DEUTSCHE BUNDESBANK
EUROSYSTEM

New Blocks for the Kids?

On the Potential Role of Blockchain for Payment and Settlement Systems

14th Payment and Settlement System Simulation Seminar, Helsinki, Bank of Finland

25 August 2016 Martin Diehl

This presentation and the concomitant statements reflect the personal opinion of the author and not necessarily the opinion and judgement of the Deutsche Bundesbank.

Blockchain among the Megatrends 2016

SITRA
Megatrends New Technologies

Virtualisation and data digitisation
Artificial intelligence
The instrumentation of everything
Nanomaterials
Biotechnology and pharmacology
Energy technology
Digital platforms
Globalisation of ICT structures
Blockchain technology

”Blockchain on teknologia, jonka myötä Bitcoin on syntynyt, ja se saattaa toimia myös **radikaalina pelinmuuttajana** monilla aloilla tulevaisuudessa.”

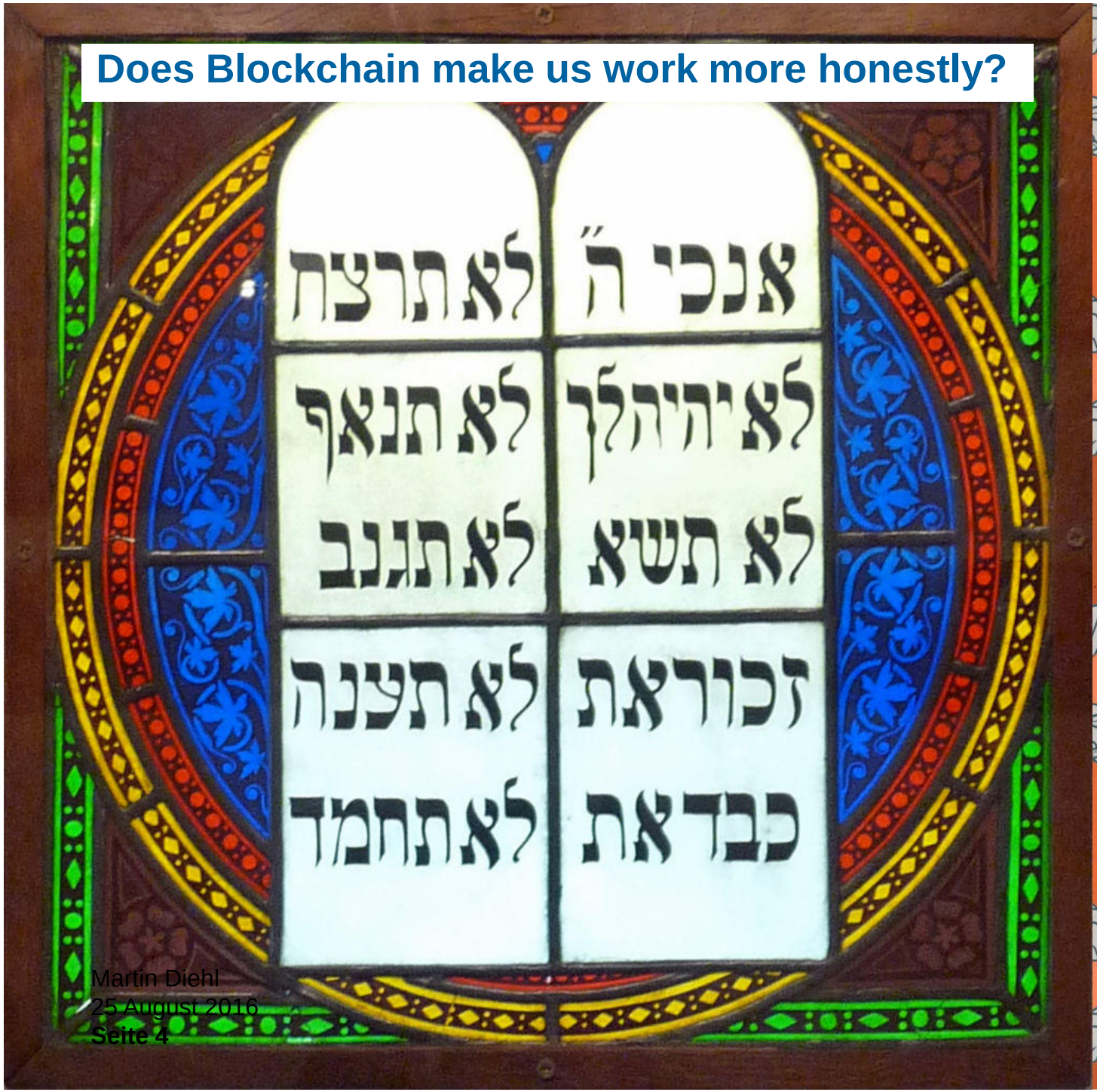
Megatrends 2016. The future happens now. ISBN 978-951-563-960-8 (PDF) www.sitra.fi

