Blockchain and other distributed ledgers

VNO-NCW | 9 October 2018

prof.dr. Eddy Vaassen RA

Tilburg University | Erasmus University Rotterdam | BDO

Jheronimus Academy of Data Science

Program

- Blockchain: the technology underlying cryptocurrencies
- Other distributed ledgers
- Use Cases beyond cryptocurrencies

Blockchain

- Blockchain technology is the technology underlying the Bitcoin, Ether, Bitcoin Cash, and other (over 3000) cryptocurrencies
- A blockchain is a distributed database that contains sequentially interlinked ('chained') clusters of transactions ('blocks') with tokens that follow the rules of a specific trust protocol
- A transaction can only be recorded in the blockchain if it has been validated by a majority of the nodes that participate in the network of that blockchain
- Once a transaction is recorded in the blockchain it cannot be removed or altered
- There is not just one blockchain, each cryptocurrency has its own blockchain or its own part of a certain blockchain
- A blockchain is not a substitute for information systems such as ERP, CRM, SCM, or BI; it complements information systems:
  - to enhance reliability
  - to safeguard assets
  - to enforce compliance with applicable laws and regulations
  - to make interactions between members of ecosystems more efficient and effective

The language of blockchain

- Hashing
- Public and private keys
- Digital signatures
- Distributed ledgers
- Mining
- Nodes
- Smart contracts
- Proof-of-work
- Trust protocol
- Peer-to-peer network
- Open source protocol
- Shared single-source-of-truth
- Tokenization
- Oracles

Bitcoin wallets, full nodes, and miners

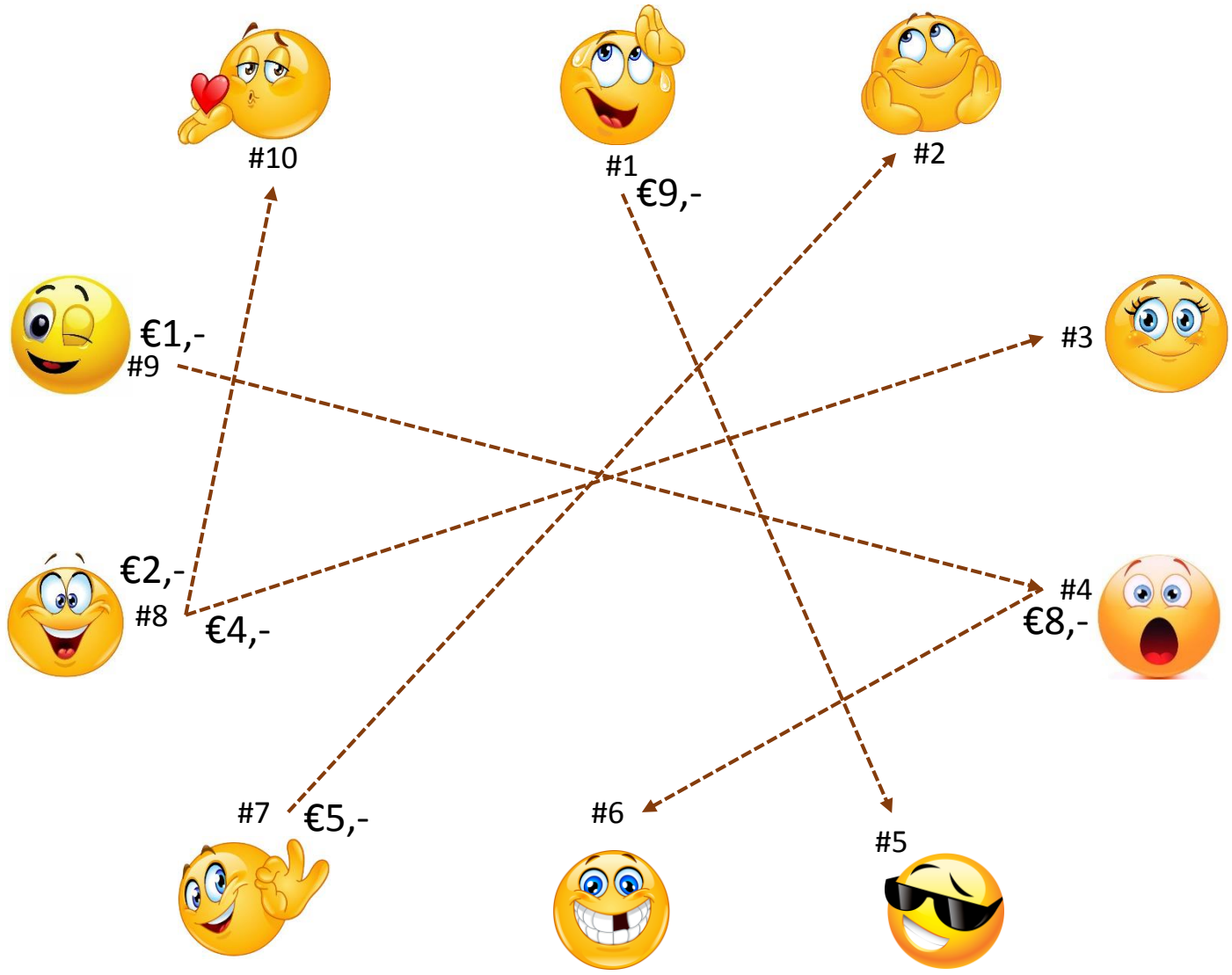
- Wallets just store bitcoins
- Full nodes verify and relay transactions and blocks, and store bitcoins
- Miners verify and validate transactions, create blocks, and store bitcoins

