

Trustlines Explained

Hello, I'm Kristoffer

- From Denmark
- Trustlines since 2016
- Role Comms
- Location Austria

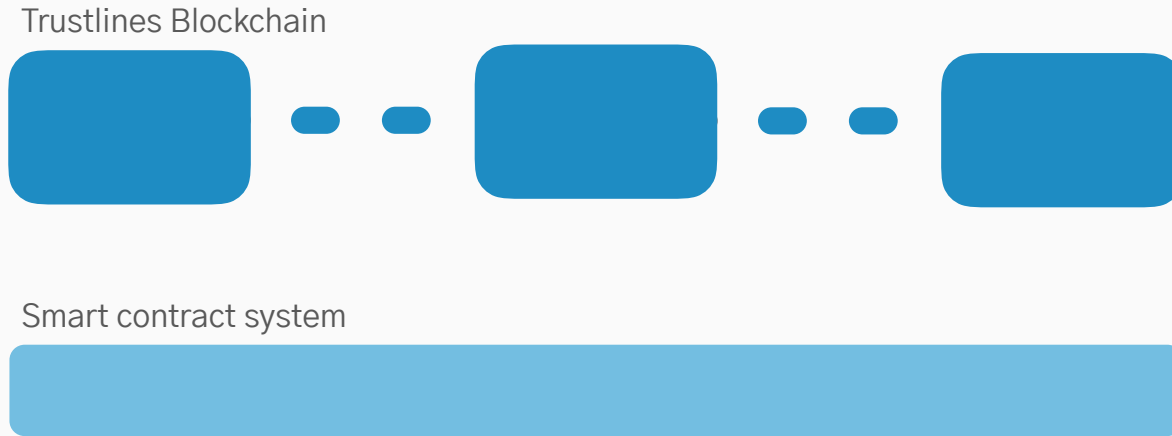
Disclaimer: Please note, that even though we do our best to ensure the quality and accuracy of the information provided, this publication may contain views and opinions, errors and omissions for which the content creator(s) and any represented organization cannot be held liable.

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.

- Introduction
- Trustlines Protocol
- People-Powered Money
- Bootstrapping the Network
- Summary

Trustlines Protocol

What is the Trustlines Protocol?

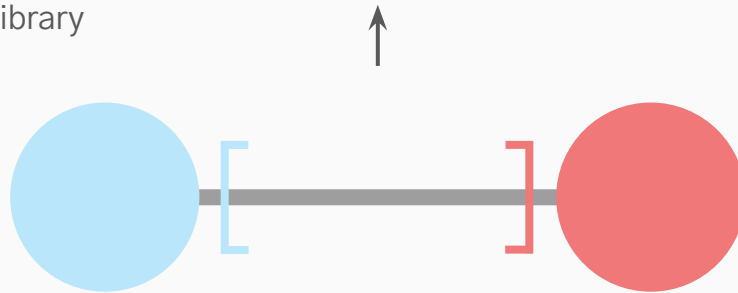


What is the Trustlines Protocol?

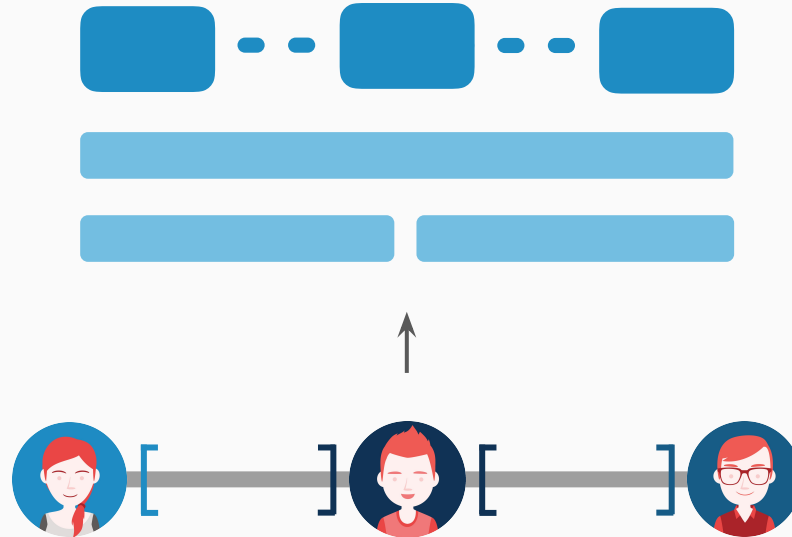
Relay servers



Client library



What is the Trustlines Protocol?



Maps trust based relationships onto trustless infrastructure

Mission of the Trustlines Blockchain

Store transactions made by a decentralized network of mutual trust relationships

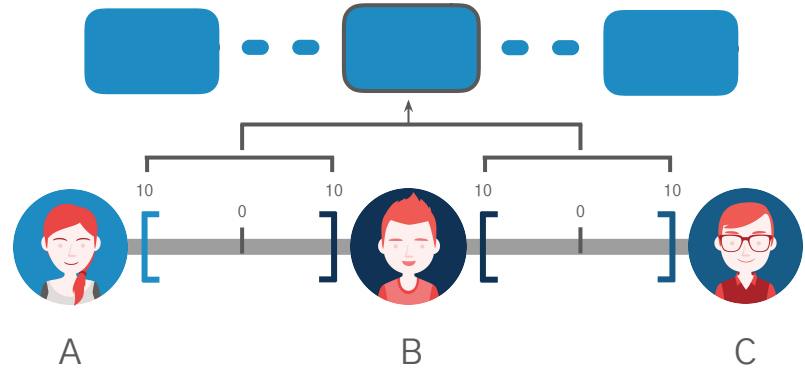
Requirements

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

Can we run Trustlines on Ethereum?

