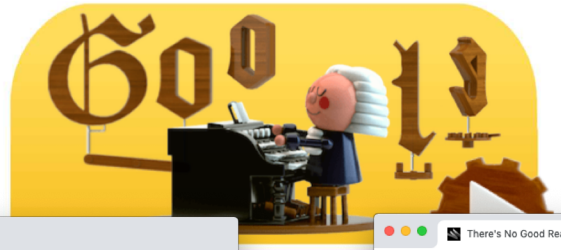
AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CAN A BLOCKCHAIN SOLVE THE TRUST PROBLEM?

NGI Talks

2019-03-26

Dr. Bernhard Haslhofer
Senior Scientist
Center for Digital Safety & Security



Blockchain: The New Technolo

Goldman Sachs & Co. LLC [US] | https://www.goldmansachs.com/insights/pages/blockchain/

Goldman Sachs

SECURITY

OUR FIRM WHAT WE DO INSIGHTS CITIZENSHIP CAREERS INVESTOR RELATIONS MEDIA RELATIONS WORLDWIDE LOGIN

Blockchain

—The New Technology of Trust

A new technology is redefining the way we transact. If that sounds incredibly far-reaching, that's because it is.

Blockchain has the potential to change the way we buy and sell, interact with government and verify the authenticity of everything from property titles to organic vegetables.

It combines the openness of the internet with the security of cryptography to give everyone a faster, safer way to verify key information and establish trust.

SCROLL DOWN TO EXPLORE BLOCKCHAIN

Auf gut

There's No Good Reason to Tr

https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/

WIRED There's No Good Reason to Trust Blockchain Technology SIGN IN | SUBSCRIBE

BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY TRANSPORTATION

GET WIRED AD-FREE BROWSING → SUBSCRIBE

SHARE

SHARE 4457

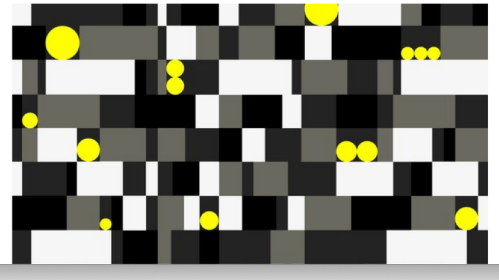
TWEET

COMMENT

EMAIL

BRUCE SCHNEIER OPINION 02.06.19 09:00 AM

THERE'S NO GOOD REASON TO TRUST BLOCKCHAIN TECHNOLOGY



GET WIRED AD-FREE BROWSING + UNLIMITED ACCESS

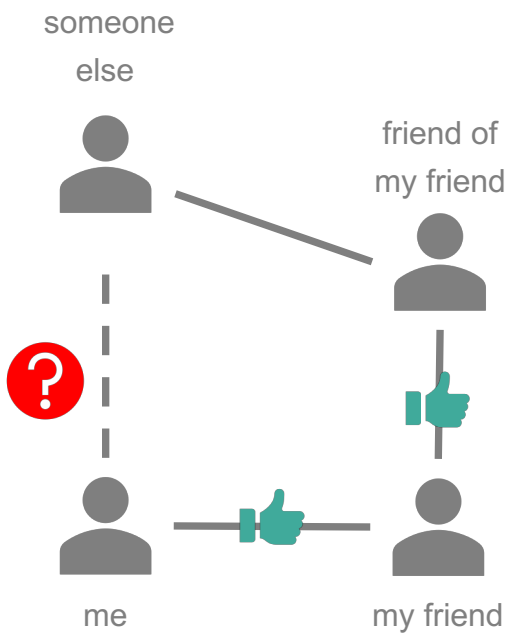
→ SUBSCRIBE

MOST POPULAR

SCIENCE
A More Humane Livestock Industry, Brought to You by Crispr
GREGORY BARBER

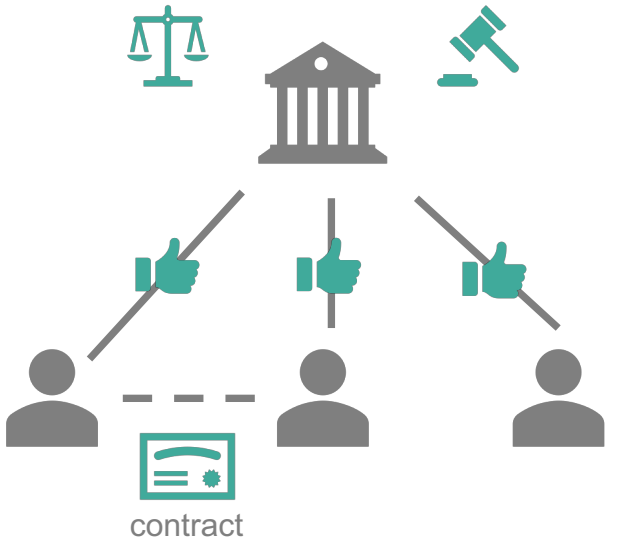
BUSINESS
Inside Airbnb's 'Guerrilla War' Against Local Governments
PARIS MARTINEAU

CAN A BLOCKCHAIN SOLVE THE TRUST PROBLEM?



