Trustlines

PROTOCOL

Trustlines Explained

→ Introduction

→ Trustlines Protocol

Hello, I’m _

→ From _

→ Trustlines since _

→ Role _

→ Location _

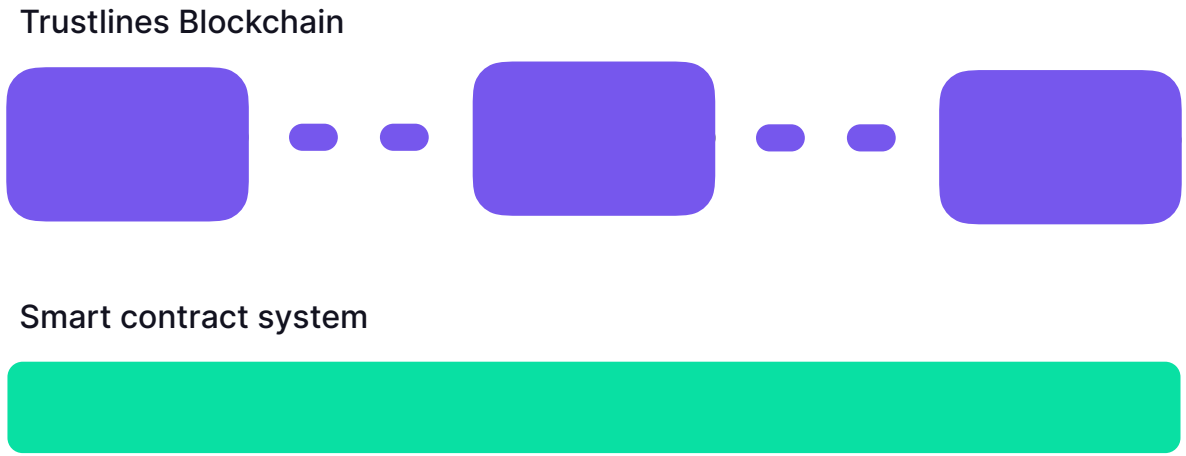
Disclaimer

Please note, that even though we do our best to ensure the quality and accuracy of the information provided, this publication may contain views and opinions, errors and omissions for which the content creator(s) and any represented organization cannot be held liable.

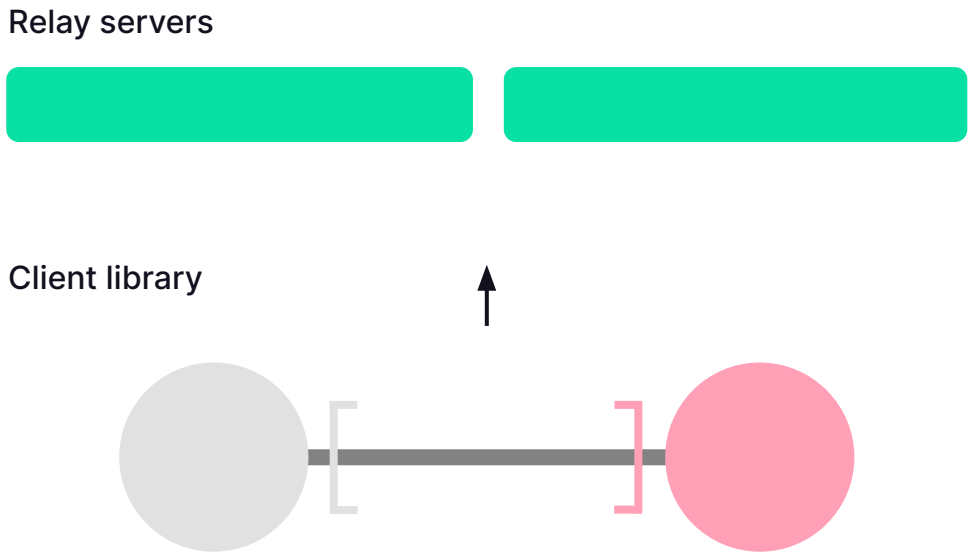
The wording and concepts regarding financial terminology (e.g. “payments”, “IOU”, “currency”, “credit”, “debt”, “transfer” [of value]) are exclusively used in an exemplary way to describe technological principles and do not necessarily conform to the real world or legal equivalents of these terms and concepts.