Trustline 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

mPoS: Aura with additional safety mechanisms

Deposits

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

Slashing

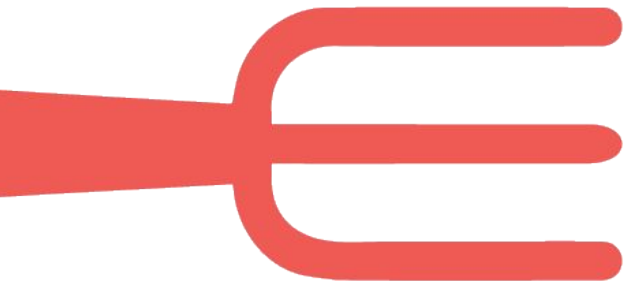
- Strong punishment for easily provable attacks
- Automatic

Hard forking

- Weak punishments for all other attacks
- Requires coordination

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

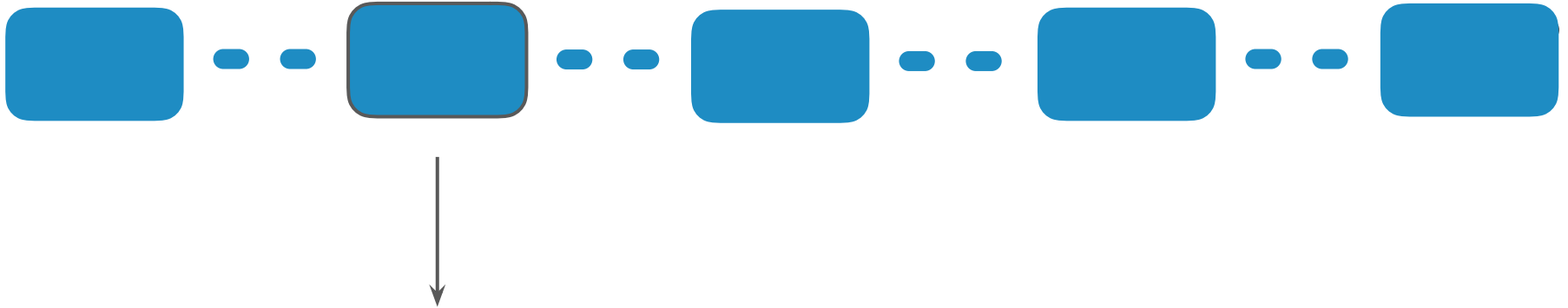
Fixed number of slots → **Auction** to decide

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

Whitelist to prevent Sybil attacks

Talk to me to register!

Why become a validator?

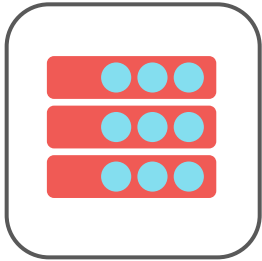


Validators earn **rewards** for

- 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!

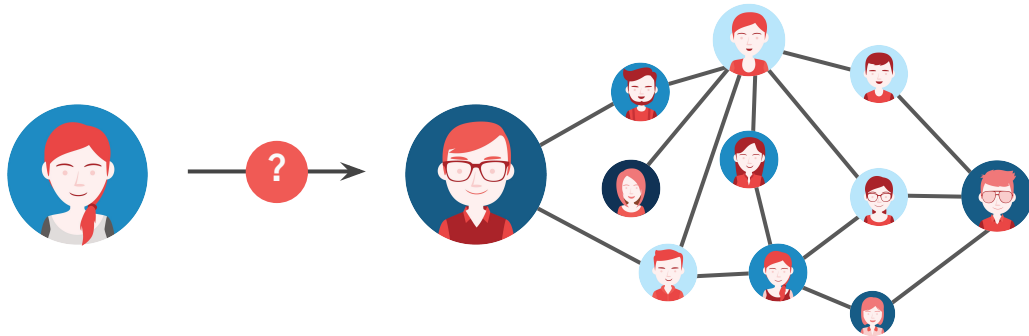
Death

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

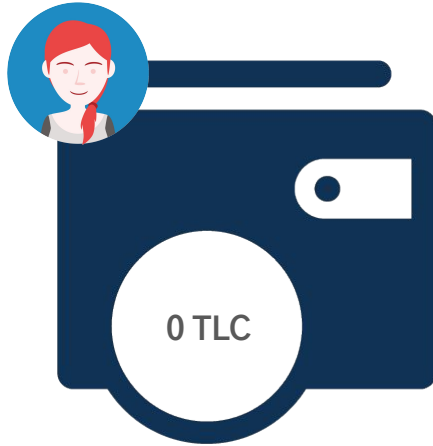
Delegate services

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

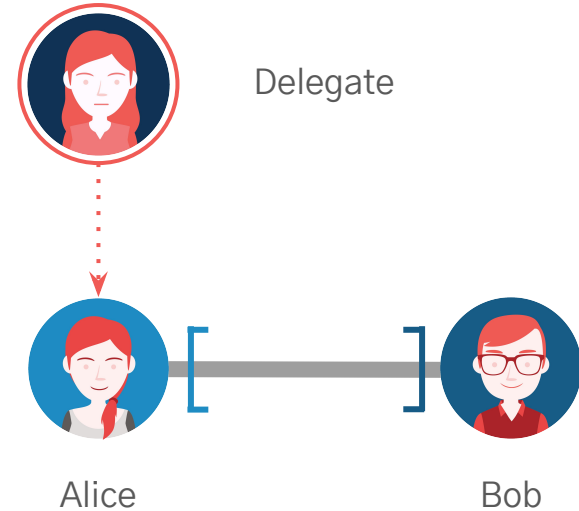
- Delegate service contract
- Delegates pay transaction fees in exchange for fees set in the smart contract system



