MUFFIN CONFERENCE | MusalaSoft

Internals of Cryptocurrencies & Digital Assets

Petyo Dimitrov

MusalaSoft
MUFFIN

Agenda

What is Blockchain?

Bitcoin

Popular Blockchain-s

Smart contracts

Issues

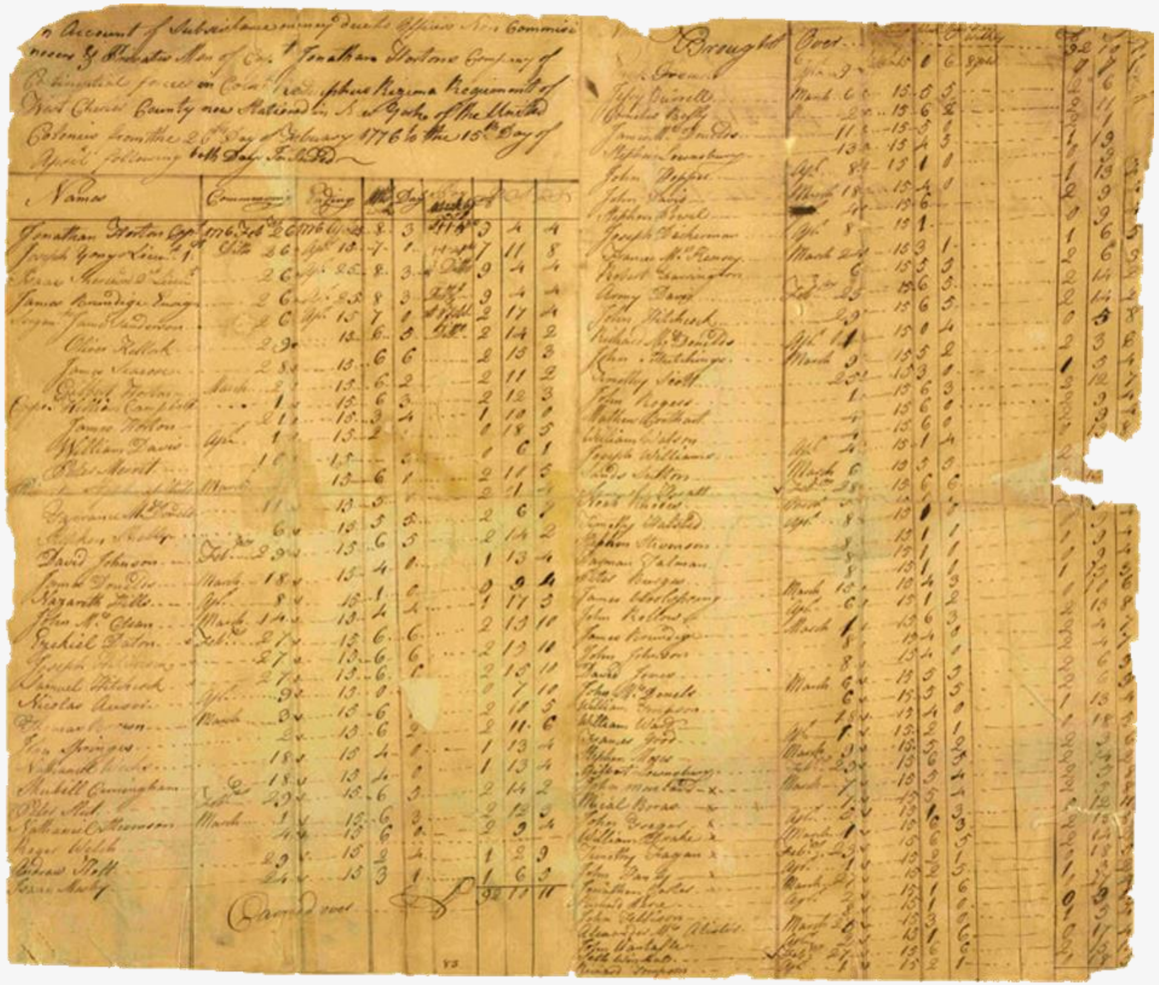
Overview

“I believe Blockchain will do for trusted transactions what the Internet has done for information.”
“We’re already talking about ten thousand transactions per second, or maybe more”

