ON DECENTRALIZED PROTOCOLS

CAL2021

Ricardo Pérez-Marco
(CNRS, Université de Paris)

Email: ricardo.perez.marco@gmail.com
Twitter: @rperezmarco
Web: https://webusers.imj-prg.fr/~ricardo.perez-marco/

Bitcoin

- First decentralized form of electronic money.
- First decentralized consensus algorithm.
- First programmable currency.
- First decentralized clock.
- New financial asset class.
- Birth of Decentralized Finance (DeFi).

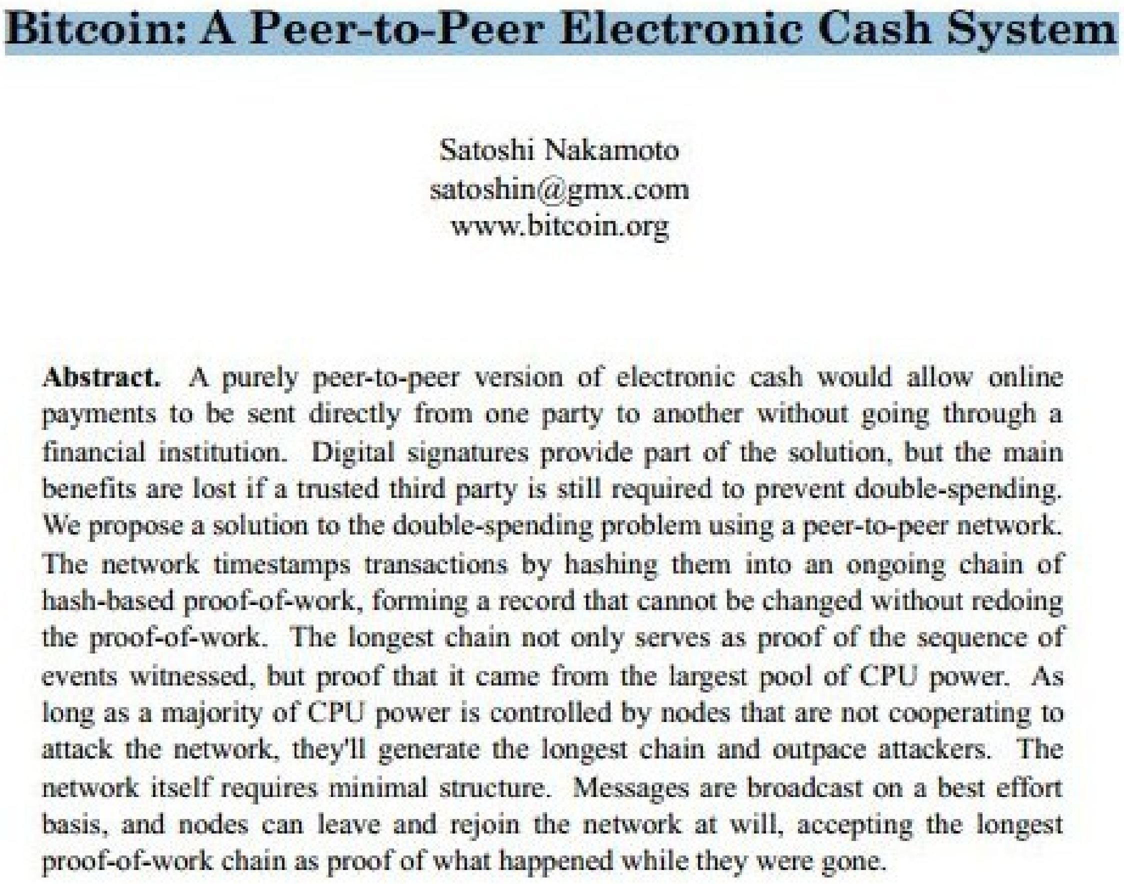
13th years of Bitcoin history

November 2008:

Bitcoin paper by Satoshi Nakamoto.

January 2009:

Code released and network started.