Trustlines delegate service

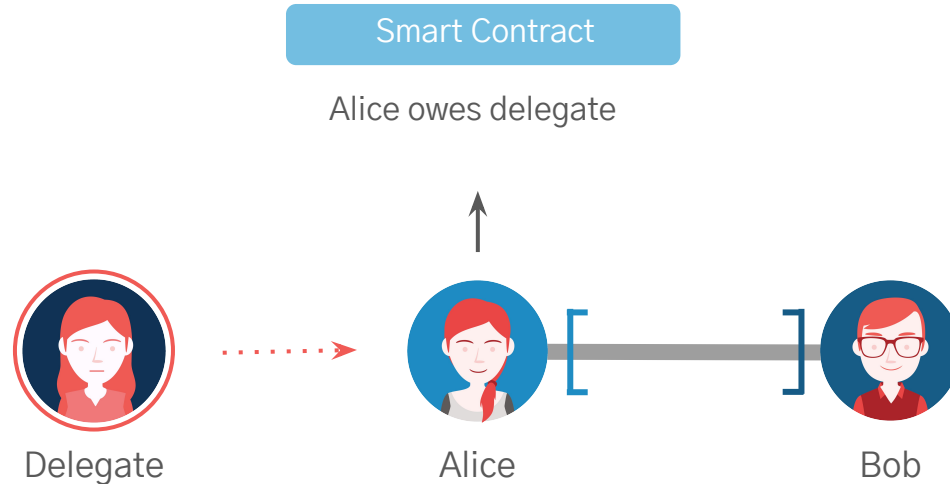


Alice wants to join the Trustlines Network,
but she has no TLC or any other crypto



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

Trustlines delegate service

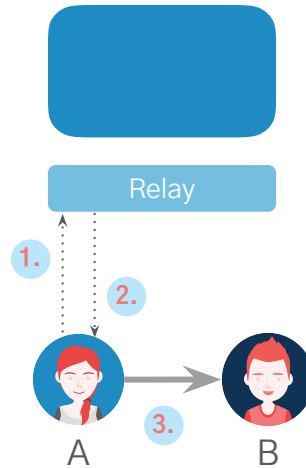


Alice and Delegate both sign the transaction. The currency network registers that Alice owes a delegate a currency network fee.

Relay Services

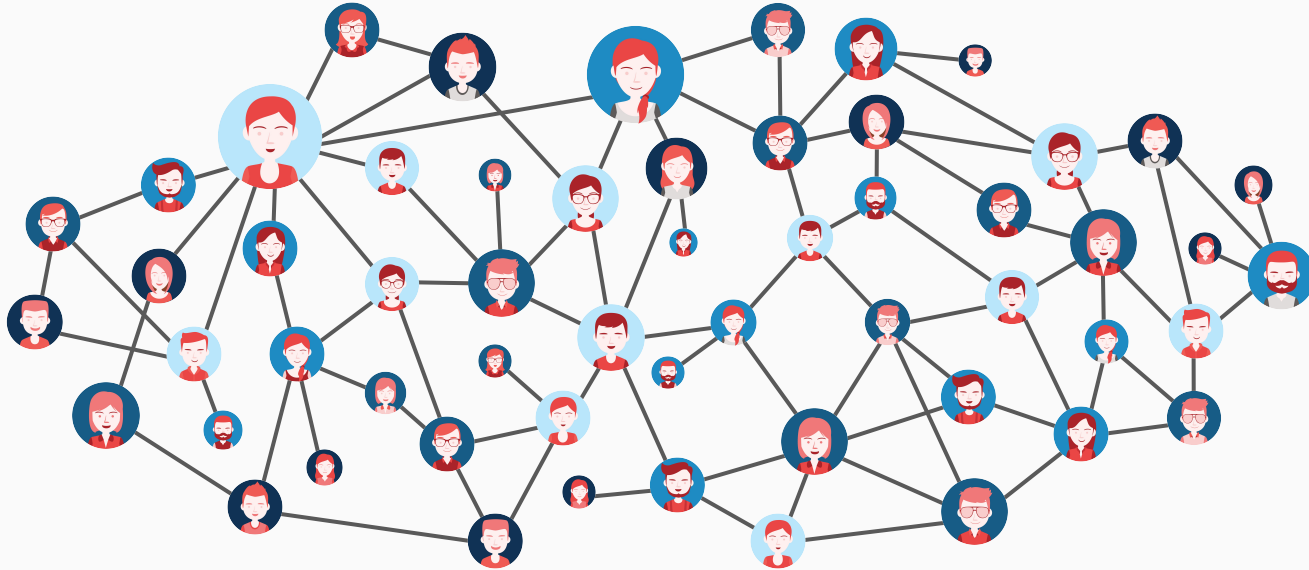
- Helper services for path calculations that are not feasible to do on-chain
- Can be paid in currency network fees and/or Trustlines Coins

1. Query
2. Path
3. Transaction



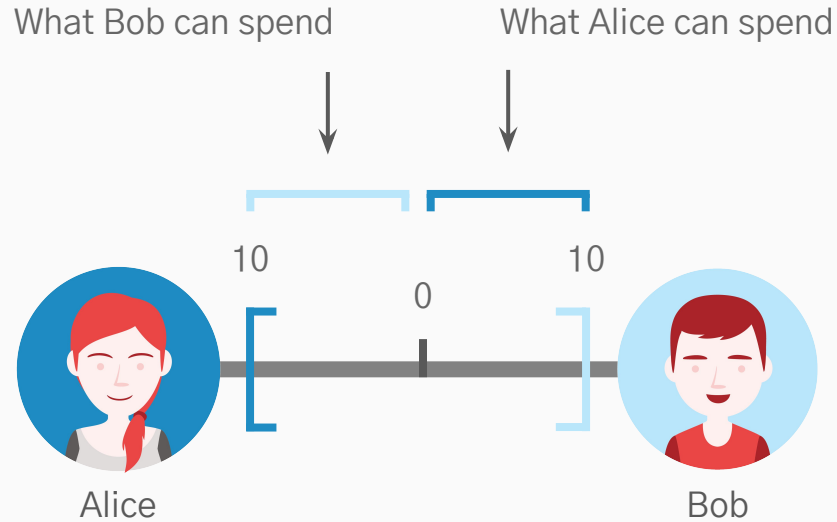
What is People-Powered Money?