Rometty

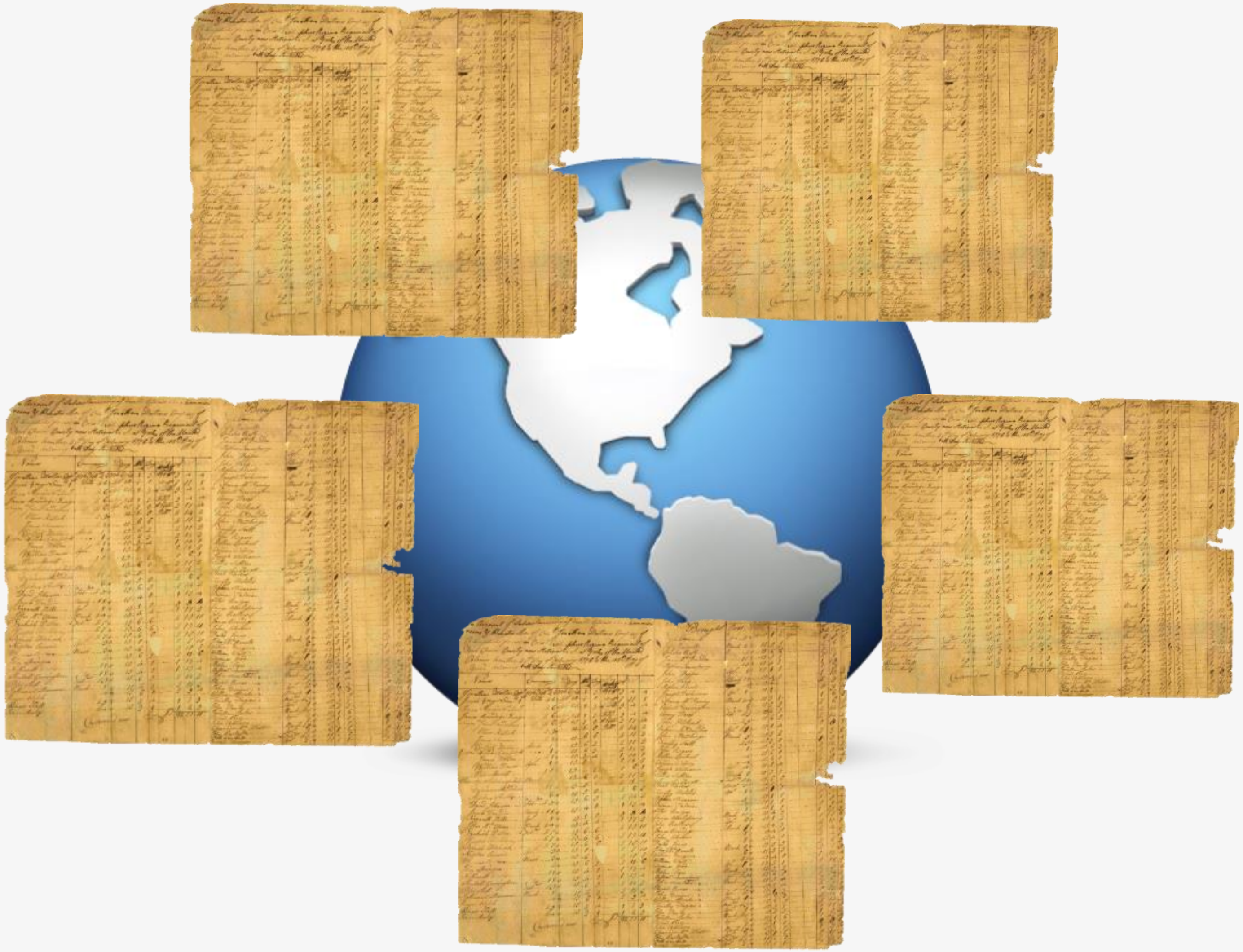
Distributes trust vs Intermediaries

What is Blockchain?

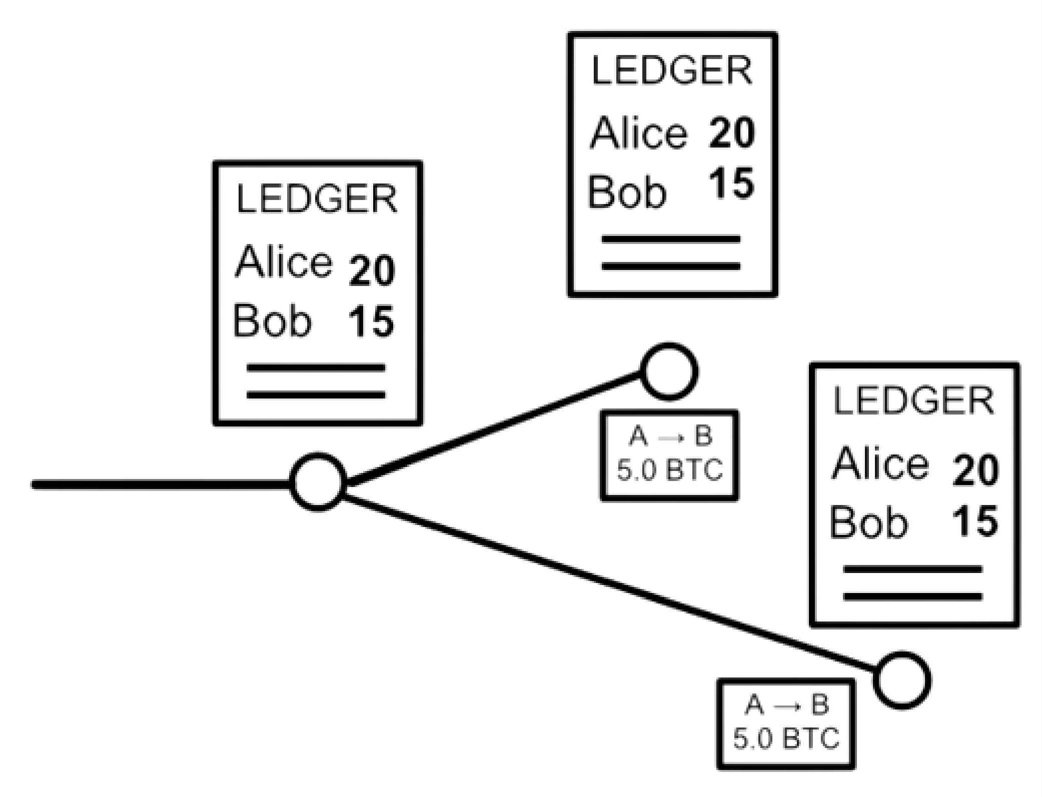


MusalaSoft MUFFIN

Distributed Ledger



Transactions, not Balance



Transaction Messages

			Digital Signature
Alice	→ Bob	5.0 BTC	04323784...
Alice	→ Dave	12 BTC	88432738...
Alice	→ Juan	2000 BTC	00328434...
Alice	→ Bob	14 BTC	19382637...