Direct trust does not scale in larger groups

Institutions have rules and laws and can act as trusted third parties



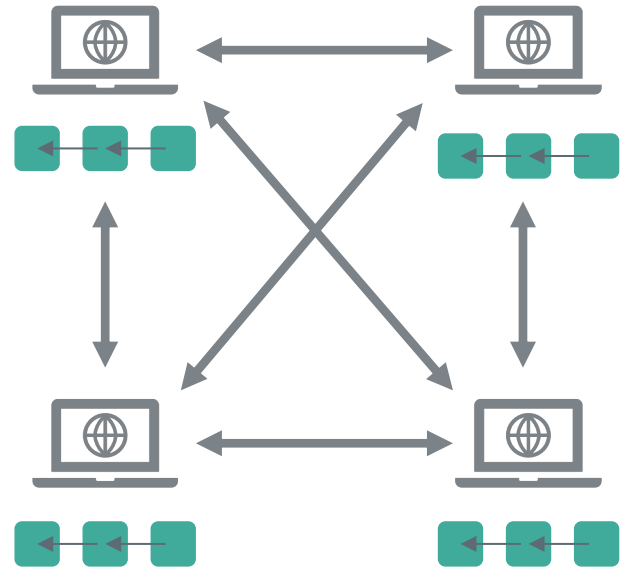
Trust is relationship between individuals and key in functioning society

Contracts regulate relationships between parties that do not necessarily trust each other

Whenever a conflicts arises the trusted third party acts as arbiter

CAN A BLOCKCHAIN SOLVE THE TRUST PROBLEM?

- A type of ***Distributed Ledger***
- Data are stored in structures known as **blocks**
- Each block holds a reference to the previous block and thereby forms a chain of blocks
- Blockchain is synchronized via a P2P network