Wallets

Full nodes

Miners

Broadcasting transactions



Transactions

Tx	From	Amount (€)	To
1	#9	1,-	#4
2	#8	2,-	#10
3	#1	9,-	#5
4	#7	5,-	#2
5	#8	4,-	#3
6	#4	8,-	#6

A block in the blockchain

Tx	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
1.1				+1					-1	
1.2								-2		+2
1.3	-9				+9					
1.4		+5					-5			
1.5			+4					-4		
1.6				-8		+8				

Mining serves to make a block immutable
by cryptographically sealing it

Mining

- By mining a block of transactions it is made sure that the block, after it has been written to the blockchain, cannot be changed anymore
- Mining uses hashing
- Hashing is a one-way function: a certain input leads to a certain output, but it is impossible to calculate the input from the output

Example: hashing

1. Take the identification number

RABO 0123456789

2. Add the country code

RABO 0123456789 NL

3. Replace the letters by their number in the alphabet +9 (A=10; B=11;…; Z=35)

RABO 0123456789 NL becomes 2710112401234567892321

4. Add two zeros

271011240123456789232100

*5. Calculate **g mod p** with g*=271011240123456789232100 and p=97, this gives 54

6. Subtract this number from 98

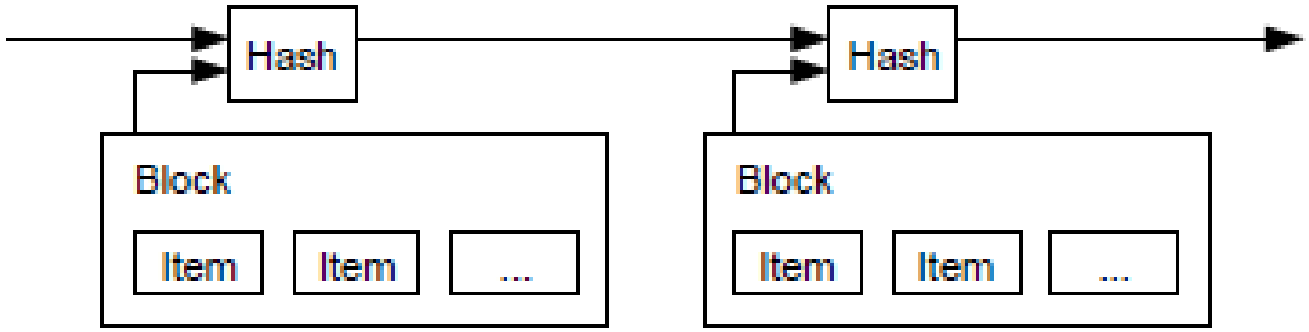
98-54=44 [will always be in the range 1-98]

