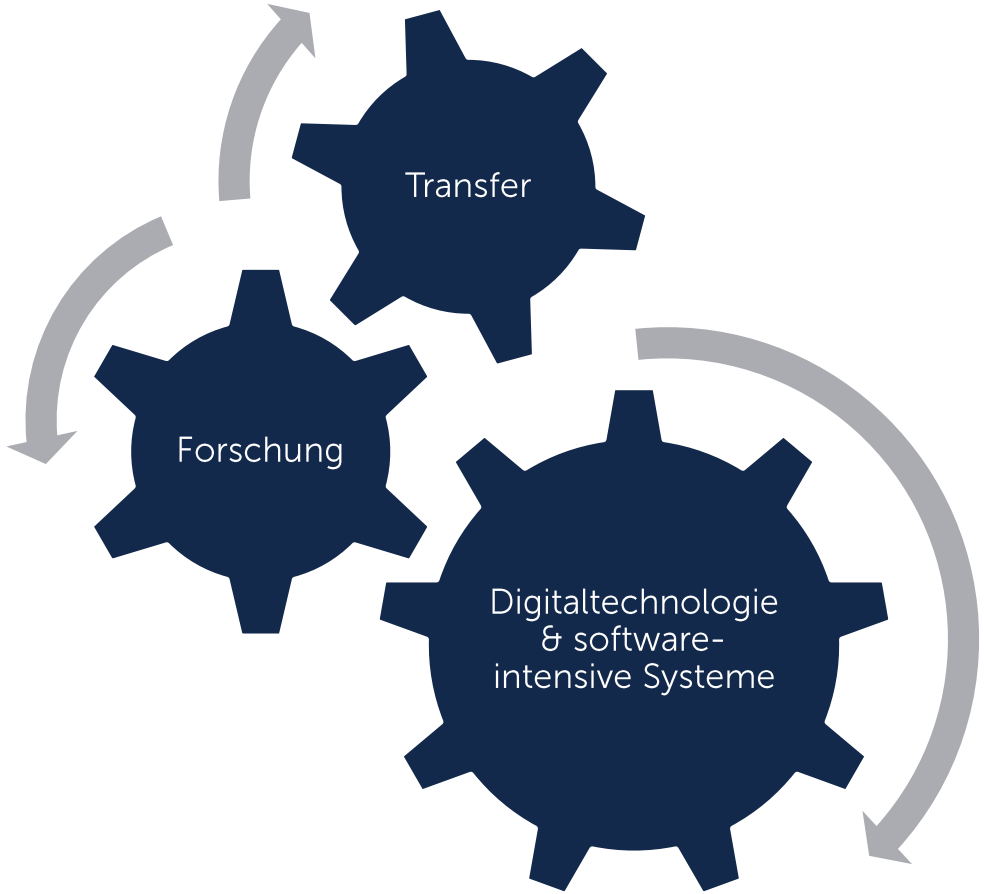
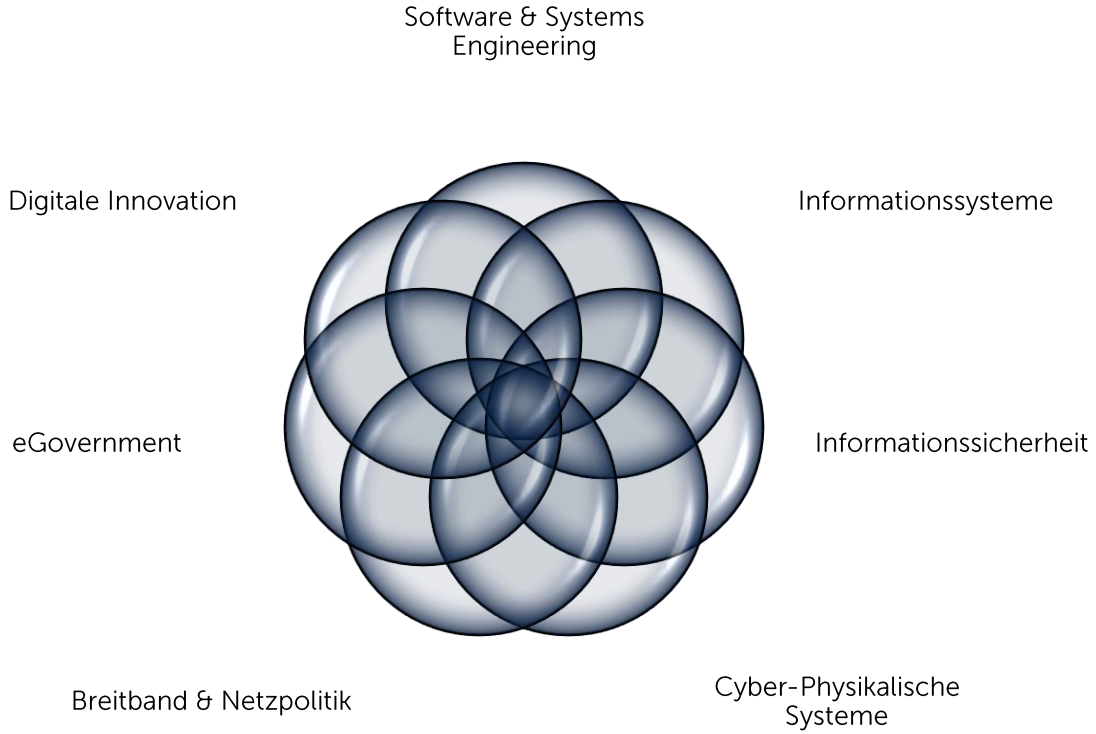
fortiss Gmbh

Bayerisches Landesinstitut und An-Institut der TU München





fortiss GmbH – An-Institut der TU München

Kompetenzfeld Open Data & Information Management

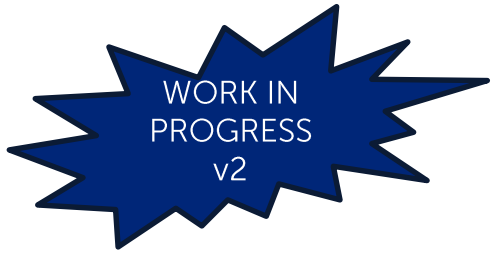
Dr. Marcus M. Dapp
Leiter Kompetenzfeld OD&IM
Co-Dir ipima

dapp@fortiss.org
@digisus | 089 36035 22 19

Prof. Dr. Helmut Krcmar
Lehrstuhl für Wirtschaftsinformatik
TU München

Wissenschaftlicher Geschäftsführer
fortiss

Who let the blocks out?