AUSTRIAN INSTITUTE OF TECHNOLOGY

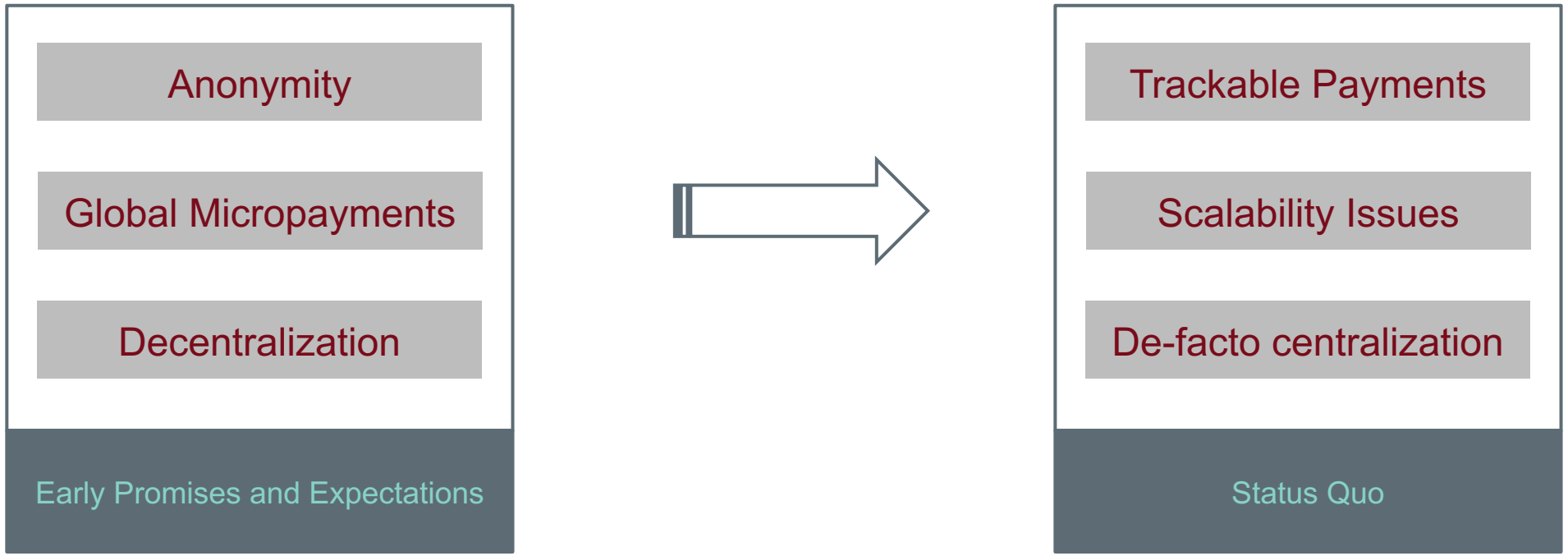
TRUST IN PUBLIC BLOCKCHAINS

12. Conclusion

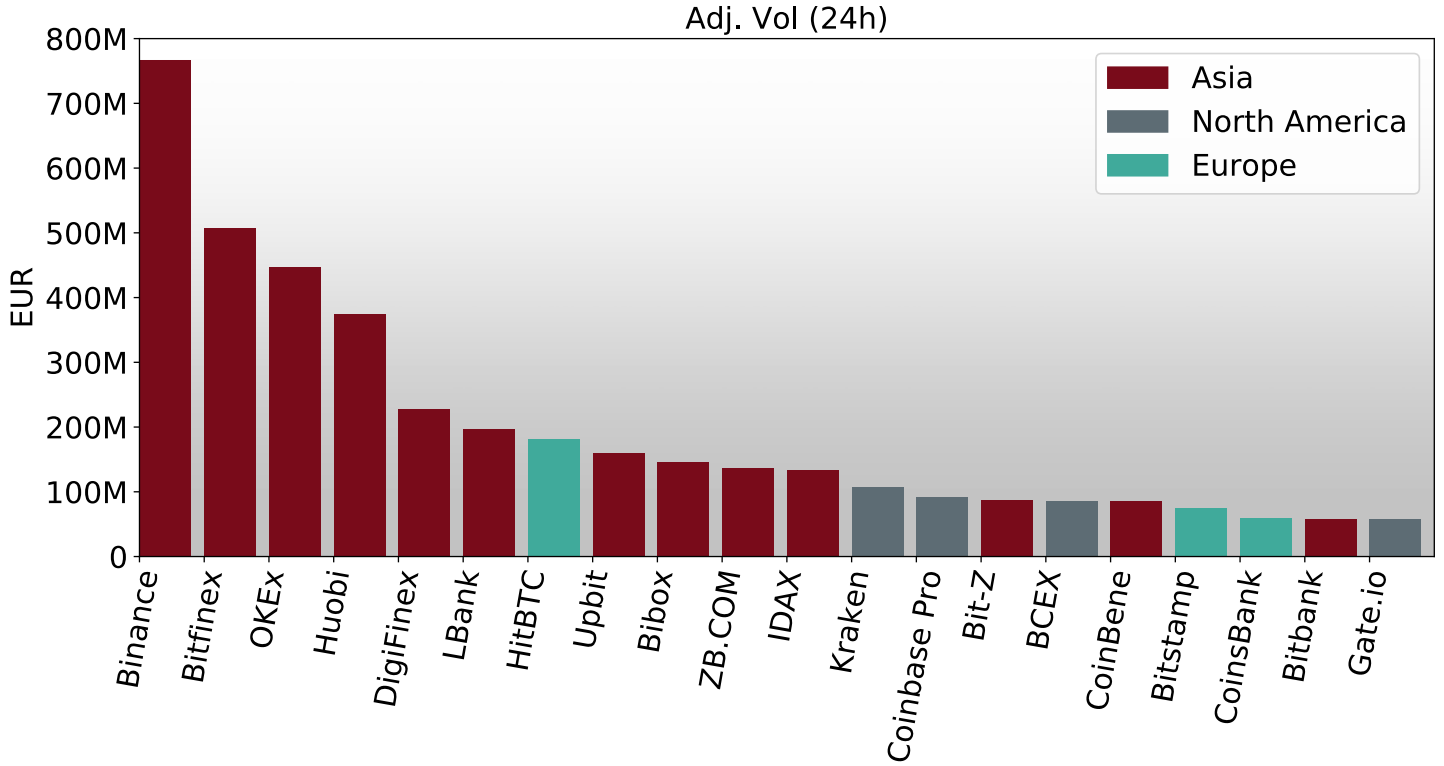
We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes

[Nakamoto 2008]