7. This is the check sum (in the form of a hash)

The IBAN number is: NL44RABO0123456789

http://www.xorbin.com/tools/sha256-hash-calculator

Hashes form the chain



Hashing in the blockchain

Tx	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Bb	10	10	10	10	10	10	10	10	10	10
1.1				+1					-1	
1.2								-2		+2
1.3	-9				+9					
1.4		+5					-5			
1.5			+4					-4		
1.6				-8		+8				
Eb	1	15	14	3	19	18	5	4	9	12

b39667cf64cd5bc6cd7adbfc711cd8446036f9144c1cceb604897b0e824a027d

Hash1 = f(T1.1-T1.6, nonce) = 7dc0b

hash of all the transactions in this block

number used once

The next block

Tx	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Bb	1	15	14	3	19	18	5	4	9	12
2.1	+7		-7							
2.2					+16	-16				
2.3								+2	-2	
2.4	+3			-3						
Eb	11	15	7	0	35	2	5	6	7	12

Hash2 = f(T2.1-T2.4, hash1, nonce)
Hash2 = f(19efe, 7dc0b, 35ea2) = f3e44

And another one

Tx	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Bb	11	15	7	0	35	2	5	6	7	12
3.1	+2					-2				
3.2				+8						-8
Eb	13	15	7	8	35	0	5	4	9	4

Hash3 = f(T3.1-T3.2, hash2, nonce)
Hash3 = f(abdf7, f3e44, 41e69) = cbc39

And so on ...

Proof-of-work

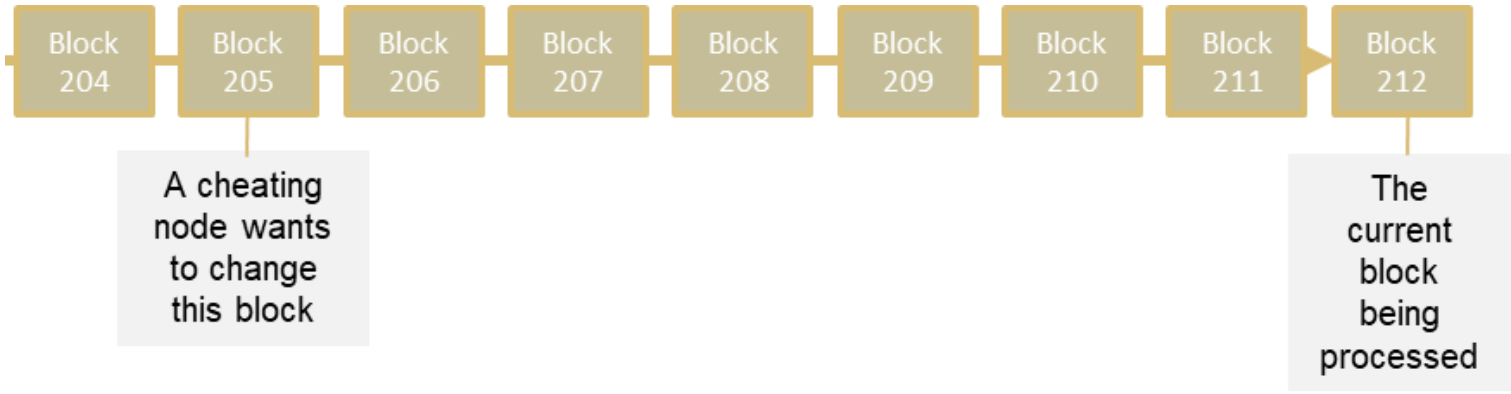
- Writing a block of valid transactions to the blockchain can only be done after proof-of-work allows a node to do so
- The incentive to provide proof-of-work is a prize of 12,5 BTC + some transaction fees
- The prize goes to the node that finds such a nonce that combined with the hash of the previous block, and the hash of all the transactions in the current block gives a hash that is smaller than the (system provided) target hash