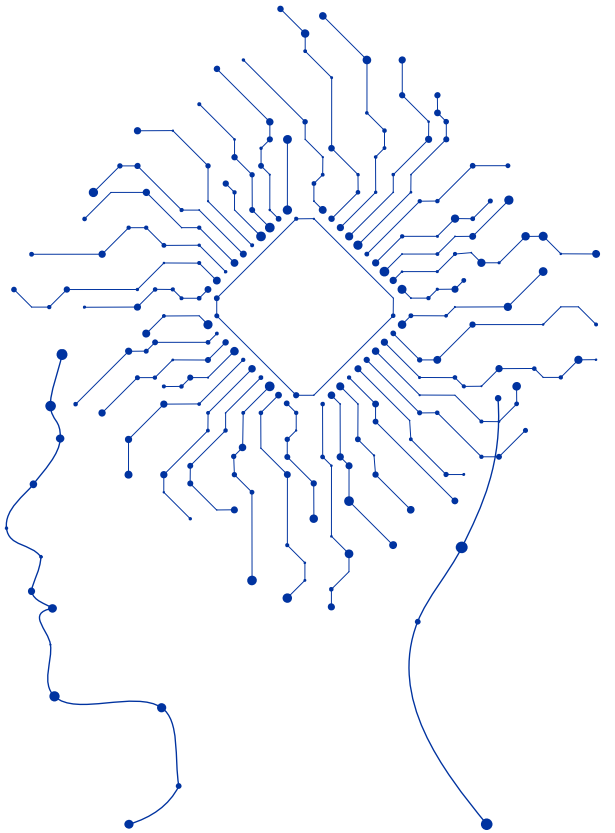
Making sense of blockchain technology

Dr. Marcus M. Dapp

Head “Open Data & Information Management”

Co-Dir “Institute for Public Information management”

fortiss GmbH
An-Institut Technische Universität München



“They gave us a fully decentralized Internet and we used it to build web services–Facebook, Twitter, Gmail, iCloud–so massively centralized they verge on being quasi-medieval fiefdoms.

Now we’re building the Internet of Someone Else’s Things, wherein every room of every home will contain devices controlled by servers the homeowners don’t know, control, or understand.

What is wrong with us?”

http://techcrunch.com/2015/01/10/decentralize-all-the-things/

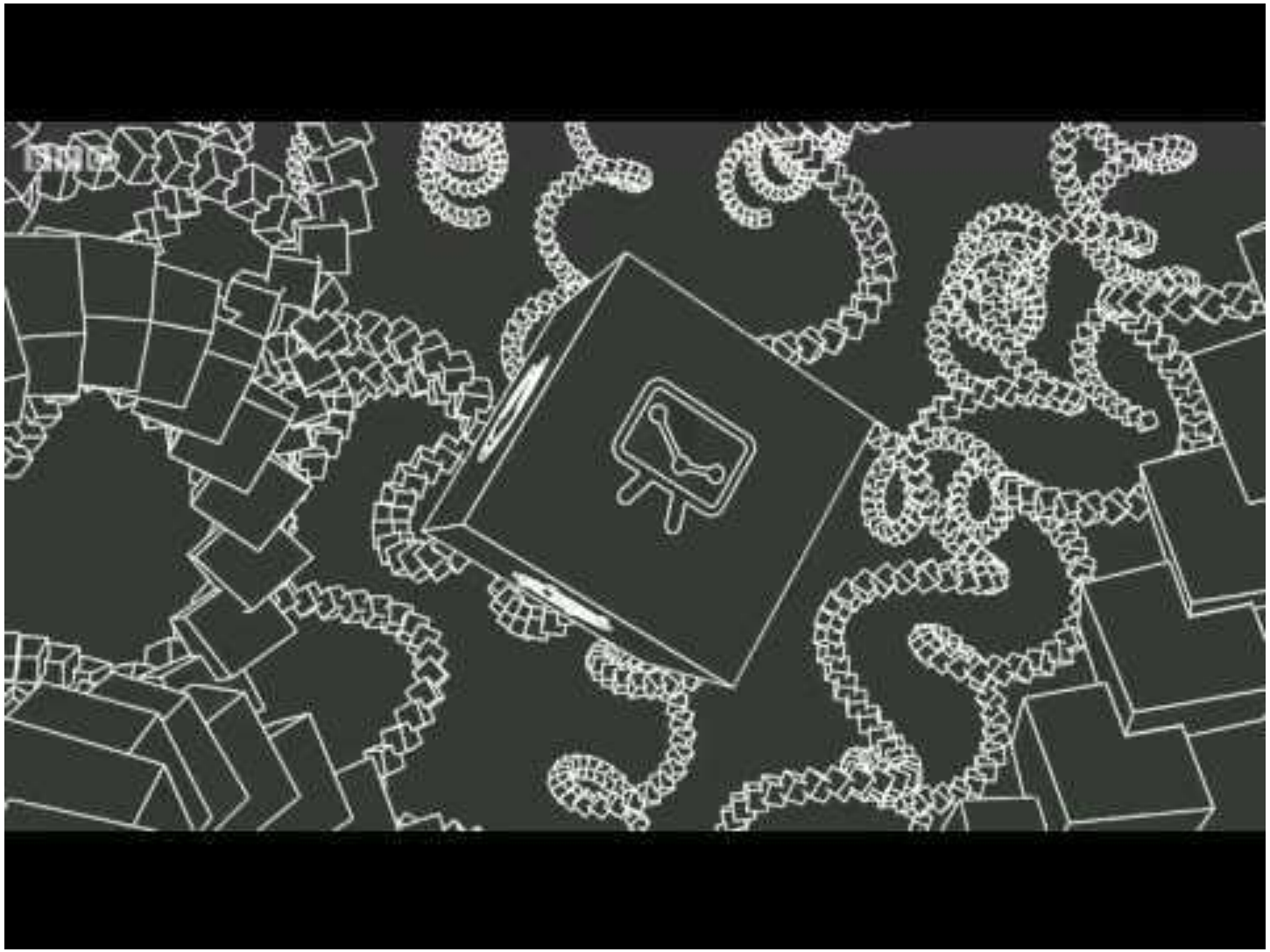
Can we do without „trusted third parties“ ?