Trustlines Protocol

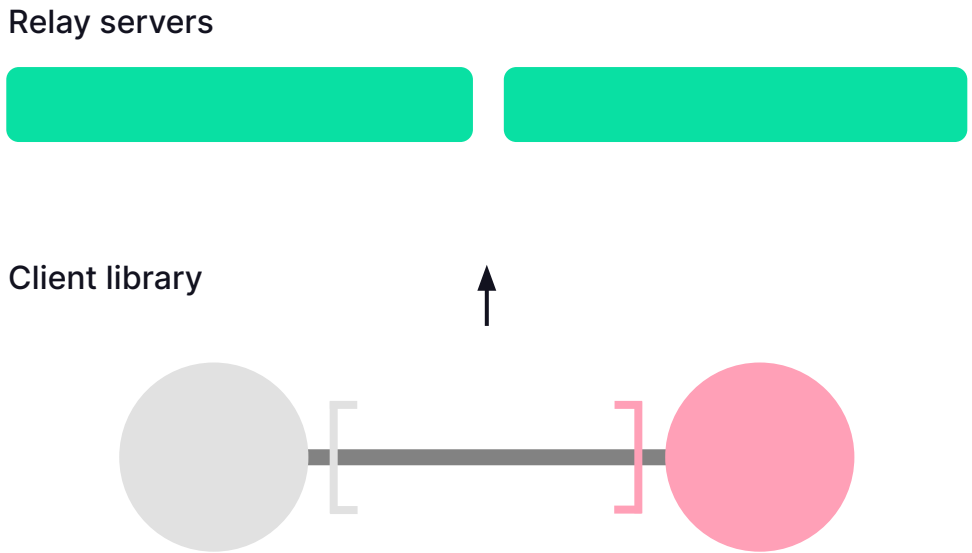
What Is The Trustlines Protocol?



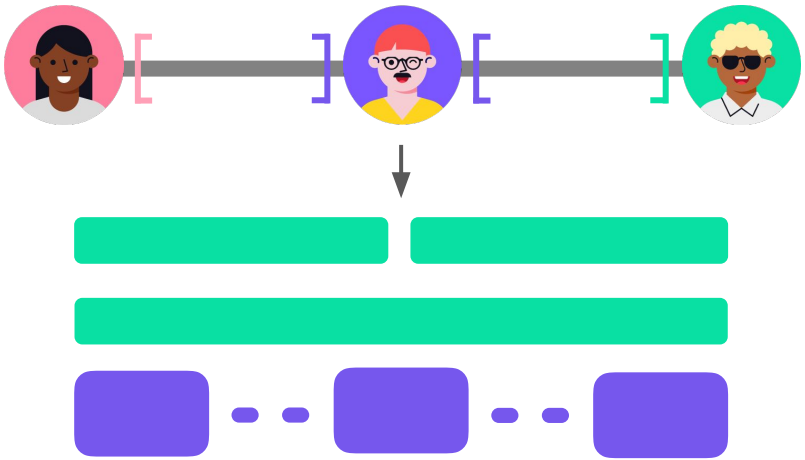
What Is The Trustlines Protocol?



What Is The Trustlines Protocol?



What Is The Trustlines Protocol?



Maps trust based relationships onto trustless infrastructure

mPoS: Aura With Additional Safety Mechanisms

Deposits

- Validators are required to deposit ETH
- Provable attacks are slashed

Slashing

- Strong punishment for easily provable attacks
- Automatic

Hard forking

- Weak punishments for all other attacks
- Requires coordination

Mission Of The Trustlines Blockchain

Store transactions made by a decentralized network of mutual trust relationships

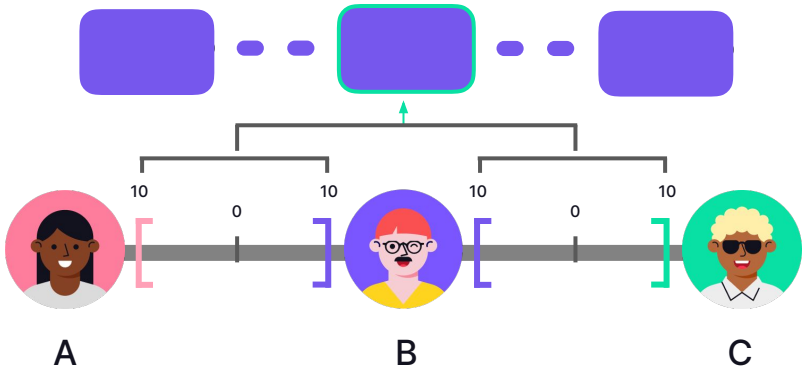
Requirements

- 10m trustlines transfers per day
- Transaction costs should be > €0.01
- Must be censorship resistant
- Must feature the Ethereum Virtual Machine (EVM)

Can We Run Trustlines On Ethereum?