BITCOIN | OBSERVATIONS

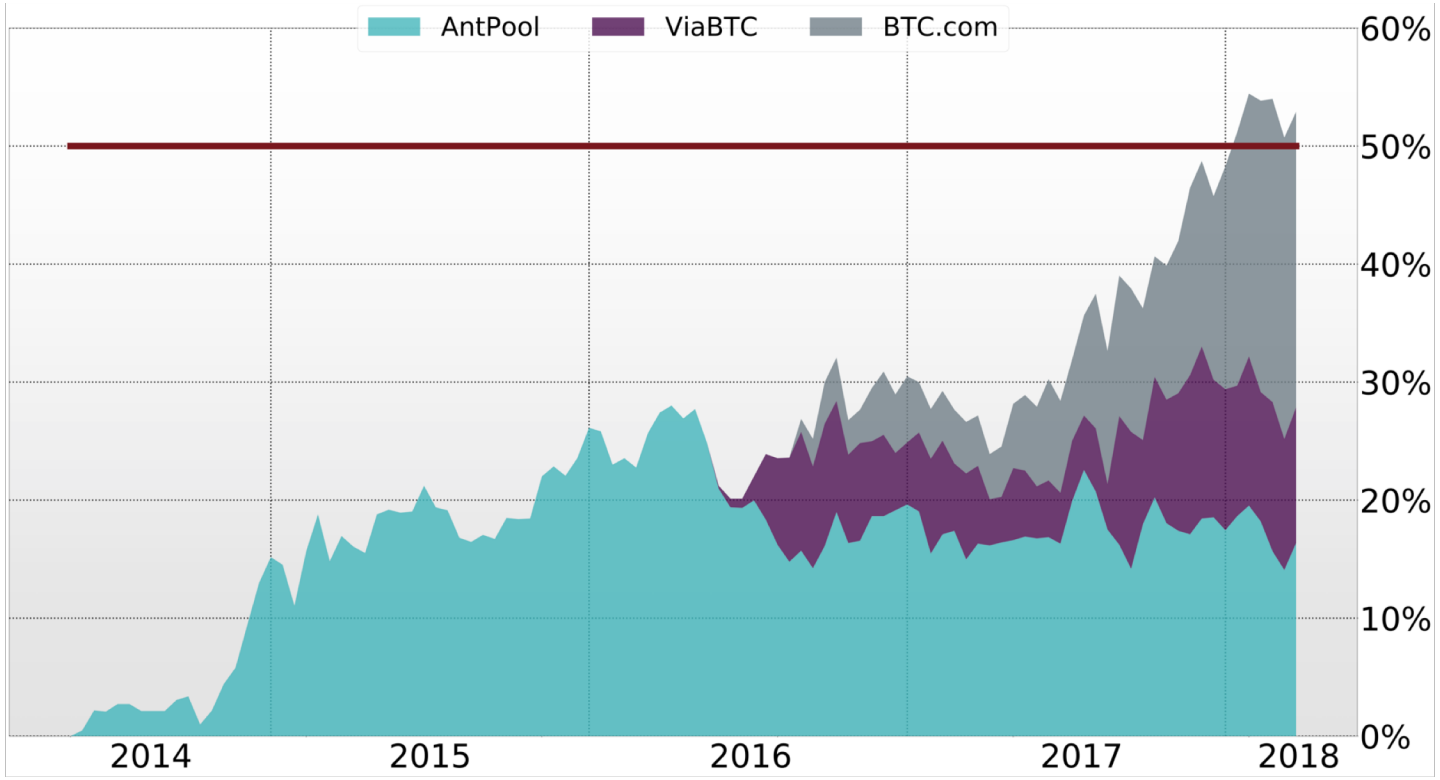


BITCOIN | EXCHANGE CENTRALIZATION



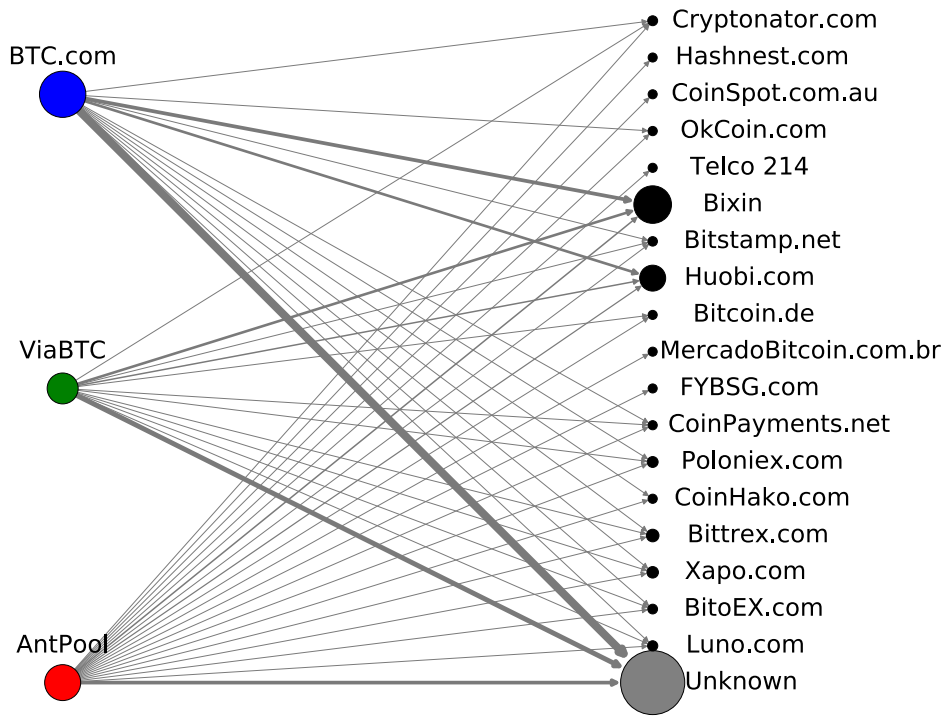
Source: coinmarketcap.com (2018-10-15)

BITCOIN | MINER CENTRALIZATION



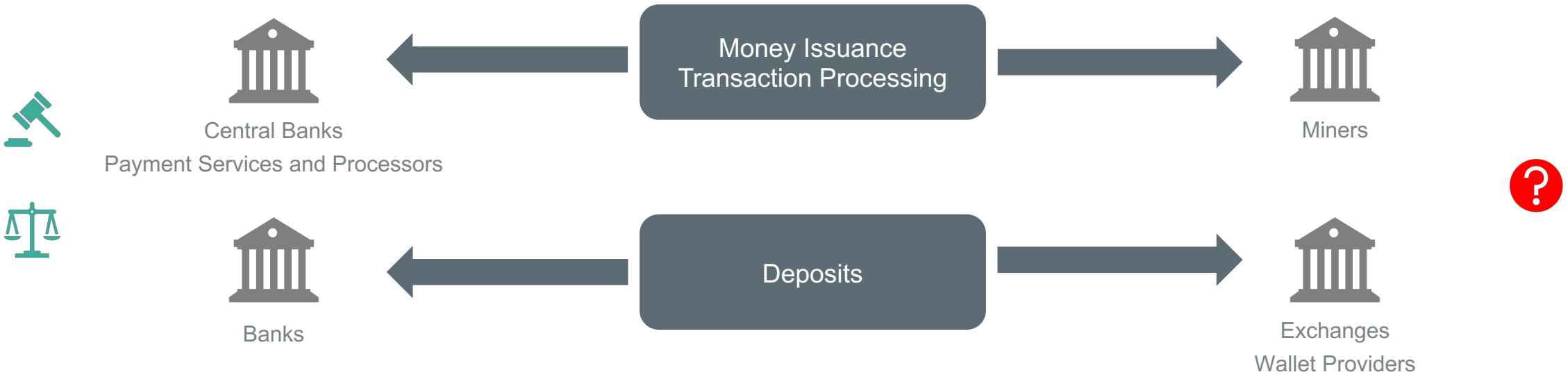
Adapted from: Romiti, M. et al.: A Deep Dive into Bitcoin Mining Pools – An Empirical Analysis of Mining Shares (2019). Forthcoming.

