Blockchain

The worst database in the world

HOLDER

Jeroen Bulters

Manager Blockchain Team, Deloitte Risk Advisory

Managing Partner, Holder Consulting (Nov. 2017)

Agenda

- Value and Information
- Blockchain 101
- Future of Blockchain
- What will you do?

Information and Value

Information

- Word of mouth
- Courier
- Mail
- Telegraph
- Telephone
- Internet

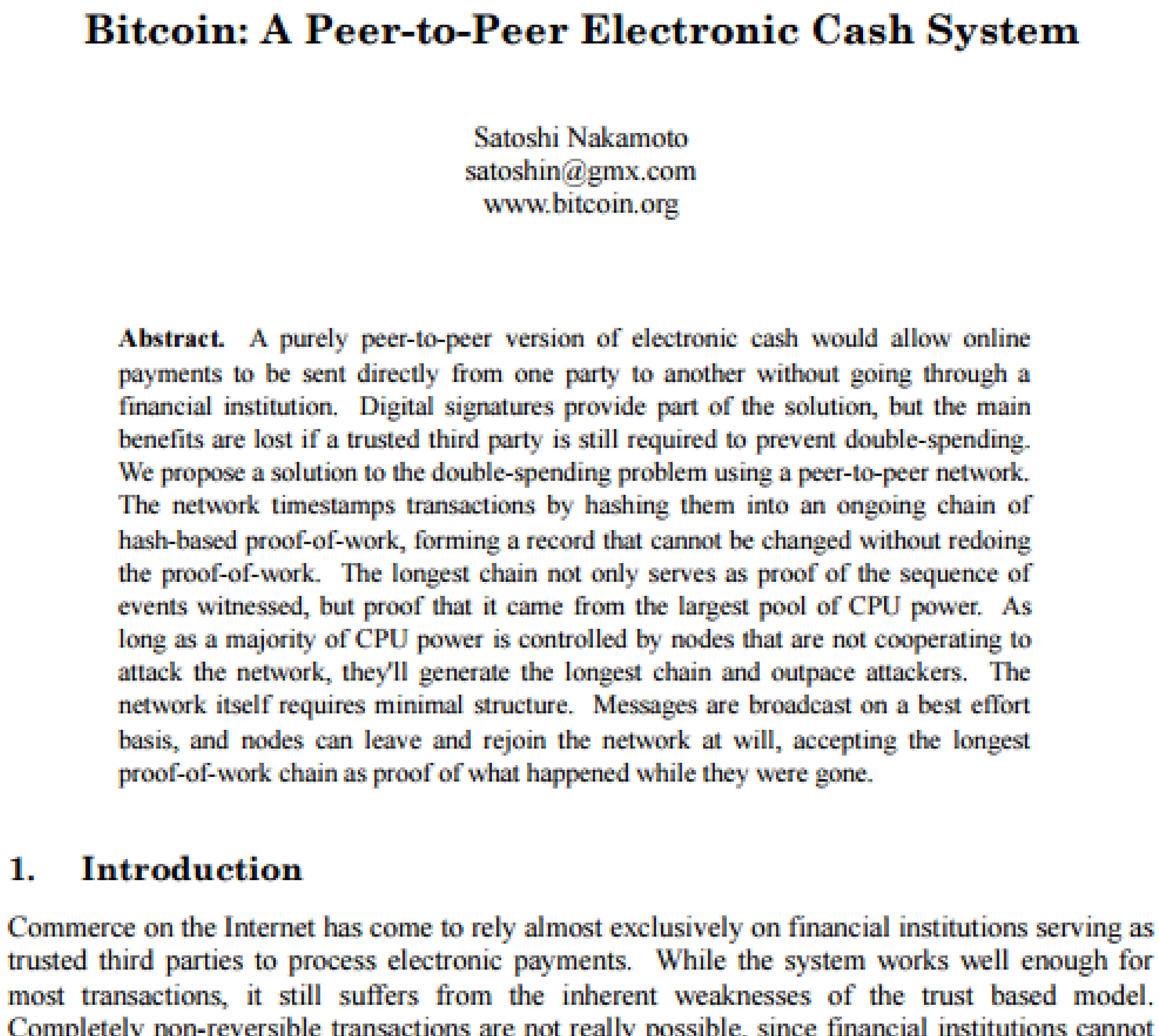
How far apart?

Value

- Shells
- Gold nuggets
- Coins
- Letters of Credit
- Electronic Banking
- Bitcoin?

How far apart?

Blockchain 101



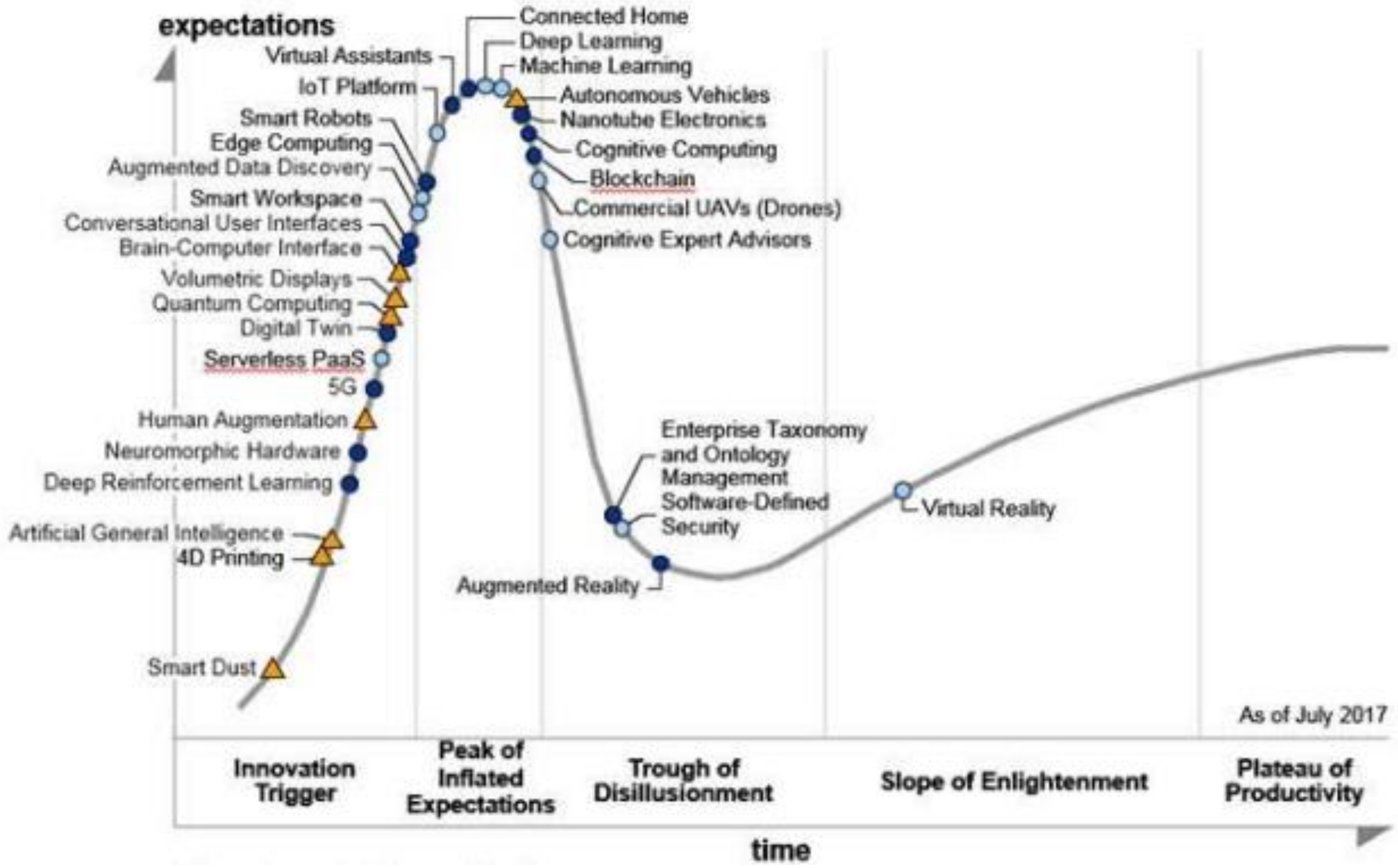
Bitcoin: A Peer-to-Peer Electronic Cash System

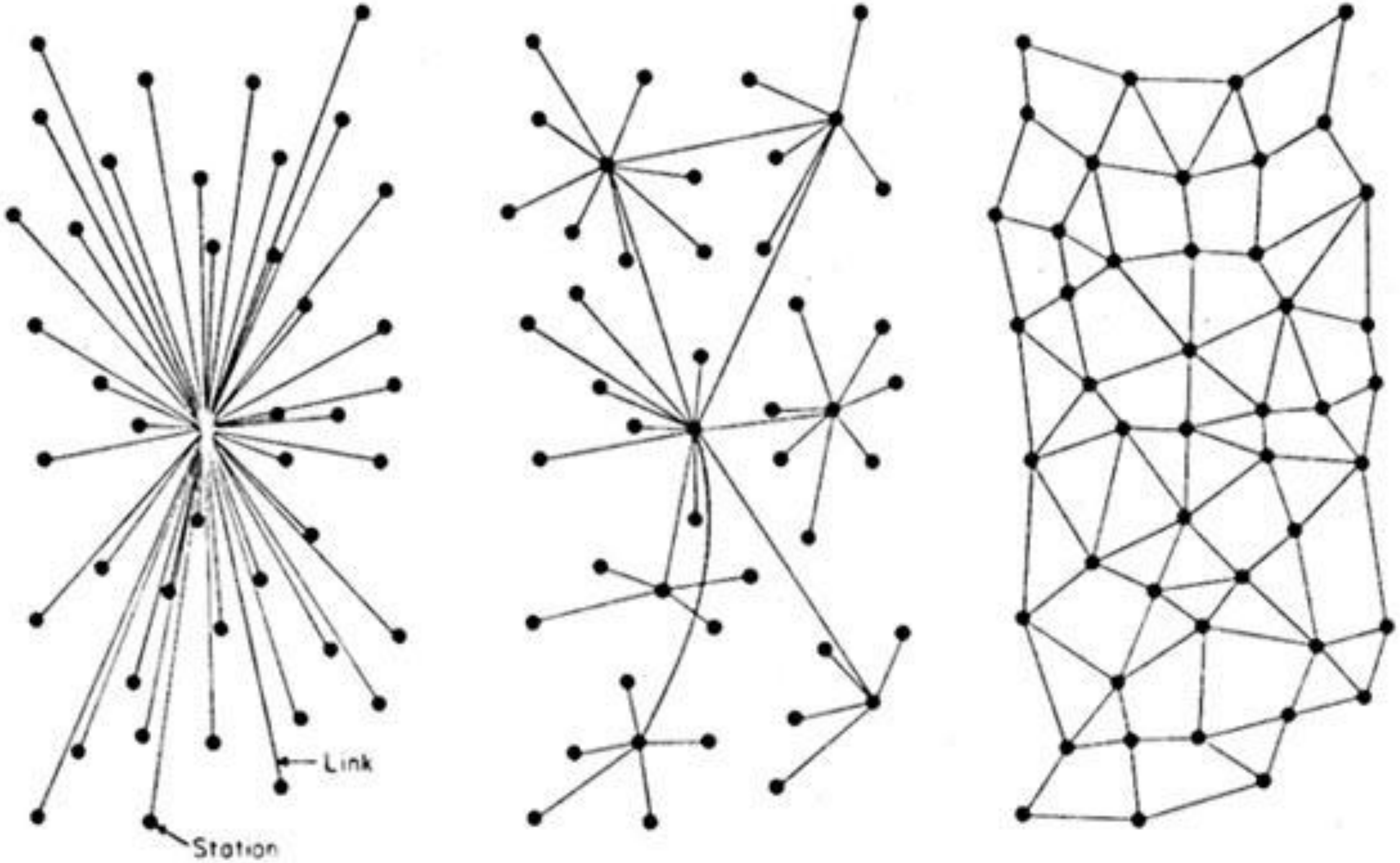
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot

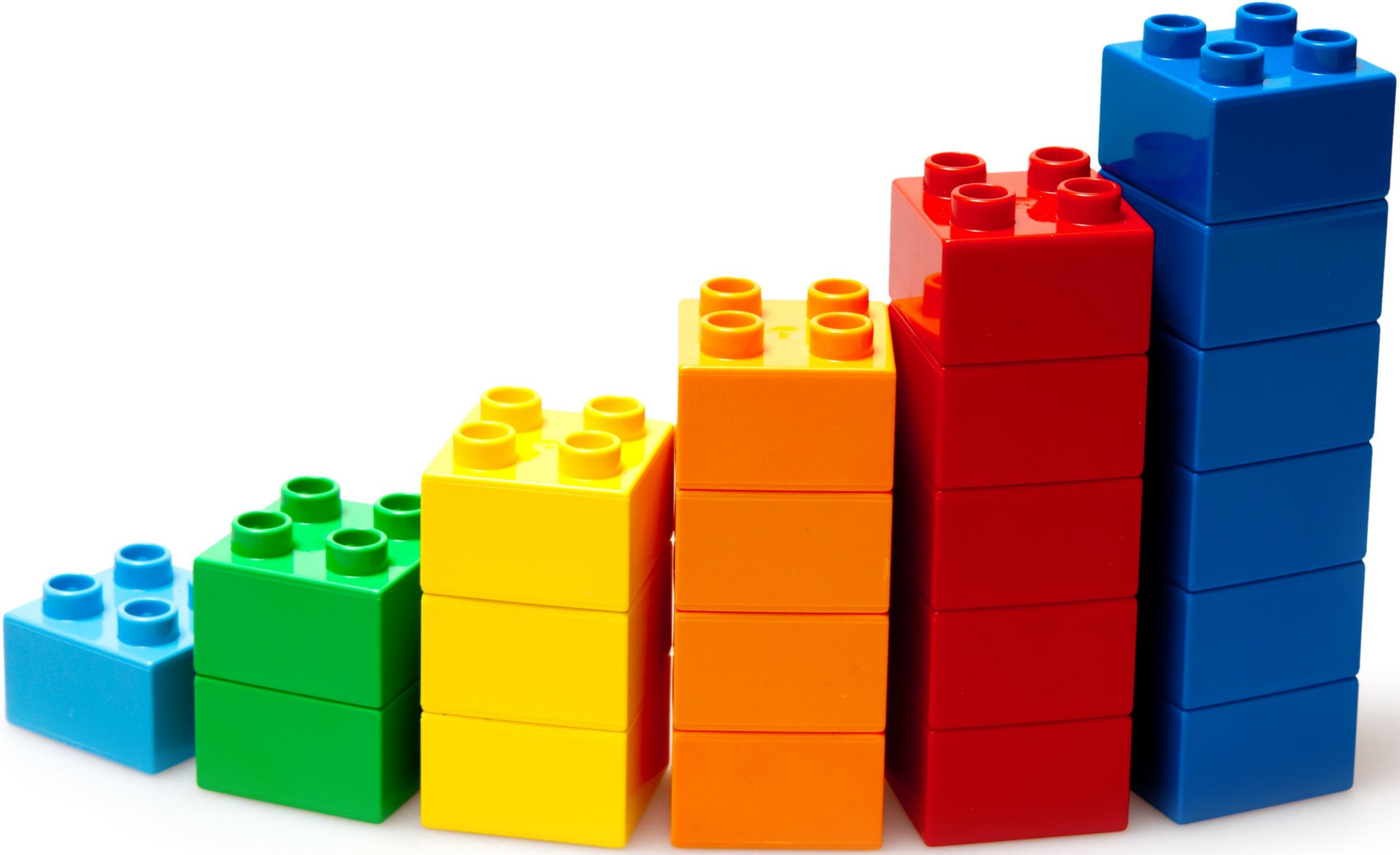

expectations
Virtual Assistants
IoT Platform
Smart Robots
Edge Computing
Augmented Data Discovery
Smart Workspace
Conversational User Interfaces
Brain-Computer Interface
Volumetric Displays
Quantum Computing
Digital Twin
Serverless PaaS
5G
Human Augmentation
Neuromorphic Hardware
Deep Reinforcement Learning
Artificial General Intelligence
4D Printing
Smart Dust
Connected Home
Deep Learning
Machine Learning
Autonomous Vehicles
Nanotube Electronics
Cognitive Computing
Blockchain
Commercial UAVs (Drones)
Cognitive Expert Advisors
Enterprise Taxonomy and Ontology Management
Software-Defined Security
Augmented Reality
Virtual Reality
As of July 2017
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
time