Finding the nonce that gives a hash smaller than the target hash can only be done through trial and error (billions of trials)

Checking if a certain number indeed gives a hash smaller than the target hash is a simple calculation

Data quality

- Changing a transaction in a mined block requires redoing the proof-of-work
- The more blocks are mined after the block that contains the transaction a fraudster wants to change the more difficult it is to redo the proof-of-work
- After 6 blocks it is not just difficult, it is impossible to change a transaction in a mined block
- That is why a blockchain is immutable and as a result leads to highly reliable information



Ownership and provenance

- Tokens are the cryptographic representation of (digital or physical) assets
- When in the real world an asset moves from A to B, in the blockchain the token also moves from A to B
- Provenance and ownership can always be determined
- That is why a blockchain can help safeguarding assets

Smart contracts

- Merely pieces of software that execute pre-programmed actions if certain conditions are met
- Can run on a blockchain
- Unstoppable
- Compliance by default
- That is why a blockchain can enforce compliance with applicable laws and regulations

Disintermediation

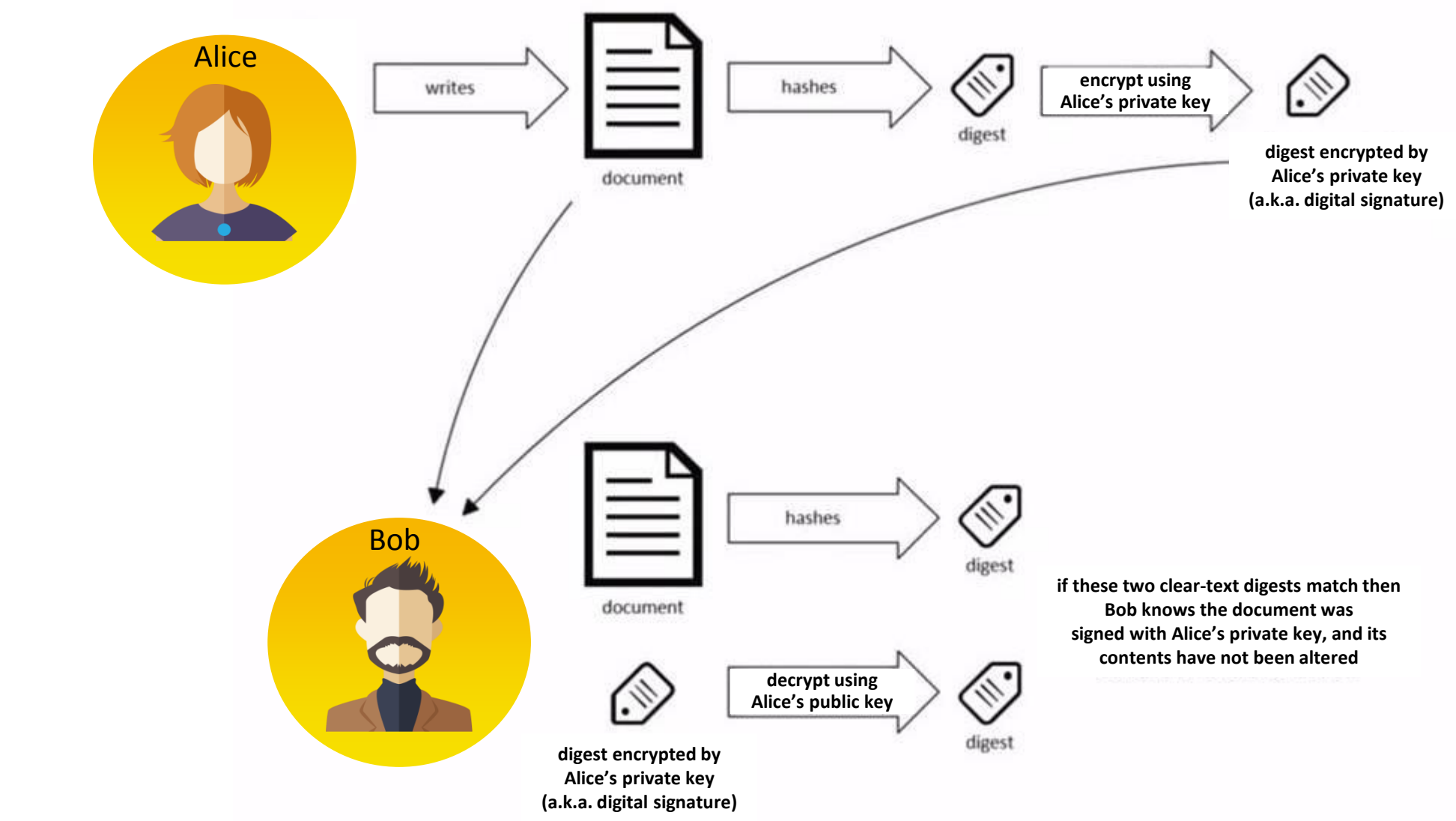
- The trust protocol replaces a trusted third party
- So, disintermediation
- No man-made delays or mistakes
- That is why a blockchain makes interactions between members of ecosystems more efficient and effective