IF we want to is a different question ;-)

- Since the beginning of time, third parties facilitate contracts/transactions between humans.
  - Church, State, Companies, etc.
- Usually, we need
  - Banks to transfer money for us
  - Notaries to help us enter into agreements with others
  - Lawyers to enforce contracts for us
  - Facebook to help us exchange cat pictures
  - Large utility companies to distribute energy for us
  - Insurance companies to manage risk for us
  - Etc.

Whom do you (*need to*) trust?

How the BBC explains what blockchain is



Wof blockchain development

Our current thinking of what is happening

Bitcoin

- Currency

Blockchain

- Building block

Ecosystem?

- Many chains

1st wave: Bitcoin

Bitcoin 101-1

Separating the myth from the math

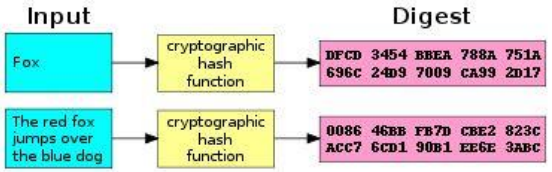
MYTH

- 2009 Satoshi Nakamoto publishes “Bitcoin: A Peer-to-Peer Electronic Cash System”
- Nobody knows who the person is (till today)
- Satoshi publishes core software and creates genesis block to start the chain …

MATH

- Clever Combination of several research breakthroughs
  - Hashing
  - E-cash
  - ..?

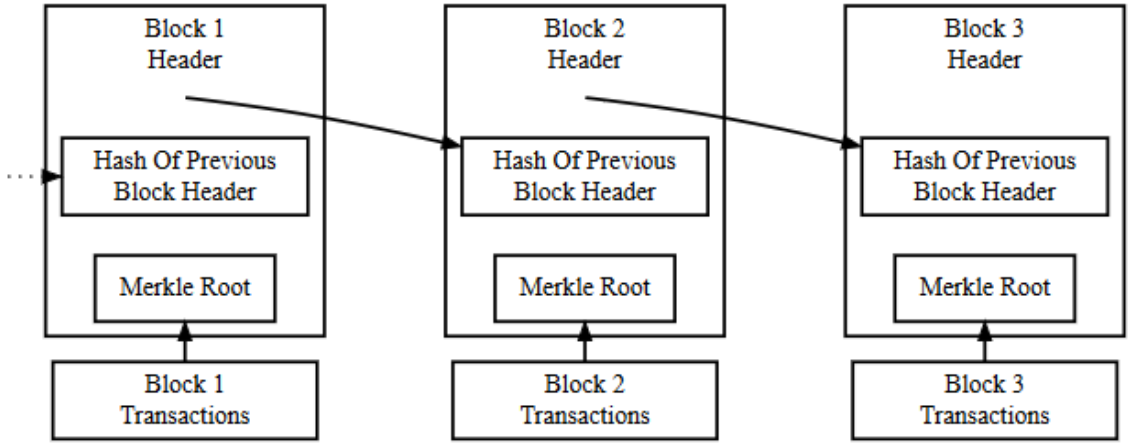
- <Img: E-cash>



Bitcoin 101-2

transactions → blocks → chain → consensus

- **Transactions** form a block
  - New transactions collected and hashed pairwise.
  - Merkle root of a Merkle tree generated and stored.
- **Blocks** form a chain
  - Each block stores hash of previous block's header, chaining the blocks together. *Ensures a transaction cannot be modified without modifying the block that records it and all following blocks.*
  - Transactions are also chained together.
- **Blockchain** is an ordered, timestamped record of transactions.



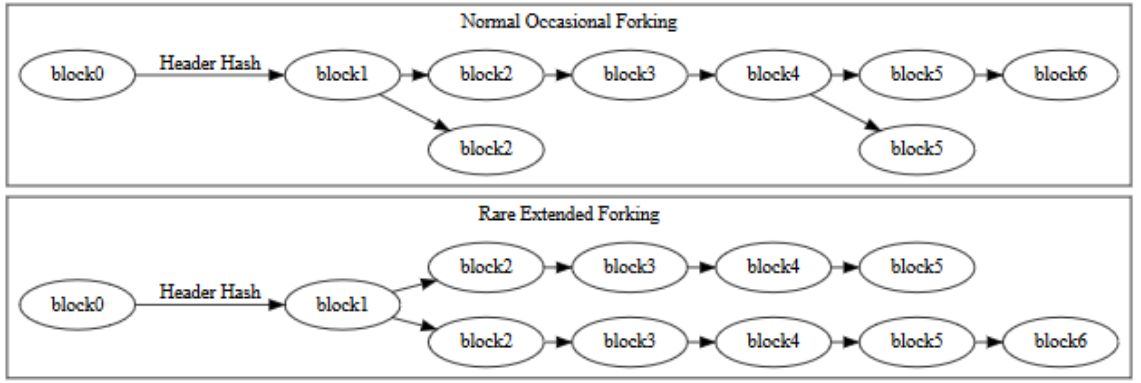
Simplified Bitcoin Block Chain

S: Bitcoin.org/en/developer-guide
S: Bitcoin.org/developer-guide

Bitcoin 101-3

Mining, consensus & proof of work

- **Chain** is collaboratively maintained by anonymous peers on the network. **Mining** adds new blocks to the chain, making transaction history hard to modify.
- **Proof of work**. Difficulty level requires each block to prove a significant amount of work was invested in its creation. This ensures that *untrustworthy peers who want to modify blocks have to work harder* than honest peers who only want to *add* blocks. Cost to modify a particular block increases with every new block added to the block chain, magnifying the effect of the p-o-w.
- Nodes in **consensus** have the same blocks.

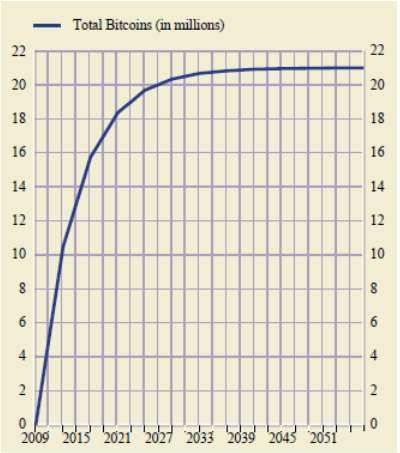


The longest chain wins in the end.

