost and privacy properties for token transfers, compared to the Raiden Network. In order to scale token transfer capacity using shards, cross-shard communication is necessary, which is expected to be even slower and similarly expensive as transfers on Ethereum. While sharding is important, it is not an optimal solution for token transfers.

How is it different from Plasma?

Plasma (http://plasma.io/) is a proposed concept to scale transaction capacity using hierarchical trees of side chains. Similar to sharding, it will not be able to provide the latency and low fee properties as provided by the Raiden Network. Implementations of Plasma will be complementary to the Raiden Network.

How is it different from IOTA’s tangle?

Tangles are a new, interesting technology. Some aspects of them, however, are not clear.

Concerning token transfers, current implementations of tangles require a lot of computational resources because transaction mining and validation are combined into a single process. This makes them largely unfit for less powerful systems such as smartphones or IoT devices. In contrast, Raiden transfers are quick to create, requiring only a single elliptic curve signature to be computed.

How is the project related to the RaidEX (http://raidex.io) decentralized exchange?

RaidEX is a Proof-of-Concept of a decentralized exchange built on top the Raiden Network based on its atomic token swap feature.

How is the project related to the Trustlines Network (http://trustlines.network)?

The Trustlines Network implements the original Ripple (https://ripple.com/) idea on Ethereum. Both projects are based on the idea of channel networks and are complementary. At some point, Trustlines could be built on top of the Raiden Network.

Can the Raiden Network be used with other blockchains?

Blockchains supporting the Ethereum Virtual Machine will be able to use the Raiden Network after manual modification to work with their API. While this is not a focus of current development, it is reasonable to expect the Raiden Network to work with Polkadot, Dfinitiy, Cosmo, Hyperledger Burrow, EOS and others.