Blocks are cryptographically linked

Digital signatures (1)

- A digital signature is a mathematical scheme for presenting the authenticity of digital messages or documents
- A valid digital signature gives a recipient reason to believe:
  - that the message was created by a known sender (authentication)
  - that the sender cannot deny having sent the message (non-repudiation)
  - that the message was not altered in transit (integrity)
- Digital signatures are added to the digital message or document using private and public keys

Digital signatures (2)



An electronic coin is a chain of digital signatures

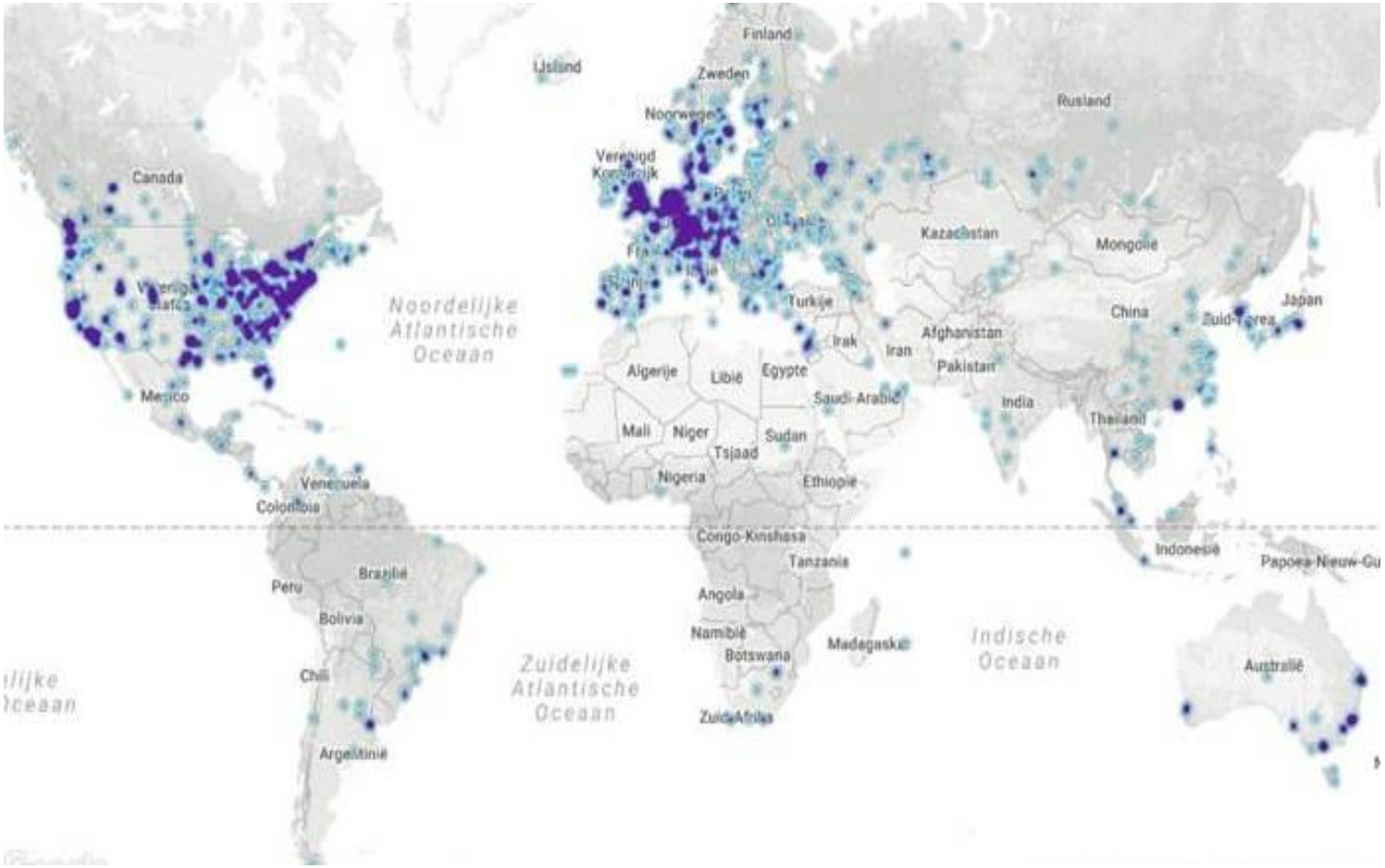
Important conditions for blockchain

1. Shared database
2. Multiple parties who write data to the shared database
3. Those parties are members of different legal or economical entities
4. No or limited trust between these parties
5. No trusted third party possible or desired

Mining farms

A mining farm is a mining node (‘miner’) that has as its business model expending hashing power to find a nonce that gives a hash that is smaller than the target hash