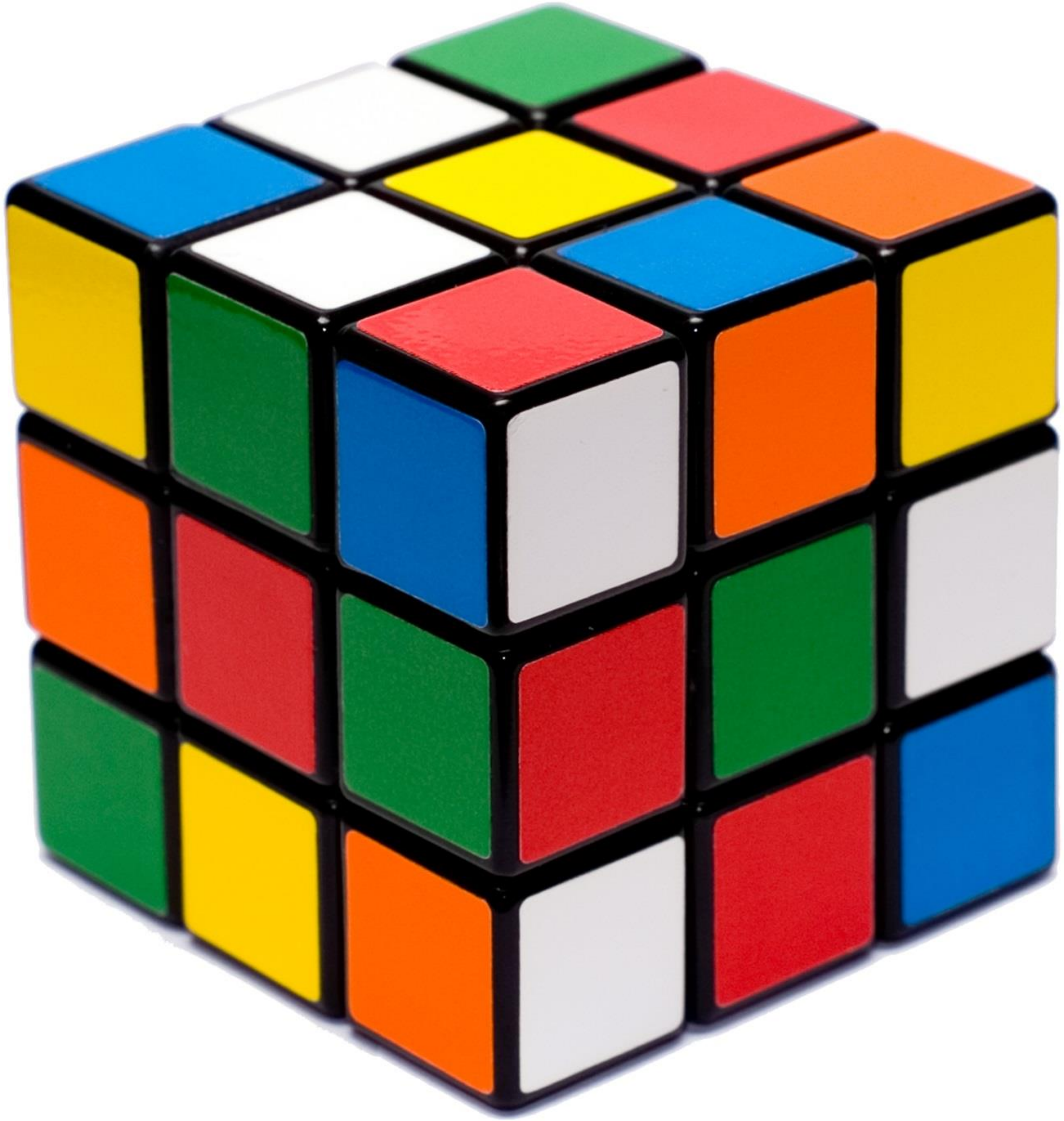


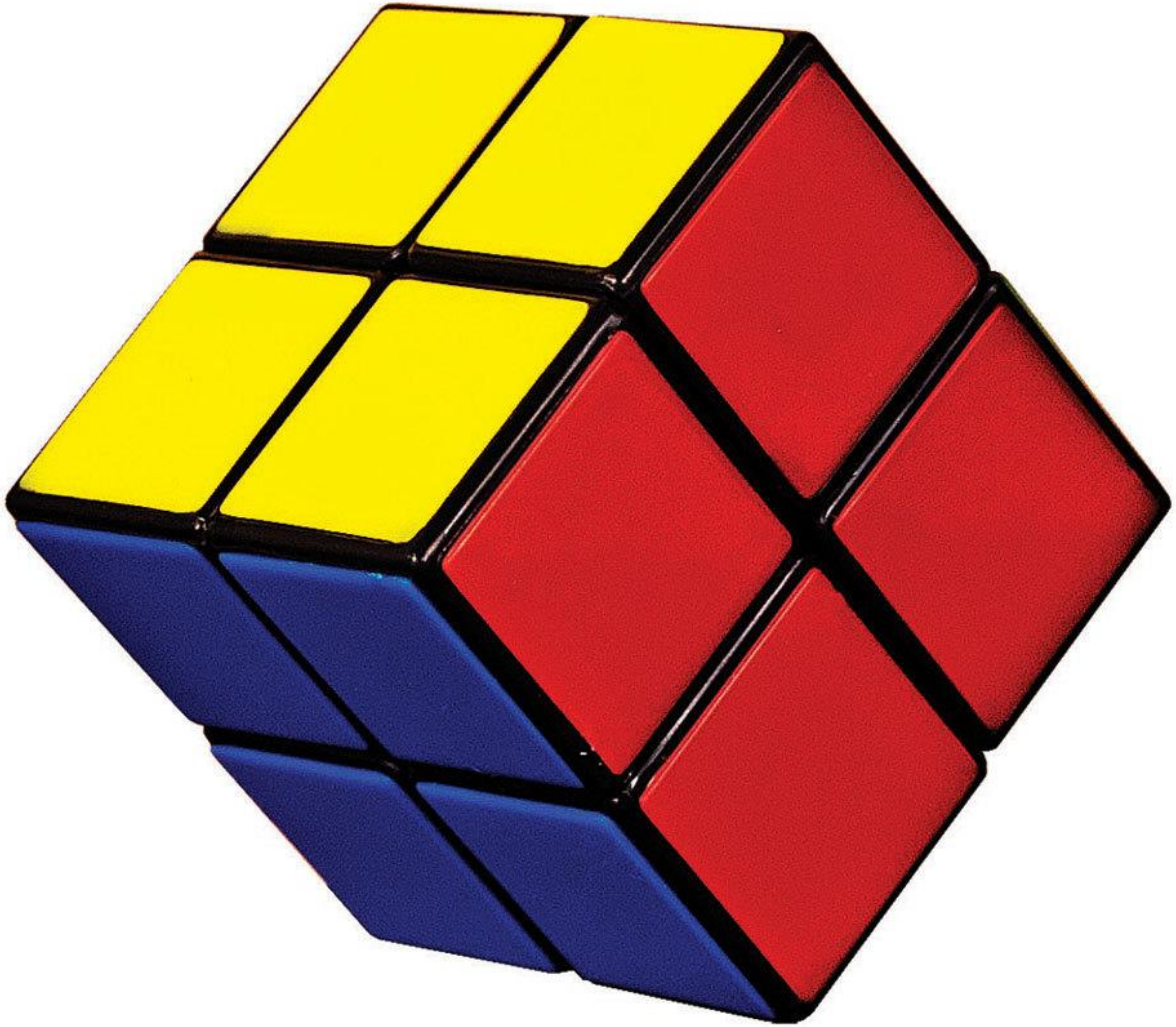
CENTRALIZED
(A)

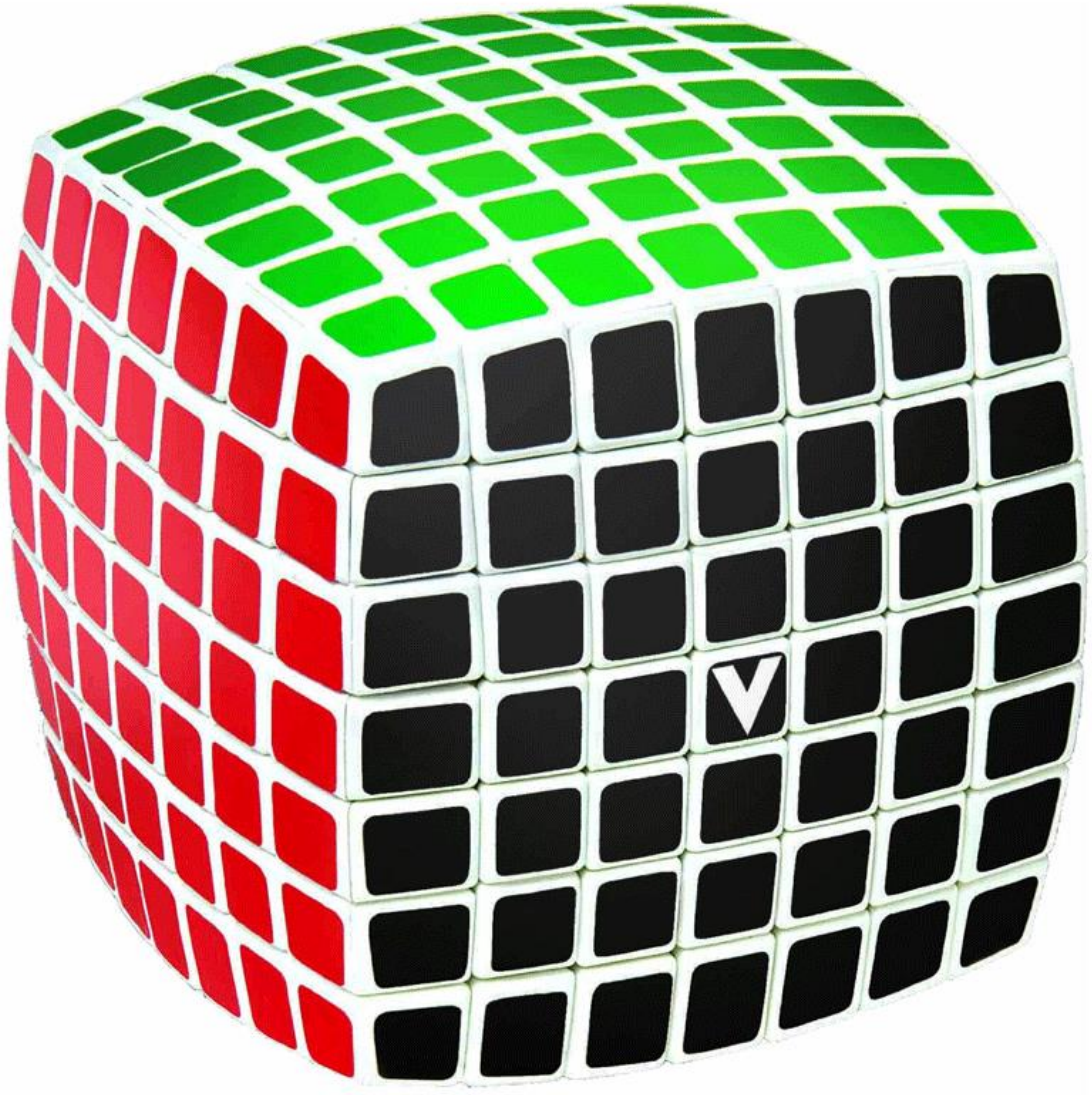
DECENTRALIZED
(B)

DISTRIBUTED
(C)








V

But is it new?

Blockchain new?

- Cryptographic signatures
- Public Key Cryptography
- Cryptographic Hash Functions
- Proof-of-work
- Time-Stamping
- Merkle Trees
- Byzantine fault tolerance
- Smart contracts

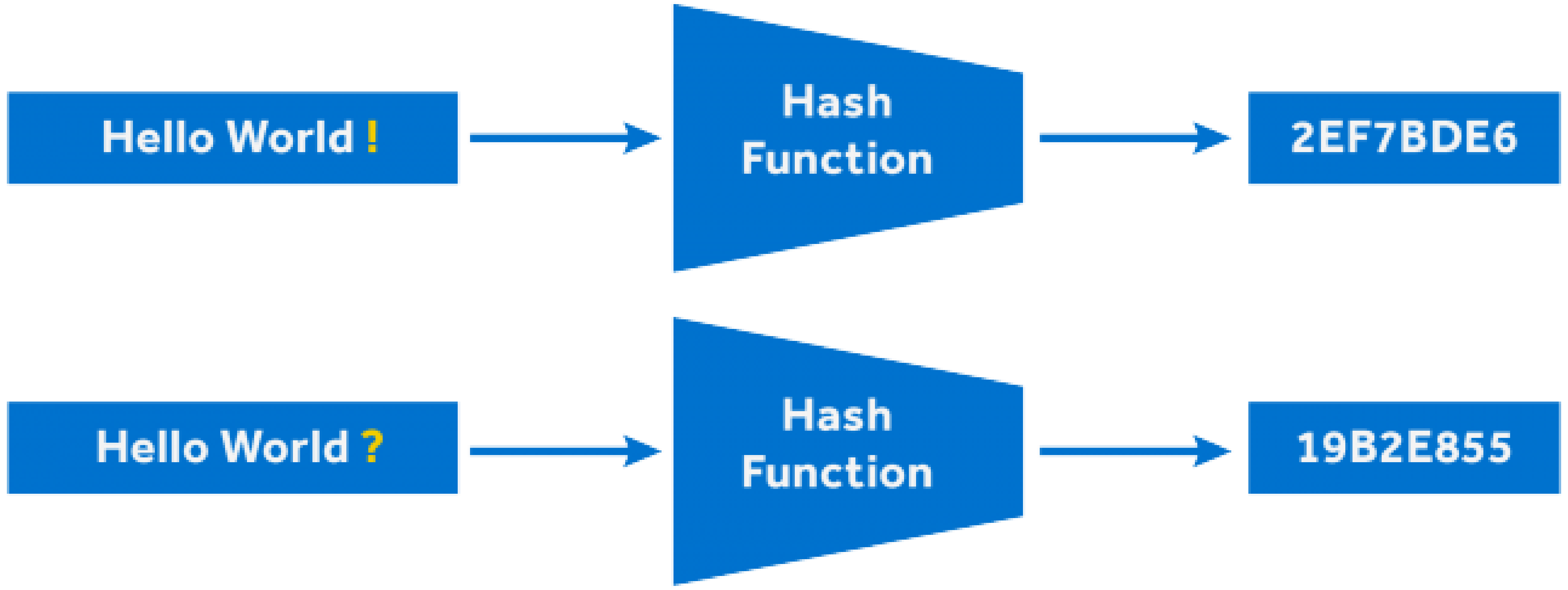
Blockchain new?

- Cryptographic signatures
- Public Key Cryptography
- Cryptographic Hash Functions
- Proof-of-work
- Time-Stamping
- Merkle Trees
- **Byzantine fault tolerance**
- Smart contracts

DON'T ATTACK
ATTACK

Blockchain new?