World Economic Forum
Top 10 Emerging Technologies:

Nanosensors and the Internet of Nanothings
Next Generation Batteries
The Blockchain
Two Dimensionsional Materials
Autonomous Vehicles
Organs-on-chips
Perovskite Solar Cells
Open AI Ecosystem
Optogenetics
Systems Metabolic Engineering

“Perhaps the most encouraging benefit of blockchain technology is **the incentive it creates for participants to work honestly where rules apply equally to all**. […], blockchain technology has the potential to enhance privacy, security and freedom of conveyance of data—which surely ranks up there with life, liberty and the pursuit of happiness.”

Does Blockchain make us work more honestly?



Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System

What is needed is an electronic payment system
based on cryptographic proof instead of trust,
allowing any two willing parties to transact directly with each other
without the need for a trusted third party.

Satoshi Nakamoto, 2008

Different Levels of Discussion about DLT

- First level: technological synchronisation within distributed databases in a network
- Second level: a unique (logical) ledger with bookkeeping of transactions and a replica at all participants
- Third level: contractual relations between the participants of the system
- Fourth level: an overall perspective of „trust“ between participants

Source: Bott and Milkau, 2016

Trust in Legal Tender

Trust in Money

- bills of exchange have facilitated the long distance trade since the medieval times

- Basis: Trust
  - in personal integrity
  - and creditworthiness of a merchant

Abbildung 1: Jakob Fugger der Reiche und sein Hauptbuchhalter Matthäus Schwarz im Kontor der Augsburger Firmenzentrale (1517)

Aspects of Different Forms of Money

Function	• exchange • store of value • unit of calculation
Occurrence	• physical • electronic / digital
Proof of Ownership	• bearer • IOU / account statement • registry

basis of value	• trust in a central bank
	• exchange value
	  • merchandise value
	  • virtual

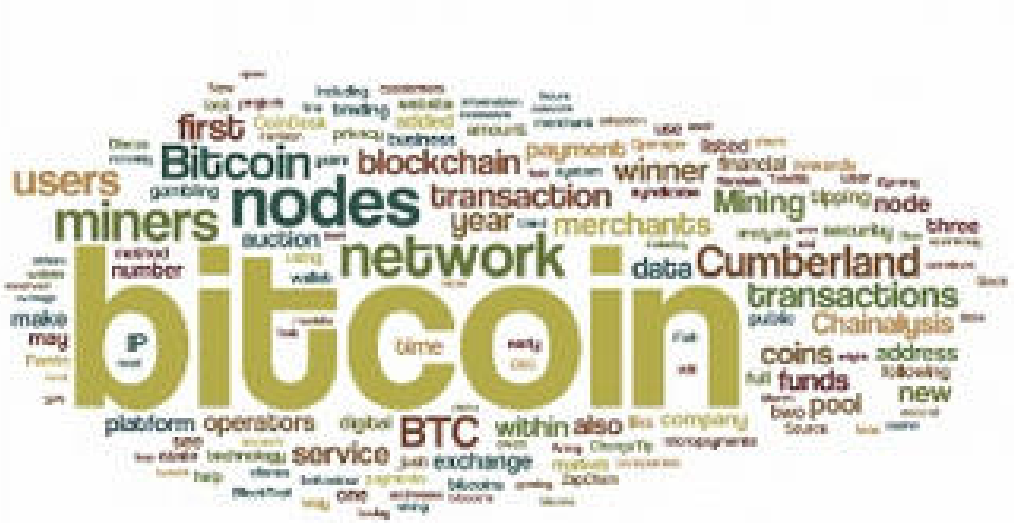
acceptance	• obligatory • forced

It is difficult to understand how a plain numerical record – without any backing – can have a long-term monetary value.