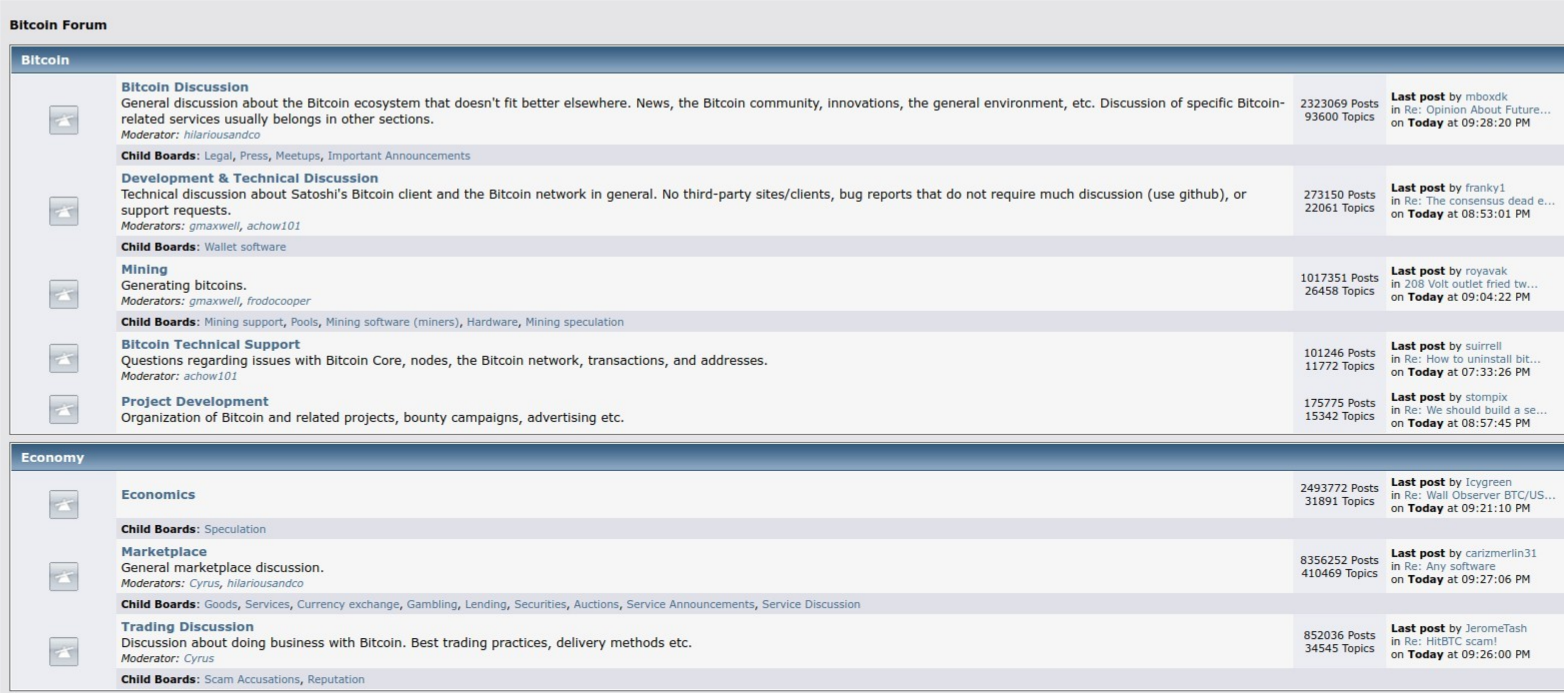
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcointalk forum

November 2009: Bitcointalk forum created.



Bitcoin Forum

Bitcoin

Bitcoin Discussion General discussion about the Bitcoin ecosystem that doesn't fit better elsewhere. News, the Bitcoin community, innovations, the general environment, etc. Discussion of specific Bitcoin-related services usually belongs in other sections. *Moderator:* *hilariousandco*	2323069 Posts 93600 Topics	**Last post** by mboxdk in Re: Opinion About Future... on **Today** at 09:28:20 PM
Child Boards: Legal, Press, Meetups, Important Announcements		
Development & Technical Discussion Technical discussion about Satoshi's Bitcoin client and the Bitcoin network in general. No third-party sites/clients, bug reports that do not require much discussion (use github), or support requests. *Moderators:* *gmaxwell*, *achow101*	273150 Posts 22061 Topics	**Last post** by franky1 in Re: The consensus dead e... on **Today** at 08:53:01 PM
Child Boards: Wallet software		
Mining Generating bitcoins. *Moderators:* *gmaxwell*, *frodocooper*	1017351 Posts 26458 Topics	**Last post** by royavak in 208 Volt outlet fried tw... on **Today** at 09:04:22 PM
Child Boards: Mining support, Pools, Mining software (miners), Hardware, Mining speculation		
Bitcoin Technical Support Questions regarding issues with Bitcoin Core, nodes, the Bitcoin network, transactions, and addresses. *Moderator:* *achow101*	101246 Posts 11772 Topics	**Last post** by suirrell in Re: How to uninstall bit... on **Today** at 07:33:26 PM
Project Development Organization of Bitcoin and related projects, bounty campaigns, advertising etc.	175775 Posts 15342 Topics	**Last post** by stompix in Re: We should build a se... on **Today** at 08:57:45 PM