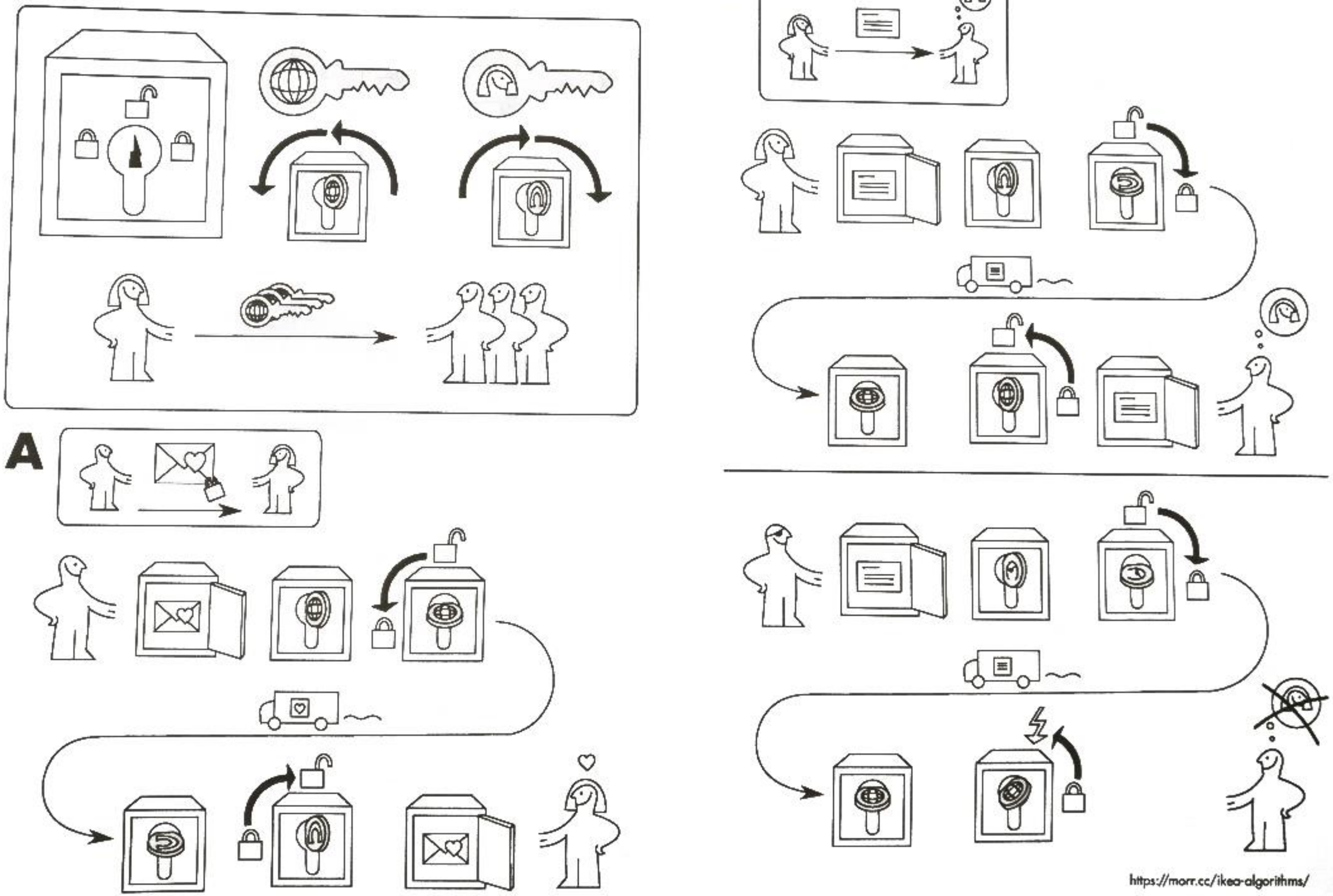
- Cryptographic signatures
- Public Key Cryptography
- **Cryptographic Hash Functions**
- Proof-of-work
- Time-Stamping
- Merkle Trees
- Byzantine fault tolerance
- Smart contracts


Hello World !
Hash Function
2EF7BDE6
Hello World ?
Hash Function
19B2E855

Blockchain new?

- **Cryptographic signatures**
- **Public Key Cryptography**
- Cryptographic Hash Functions
- Proof-of-work
- Time-Stamping
- Merkle Trees
- Byzantine fault tolerance
- Smart contracts

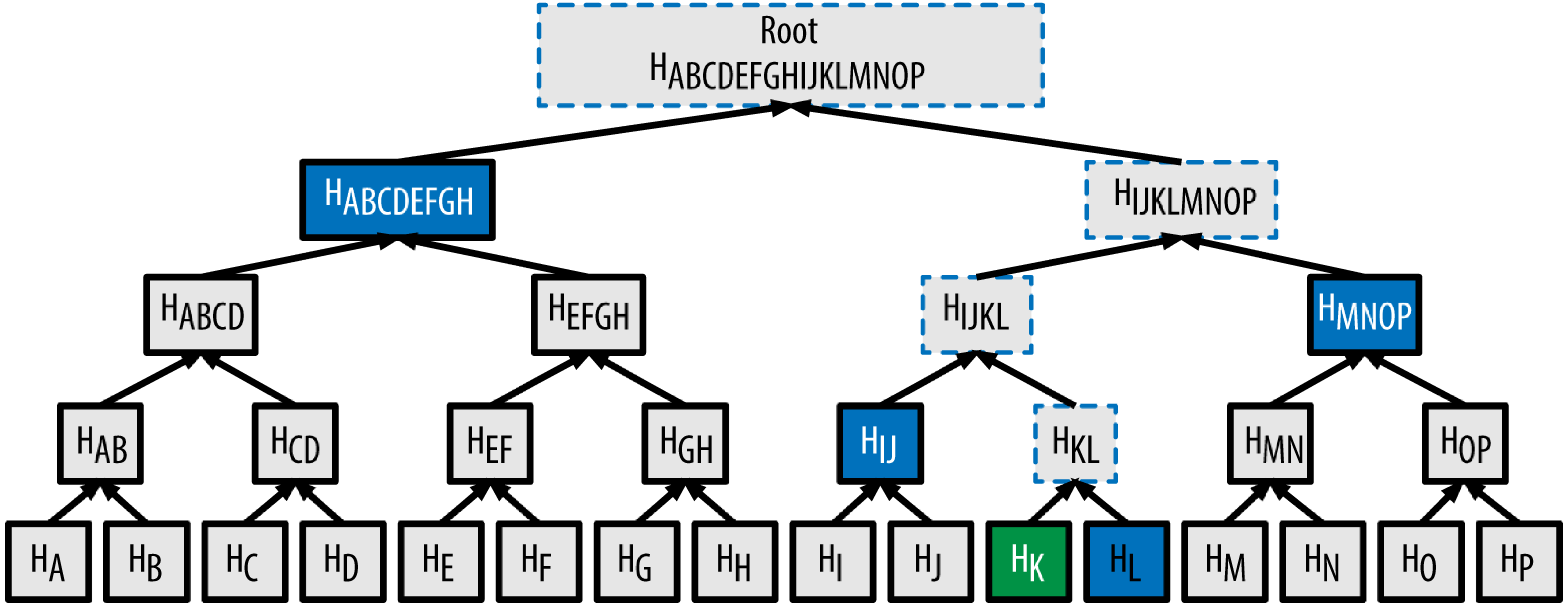
PUBLIC KEY KRÜPTO



https://morr.cc/ikea-algorithms/

Blockchain new?

- Cryptographic signatures
- Public Key Cryptography
- Cryptographic Hash Functions
- Proof-of-work
- Time-Stamping
- **Merkle Trees**
- Byzantine fault tolerance
- Smart contracts


Root
$H_{ABCDEFGHIJKLMNOP}$
$H_{ABCDEFGH}$
$H_{IJKLMNOP}$
H_{ABCD}
H_{EFGH}
H_{IJKL}
H_{MNOP}
H_{AB}
H_{CD}
H_{EF}
H_{GH}
H_{IJ}
H_{KL}
H_{MN}
H_{OP}
H_A
H_B
H_C
H_D
H_E
H_F
H_G
H_H
H_I
H_J
H_K
H_L
H_M
H_N
H_O
H_P

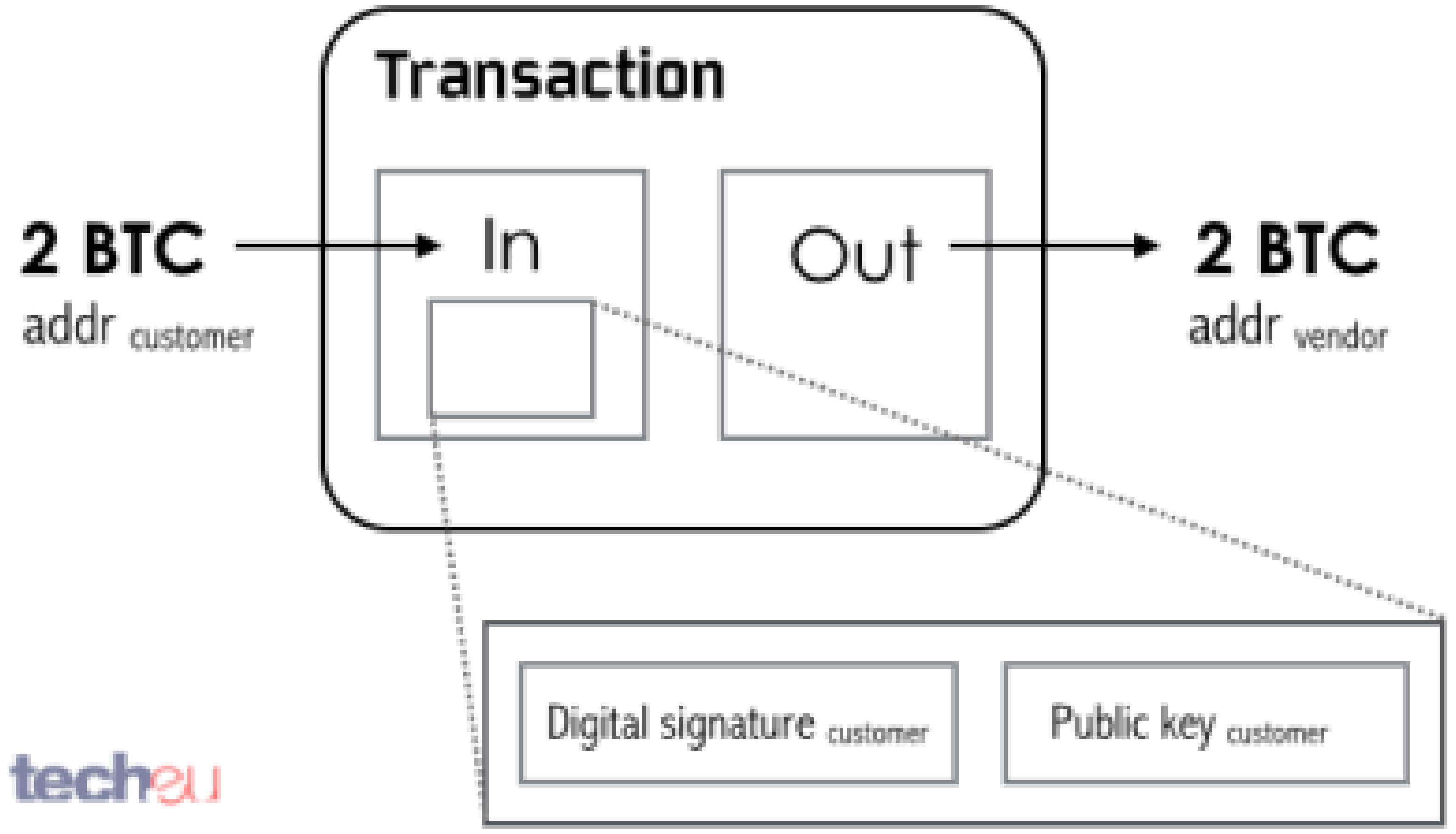
Blockchain new?