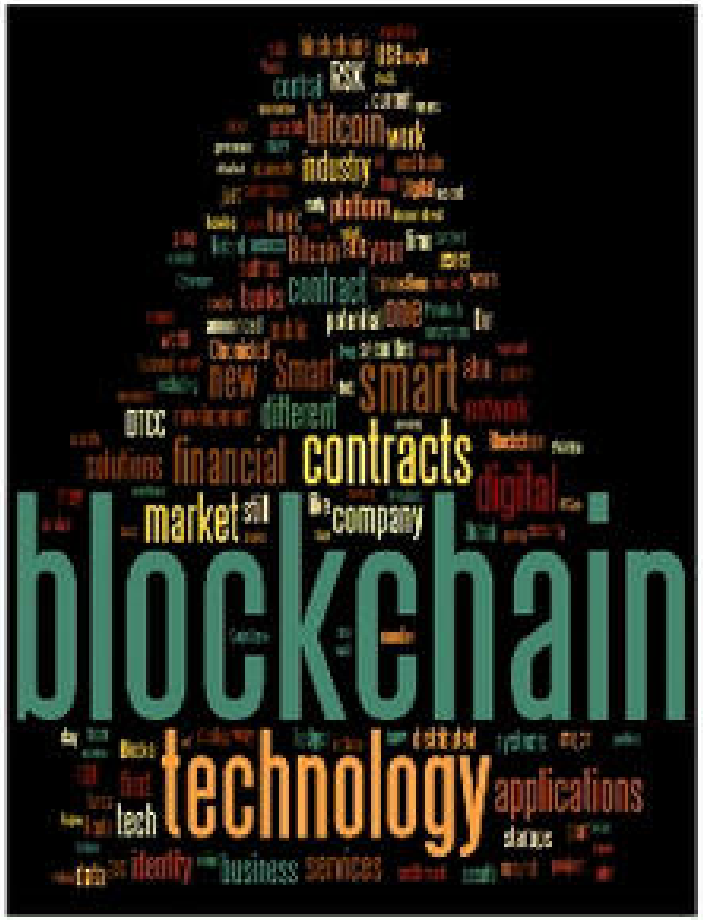
Harry Leinonen, 2016

From Cryptotarians to Execs: 'Bitcoin' – 'Blockchain' Terminology Change Reflects Shifting User Base

2015



2016



Notes and Data source: Word clouds constructed based on word frequency of CoinDesk articles. More info here: CoinDesk

Advantages of Blockchain

- safe transfer of value from peer to peer without a central organ
- decentral storage with all participants

  ⇒ less prone against manipulation and cyber attacks „Distributed Ledger Technology“
- automated processing of codes („smart contracts“)

Blockchain = decentralized database
where conditioned or unconditioned transactions
of digitalised scarce goods
are automatically verified

Disadvantages of the Blockchain (Bitcoin-Version)

- proof-of-work causes extreme high costs (CPU-capacity and energy use)
- hitherto not sufficiently scalable
- danger of a Sybil attack (in the end a voting scheme)
- no true anonymity
- only relative finality

risks of the cryptography:

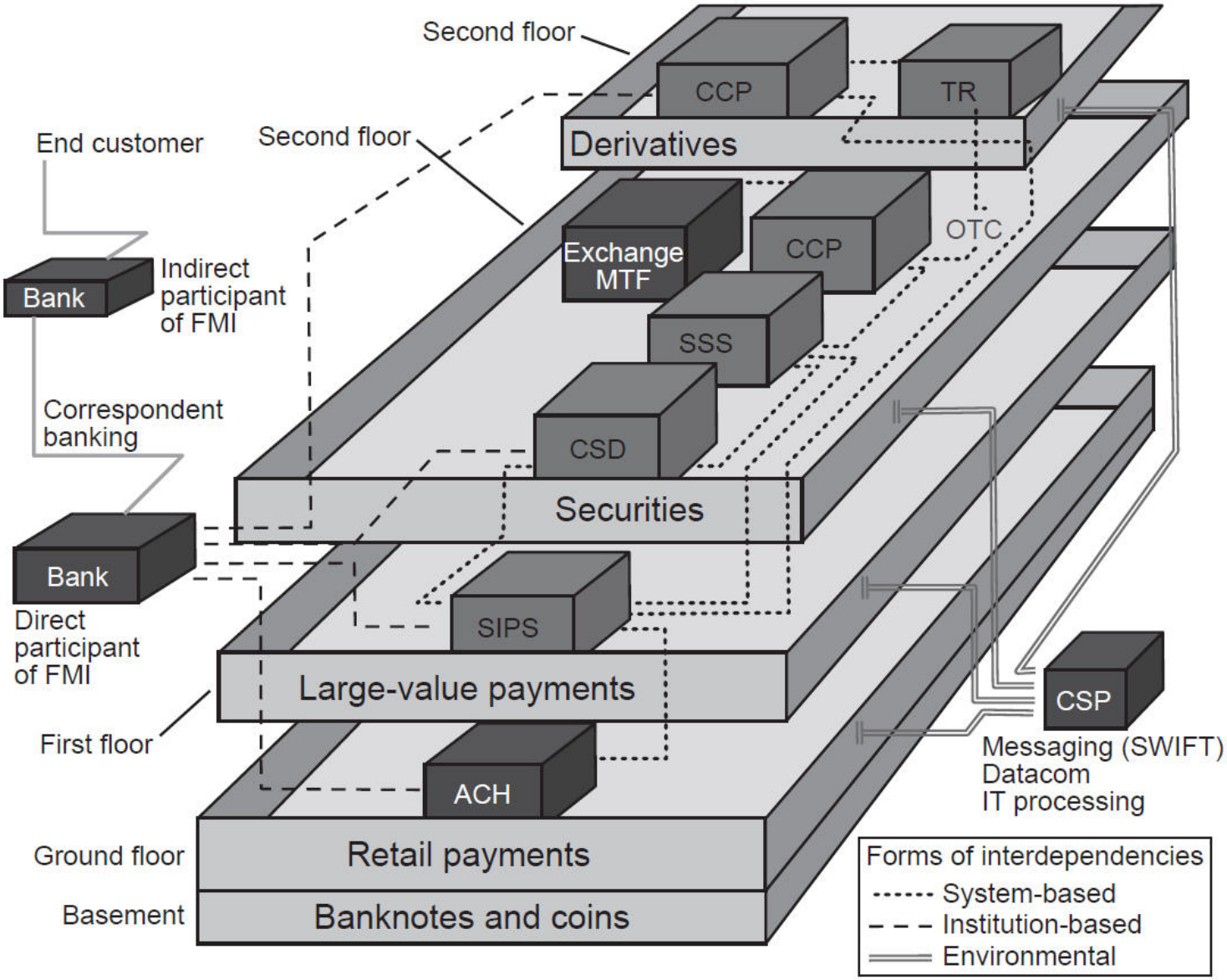
- quantum computers may crack the system
- encription not absolutely distinct

Adjustments for Financial Purposes

- no native currency – only pure blockchain as a database and transaction mechanism