People-powered money



Mutual credit based on a network of individual trust relationships

This is a trustline

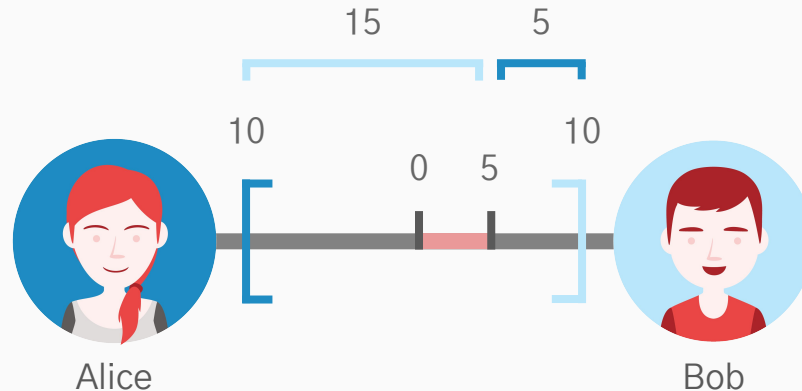


Two credit lines issued bilaterally between two people who trust each other

A trustline with a balance

Alice issues a \$5 IOU to Bob

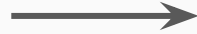
- Sending the IOU → increases credit for Bob and decreases credit for Alice
- Bob now has \$15 in credit
- Alice now has \$5 in credit



Receiving credit from a stranger



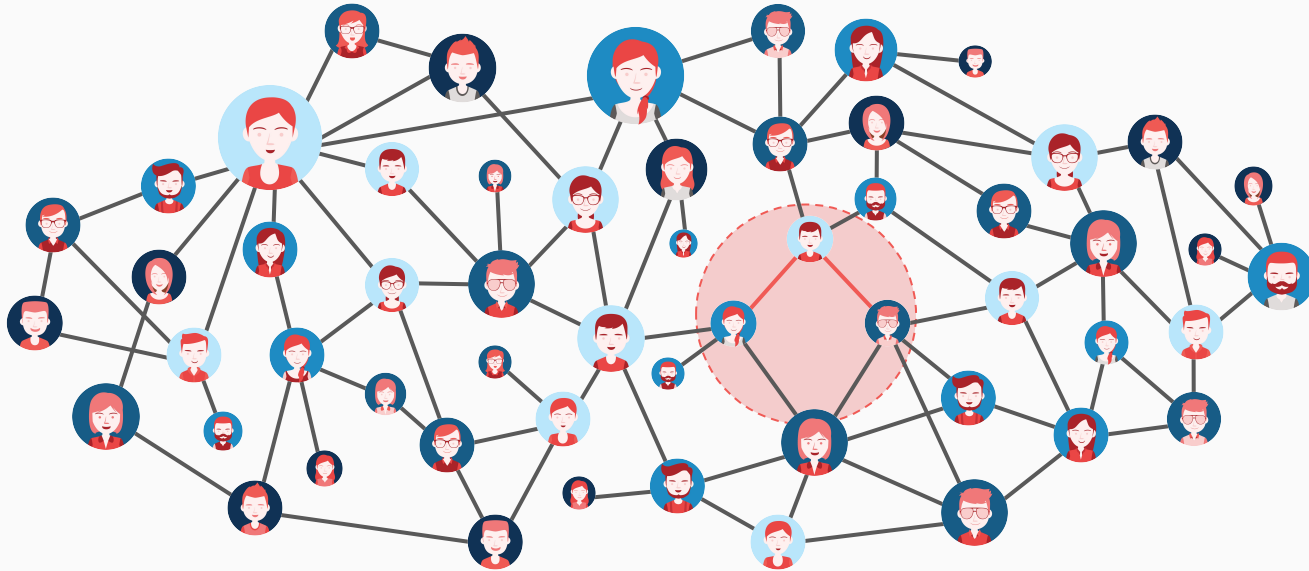
Alice



Charlie

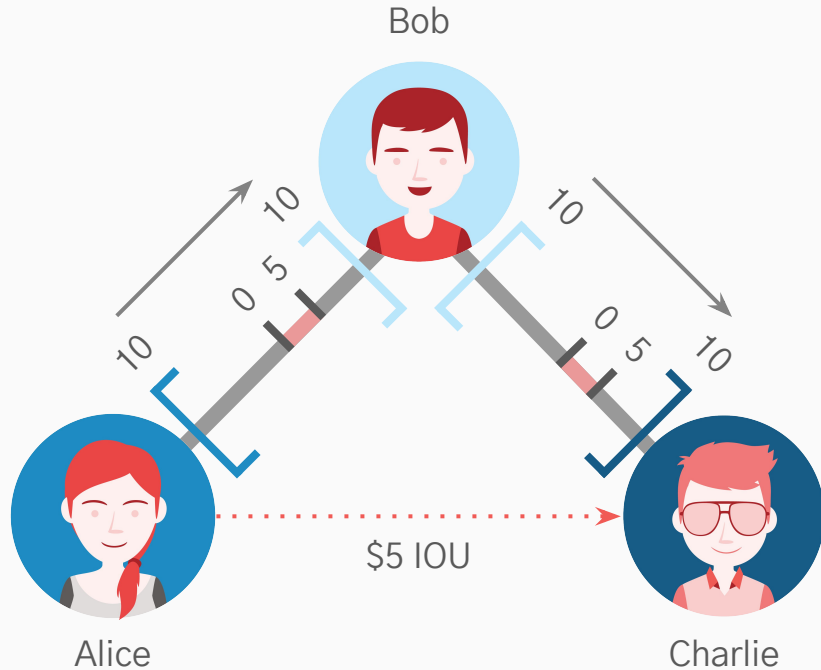
Charlie is a stranger and **does not trust** Alice with credit