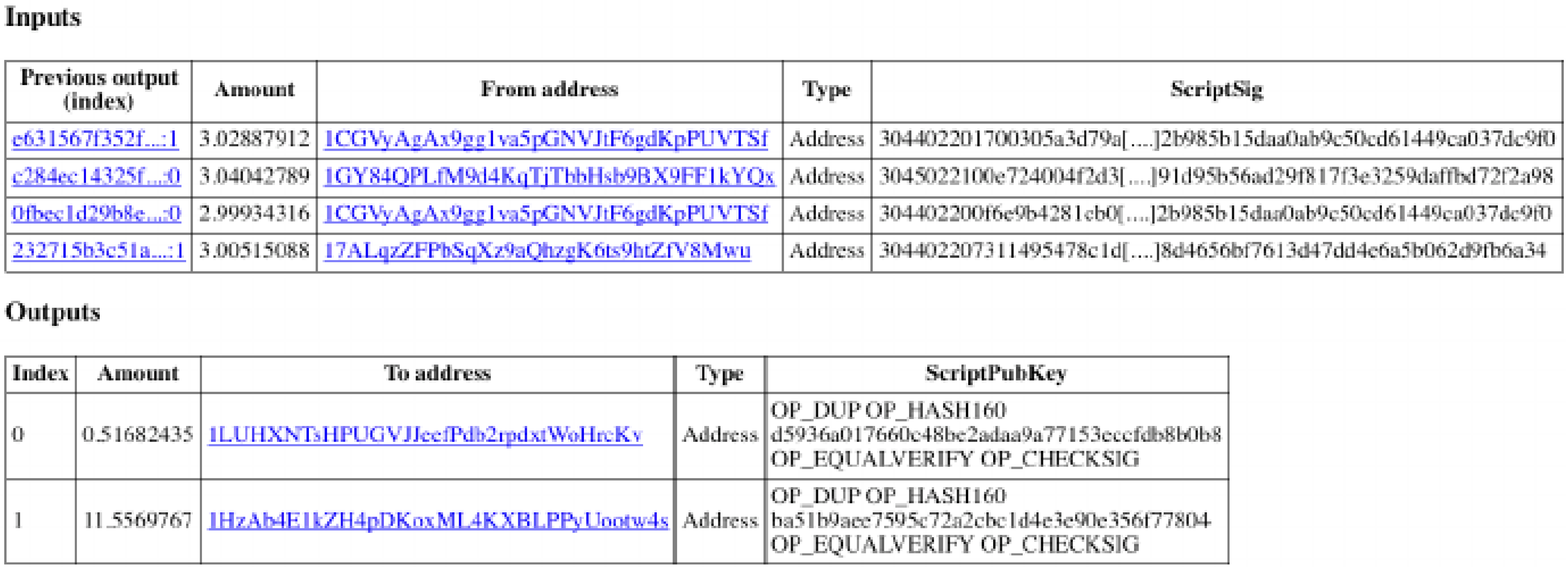
- Cryptographic signatures
- Public Key Cryptography
- Cryptographic Hash Functions
- Proof-of-work
- Time-Stamping
- Merkle Trees
- Byzantine fault tolerance
- **Smart contracts**

Blockchain new?

- **Cryptographic signatures**
- **Public Key Cryptography**
- **Cryptographic Hash Functions**
- **Proof-of-work**
- **Time-Stamping**
- **Merkle Trees**
- Byzantine fault tolerance
- Smart contracts

What’s in a transaction?


Transaction
2 BTC
addr customer
In
Out
2 BTC
addr vendor
Digital signature customer
Public key customer



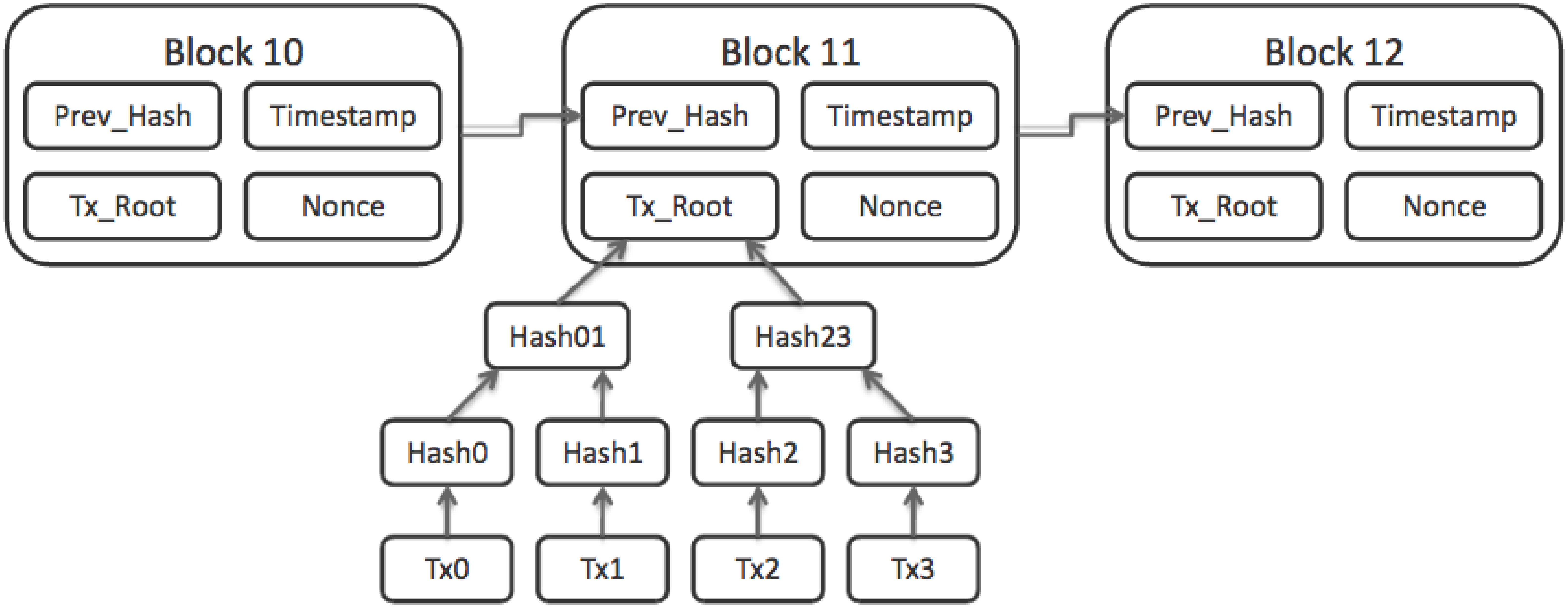
Inputs

Previous output (index)	Amount	From address	Type	ScriptSig
e631567f352f...:1	3.02887912	1CGVyAgAx9gg1va5pGNVJtF6gdKpPUVTSf	Address	304402201700305a3d79a[....]2b985b15daa0ab9c50cd61449ca037dc9f0
c284ec14325f...:0	3.04042789	1GY84QPLfM9d4KqTjTbbHsb9BX9FF1kYQx	Address	3045022100e724004f2d3[....]91d95b56ad29f817f3e3259daffbd72f2a98
0fbec1d29b8e...:0	2.99934316	1CGVyAgAx9gg1va5pGNVJtF6gdKpPUVTSf	Address	304402200f6e9b4281cb0[....]2b985b15daa0ab9c50cd61449ca037dc9f0
232715b3c51a...:1	3.00515088	17ALqzZFPhSqXz9aQhzgK6ts9htZfV8Mwu	Address	3044022073114954 78c1d[....]8d4656bf7613d47dd4e6a5b062d9fb6a34

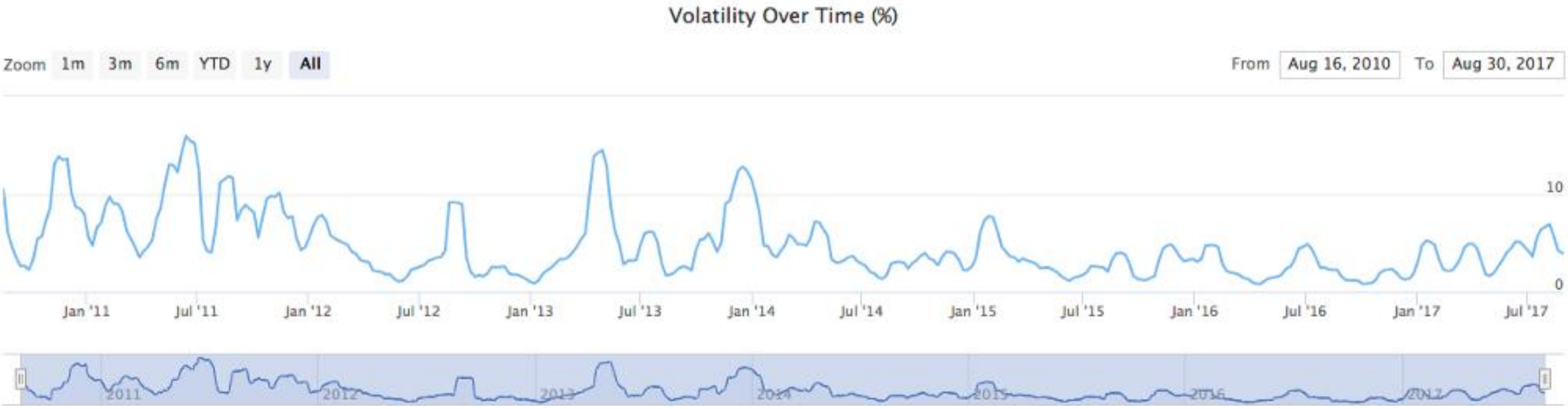
Outputs

Index	Amount	To address	Type	ScriptPubKey
0	0.51682435	1LUHXNTsHPUGVJJeefPdb2rpdxtWoHrcKv	Address	OP_DUP OP_HASH160 d5936a017660c48be2adaa9a77153eccfdb8b0b8 OP_EQUALVERIFY OP_CHECKSIG
1	11.5569767	1HzAb4E1kZH4pDKoxML4KXBLPPyUootw4s	Address	OP_DUP OP_HASH160 ba51b9aee7595c72a2cbc1d4e3e90e356f77804 OP_EQUALVERIFY OP_CHECKSIG

What’s in a block?