BITCOIN | MINER & EXCHANGE CENTRALIZATION



Source: Romiti, M. et al.: A Deep Dive into Bitcoin Mining Pools – An Empirical Analysis of Mining Shares (2019). Forthcoming.

BITCOIN | A SYSTEM WITHOUT TRUST ?



Fiat currency ecosystem

Cryptocurrency ecosystem

SHIFT OF TRUST

BITCOIN | A SYSTEM WITHOUT TRUST ?

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes

"*We have proposed a system that can agree on a global state of a shared transaction ledger without central nodes*"

AUSTRIAN INSTITUTE OF TECHNOLOGY

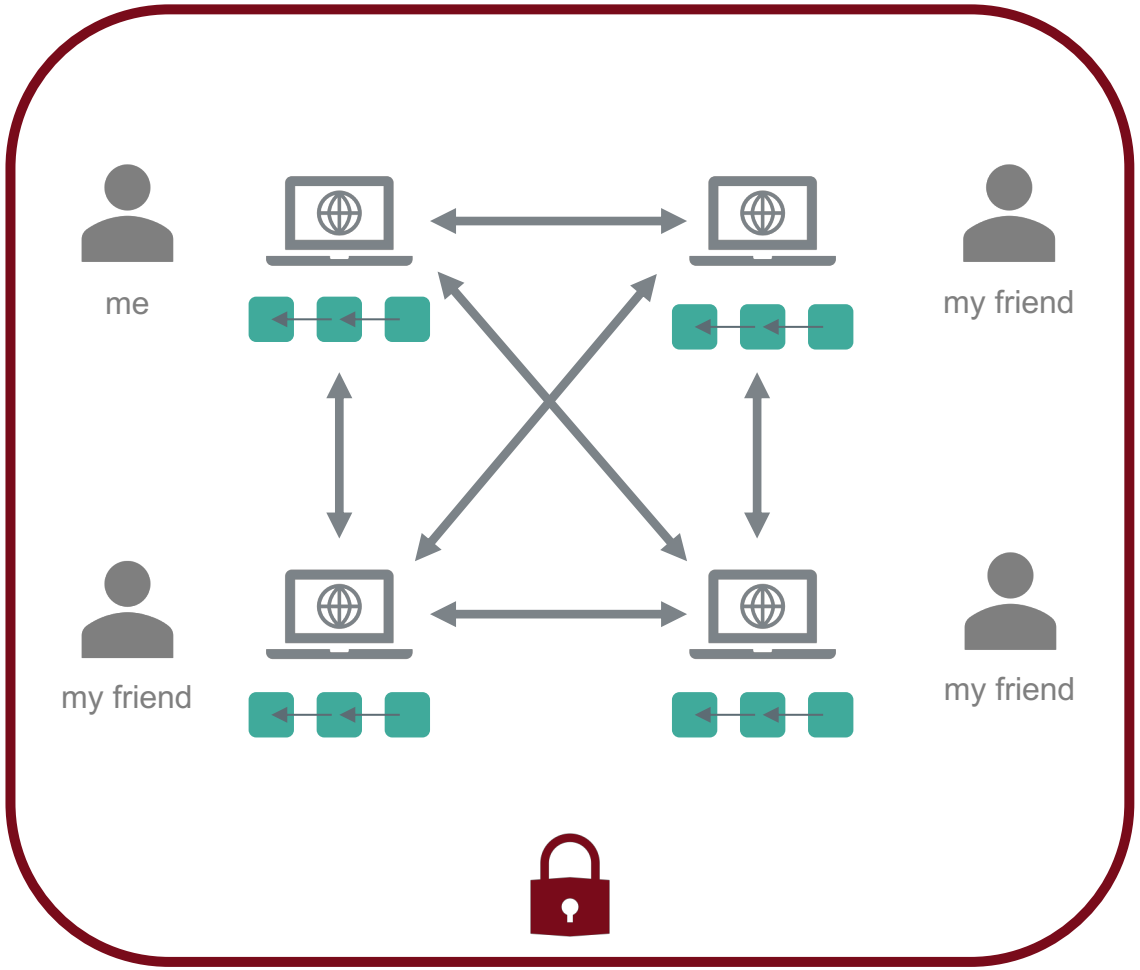
TRUST IN PRIVATE BLOCKCHAINS

PRIVATE BLOCKCHAIN | MOTIVATION

Public blockchains don't work for my use case. I want to know who else participates in the network.

(because I do not trust the others)

me



OK, let's use a private, permissioned blockchain that includes only our friends!