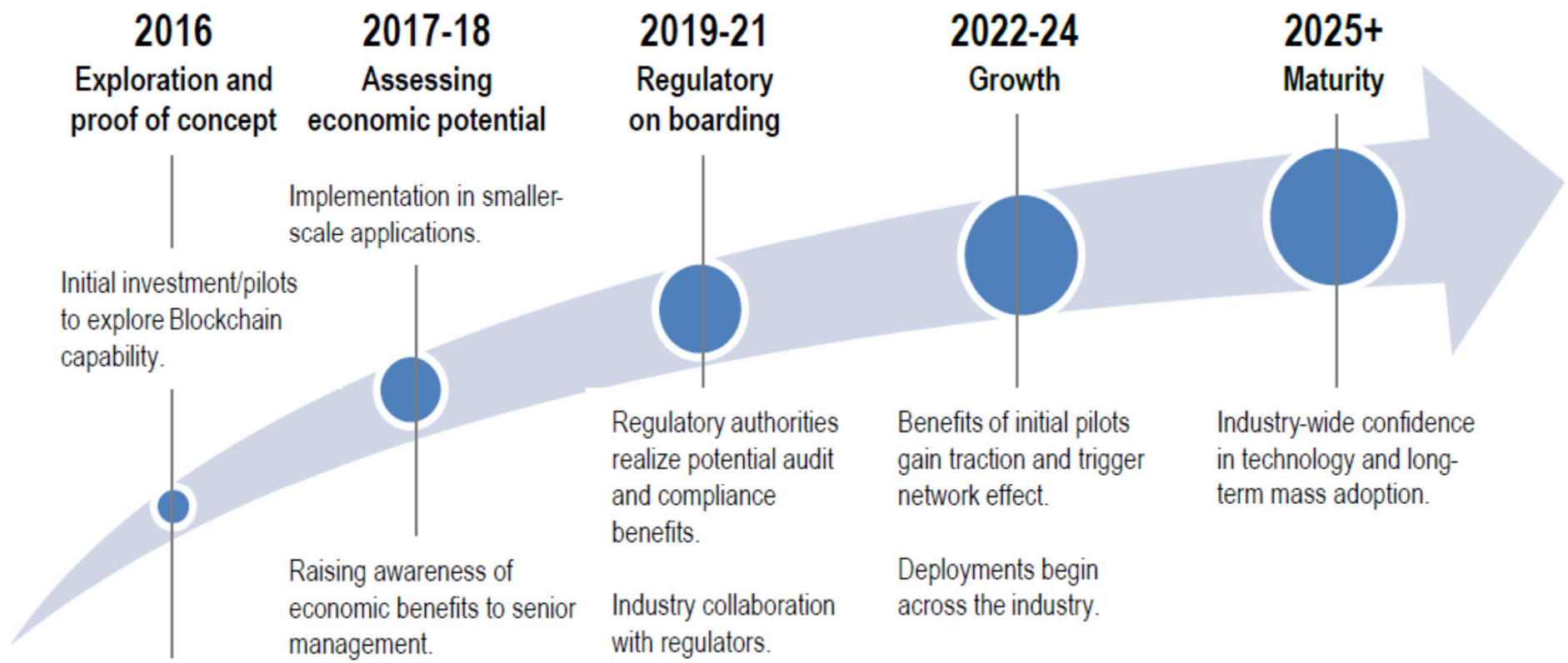
- permissioned blockchains
  - admission to be controlled by some central entity
  - identity of participants must be revealed
- no open storage, but need-to-know principle
- pre-defined governance – no anarchical structure
- fast settlement
- ultimate finality
- cooperation

Disintermediation von Finanzmarktinfrastrukturen? The warehouse of FMI



Source: Berndsen, Ron (2012): Letter from the editor. The Journal of Financial Market Infrastructures, Vol. 1 / No. 2, Winter 2012/2013.

Example of the Development Path



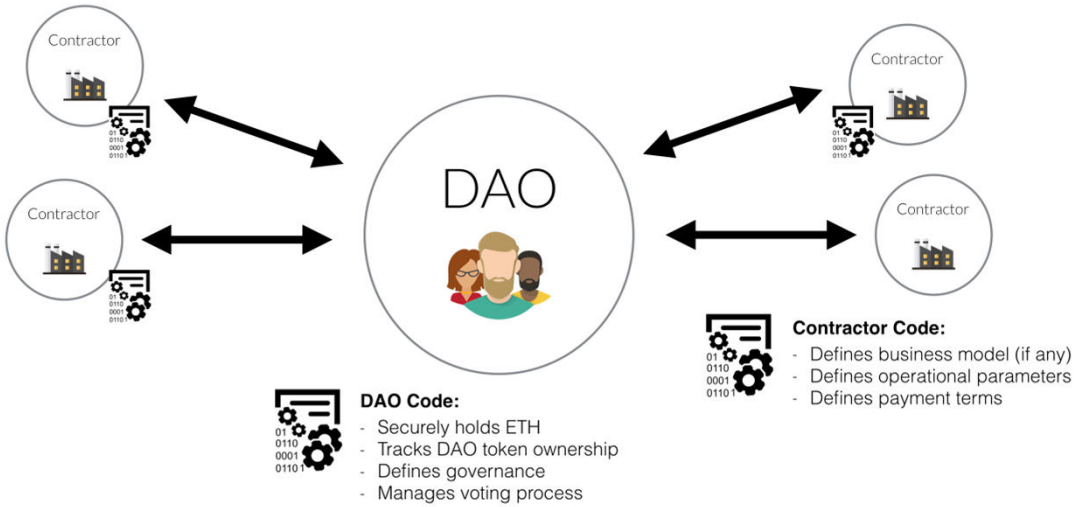
Source: J.P. Morgan.