Economy

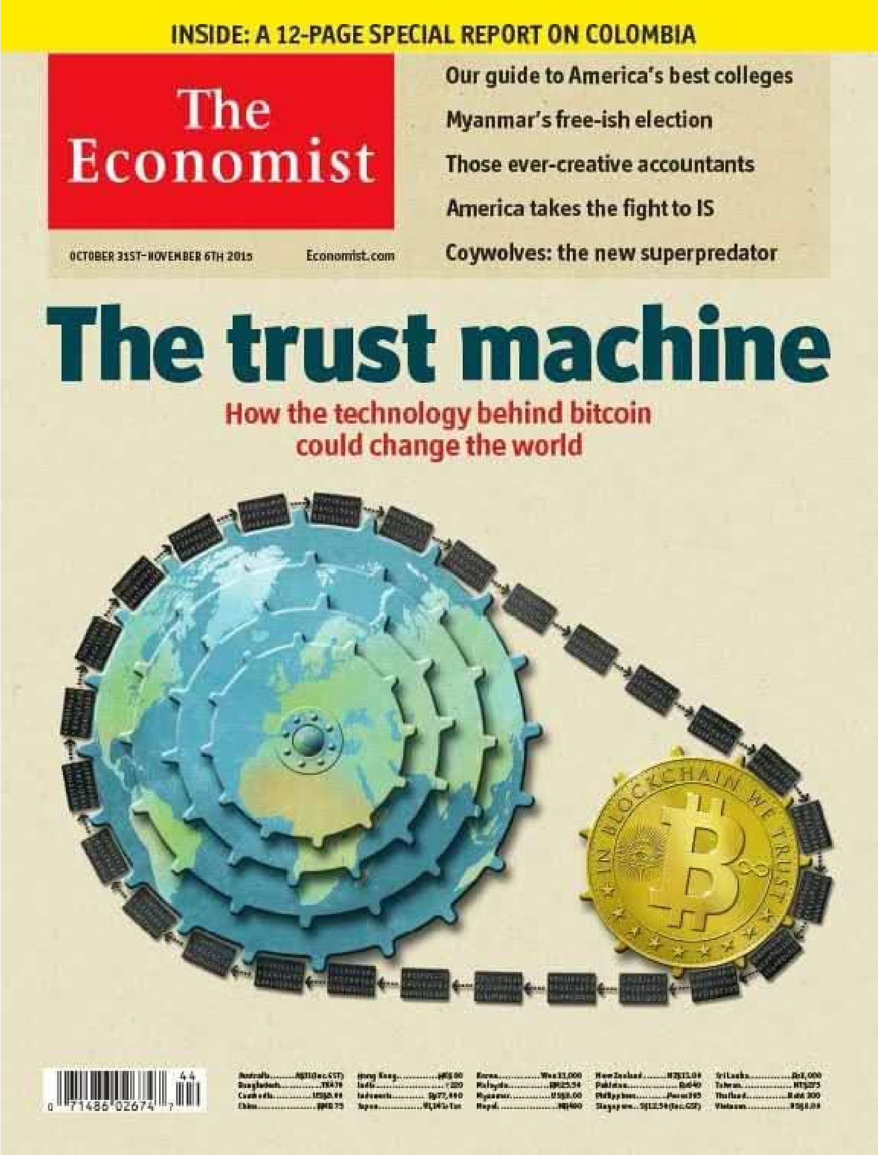
Economics	2493772 Posts 31891 Topics	**Last post** by Icygreen in Re: Wall Observer BTC/US... on **Today** at 09:21:10 PM
Child Boards: Speculation		
Marketplace General marketplace discussion. *Moderators:* *Cyrus*, *hilariousandco*	8356252 Posts 410469 Topics	**Last post** by carizmerlin31 in Re: Any software on **Today** at 09:27:06 PM
Child Boards: Goods, Services, Currency exchange, Gambling, Lending, Securities, Auctions, Service Announcements, Service Discussion		
Trading Discussion Discussion about doing business with Bitcoin. Best trading practices, delivery methods etc. *Moderator:* *Cyrus*	852036 Posts 34545 Topics	**Last post** by JeromeTash in Re: HitBTC scam! on **Today** at 09:26:00 PM
Child Boards: Scam Accusations, Reputation		