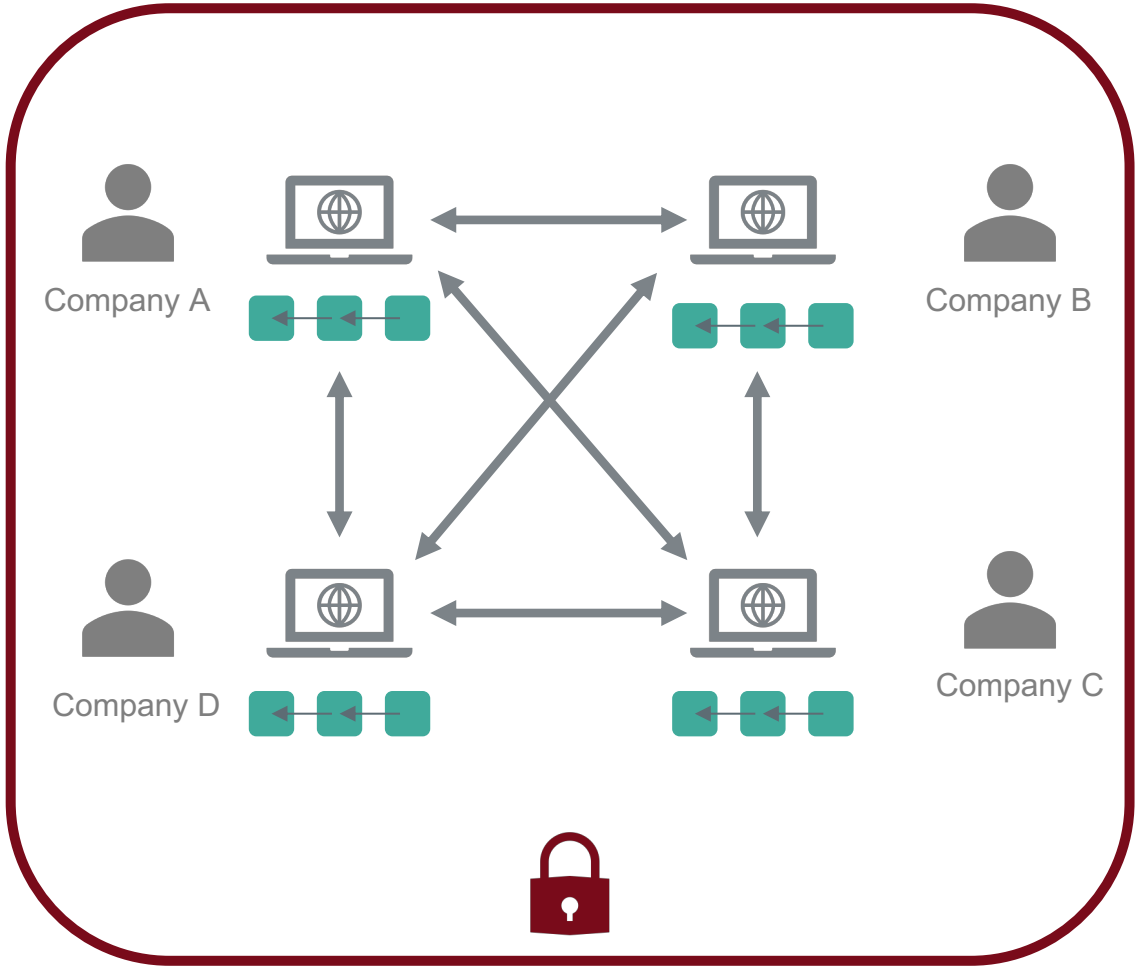
my friend

PRIVATE BLOCKCHAIN | KEY QUESTIONS

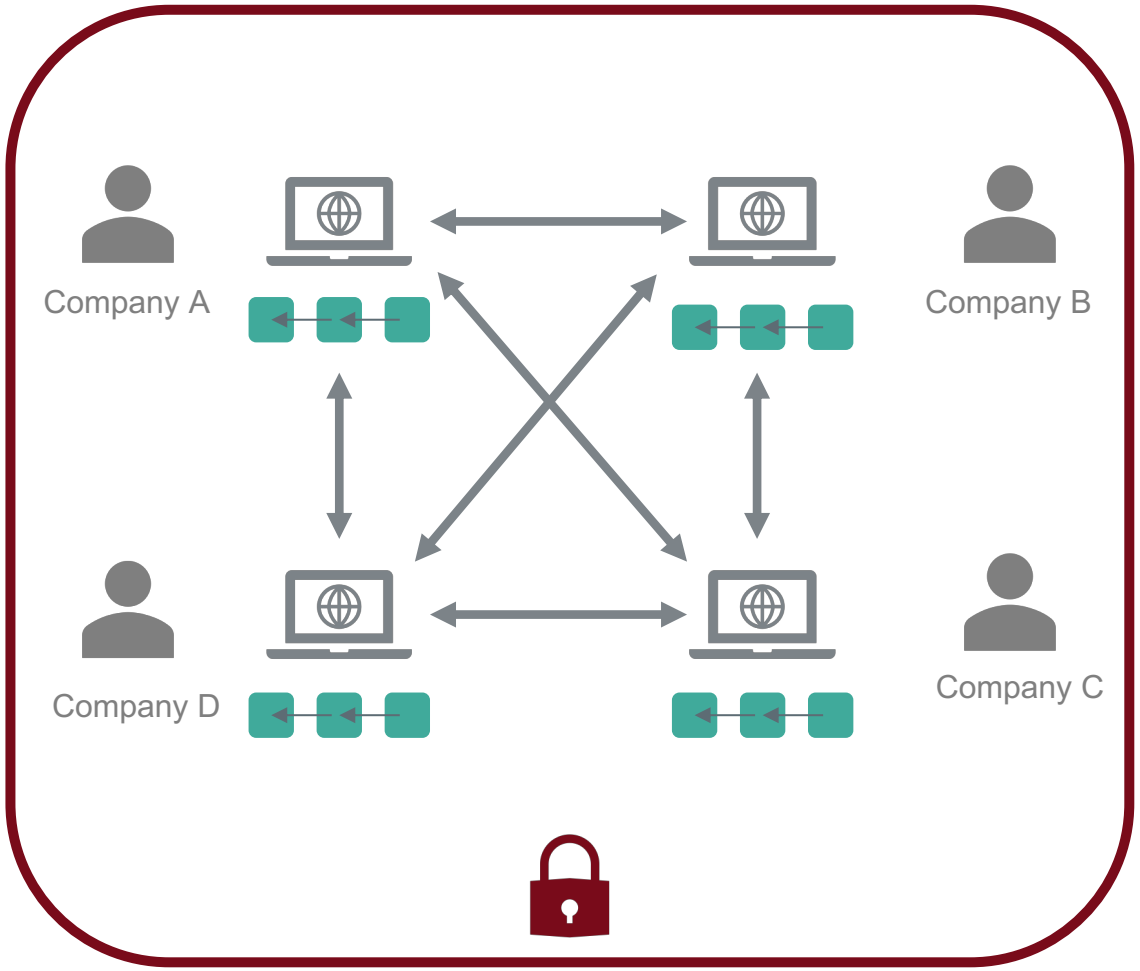
Who is trustworthy enough to build and run our private blockchain?