Blockchain Supply Structure

Approach	How it's done	Examples
IT Services	We will build you anything	Big IT firms
Blockchain First	You work directly with the blockchain's tools and services	Bitcoin, Ethereum
Development Platforms	Tools for IT professionals	BlockApps, Blockstream, Eris, EthCore, Hyperledger, Tendermint
Vertical Solutions	Industry specific	Axoni, Chain, Clearmatics, DAH, itBit, R3
Special APIs & Overlays	DIY building blocks	Blockstack, Factom, Open Assets, Tierion

Quelle: William Mougayar, http://www.coindesk.com/which-blockchain-implementations/ vom 4. Mai 2016.

Ethereum and DAO



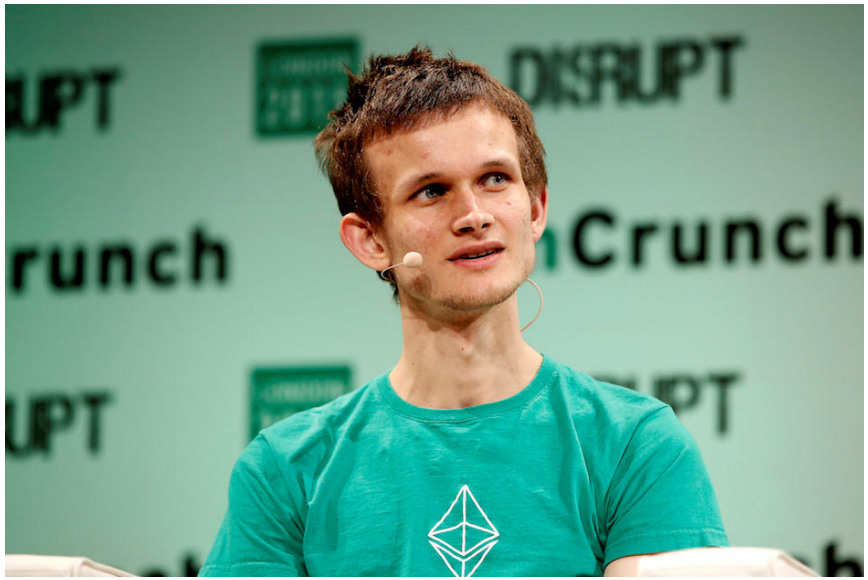
- **Decentralized Autonomous Organization (“DAO”)** - immutable, unstoppable, and irrefutable computer code, operated entirely by its members
- **Inclusion:** The DAO leverages smart contracts on the Ethereum blockchain so that anyone, anywhere in the world can be empowered to participate.
- **Flexibility:** The DAO backs Proposals which it selects for their innovative nature, to be delivered by Contractors.
- **Profitability and Growth:** The DAO charges for the use of its the products or services. This revenue is then sent directly to The DAO in the form of ETH.
- **Autonomous Governance:** The ETH held by The DAO will never be centrally managed. DAO Token Holders are able to vote on important decisions.
- The DAO, represented by smart contracts on the Ethereum blockchain at address 0xbb9bc244d798123fde783fcc1c72d3bb8c189413

Code versus Consensus

- a DAO: decentralized autonomous organization
- The DAO: a code to function as a venture capital firm
- collected 160 million USD
- 50 million were stolen within a few minutes
- code allowed so
- code (of Ethereum) was changed to regain the money