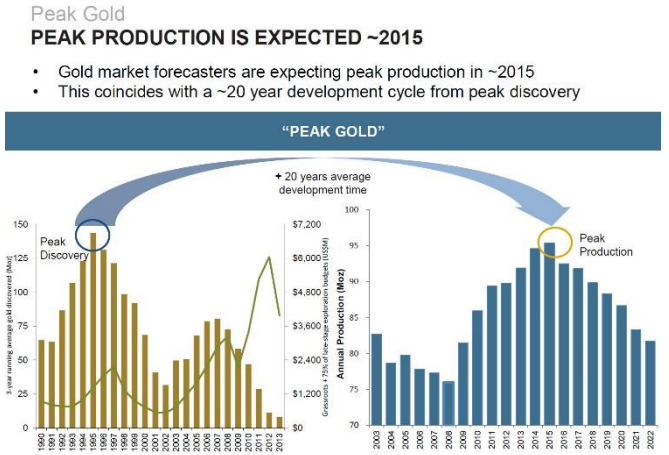
Bitcoin 101-4

Mining reward, growth, deflationary currency

- (Winning) Miners get a reward for investing in proof of work. Difficulty is self-adjusting and increasing.
- BTC as currency in deflationary because amount of bitcoins is capped at 21'000'000.*00000000* BTC
  - Fun fact: Smallest amount is 1 Satoshi (10E-8 BTC)
- Growth curve is flattening over time as rewards are regularly halved. Saturation is modeled after precious metal discovery (e.g. gold).
- Performance
  - Computing power measured (hashrate)
  - 7 transactions per second, block size debate



Source: European Central Bank: Virtual Currency Schemes, 2012



S: Bitcoin.org/developer-guide

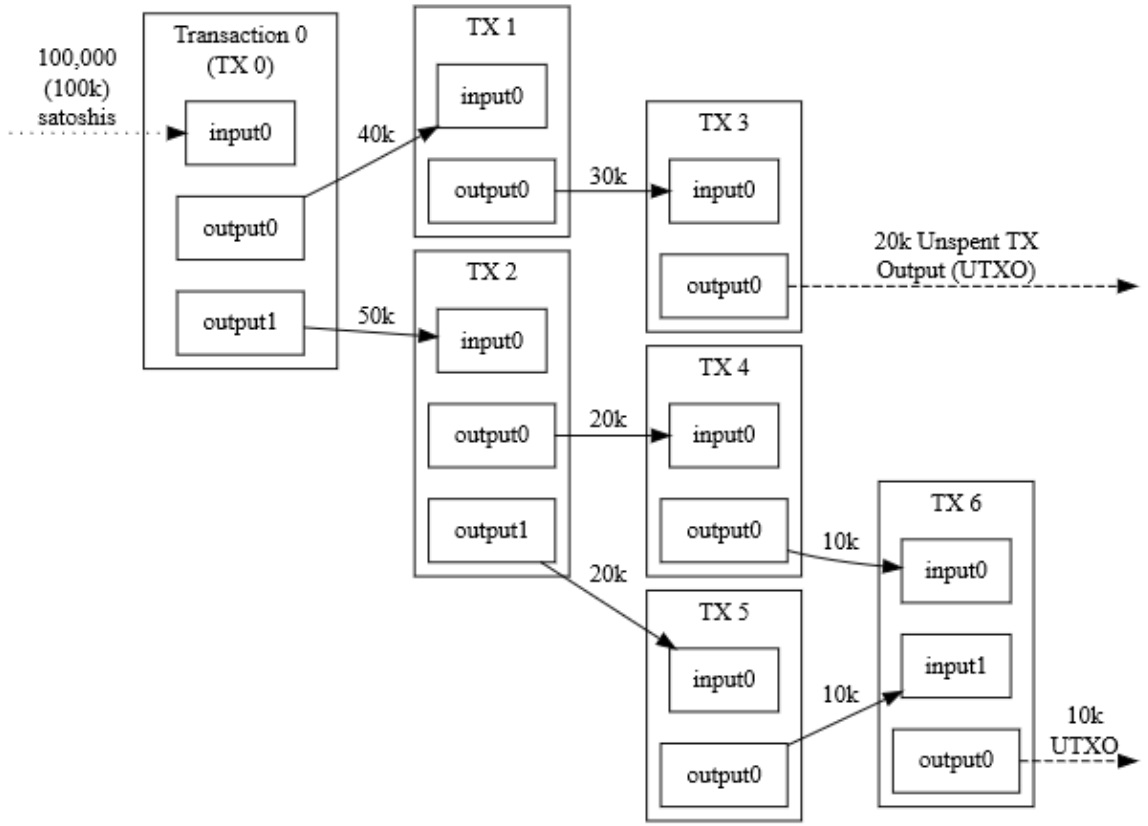
fortiss

Bitcoin 101-5

The „hard core techie/developer slide“

- *Bitcoins are not sent from and to wallets*, but really move from transaction to transaction. The output of a transaction becomes the input of a next transaction.
- Transaction diagram -> my paper notes
- Bitcoins at your disposal = unspent outputs

- Multi-signature transactions
- Side-chains
- Block size debate



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Source: Bitcoin.org/en/developer-guide

Bitcoin – Putting the mosaic together

A unique system to transfer value digitally

- Peer-to-peer
- Public
- Pseudonymous
- Trustless
- Immutable
- Permanent
- Global