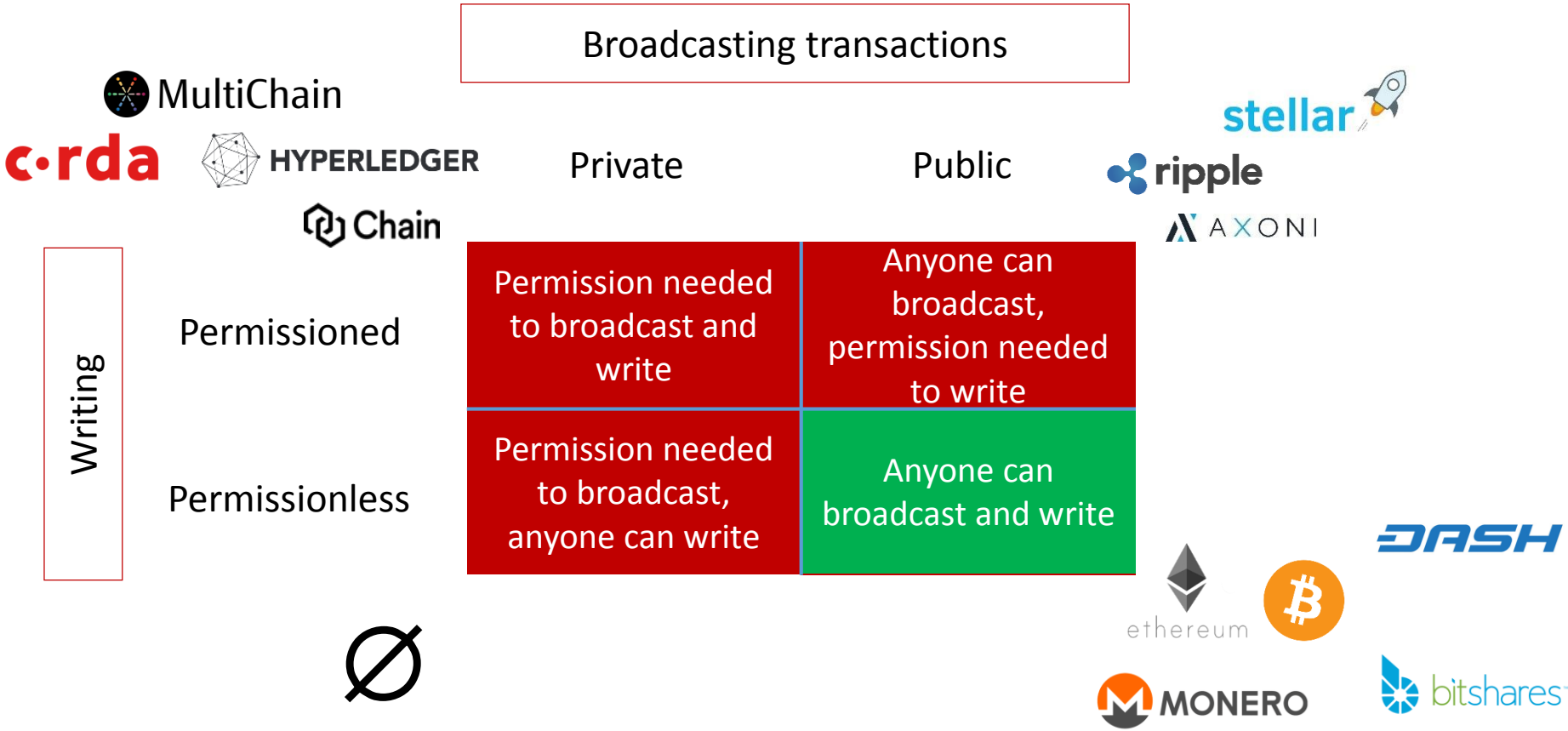
Nodes are all over the world



Reachable nodes as of Sat Apr 28 2018

RANK	COUNTRY	NODES
1	United States	2570 (24.43%)
2	Germany	2041 (19.40%)
3	China	732 (6.96%)
4	France	683 (6.49%)
5	Netherlands	488 (4.64%)
6	United Kingdom	395 (3.76%)
7	Canada	391 (3.72%)
8	Russian Federation	349 (3.32%)
9	n/a	328 (3.12%)
10	Japan	230 (2.19%)
	Total	10519 (100%)