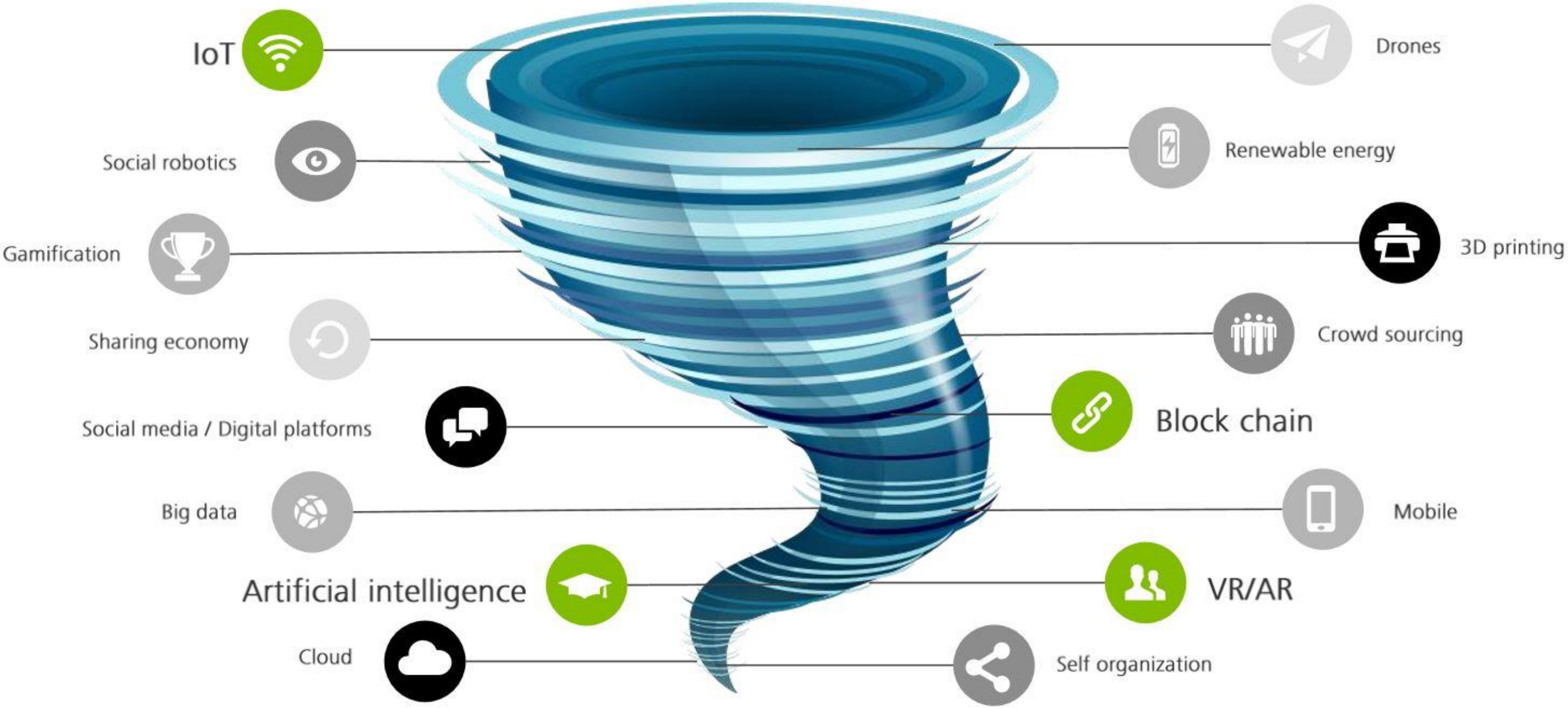

Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Future of Blockchain



From Aug 16, 2010 To Aug 30, 2017

Bitcoin’s volatility over time against the US Dollar. Source: https://bitvol.info/

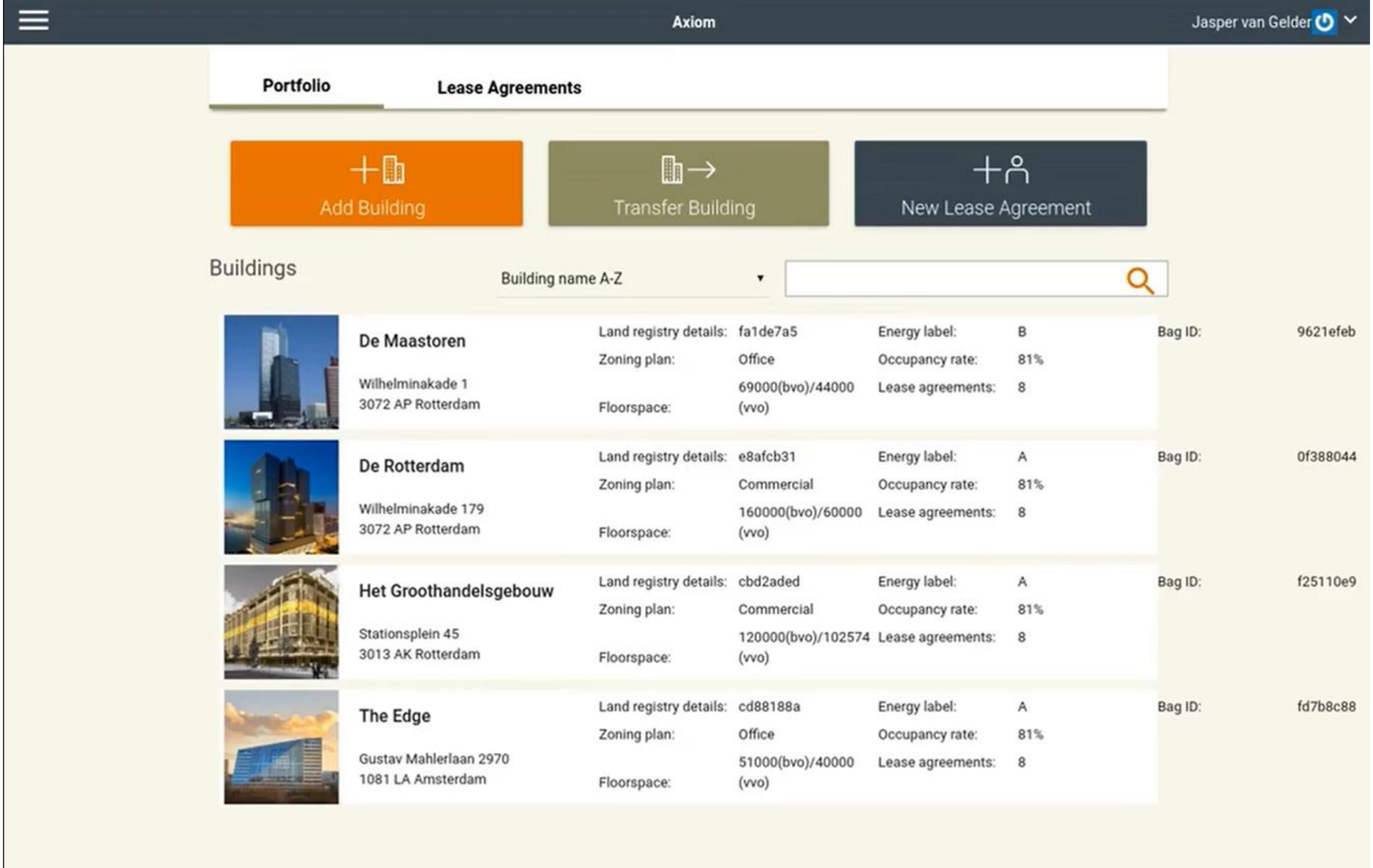

IoT
Drones
Social robotics
Renewable energy
Gamification
3D printing
Sharing economy
Crowd sourcing
Social media / Digital platforms
Block chain
Big data
Mobile
Artificial intelligence
VR/AR
Cloud
Self organization