Discovering a path



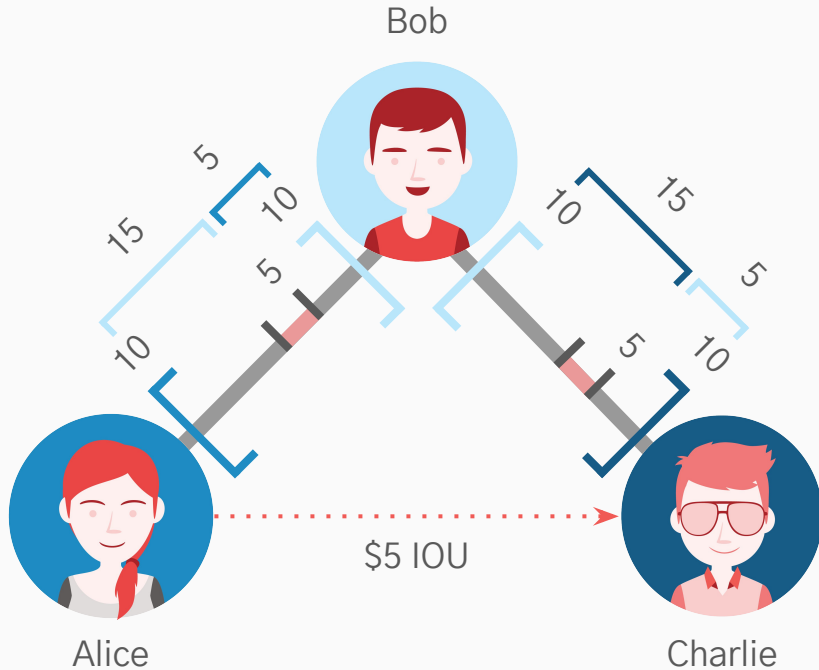
A path of **connected trustlines** can be used to connect strangers

Discovering a path



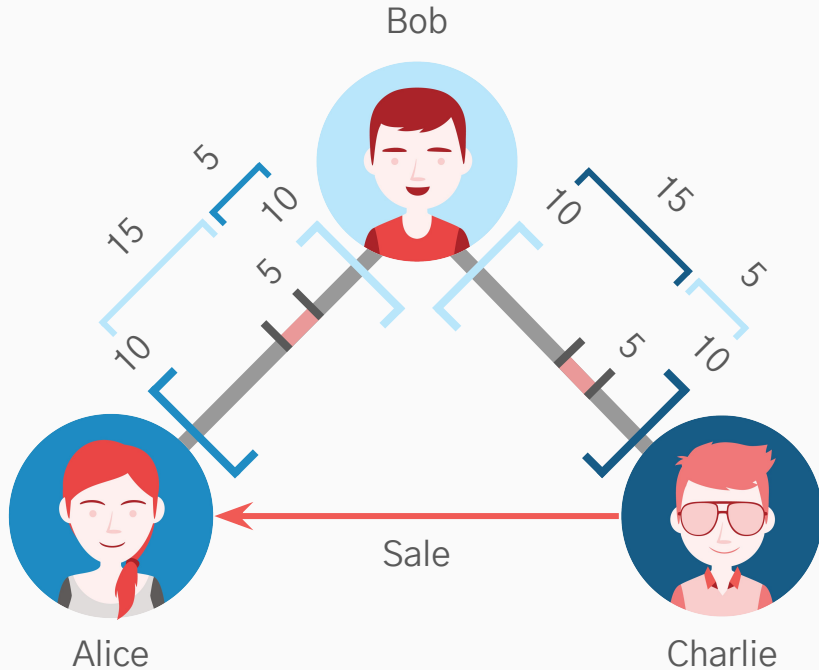
- Alice sees there is a path with sufficient capacity

Multihop Payment



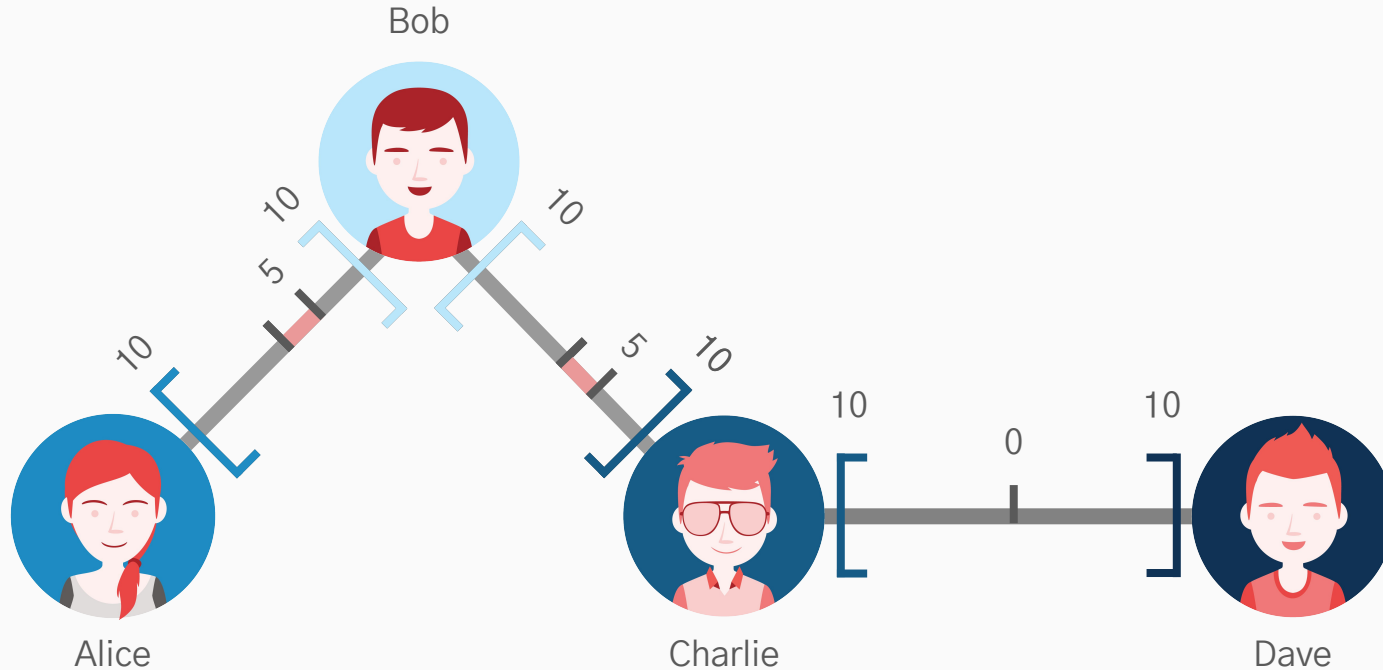
- Alice issues an IOU to a stranger
- Bob's net balance remains unchanged
- Charlie is owed by someone he trusts