Distributed ledgers



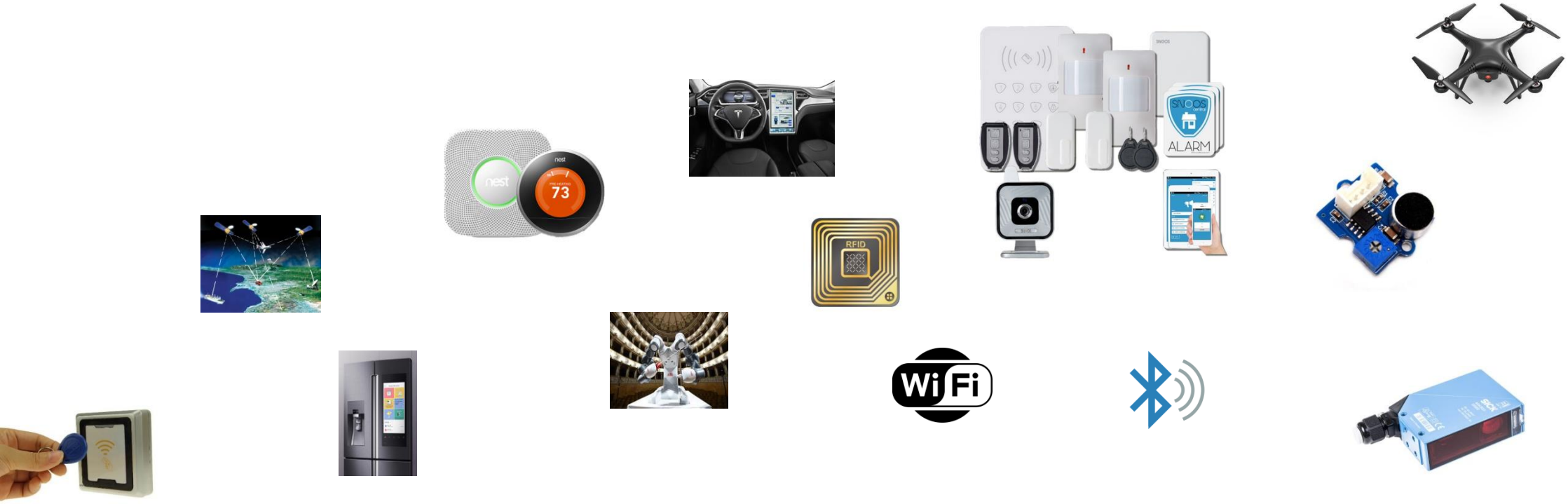
Ethereum

- Ethereum is a decentralized platform for building smart contracts
- These smart contracts run on a blockchain
- Smart contracts can be used for creating markets, registries of debts or obligations, move funds according to instructions that were given in the past (such as in a will or futures contract), or any other application that involves the transfer of physical or virtual assets (including information)
- Ethereum can be considered a platform as a service (PaaS)
- The cryptocurrency is Ether
- The programming language is Solidity

ethereum

Oracles

- An oracle is a tool for making data outside a blockchain network available for that blockchain
- This data triggers smart contract execution when pre-defined conditions (e.g., outside temperature, order receipt, successful payment, a price change) are met



Types of oracle

	Inbound	Outbound
Software	Temperature Inventory level Money receipt Price change Train delay	Send confirmation Place and order Make journal entry Transfer money Populate picking list
Hardware	RFID GPS WiFi Drones Sensors	Switch on heating Open a lock Move a robot Launch a drone Pick goods

Use cases

Use case	Reliability	Safeguarding	Compliance	Efficiency & effectiveness
Land registry	v	v		v
Tickets			v	v
Elections	v		v	v
Track and trace in supply chains		v		v
Electronic markets	v	v		v
Intellectual rights management	v	v	v	v
Licenses			v	v
Personal credentials for job applications	v			v
Zero knowledge range proof for privacy	v		v	v
Liquid assets swapping at banks	v	v		v
Energy exchange		v		v
Triple-entry accounting	v			v

The language of blockchain

- Hashing
- Public and private keys
- Digital signatures
- Distributed ledgers
- Mining
- Nodes
- Smart contracts
- Proof-of-work
- Trust protocol
- Peer-to-peer network
- Open source protocol
- Shared single-source-of-truth
- Tokenization
- Oracles

Takeaways

- Distributed ledger technology (DLT) is the versatile variant of blockchain technology
- Through its versatility DLT has great potential in management, control, audit, finance and oversight regarding the following objectives:
  - Information reliability (for example ‘triple-entry accounting’)
  - Safeguarding of assets (for example ‘supply chains’)
  - Compliance with applicable laws and regulations (for example ‘privacy’)
  - More efficient and effective interactions between members of ecosystems (for example ‘energy’)
- Each user must have a basic understanding of the language of DLT (distributed, mining, hashing, cryptography, smart contracts) to meaningfully and safely interact with the distributed ledger