

Krijgen we ons ID op de smartphone?

Digitalisering BZK wil vooroplopen met digitalisering. Utrecht en Eindhoven krijgen een proef: identificatie op de smartphone.

Liza van Lonkhuyzen 14 juli 2018



Trustchain technology results

Dr. J.A. Pouwelse
Associate Professor
Ledger Scientist
TU Delft
peer2peer AT GMAIL

Programmable economy

Marketplace

Money

Trust

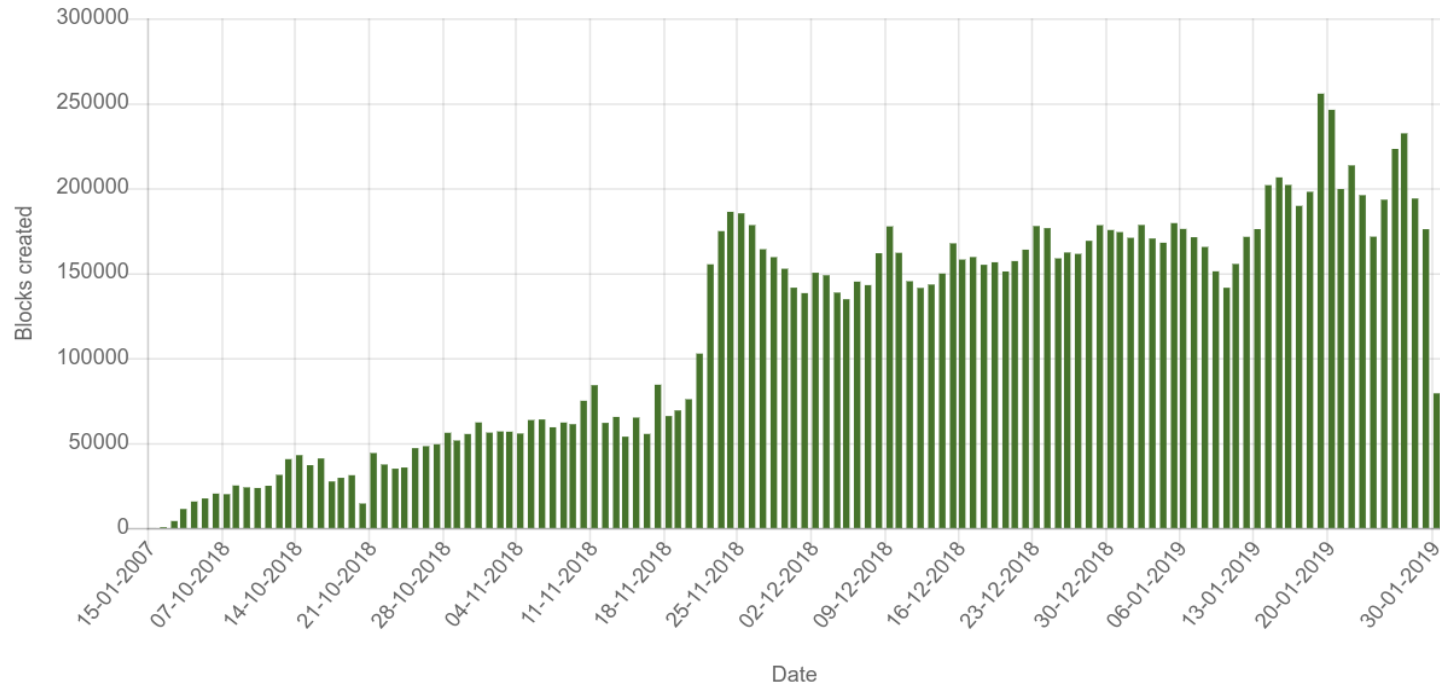
Computation

Identity

Storage

Internet Deployment

TrustChain blocks created per day:



<https://pure.tudelft.nl/portal/files/47579639/paper.pdf>

Computation beyond smart contracts: distributed apps



```
/usr/bin/python2.7 /home/mitchell/ipv8-dapps-loader/loader.py
checking torrent: execute.py
metadata complete
torrent infohash: 664aa08a1ebb1224baf7a70e32351464452606f4
starting torrent: execute.py
torrent: execute.py complete
Hello World!
First prototype dapp was executed

Process finished with exit code 0
```



<https://github.com/Tribler/tribler/issues/2943>

Market:

14.4 Peta Byte of Internet bandwidth

The screenshot shows the Tribler market interface. At the top, there is a search bar and navigation icons. The main content area is titled 'Market' and displays a table of orders. The currency is set to 'DUM2 / MC'. The table is divided into 'BUYING' and 'SELLING' sections. Below the table, there are buttons to 'Buy DUM2 for MC' and 'Sell DUM2 for MC'. At the bottom, there is a summary of the current order: Trader ID, Order Number, Price, Volume, and Time created.