Multihop Payment

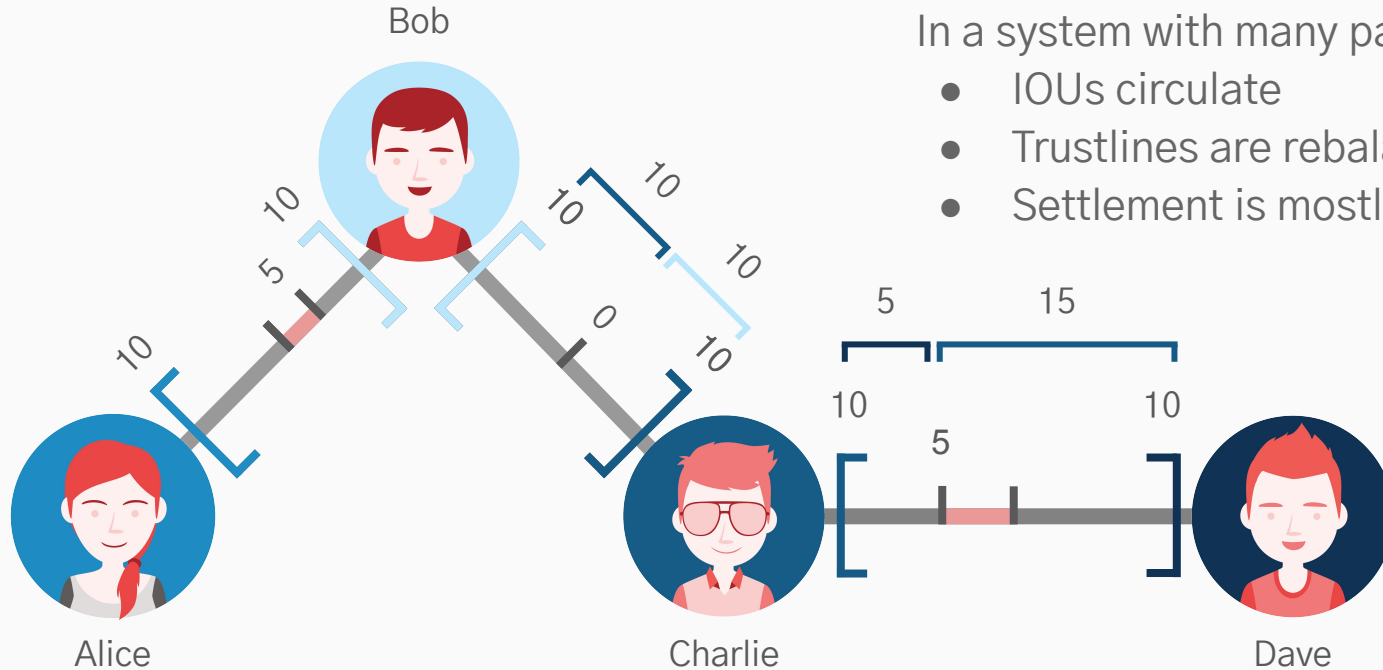


- Multihop payment function like a payment in kind
- Charlie agrees to a sale because he receives additional credit in a trustline he finds valuable

How do participants settle?