Bitcoin in one sentence

Confidence and consensus mathematical algorithm

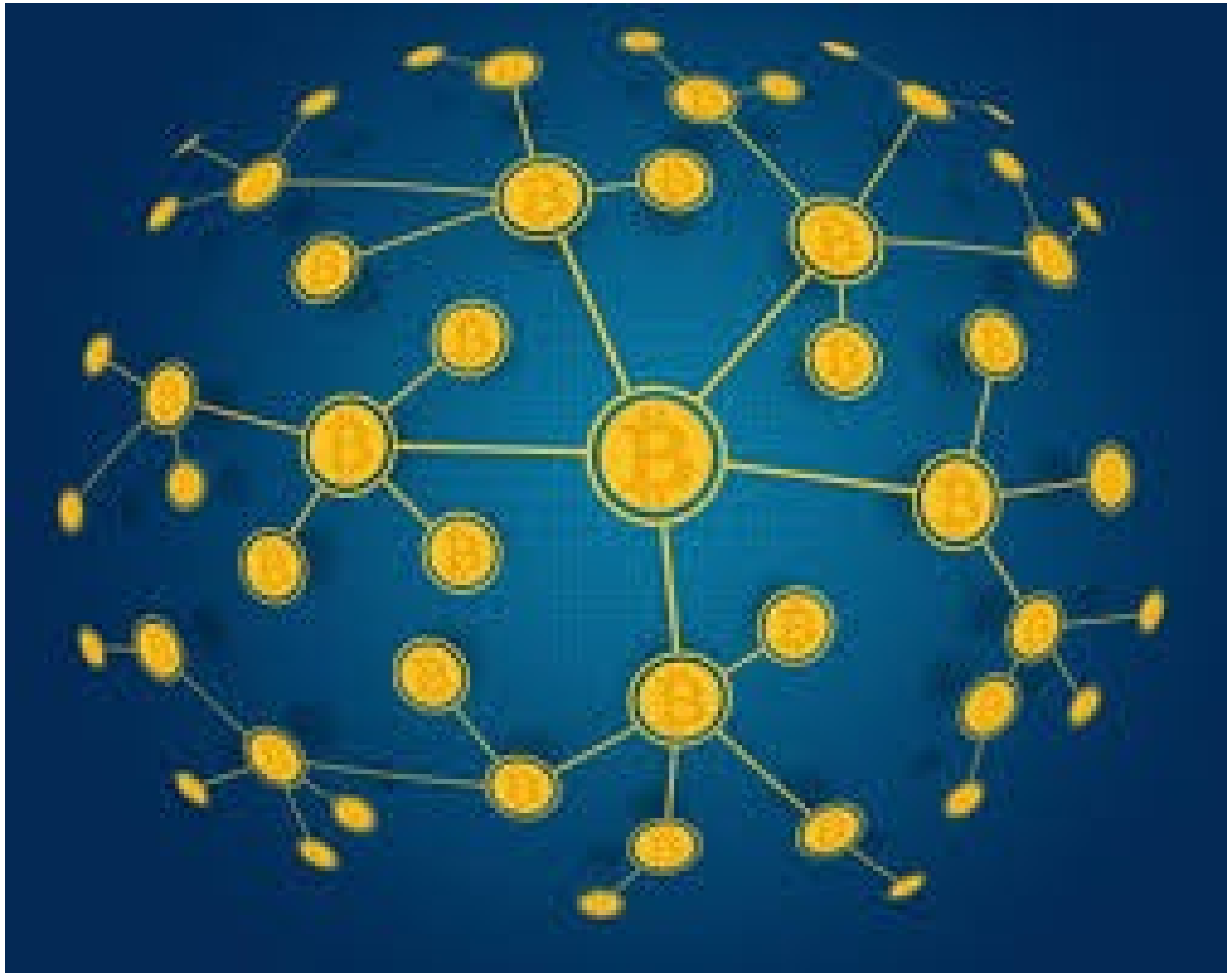
Network agrees on valid transactions

Mathematical alchemy: Digital gold


INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA
The Economist
OCTOBER 31ST–NOVEMBER 6TH 2015
Economist.com
Our guide to America's best colleges
Myanmar's free-ish election
Those ever-creative accountants
America takes the fight to IS
Coywolves: the new superpredator
The trust machine
How the technology behind bitcoin could change the world
IN BLOCKCHAIN WE TRUST