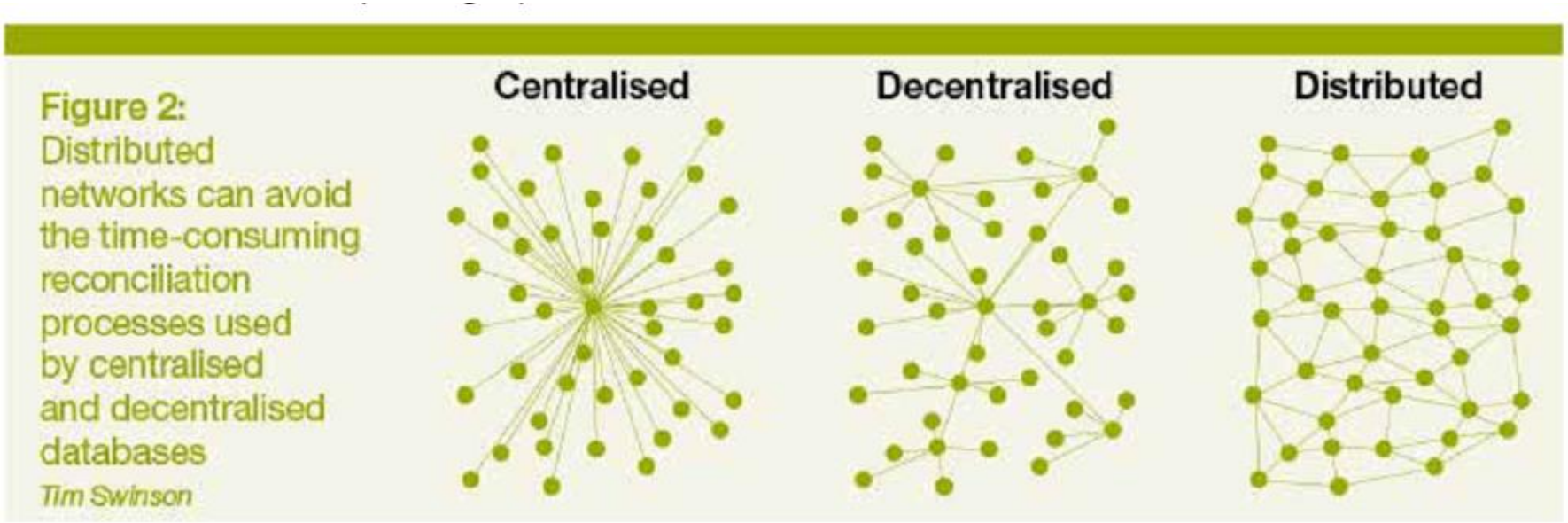


Figure 2: Distributed networks can avoid the time-consuming reconciliation processes used by centralised and decentralised databases

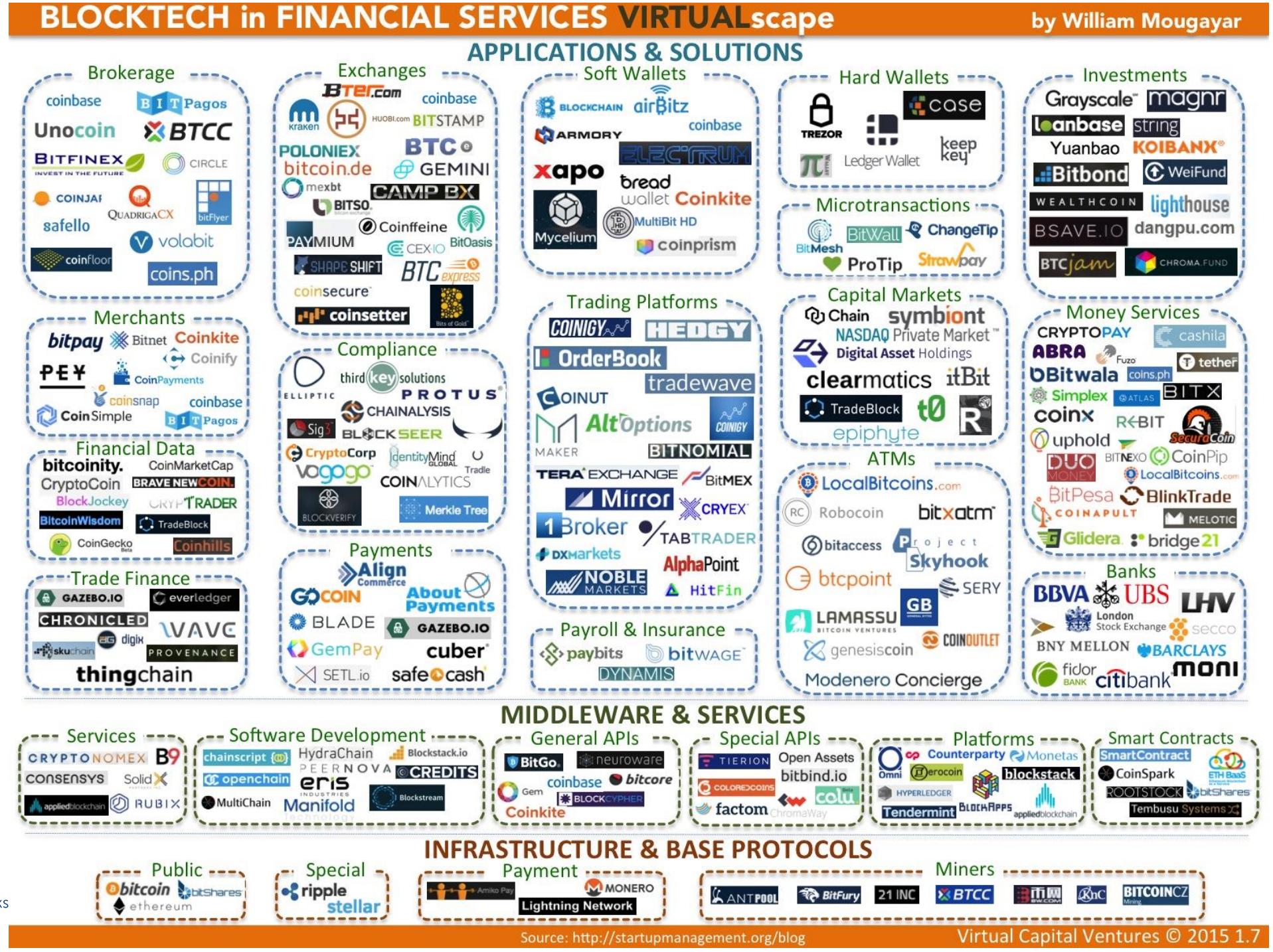
Tim Swinson

Bitcoin Development

e.g. BTC ~ EUR

Bitcoin Dev.