Current risks

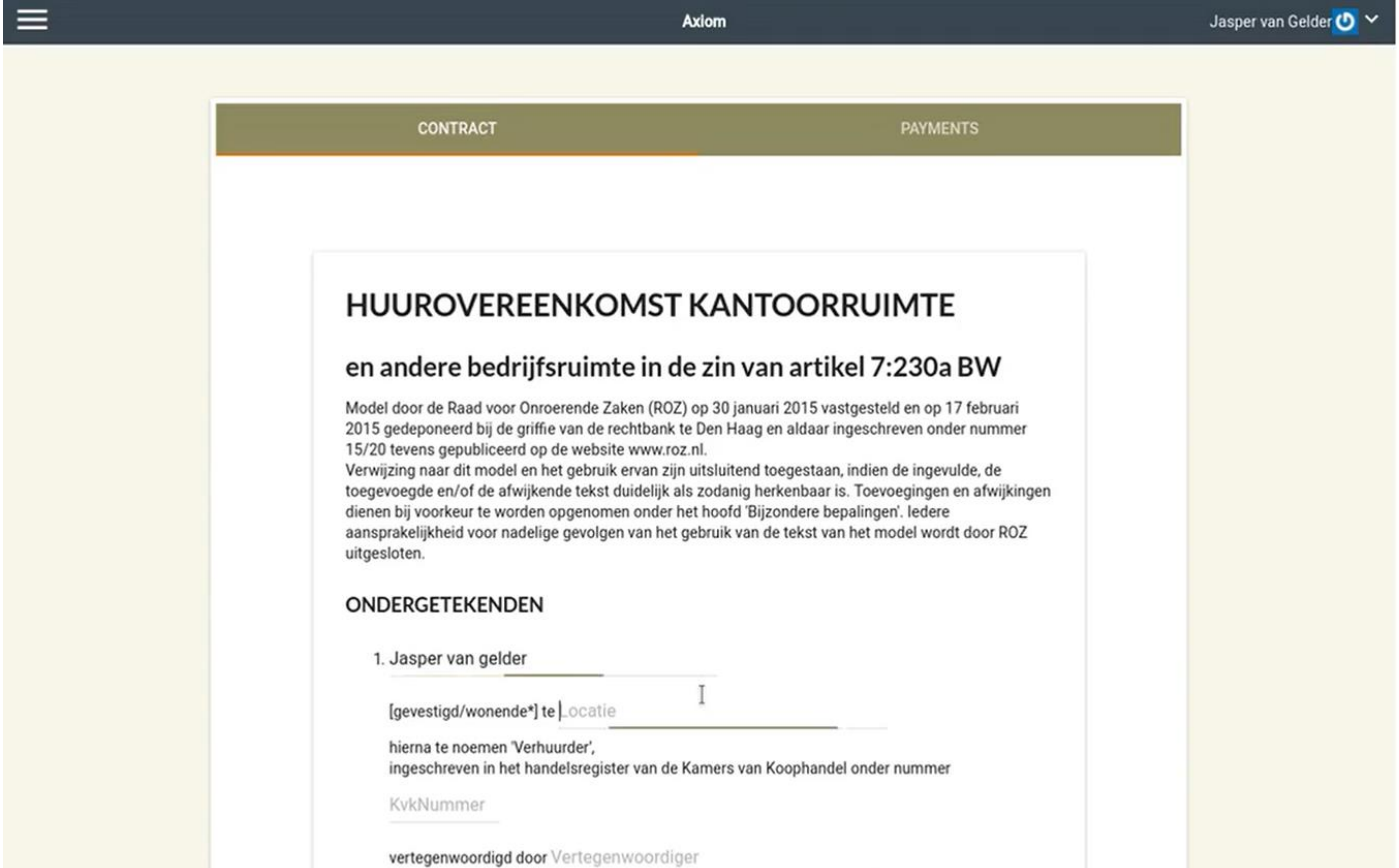
- Smart contracts used for ICO’s
- Speculation bubble
- Lack of real world applications

Current opportunities

- Ample room for innovation in the application space
- Next to no consumer (end-user) applications
- Pick what’s applicable to your problem



De Maastoren Wilhelminakade 1 3072 AP Rotterdam	Land registry details: Zoning plan: Floorspace:	fa1de7a5 Office 69000(bvo)/44000 (vvo)	Energy label: Occupancy rate: Lease agreements:	B 81% 8	Bag ID:	9621efeb
De Rotterdam Wilhelminakade 179 3072 AP Rotterdam	Land registry details: Zoning plan: Floorspace:	e8afcb31 Commercial 160000(bvo)/60000 (vvo)	Energy label: Occupancy rate: Lease agreements:	A 81% 8	Bag ID:	0f388044
Het Groothandelsgebouw Stationsplein 45 3013 AK Rotterdam	Land registry details: Zoning plan: Floorspace:	cbd2aded Commercial 120000(bvo)/102574 (vvo)	Energy label: Occupancy rate: Lease agreements:	A 81% 8	Bag ID:	f25110e9
The Edge Gustav Mahlerlaan 2970 1081 LA Amsterdam	Land registry details: Zoning plan: Floorspace:	cd88188a Office 51000(bvo)/40000 (vvo)	Energy label: Occupancy rate: Lease agreements:	A 81% 8	Bag ID:	fd7b8c88



HUUROVEREENKOMST KANTOORRUIMTE

en andere bedrijfsruimte in de zin van artikel 7:230a BW

Model door de Raad voor Onroerende Zaken (ROZ) op 30 januari 2015 vastgesteld en op 17 februari 2015 gedeponeerd bij de griffie van de rechtbank te Den Haag en aldaar ingeschreven onder nummer 15/20 tevens gepubliceerd op de website www.roz.nl.
Verwijzing naar dit model en het gebruik ervan zijn uitsluitend toegestaan, indien de ingevulde, de toegevoegde en/of de afwijkende tekst duidelijk als zodanig herkenbaar is. Toevoegingen en afwijkingen dienen bij voorkeur te worden opgenomen onder het hoofd 'Bijzondere bepalingen'. Iedere aansprakelijkheid voor nadelige gevolgen van het gebruik van de tekst van het model wordt door ROZ uitgesloten.

ONDERGETEKENDEN

1. Jasper van gelder

[gevestigd/wonende*] te Locatie

hierna te noemen 'Verhuurder',
ingeschreven in het handelsregister van de Kamers van Koophandel onder nummer

KvkNummer

vertegenwoordigd door Vertegenwoordiger

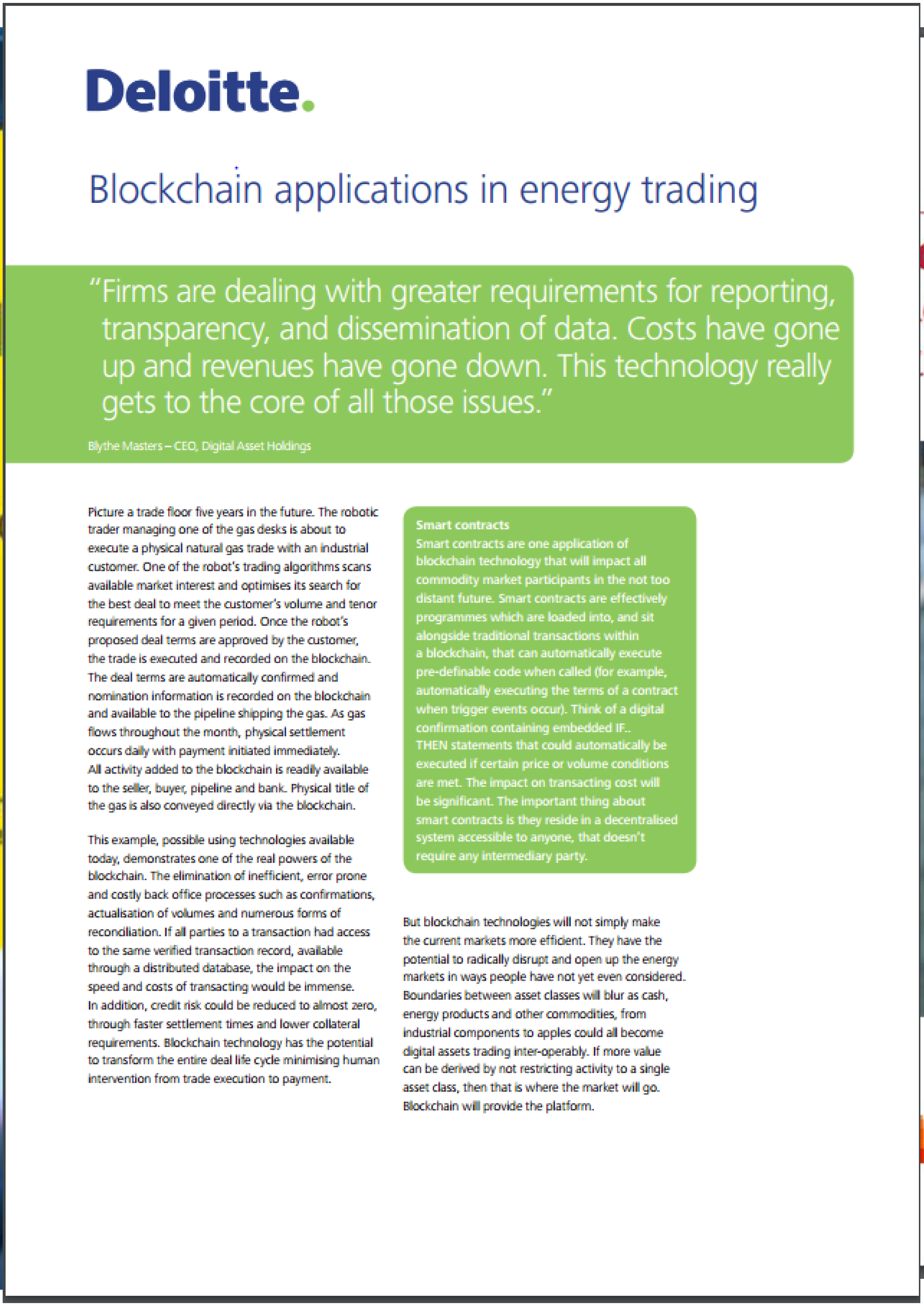
What will you do?

Energy, commod
blockchain

North American Power Cre
(NAPCO) conference

February 10, 2017

These slides are for educational purposes only ar
should not be relied upon, as advice. The views e
are not necessarily those of Ernst & Young LLP.



Deloitte.

Blockchain applications in energy trading

> "Firms are dealing with greater requirements for reporting, transparency, and dissemination of data. Costs have gone up and revenues have gone down. This technology really gets to the core of all those issues."

Blythe Masters – CEO, Digital Asset Holdings

Picture a trade floor five years in the future. The robotic trader managing one of the gas desks is about to execute a physical natural gas trade with an industrial customer. One of the robot's trading algorithms scans available market interest and optimises its search for the best deal to meet the customer's volume and tenor requirements for a given period. Once the robot's proposed deal terms are approved by the customer, the trade is executed and recorded on the blockchain. The deal terms are automatically confirmed and nomination information is recorded on the blockchain and available to the pipeline shipping the gas. As gas flows throughout the month, physical settlement occurs daily with payment initiated immediately.
All activity added to the blockchain is readily available to the seller, buyer, pipeline and bank. Physical title of the gas is also conveyed directly via the blockchain.

This example, possible using technologies available today, demonstrates one of the real powers of the blockchain. The elimination of inefficient, error prone and costly back office processes such as confirmations, actualisation of volumes and numerous forms of reconciliation. If all parties to a transaction had access to the same verified transaction record, available through a distributed database, the impact on the speed and costs of transacting would be immense.
In addition, credit risk could be reduced to almost zero, through faster settlement times and lower collateral requirements. Blockchain technology has the potential to transform the entire deal life cycle minimising human intervention from trade execution to payment.