BUYING		SELLING	
Volume	Price per unit	Volume	Price per unit
1000.0 DUM2	1000.0 MC	999.0 DUM2	1000000000.0 MC
999.0 DUM2	1000000000.0 MC	1000.0 DUM2	1000000000.0 MC
		999.0 DUM2	1000000000.0 MC
		999.0 DUM2	1000000000.0 MC
		1.0 DUM2	10000000000.0 MC
		1.0 DUM2	10000000000.0 MC

Buy DUM2 for MC Sell DUM2 for MC

Trader ID 3ff01e88249017ae24270f3996f5977a19a3b5fe
Order Number 18
Price 1000.0 MC
Volume 1000.0 DUM2
Time created 2017-06-09 12:13:23

github.com/Tribler/tribler/issues/2559

Self-sovereign identity



IETF "Trustchain" Internet Standards Draft

4.2.1.2.2.2. The Attestation Request Message

Number	Description	Type	Size (bytes)
0	Preamble / Prefix	Char Array	23
1	Public Key in Binary Format	Unsigned Short Array	n
2	Global Time (Lamport Timestamp)	Unsigned Long Long	8
3	Attestation Metadata	Char Array (Raw)	33 + m
	Total:		64 + n + m

<https://ec.europa.eu/digital-single-market/en/news/tu-delft-helps-develop-digital-id-use-your-phone>

universal mechanism to create trust

1995



1997



2008



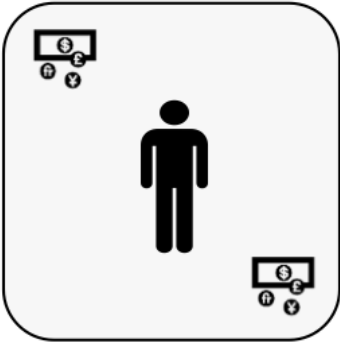
2009



2014



2017



2019

Distributed Trust Design

★★★★☆



TU Delft

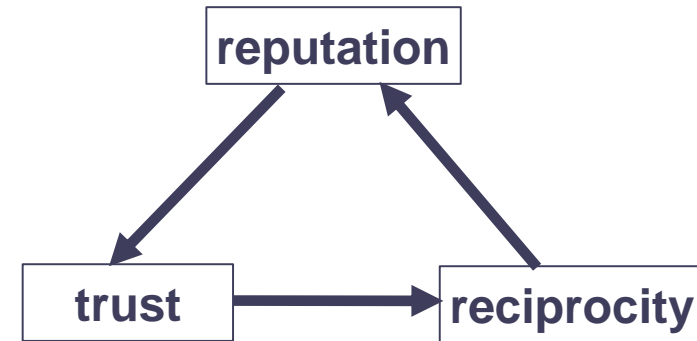
A rounded rectangular box with a black border. On the left side, the text "Distributed Trust Design" is stacked vertically. To the right of the text is a row of five stars: four are solid blue, and the fifth is a lighter, semi-transparent blue. Below the stars is the TU Delft logo, which consists of a stylized flame icon above the text "TU Delft".

Mathematics of trust

Mui et al 2001

- **Reputation:** perception that an agent creates through past actions about its intentions and norms
- **Trust:** a subjective expectation a peer has about another's future behaviour based on the history of their encounters
- **Reciprocity:** mutual exchange of deeds

$$\mathbb{P}(W_{ij} = x) = \mathbb{P} \left(\left[\sum_{t=0}^{\infty} \mathbb{1}_{\{X_t=j\}} \right] = x \mid X_0 = i \right)$$



github.com/Tribler/tribler/issues/2805

Conclusion: Programmable economy *is coming*

Marketplace

Money

Trust

Computation

Identity

Storage