^

different every time

Bitcoin Overview

Started in 2008 by Satoshi Nakamoto*

Most popular crypto-currency

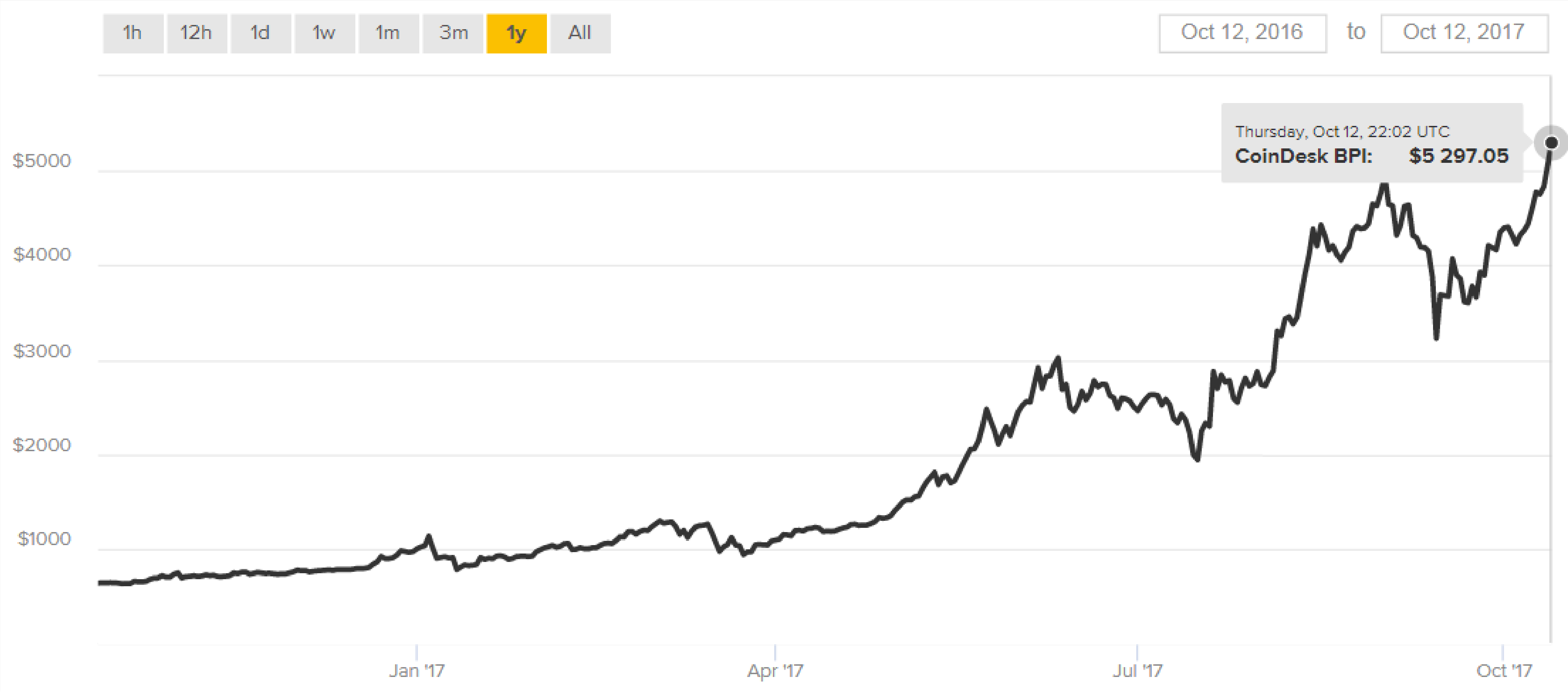
Non-government controlled

Fiat currency

Anonymous

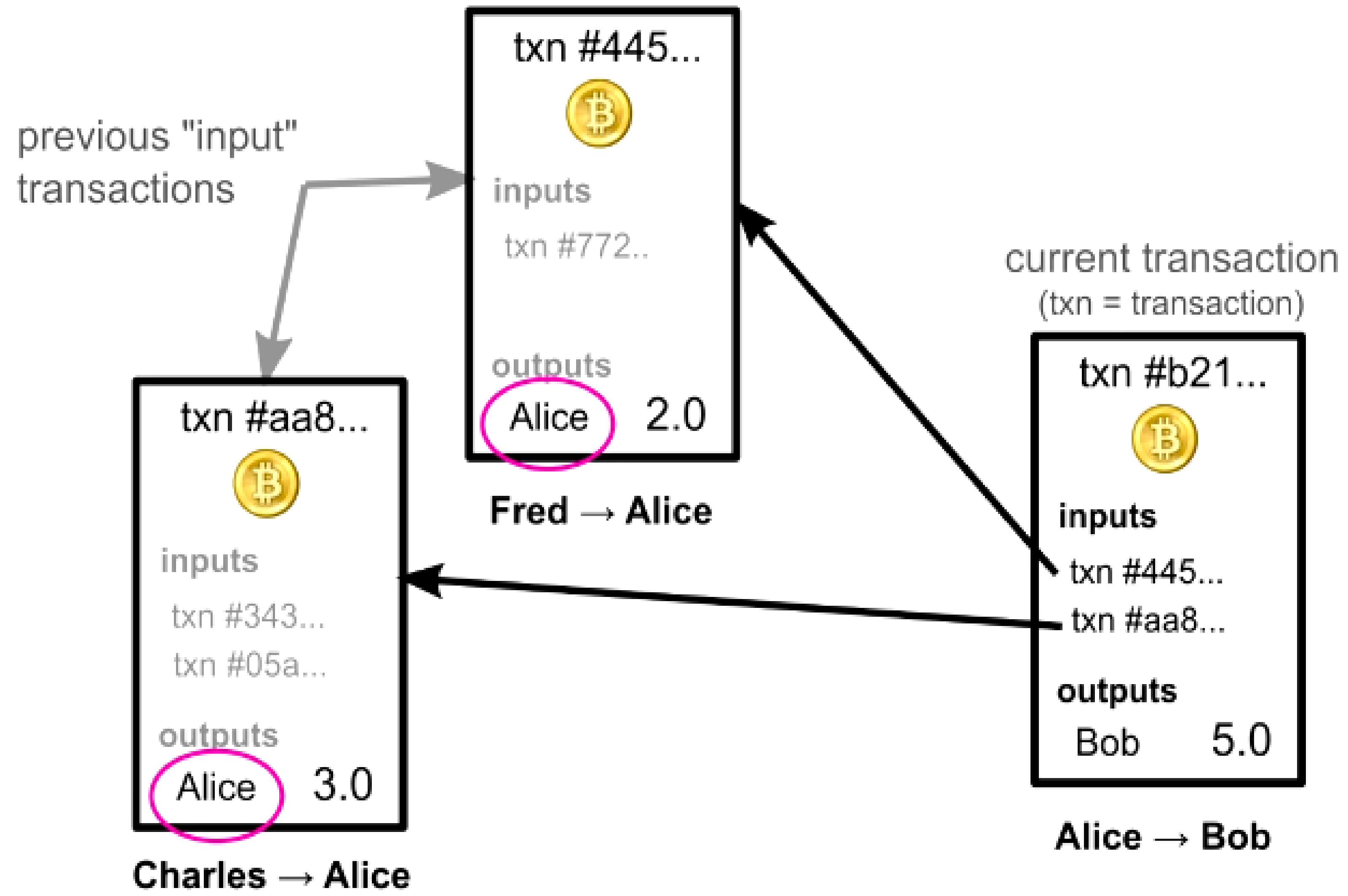
Current Bitcoin price: ~9000 lv

Bitcoin’s price



Bitcoin wallet

Bitcoin: transactions (1)



Bitcoin: transactions (2)