$\Rightarrow$ can code become law ?
- requires a static world
- neglects the teleological interpretation of law

Creators of the DAO



Vitalik Buterin, creator of Ethereum

R3

- Richard Gendal Brown
- basic features of the R3 concept for a prototype to use blockchain for financial transactions
  - Corda is supposed to help in documentation and management of financial transactions
- Core features, especially in comparison to Bitcoin :
  - need to know principle
  - workflow between firms is choreographed without a central controller
  - consensus is achieved between firms at the level of individual deals, not the level of the system
  - direct access for regulatory and supervisory observer
  - validation by parties to the transaction rather than a broader pool of unrelated validators
  - explicit link between human-language legal prose documents and smart contract code
  - Corda is built on industry-standard tools
  - no native cryptocurrency

Siehe https://gendal.me/.

Siehe https://www.youtube.com/watch?v=1UhrmsTZNvc

Meaning of DLT for Financial Sector

- is it about
  - a messaging system?
  - a bookkeeping system?
  - a payment system?
  - a settlement system?
- are distributed ledgers simply some kind of advanced distributed database?
- harvesting the benefits by close cooperation (standardization, interoperability and automated through-processing enables many efficiency gains)
- current developments
  - hierarchies are creeping in
  - centralisation remains
  - aversion against opaque groups
- many different applications conceivable – refined to special niches
- no broad substitution for current payment and settlement system
- trusting in a single entity is risky; but supervising a single entity is less costly

Central Banks and Digital Currencies (1)

- Mark Carney, Bank of England, 16. Juni 2016:
  - “[…] the prospect of a central bank digital currency for the UK, in my view, still some way off. We will work to make payments easier, and though cash may no longer be king it once was, its reign will endure for some time.”

- Carolyn Wilkins, Bank of Canada, 17. Juni 2016:
  - „In fact, the potential for DLT is actually stronger for applications outside of digital currencies.”

- Ron Berndsen, DeNederlandse Bank, 20. Juni 2016:
  - Blockchain is the “technologoy for the next generation of financial market infrastructures.”

Central Banks and Digital Currencies (2)

Implications of a possibility to work with digital cash (central bank issued digital currency)

- Three categories of central bank money
  - physical cash
  - claims on accounts with the central bank
  - digital cash
- Non-banks will demand more cash
  - they can buy more goods with digital cash via the blockchain
  - the implicit risk of losses is assumed to be much lower for digital cash (on the blockchain) in comparison to physical cash;
  - the implicit risk of holding money on the blockchain will be, assuming the blockchain is run by a trustworthy operator, lower than the risk of holding commercial bank money

Central Banks and Digital Currencies (3)

Implications for monetary aggregates

- Cash as a share of the base money will grow in importance.
- Demand deposits and M2 as well as M3 will go down.
- The money multiplier (the ratio of bank deposits / bank money to base money (by the central bank) will decrease.
- more base money has to be issued
  - holds even when rising social liquidity efficiency is assumed
  - splitting up transaction balances may decrease liquidity efficiency
- central bank would have to issue more money
  - more monetary operations - requires more eligible collateral of banks
  - or
  - securities purchases - is limited by the prohibition of central banks to finance the fiscal deficit

Central Banks and Digital Currencies (4)

Banks will face some severe implications for their profitability

- interest margin of banks will go down
  - cheapest way of refinancing (demand deposits) will lose in importance
- banks may need more high quality collateral for monetary operations
  - need to invest a larger share of their assets in eligible (and low interest bearing) collateral.
- lower money multiplier will imply higher interest rates for loans

Central Banks and Digital Currencies (5)

Finally, we end up in a consideration of Souvereign Money

can a central keep up trust in its currency without backing it on real claims?
can we just invent stable money?

do central bank managers have more insights in the credit-worthiness of businesses?

can we sufficienty supervise the soundness of the banks and the financial system?

Central Banks and Digital Currencies (6)

the old townhall of Amsterdam where in 1609 the *Wisselbank* was founded

Oilpainting by Pieter Janszoon Saenredam, 1657.