Financial Ecosystem



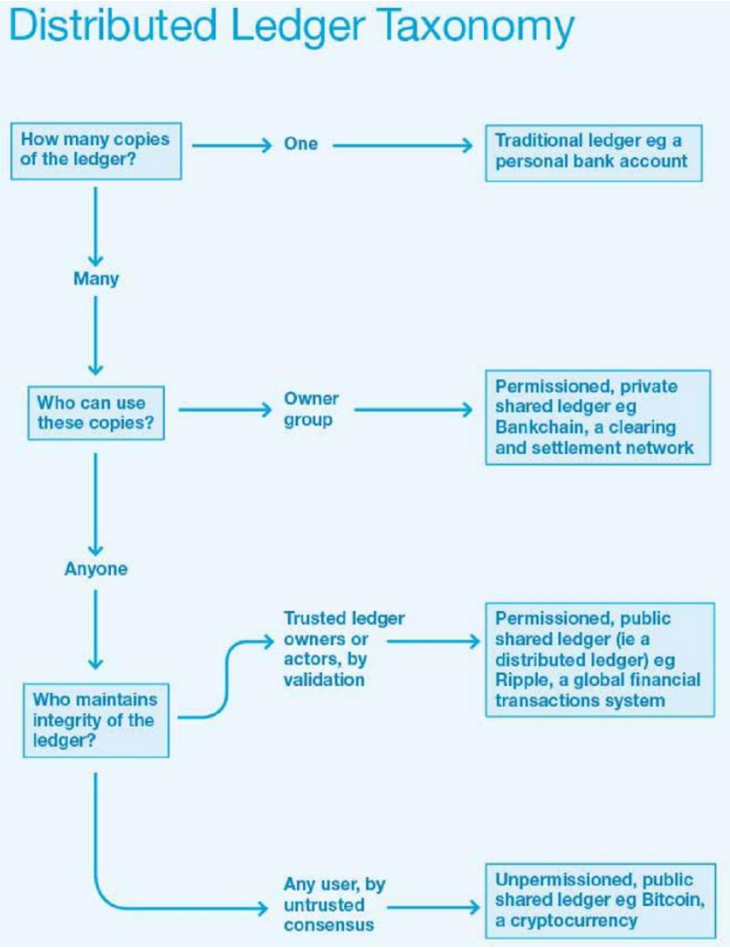
Ecological (non-)sustainability of Bitcoin

- “I consider Bitcoin’s $600 million/year wasted electricity on proof of work to be an utter environmental and economic **tragedy**.”
  VITALIK BUTERIN (blog.ethereum.org, Dec14)

- According to my calculations, if the bitcoin network keeps expanding the way it has done recently, it could lead to a continuous electricity consumption that lies between the output of a small power plant and the total consumption of a small country like **Denmark** by 2020.”
  SEBASTIAAN DEETMAN (vice.com, Mar16)

Bitcoin ≠ Blockchain

Disentangling Bitcoins design parameters



Government Office for Science, Distributed Ledger Technology: beyond the block chain. UK, 2016.

1 centr.

Many (decentralized)

PRIVATE (group)

PUBLIC (anyone)

PERMISSIONED by trusted validation (ledger owners)

UNPERMISSIONED By untrusted consensus (any user)

Degree of decentralisation

2nd wave: blockchain

Towards a blockchain-based stack

Applications

- On Bitcoin's blockchain
- On other blockchains

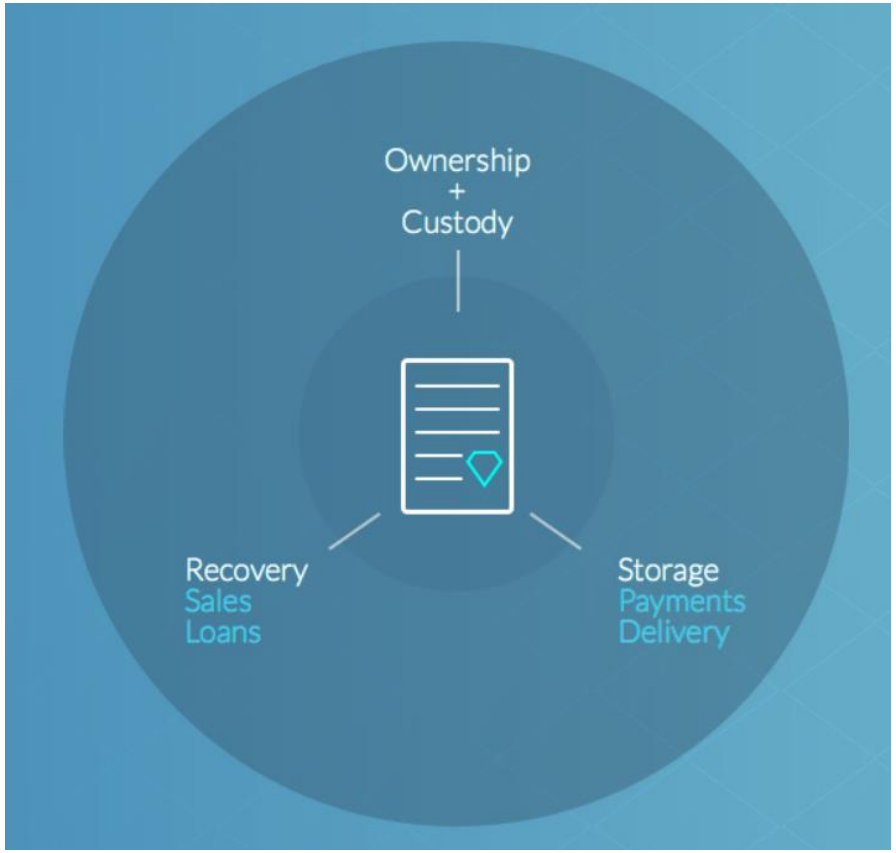
Blockchain

- Built-in currency
- Access and validation management

Blockchain's second wave

Tracing diamonds with Everledger

- a permanent ledger for diamond certification & related transaction history
- a fraud detection and verification system, overlaying big data from closed sources like insurers and law enforcement
- Outlook: track any asset that carries a Unique Identifier which is difficult to destroy or replicate



<TODO> Blockchain's second wave

"Factomizing" the world with factom.com

Factom Apollo

Factom Apollo gives businesses and governments the tools they need to ensure their data can't be changed without them knowing about it.

Factom Iris

Factom Iris is a paradigm shift. It is a "Distributed Network of Authority" vs a traditional "Certification Authority". By decentralizing a hackers point of attack, it becomes exponentially more difficult to spoof a Certificate of Authority.

Factom Hera

Get a handle on disparate data, conduct in-depth analysis, and discover more valuable insights in a unified, customizable environment. Sync legacy systems, communicate easily with partners, and meet regulatory mandates. Have meaningful trade oversight by monitoring risk exposure in real time.