Inputs

Previous output (index)?	Amount?	From address?	Type?	ScriptSig?
eb38f77560ca...:1	8	1P9SgqzjFWgWVAuZBFwimNPV7LuuaJpgTj	Address	30450220078df7c48ed152bd40eaee4a73afefc3 044760639da2c0d6158484e1a4dab332fefc4bb
b912994fca58...:1	0.03	18Mk65wV1E5kCVHFShvUTU6zt4yVFKM5Ft	Address	304502204e877fc5ca3783e165052e64c4788dd 04769bbfc55cbd412784e024c8624f8c4f42d7cb
58379d94fe85...:15	1	1G4hfnM2ufAPEECdawg5gtvUTBB2PxvLr2	Address	3044022075d23fd4a8004866777210f51f46c96 046dd45b37fe3ff33f1563458cfbdfb7f922d1b4a
fc9d1cd1c2ac...:1	130	1LpQVnJSMgqqibQBGZwbobdX2Ghn9YWyC7	Address	3046022100a65a188b89a4e5ae2eaa5ba387503 04ba81a1a538c5ddf7e0c76884497ab522456b9
7b6f7d4a521c...:1	0.55357267	16Kb6XppHUbjgmYQDpRyxz9jNE9Az5Xvcb	Address	3045022100eeb76e61abe62d38fd462eafd1d11 04f4fa1d3e26f3e7058038871a31b8bf63fd127f6
544097a30e09...:0	0.03270607	1JnsDx1g6c757z8AnJUemj46YQgCTw54QN	Address	3045022100859df2ced47493e86a849cce10615 04de257fe6490bd16188be6d06ca7b34816fa4b

\+ 139.6

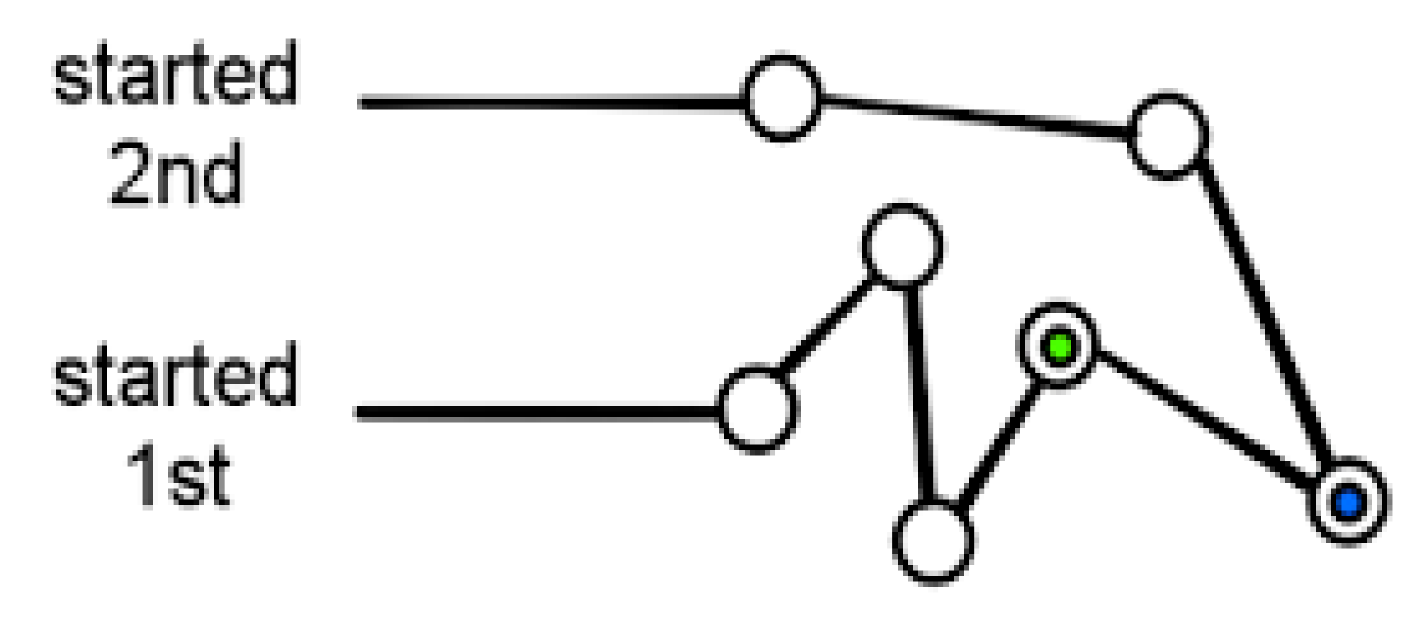
Outputs?

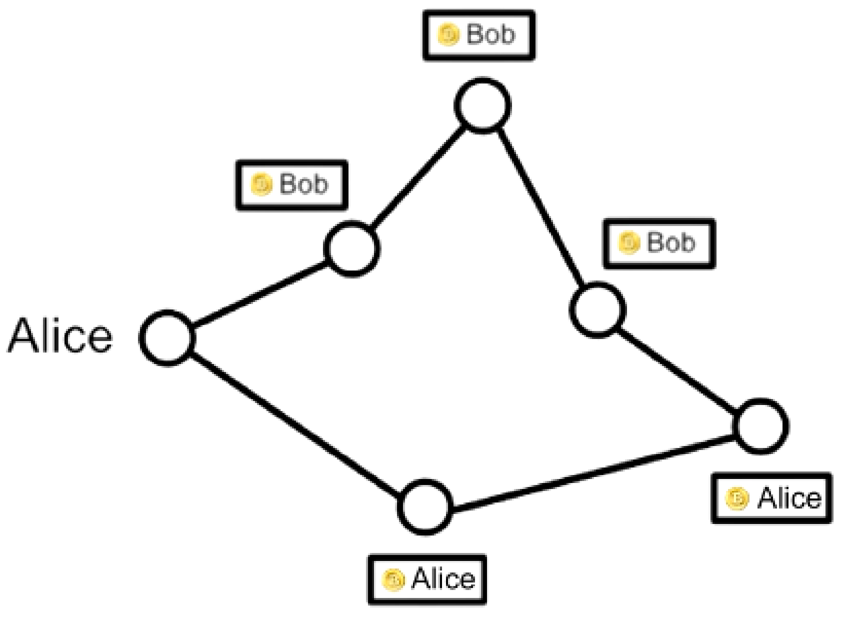
Outputs

Index?	Redeemed at input?	Amount?	To address?	Type?	ScriptPubKey?
0	8baaca27d158...	0.01071174	1F7BgzQbyWTWzEMUKNzzLdjkbjaQT9K96m	Address	OP_DUP OP_HASH160 9abd2e0c0a63dea36b75c3128fe15d82f274e394 OP_EQUALVERIFY OP_CHECKSIG
1	1bb973b4ccc8...	139.605567	1NT2zFMa11NiCZydt4kqgXRZPf3iS6ZPGZ	Address	OP_DUP OP_HASH160 eb471d7a903e538cb94c1f2faf20eaadad8479af OP_EQUALVERIFY OP_CHECKSIG