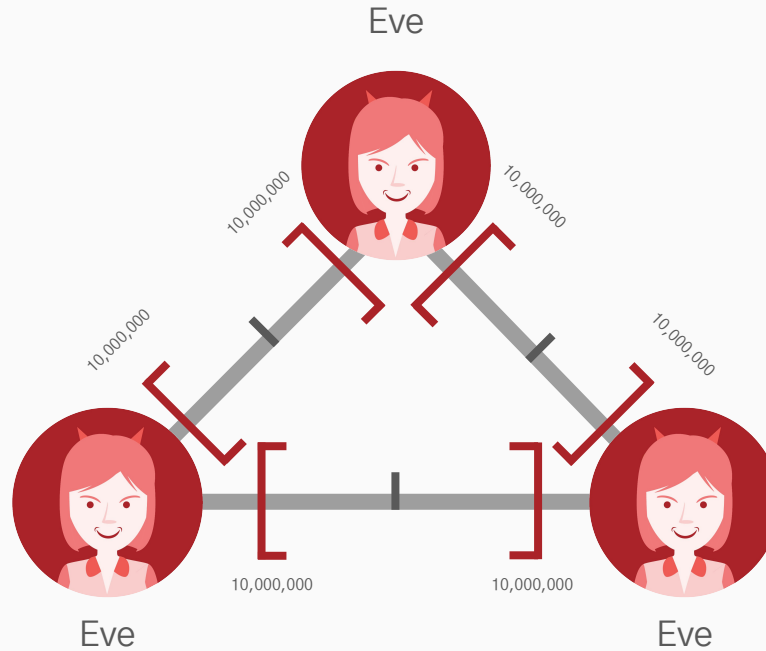
Rebalancing of trustlines



In a system with many participants

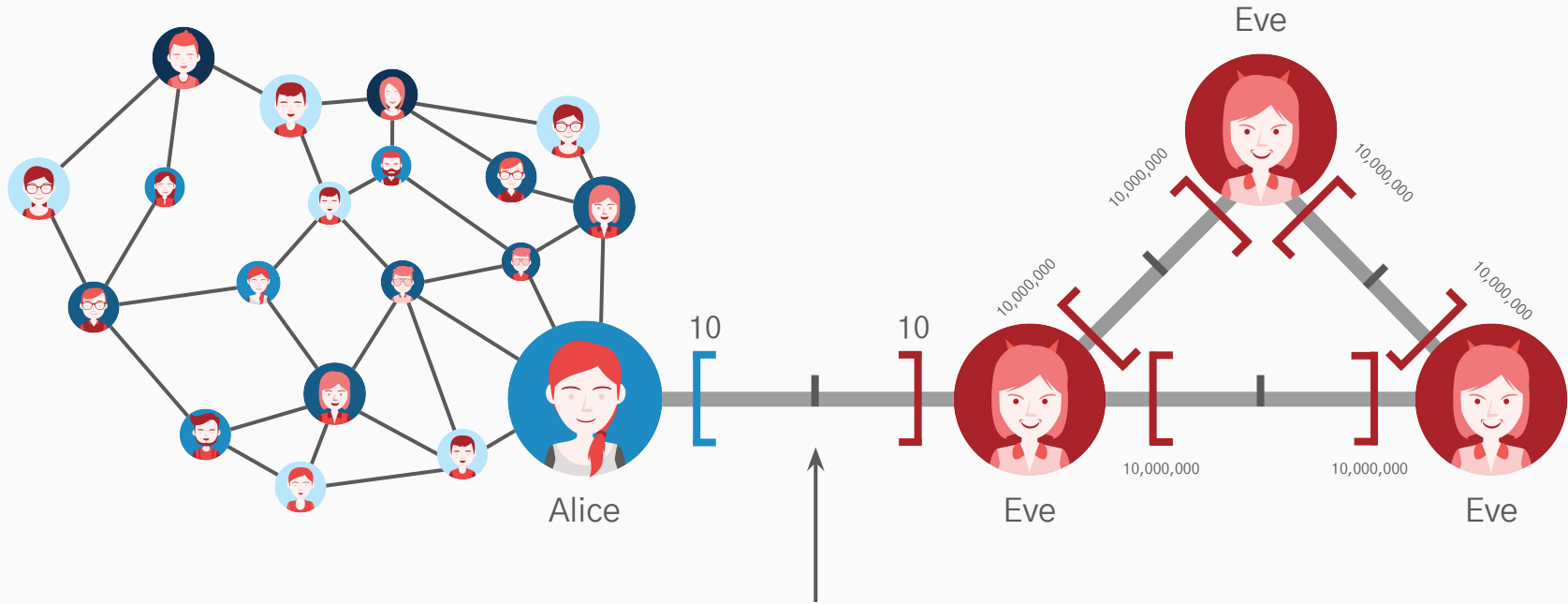
- IOUs circulate
- Trustlines are rebalanced
- Settlement is mostly unnecessary

Sybil attacks



Why not create fake accounts with “**fake credit**” to use in the network?

Sybil attacks



Eve's spending limit is determined by the credit limit her friends have given her

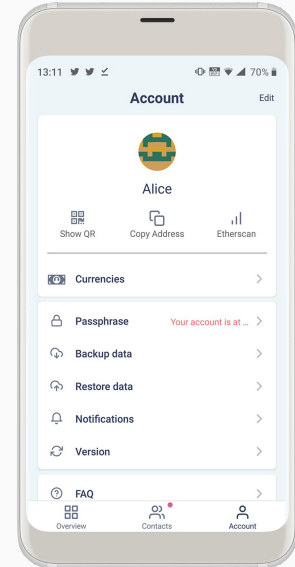
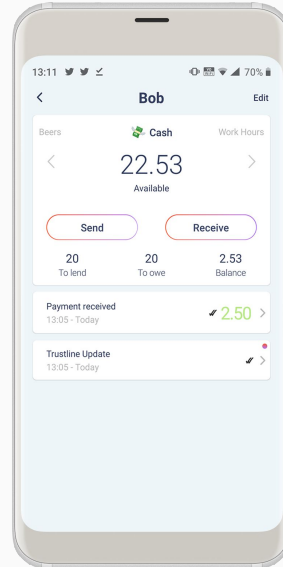
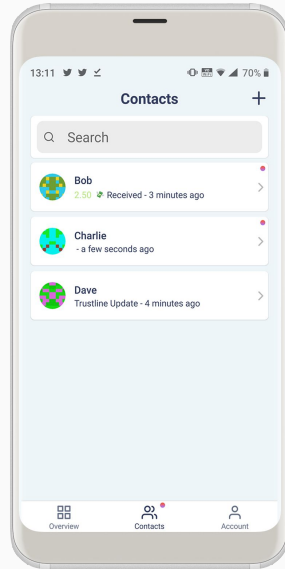
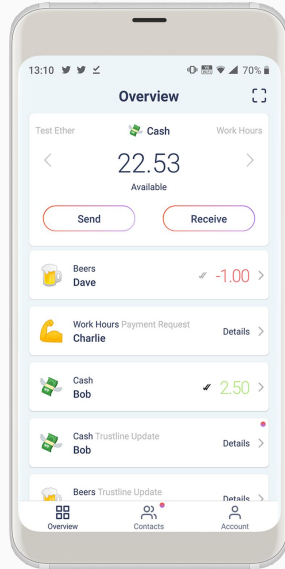
Is this money?