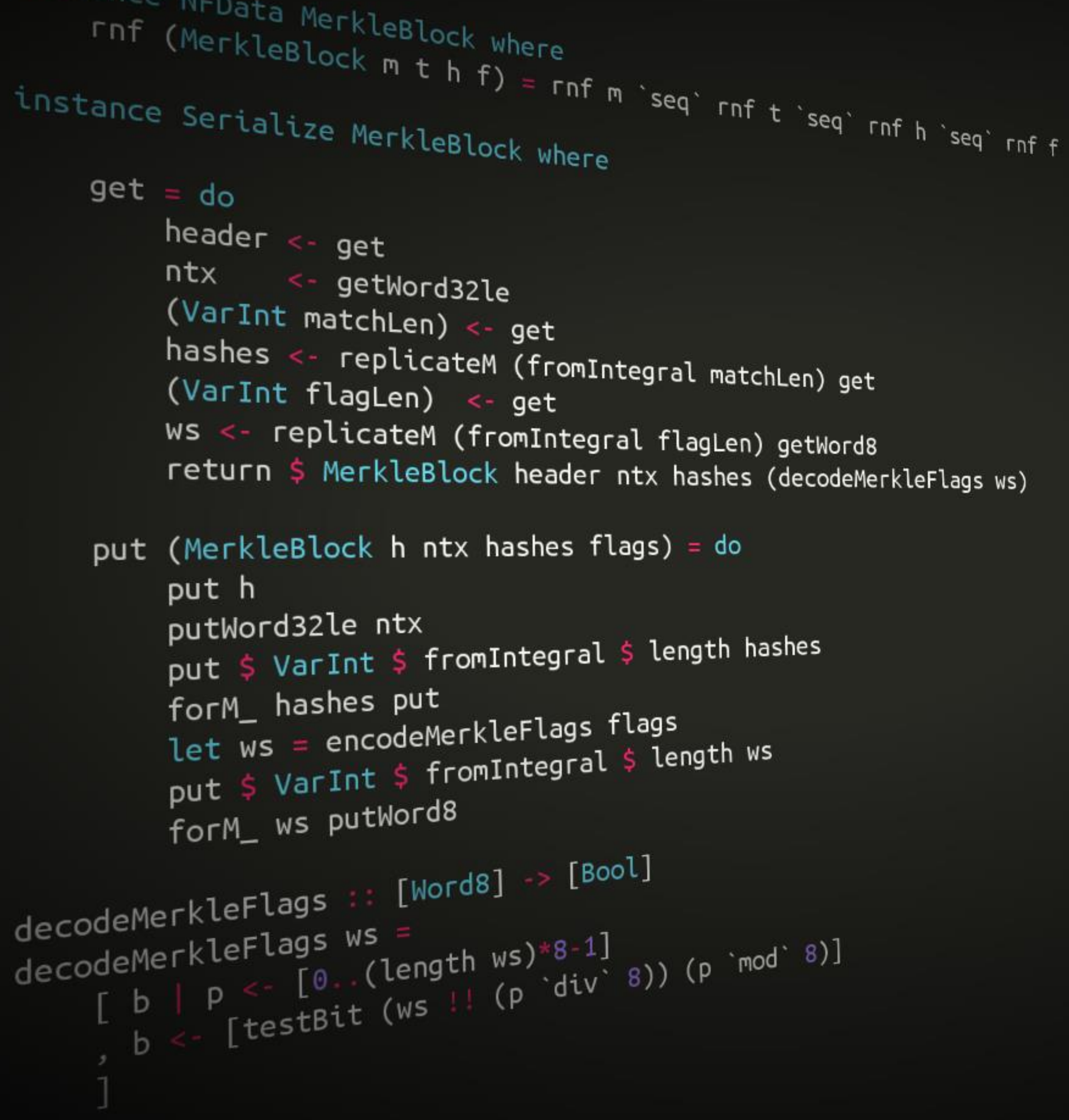
Smart contracts
Smart contracts are one application of blockchain technology that will impact all commodity market participants in the not too distant future. Smart contracts are effectively programmes which are loaded into, and sit alongside traditional transactions within a blockchain, that can automatically execute pre-definable code when called (for example, automatically executing the terms of a contract when trigger events occur). Think of a digital confirmation containing embedded IF.. THEN statements that could automatically be executed if certain price or volume conditions are met. The impact on transacting cost will be significant. The important thing about smart contracts is they reside in a decentralised system accessible to anyone, that doesn't require any intermediary party.

But blockchain technologies will not simply make the current markets more efficient. They have the potential to radically disrupt and open up the energy markets in ways people have not yet even considered. Boundaries between asset classes will blur as cash, energy products and other commodities, from industrial components to apples could all become digital assets trading inter-operably. If more value can be derived by not restricting activity to a single asset class, then that is where the market will go. Blockchain will provide the platform.

PwC global power & utilities

chain – an opportunity
ergy producers and
mers?

www.pwc.com/utilities



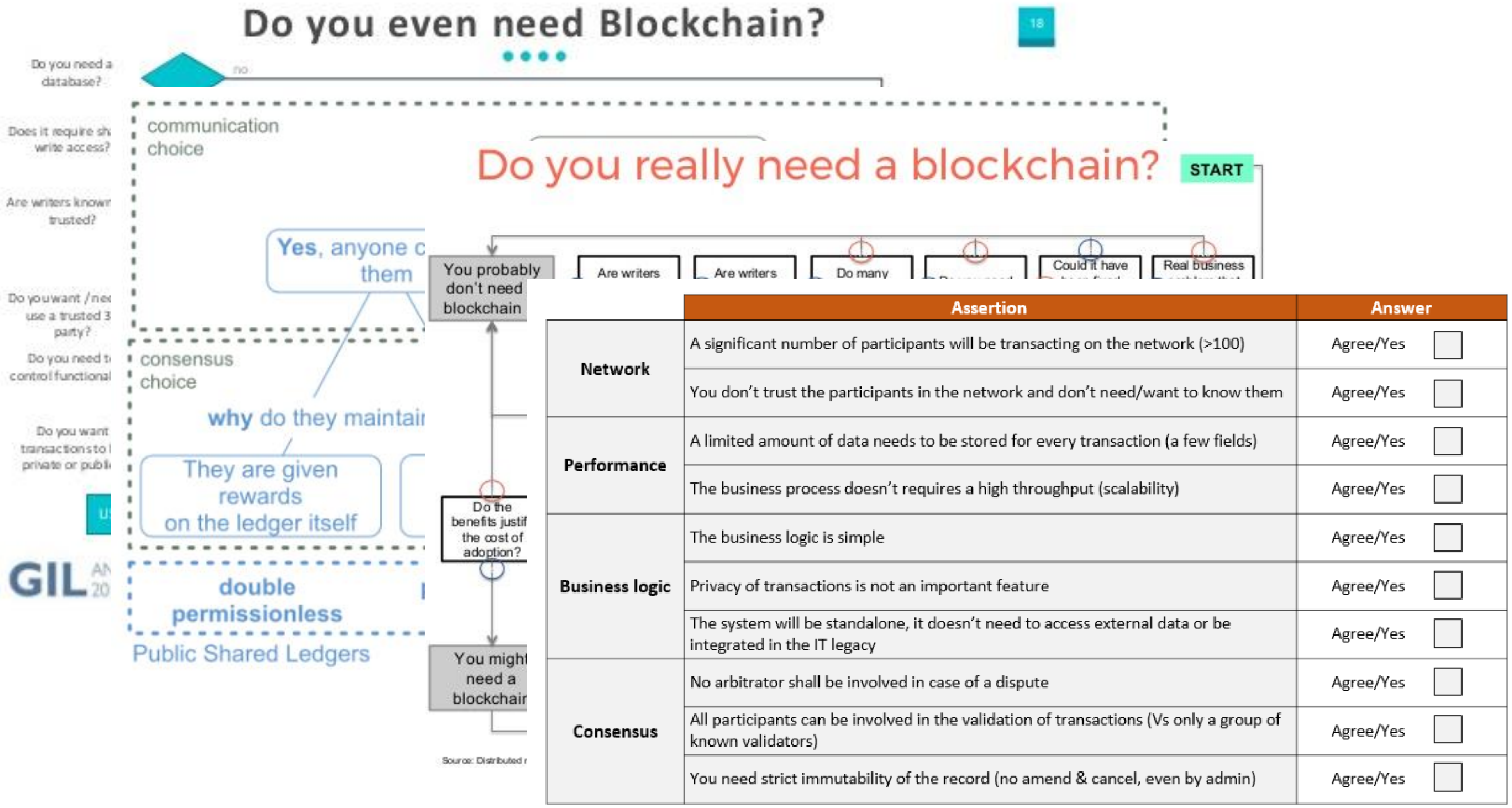
```haskell
    NFData MerkleBlock where
    rnf (MerkleBlock m t h f) = rnf m `seq` rnf t `seq` rnf h `seq` rnf f

instance Serialize MerkleBlock where

    get = do
        header <- get
        ntx    <- getWord32le
        (VarInt matchLen) <- get
        hashes <- replicateM (fromIntegral matchLen) get
        (VarInt flagLen)  <- get
        ws <- replicateM (fromIntegral flagLen) getWord8
        return $ MerkleBlock header ntx hashes (decodeMerkleFlags ws)

    put (MerkleBlock h ntx hashes flags) = do
        put h
        putWord32le ntx
        put $ VarInt $ fromIntegral $ length hashes
        forM_ hashes put
        let ws = encodeMerkleFlags flags
        put $ VarInt $ fromIntegral $ length ws
        forM_ ws putWord8

decodeMerkleFlags :: [Word8] -> [Bool]
decodeMerkleFlags ws =
    [ b | p <- [0..(length ws)*8-1]
    , b <- [testBit (ws !! (p `div` 8)) (p `mod` 8)]
    ]
```


Do you even need Blockchain?
18
Do you need a database?
no
Does it require sh write access?
Are writers known trusted?
Do you want / nee use a trusted 3 party?
Do you need t control functional
Do you want transactions to private or publ
GIL
communication choice
Yes, anyone c them
consensus choice
why do they maintai
They are given rewards on the ledger itself
double permissionless
Public Shared Ledgers
Do you really need a blockchain?
START
You probably don't need blockchain
Are writers
Are writers
Do many
Could it have
Real business
Do the benefits justif the cost of adoption?
You might need a blockchair
Source: Distributed r

	Assertion	Answer
Network	A significant number of participants will be transacting on the network (>100)	Agree/Yes □
	You don't trust the participants in the network and don't need/want to know them	Agree/Yes □
Performance	A limited amount of data needs to be stored for every transaction (a few fields)	Agree/Yes □
	The business process doesn't requires a high throughput (scalability)	Agree/Yes □
Business logic	The business logic is simple	Agree/Yes □
	Privacy of transactions is not an important feature	Agree/Yes □
	The system will be standalone, it doesn't need to access external data or be integrated in the IT legacy	Agree/Yes □
Consensus	No arbitrator shall be involved in case of a dispute	Agree/Yes □
	All participants can be involved in the validation of transactions (Vs only a group of known validators)	Agree/Yes □
	You need strict immutability of the record (no amend & cancel, even by admin)	Agree/Yes □

HOLDER

Thanks

HOLDER

Jeroen Bulters

06 – 55 71 71 51

jeroen@holder.nl