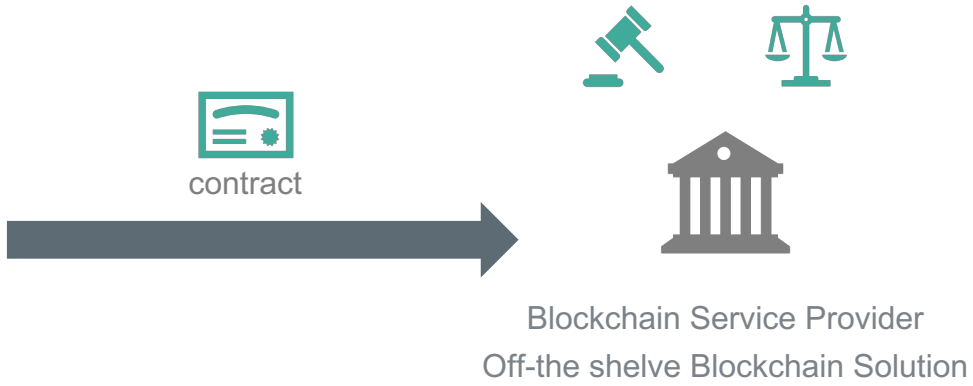
Do we really trust each other?

How can we scale trust to a larger group?



PRIVATE BLOCKCHAIN | POSSIBLE SOLUTION





Trust relationship with a (new) third party

TRUST IN SMART CONTRACTS

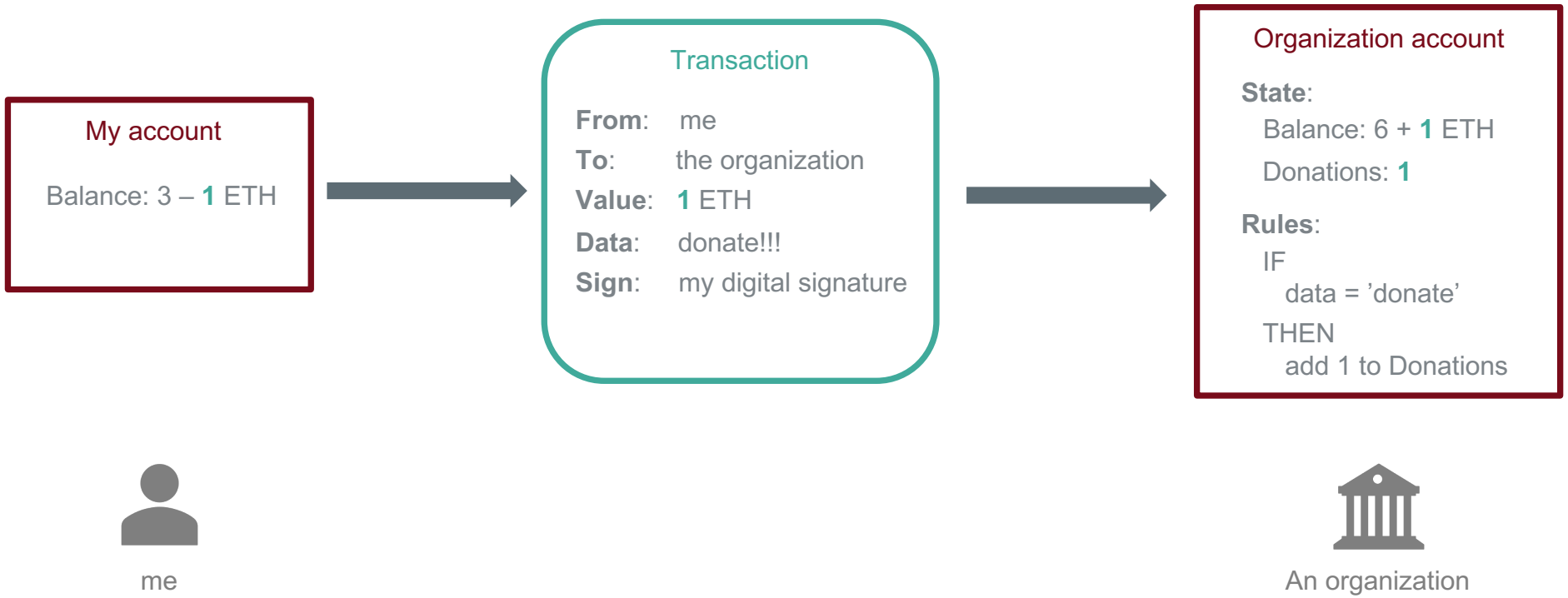
Smart Contracts eliminate the need for trust