The Bitcoin network

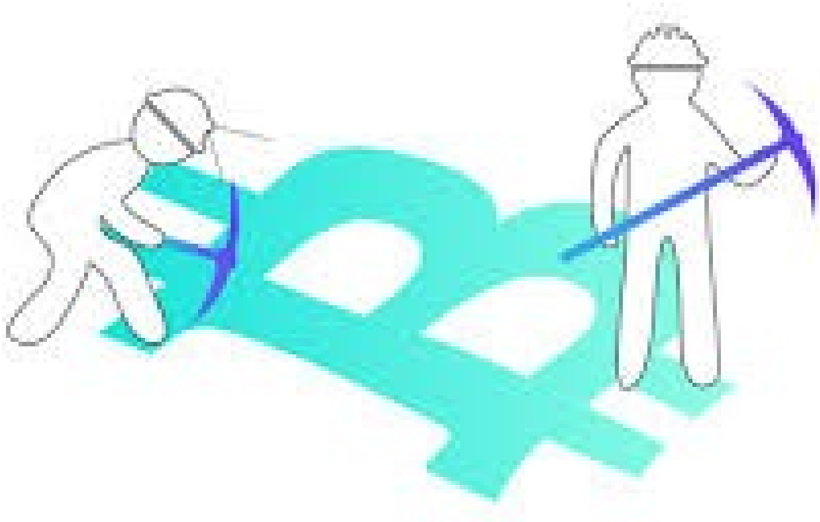
Each node of the network runs the Bitcoin code and communicates with other nodes.



Transaction propagation

Transactions propagate worldwide through the network

Mining and transaction validation



Transactions are validated with a computational task: “Proof of Work”

Reward with new minted Bitcoins

Bitcoin minting

- Initially 50 BTC/10 minute.
- “Halving” about each 4 years (production cut in half)
- Now 18.83 million of bitcoins. Total 21 million in 2140.
- Proof-of-Work prevents Sybil attack.
- Integrity of Bitcoin network based on energy.

Bitcoin blockchain or timechain

- A transaction block produced every 10 minutes.
- Set of blocks: the blockchain.
- Blockchain: Cryptographically untamperable ledger.
- Block count: First decentralized clock.
- Entropy of the network decreases: Needs input of energy (Second law of Thermodynamics).
- The blockchain has a high Bennett (logical) depth.

Crypto space

- Bitcoin code and algorithm is open.
- Can be modified to create other cryptocurrencies (altcoins).
- Not all of then are decentralized.
- Bitcoin transactions are programmable: “Smart contracts”.
- New cryptofinance ecosystem.

We learn from Bitcoin: Decentralized network

- Liberté: All nodes are free to follow the rules or not .
- Égalité: All nodes do have the same power.
- No fraternité: “Don’t trust, verify”.
- No police in the network. No way to enforce rules.
- Rules of the protocol aligned with individual interests.
- Freedom to join and leave the network.
- Rich network: Thousands of connected nodes.
- Unstoppable “Living” network. No one controls or can stop it.

Decentralize everything!

- Tempting idea: Decentralize other activities.
- Hard to build a good set of protocol rules.
- Other “smart blockchains”, more programmable than bitcoin, are replicating classical financial instruments.
- Example: Smart contracts that build a DEX (Decentralized Exchange). Trading without a broker.
- Payment channels and the Lightning Network (will replace VISA network).

Challenge for regulation

- Basic principles of decentralization are incompatible with current regulation.
- Anonimity is the rule in a decentralized system.
- Decentralization and KYC are incompatible.
- Cryptocurrencies are a new asset class.
- Currency or commodity regulations do not fit the system.
- Need for new regulation foundations.

Chalenge: Decentralized oracle protocol

- Need for a decentralized oracle protocol for linking the smart contracts to real world events.

- Example: DEXes provide oracle via arbitrage.

- Key for many other applications (insurance smart contracts,...).

Challenge: Decentralized trust protocol

- Major challenge: Build a decentralized protocol of reputation.
- Key for new more sophisticated decentralized protocols.
- Trust network → Oracle protocol
- Work for the next decades!

Thank you!