An alternative to standard mediums of exchange that anyone can issue

- Created as needed, by its users
- Obtains its value from real world trust relationships
- Is accessible to anyone with a friend

Bootstrapping the Network

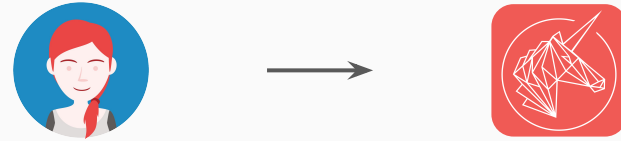
People-powered money



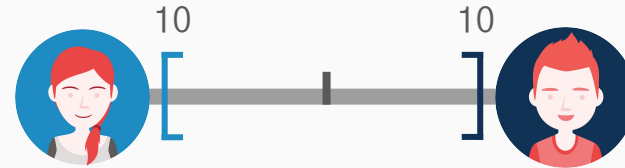
Accessible through a mobile app

Onboarding in seconds

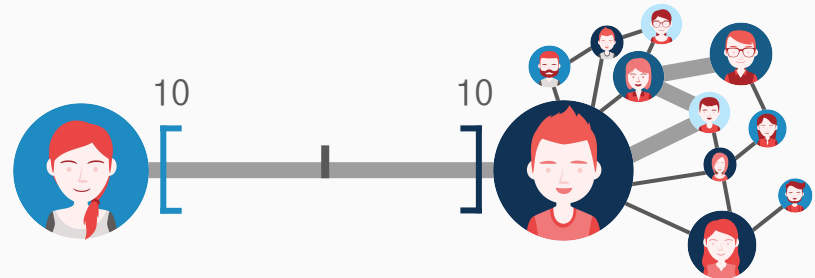
1. Download an app



2. Create a trustline with a friend



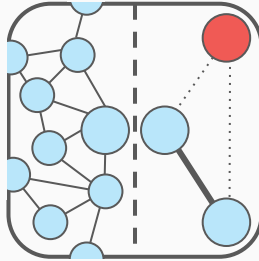
3. Interact with anyone in the network



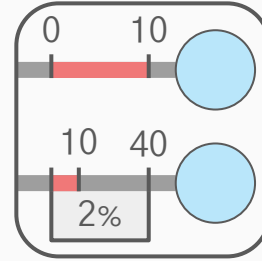
Create your own community currency network



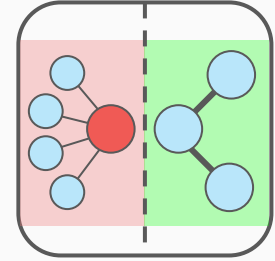
Denomination
(Eur, Time, BTC, Beers)



User group
(Open, Closed/Permissioned)



Interest



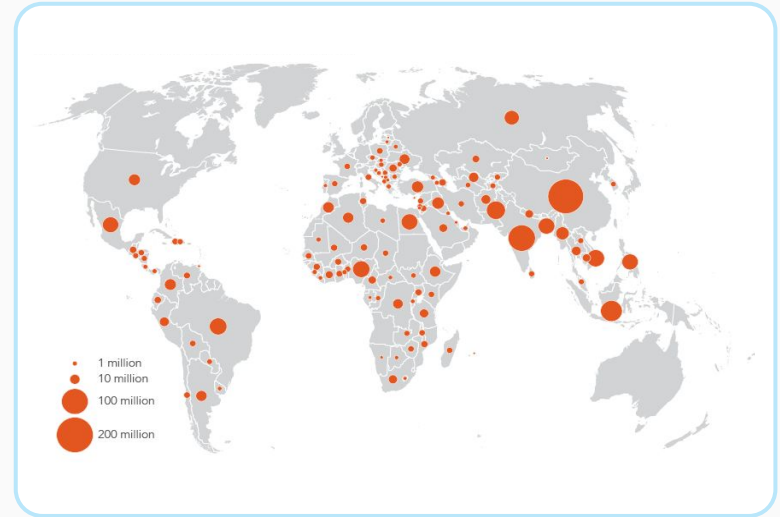
Number of trustlines

Who could benefit the most?

1.7 billion people excluded*



66% already have mobile phones*

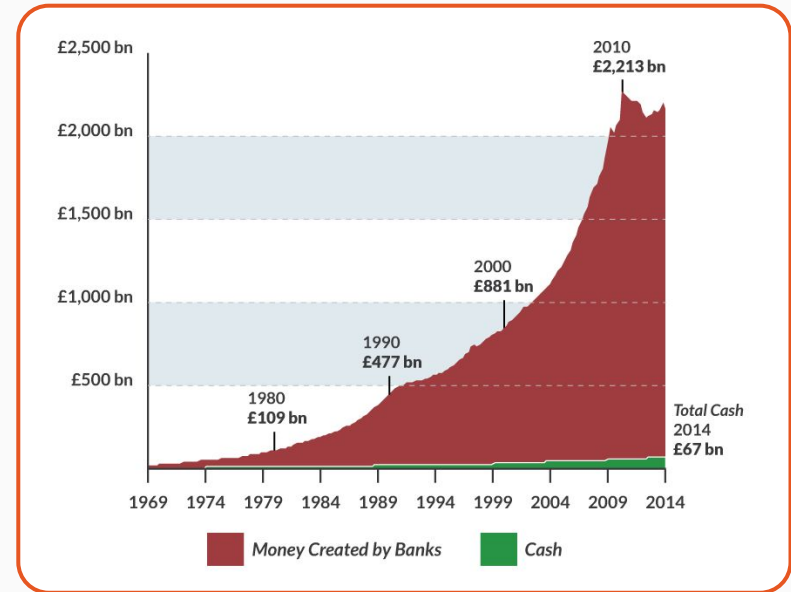


*The Global Findex Database, The World Bank 2017

Who could benefit the most?

“We identify 147 systemic banking crises and 218 currency crises between 1970–2011”

“Systemic Banking Crises Database: An Update”, IMF, 2012



“UK money in circulation, Positive Money”, Bank of England, 2014

Stay up-to-date!



@TrustlinesFound



Trustlines Foundation

Find out more!