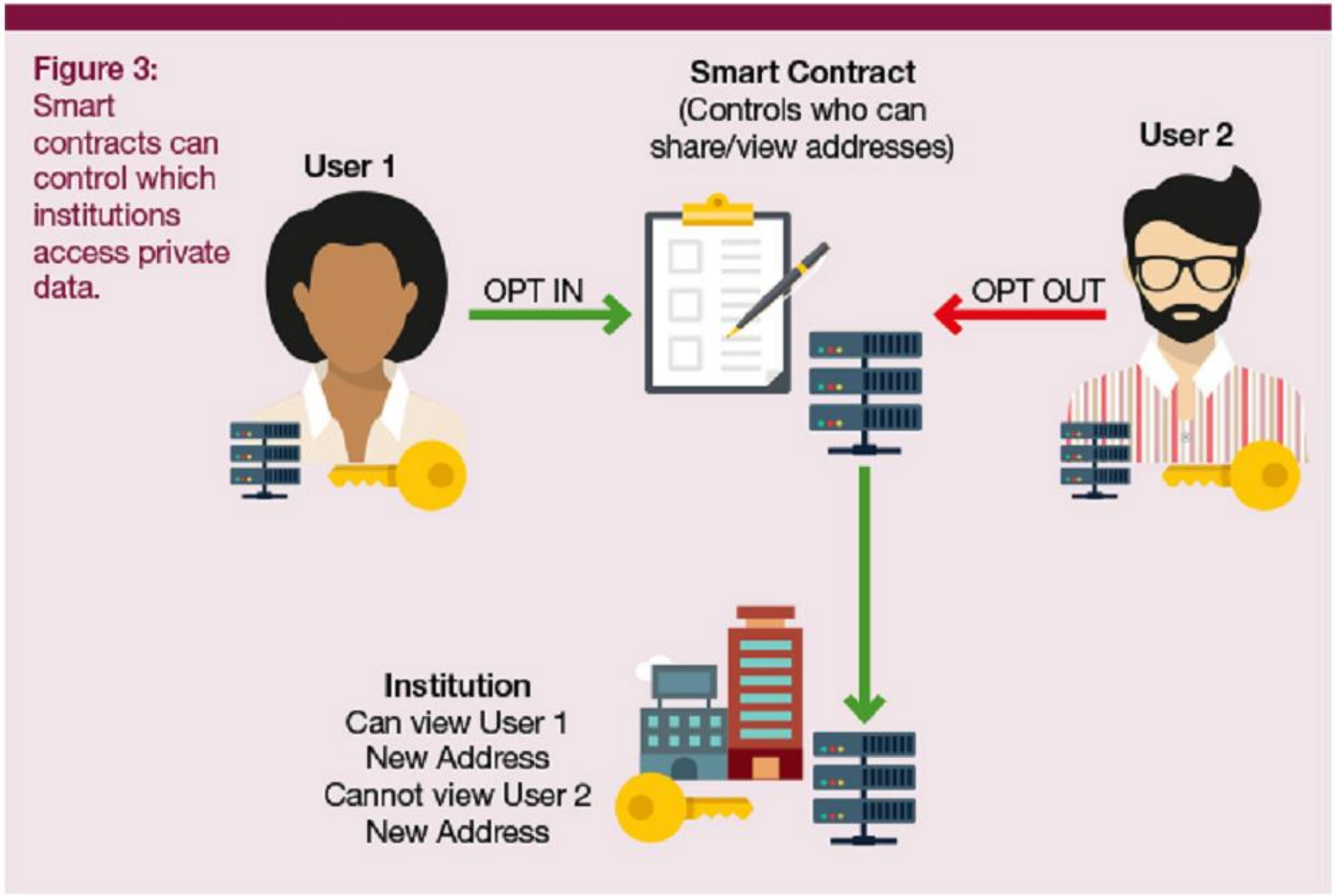
Blockchain's second wave

Building an "unstoppable world computer" with Ethereum

- decentralized platform for applications that
  - run exactly as programmed
  - without any possibility of downtime, censorship, fraud or
    third party interference
- own blockchain
- shared global infrastructure
- enables developers to create
  - markets,
  - store registries of debts or promises,
  - move funds in accordance with instructions given long in the past
- without a middle man or counterparty risk, using "smart contracts"

Blockchain's second wave

Smart contracts



Blockchain' second wave

Towards an Internet of Value

- "The Internet of Things could be one of the largest and most exciting verticals for blockchain technology in the coming years."
  – Ryan Selkis, Director Investments at Digital Currency Group

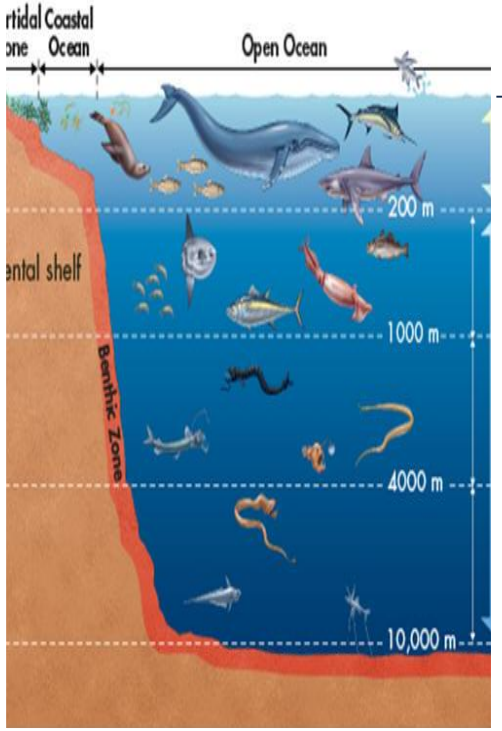
“Banking is just the start:

20 Big Industries Where Blockchain Could Be Used”

+ 3 more
Trade (OpenBazaar)
Legal records
Social Network (SteemIt, ZeroNet)

- Banking
  vault OS, R3CEV
- Real estate
  Ubitquity
- Cyber security
  Guardtime
- Healthcare
  Gem
- Voting
  FollowMyVote
- Stock trading
  t0
- Payments & money transfer
  Abra
- Insurance
  Stratumn
- Internet of Things
  IBM adept
- Online music
  ujomusic
- Cloud storage
  Storj
- Academic certificates
  Holbertson
- Forecasting
  Augur
- Energy management
  TransactiveGrid
- Ride sharing
  La‘Zooz
- Car leasing and sales
  DocuSign
- Gift card/loyalty programs
  Gyft
- Sports management
  Jetcoin
- Supply chain mangement
  Provenance ...
- Government, public benefits
  GovCoin

https://www.cbinsights.com/blog/industries-disrupted-blockchain/



3rd wave: Ecosystem(s)

The third wave is looming ...