A single trustlines transfers can require multiple on-chain transactions

- Fees are too high
- Throughput is too low
- Risk of congestion is too great



Can We Run Trustlines On...

Eth 2.0
Polkadot Parachain

Probably
but doesn't exist yet

State channels
Plasma

Maybe
but no solution available yet

PoA chain
DPoS chain

No
not censorship resistant

(Interim) Solution

A PoS sidechain, **dedicated** to Trustlines

- Straightforward to implement
- Secure for our use case
- Anonymous validators

Minimal Proof-of-Stake or mPoS

Consensus Algorithm: Aura

Battle-tested on live networks (Kovan, xDai, ...)

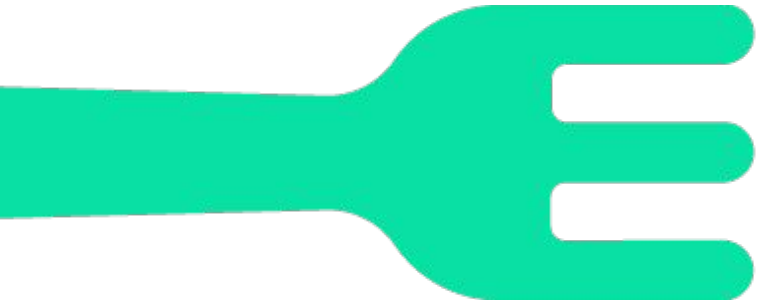
First class client implementation (Parity)

Designed for proof-of-authority

- Allow for anonymous validators
- Add security mechanisms
- Prevent a single party from taking over

Embracing Hard Forks

Great mechanism to remove misbehaving validators



Powerful
Validators can be removed for any kind of attack

Flexible
No need to specify the exact conditions in advance

Straightforward
Requires no code to be written

Aligned community makes coordination quick

Distributing Validator Slots

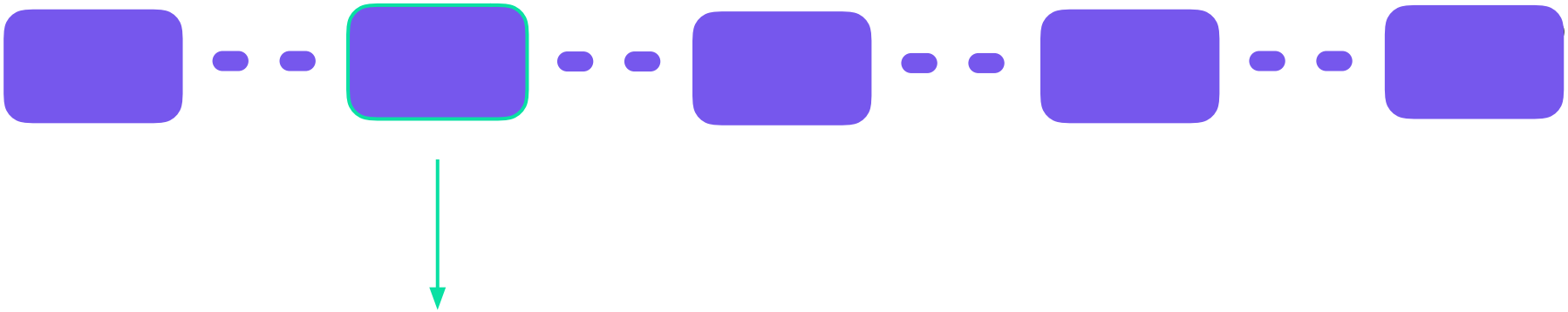
Fixed number of slots → **Auction** to decide

- Who will become a validator &
- How much they will stake

Whitelist to prevent Sybil attacks

Talk to me to register!

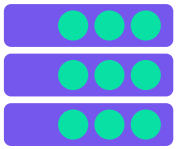
Why Become A Validator?



Validators earn **rewards** for

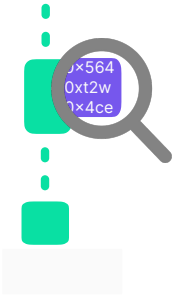
- Each block they create
- Each transaction they include

Validators Responsibilities



Run a node with high uptime

Don’t attack the network



Monitor the chain for misbehavior

Participate in governance

Life Of A Validator

Birth

1. Register for the auction
2. Wait for further instructions via email
3. Send your ETH address and get anonymized
4. Participate in the auction
5. Hopefully win!