They are trustless

Nobody has to trust a central party

Blockchain Evangelist

SMART CONTRACT | WHAT IS IT?

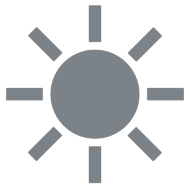


A computer program that encodes agreement between parties

Adapted from: Fröwis: Tracking Payment Flows in Ethereum, Symposium on Post-Bitcoin Cryptocurrencies, 2018

SMART CONTRACTS | TRUST ISSUES

Oracle



Gambling account

State:
Balance: 6 ETH

Rules:
IF
outcome = 'heads up'
THEN
add send 1 ETH to me

This is still just a program!

An organization

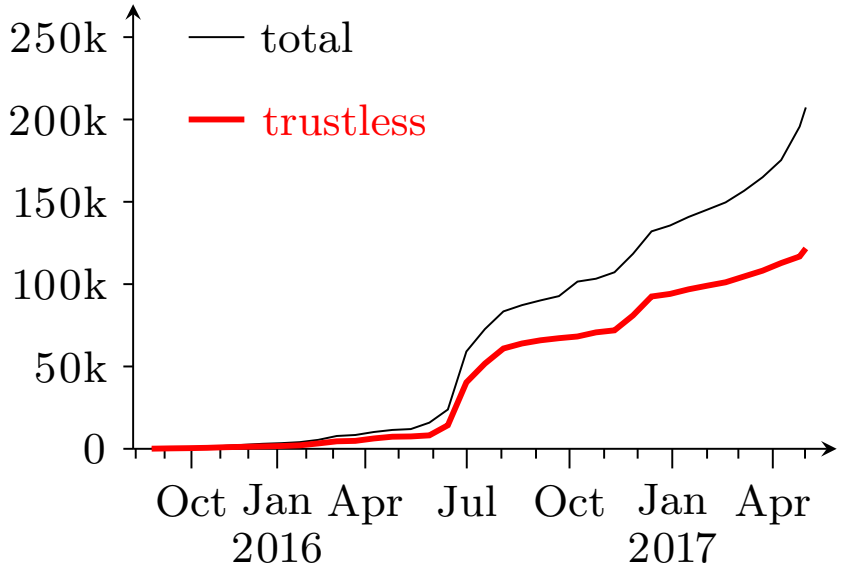
How can a program know the outcome of coin toss?

SHIFT OF TRUST

SMART CONTRACTS | MEASURING TRUST

"*Two out of five smart contracts deployed on Ethereum do require trust in at least one third party, who, in principle, can alter the control flow of the program that enforces an agreement after it is committed to the blockchain*"

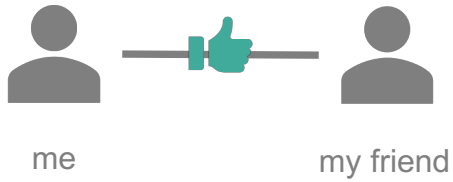
"*In simple terms, there remains a gap between vision and practice.*"



Source: Fröwis and Böhme (2017): In Code We Trust? Measuring the Control Flow Immutability of All Smart Contracts Deployed on Ethereum

CAN A BLOCKCHAIN SOLVE THE TRUST PROBLEM?

- A blockchain is a technology (system, algorithms, protocols)
- Trust is more…it is about social relationships
- Technology alone can hardly solve the trust problem
- A false trust in blockchains can be a security risk
  (e.g., exchange hacks, sabotage)



AUSTRIAN INSTITUTE OF TECHNOLOGY

HOW CAN THE TRUST PROBLEM BE SOLVED?

- There is no off-the-shelve technology that can solve the trust problem
- Trust relationships are established among people and within society
- Trusted third parties are somehow natural and not necessarily a bad thing!
- Cryptographic techniques can help us to enforce confidentiality, authenticity, and integrity of those trust relationships (in decentralized settings)

HOW CAN THE TRUST PROBLEM BE SOLVED?

- Thanks to Blockchains a number of well-known techniques have become mainstream
  - Hashing beyond MD5
  - Asymmetric encryption (public and private keys)
  - Ring signatures
  - Elliptic curve cryptography
  - …
- Those techniques won't solve the trust problem … but they can help us securing trust relationships

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

bernhard.haslhofer@ait.ac.at

https://graphsense.info