Blockchain-based organisations

The DAO (organization)

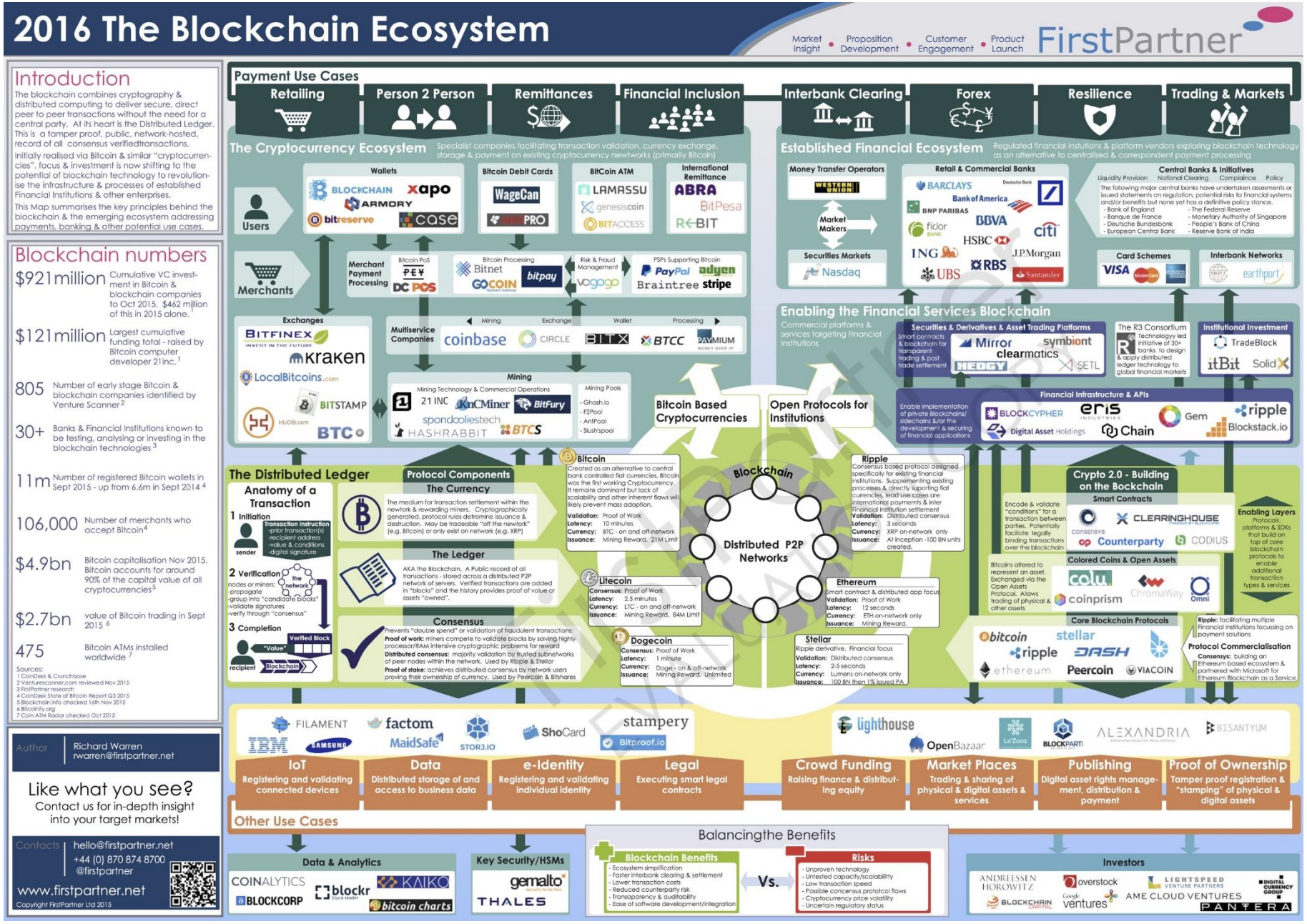
Type	Decentralized Autonomous Organization
Industry	Cryptocurrency software venture capital fund
Founded	2016
Area served	World (stateless)[1]
Key people	Stephan Tual, Simon Jentzsch, Christoph Jentzsch
Total assets	ETH 11.5 million[2]
Owners	+18 000 stakeholders[3]
Number of employees	0 (automated)[4]
Website	daohub.org

The DAO (software)

Written in	Solidity
License	GNU LGPL v3+
Website	github.com/slockit/DAO

The third wave

Ecosystems



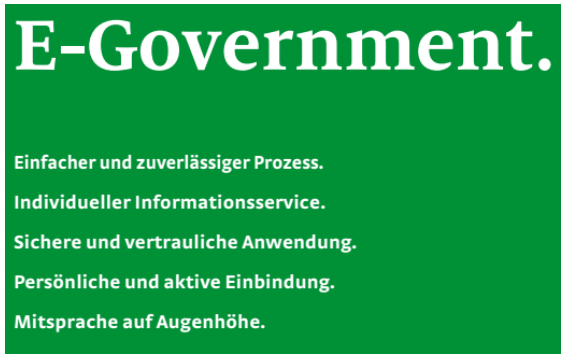
The need for blockchain research in Germany

Holistic approach

- Sectors with information management inefficiencies, e.g. energy, health, public sector

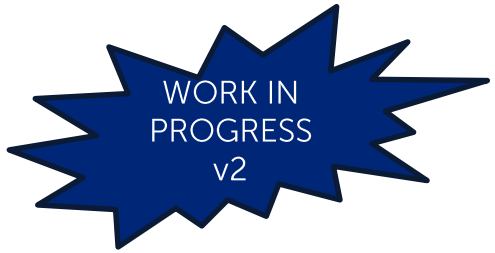
- Perspectives
  - Technology
  - Social / Culture
  - Regulatory framework / Law
  - Economics

- Potential
  - Technical analysis: security, scalability
  - Technology acceptance
  - Legal analysis
  - Business model analyses



22 Bedürfnismuster, Zukunftsstudie Band V

Who let the blocks out?



Making sense of blockchain technology

Dr. Marcus M. Dapp

Head “Open Data & Information Management”

Co-Dir “Institute for Public Information management”

fortiss GmbH
An-Institut Technische Universität München