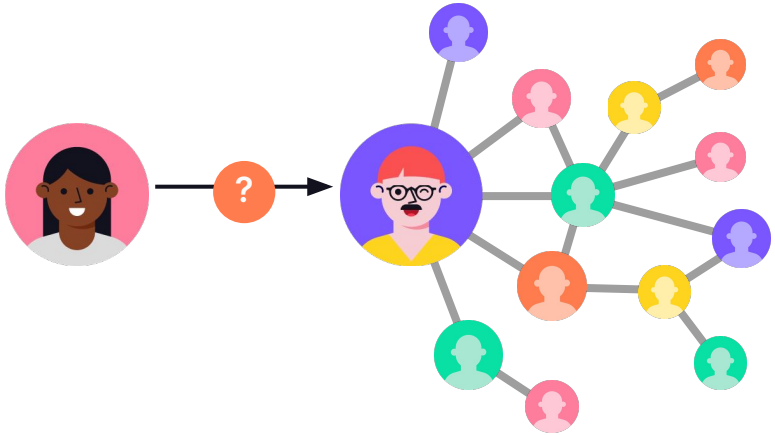
Death

- Get slashed (not recommended)
- Exit automatically after a fixed period and get your stake back

Delegate Services

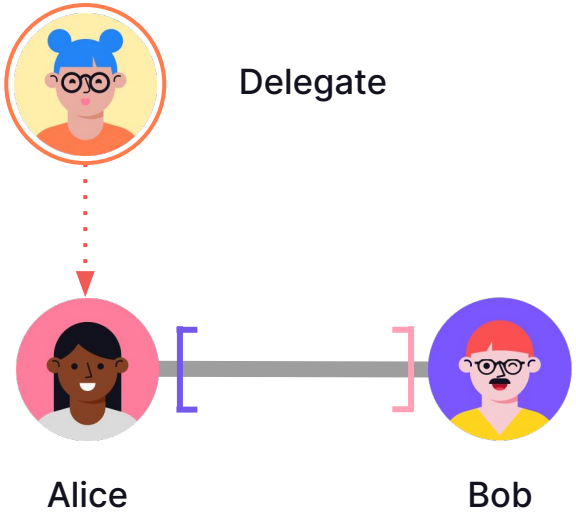
How can new users join the Trustlines Network without buying Trustlines Coins?

- Delegate service contract
- Delegates pay transaction fees in exchange for fees set in the smart contract system



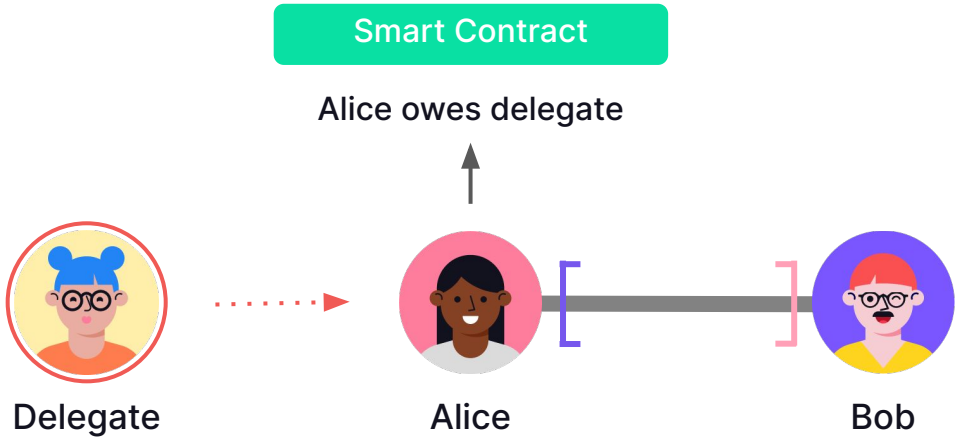
Trustlines Delegate Service

Alice wants to join the Trustlines Network,
but she has no TLC or any other crypto



She finds a **delegate** to pay her fee,
who sets a **currency network fee** in exchange

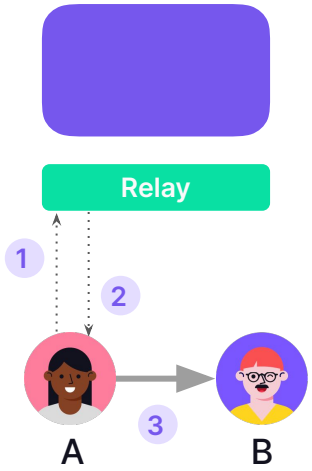
Trustlines Delegate Service



Alice and Delegate both sign the transaction. The currency network registers that Alice owes a delegate a currency network fee.

Relay Services

- Helper services for path calculations that are not feasible to do on-chain
- Can be paid in currency network fees and/or Trustlines Coins



1 Query
2 Path
3 Transaction

Trustlines

PROTOCOL