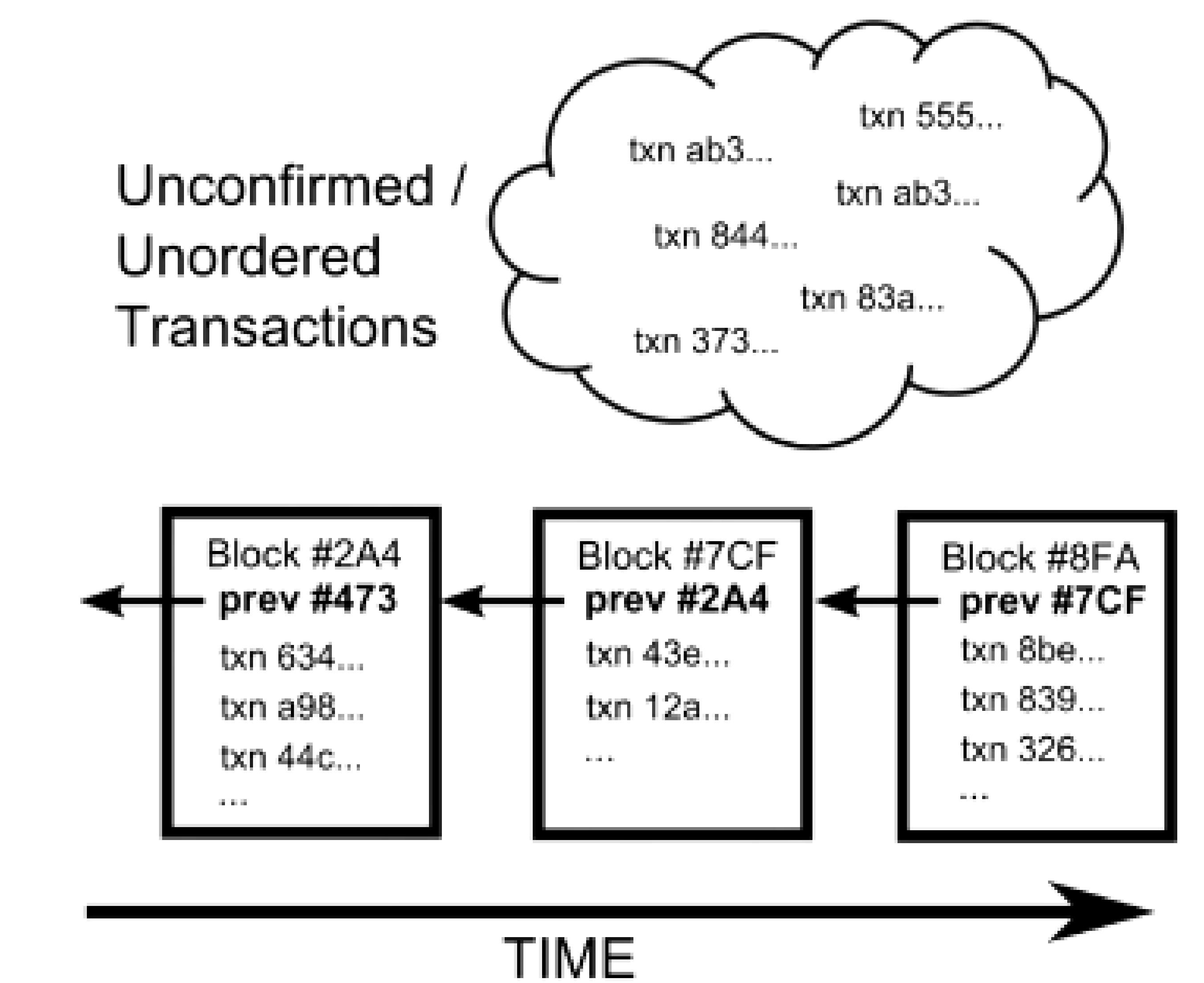
\+ 139.6

Bitcoin: transaction order

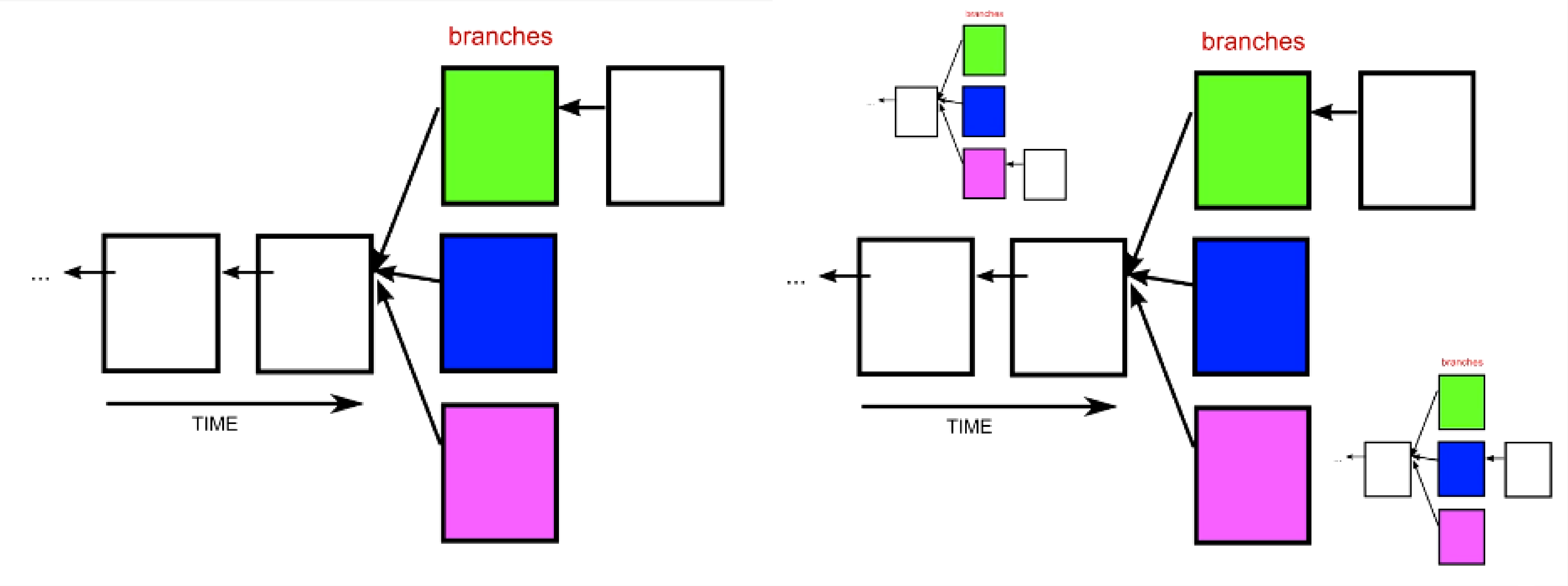




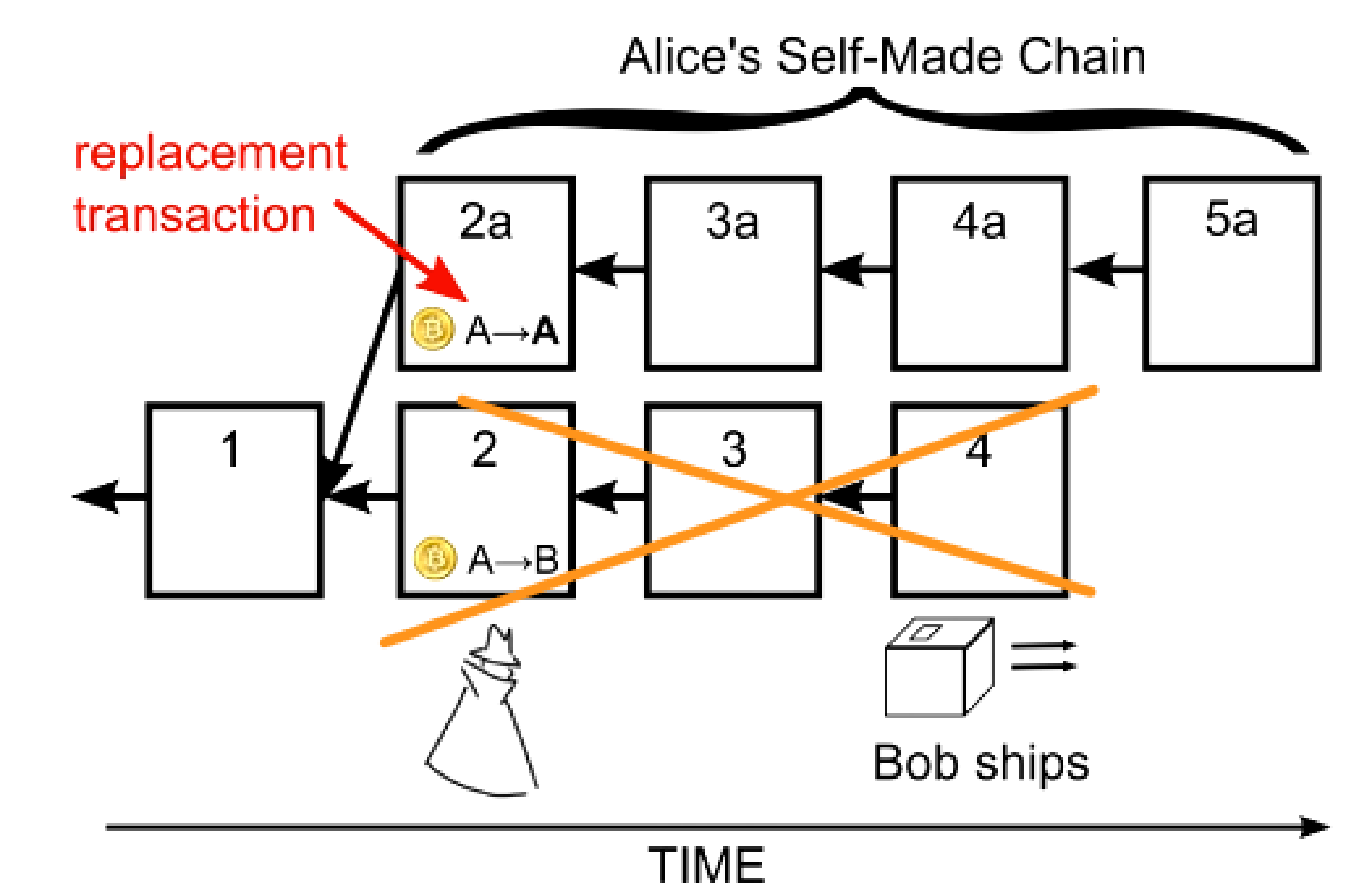
Bitcoin: blockchain



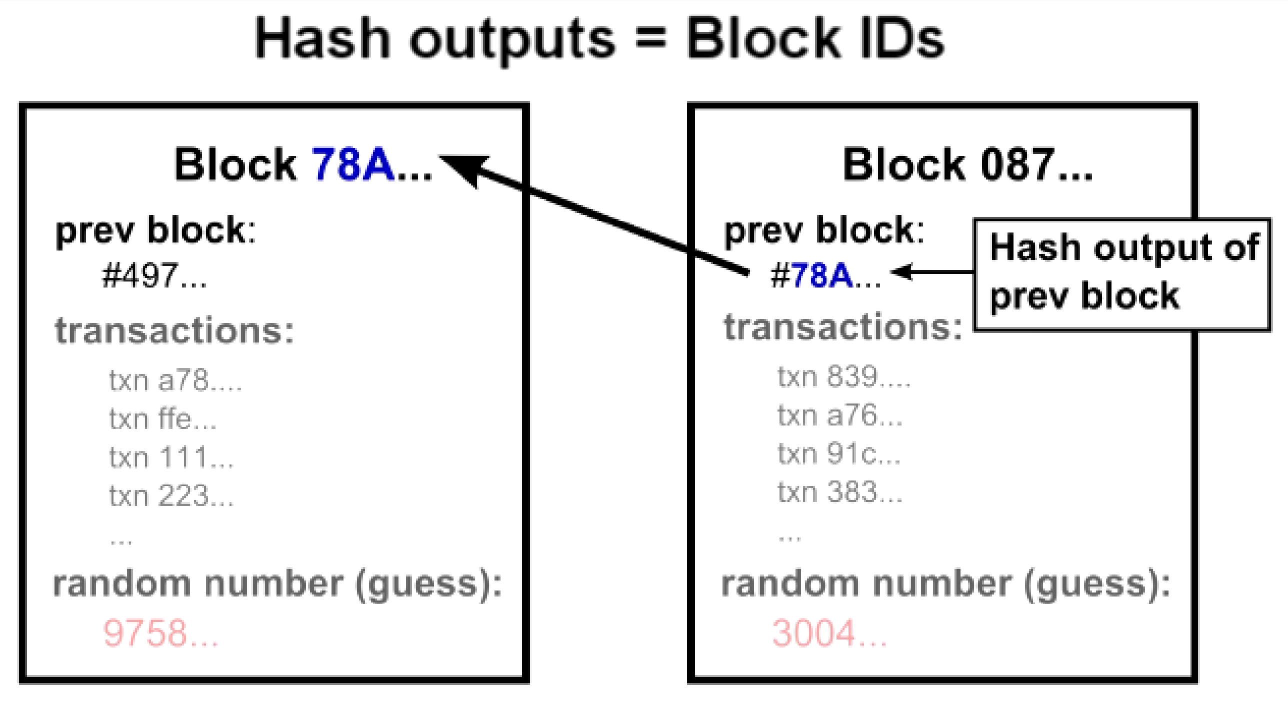
Bitcoin: conflict resolution

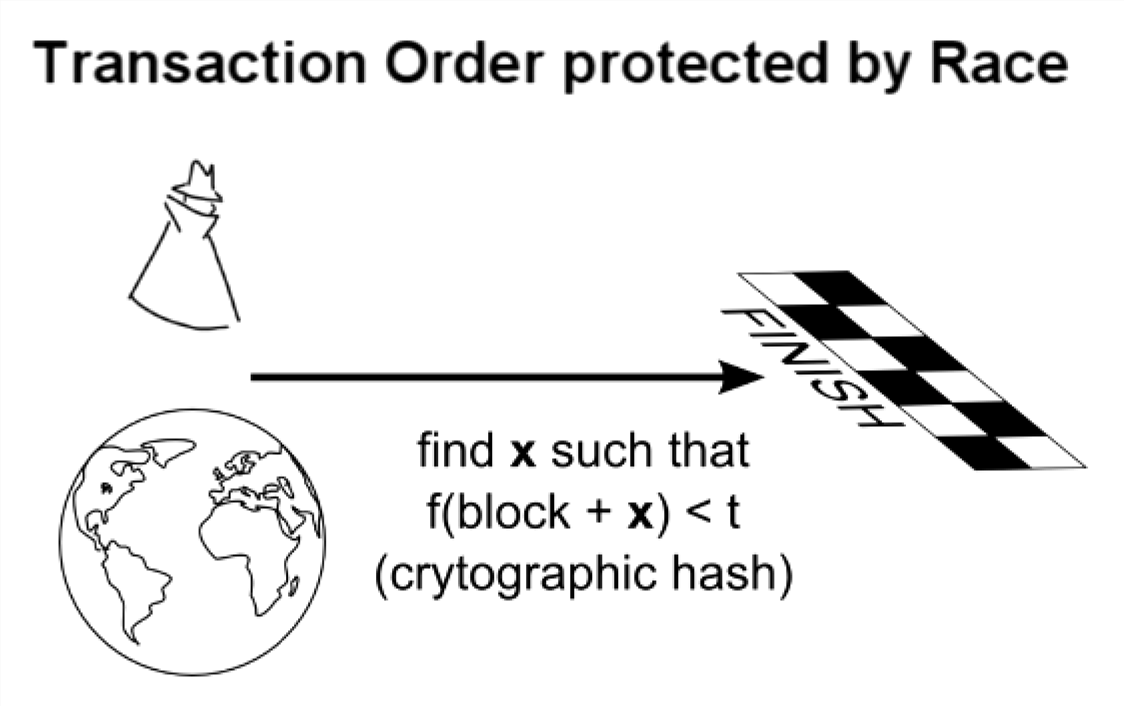


Bitcoin: fraud

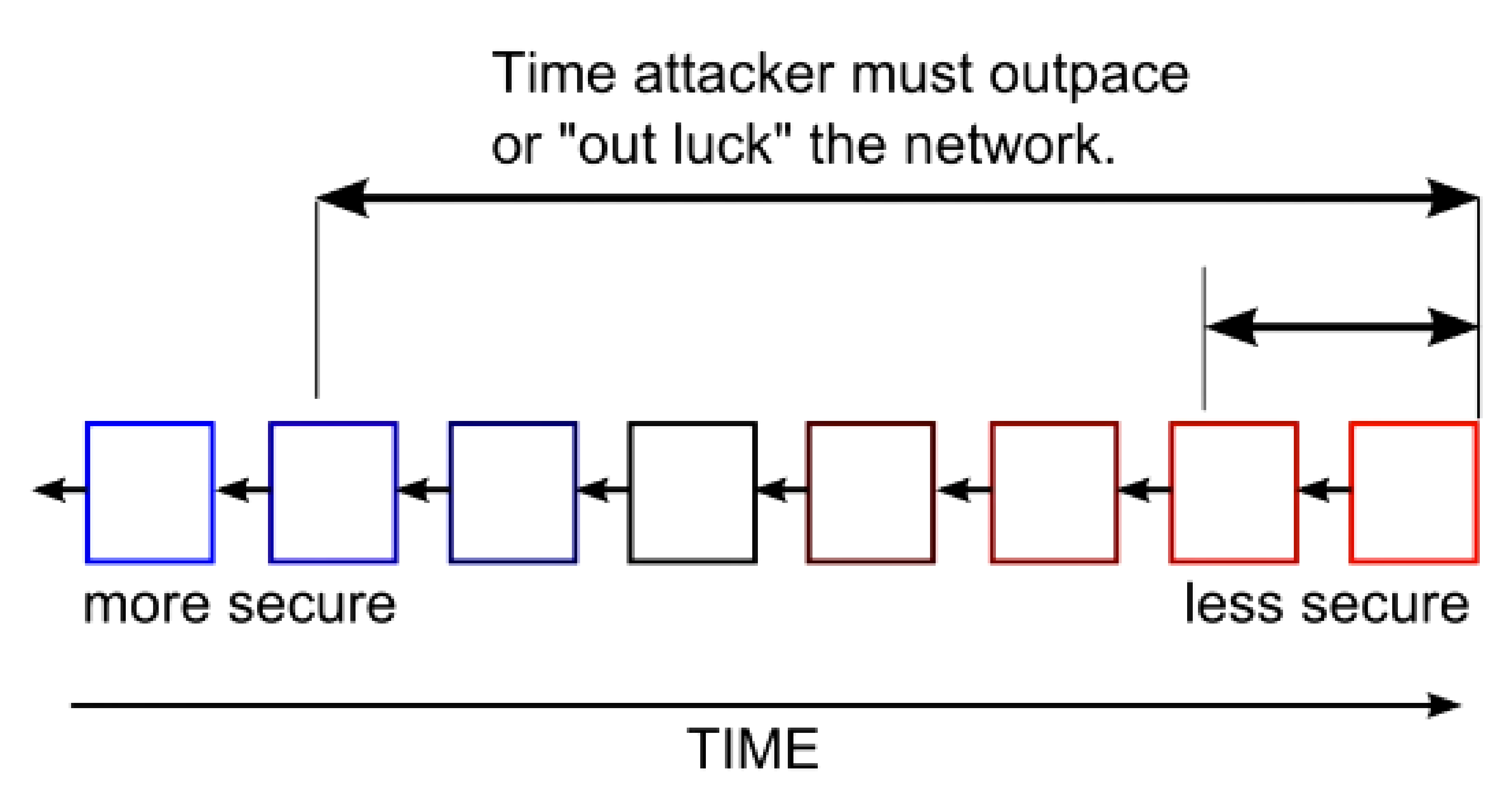


Bitcoin: fraud prevention / mining





Bitcoin: fraud prevention



Bitcoin alternatives

- Bitcoin + SegWit (soft fork)
- Bitcoin cash (8mb block hard fork)
- Bitcoin SegWitx2 (2mb hard fork)
- Bitcoin gold (ASIC resistance PoW algorithm)
- Ether
- Litecoin
- Namecoin (decentralized DNS)

Other Popular Blockchain-s

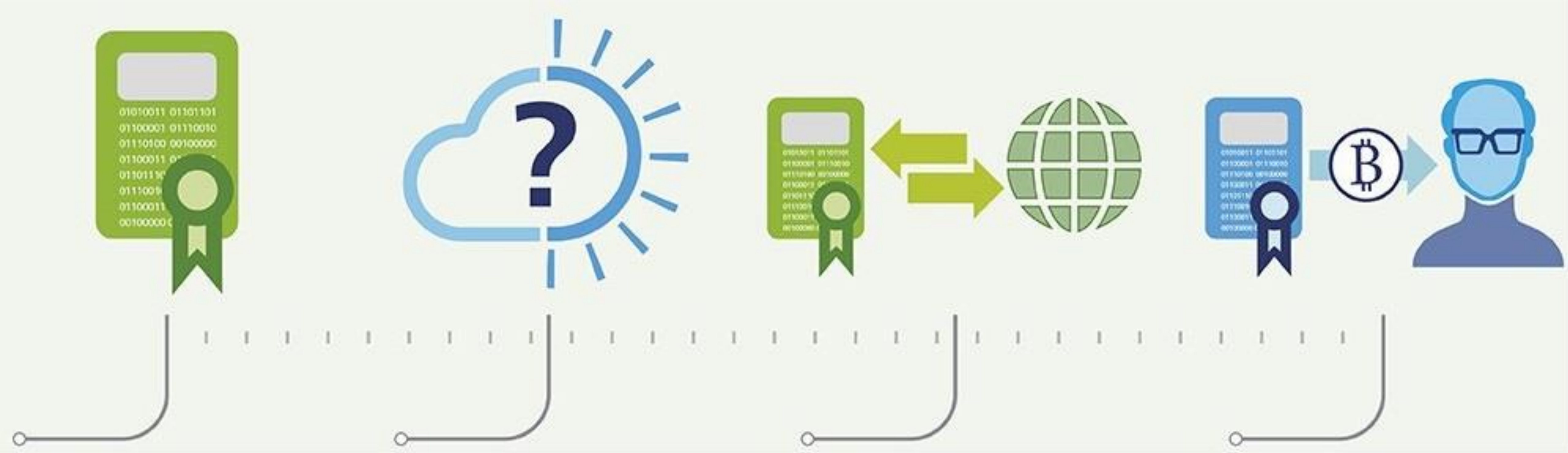
- **Ethereum** - aims to allow development of distributed applications (DApps)

- **Hyperledger Fabric** - developed by IBM and Linux Foundation & aims to give developers the ability to create private blockchains

Comparison of Blockchains

	Hyperledger Fabric	Ethereum	Bitcoin
Description of Platform	General purpose Blockchain	General purpose Blockchain	Payments Blockchain
Governance	Linux Foundation	Ethereum Developers	Bitcoin Developers
Currency	None	Ether	BTC
Mining Reward	N/A	Yes	Yes
State	Key-value database	Account data	Transaction data
Consensus Network	Pluggable : PBFT	Mining	Mining
Network	Private	Public or Private	Public
Smart Contracts	Multiple programming languages like Java, GO.	'Solidity' programming language	Possible, but not obvious

Smart Contracts / DApps



Blockchain Issues

- Solution looking for a problem
- Expected transaction cost increase
- Performance
- Security
- Immutability (GDPR)

Applicability of blockchain

- use where it…

F raud risk

I ntermediaries

T hroughput

S table data

Q&A

Petyo Dimitrov

MUFFIN CONFERENCE

MusalaSoft

Discussion panel

- Norbert Kouwenhoven
- Delyan Lilov
- Iancho Dimitrov
- Petyo Dimitrov