an introduction to

Blockchain Technology

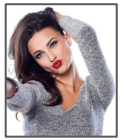
PETER LANGELA

KIVI Engineering Society

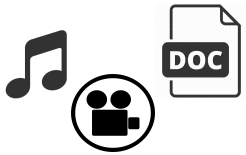
UNIVERSITY OF TWENTE.

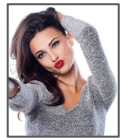
Novel-T innovate & accelerate

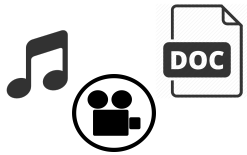
send a photo over the internet



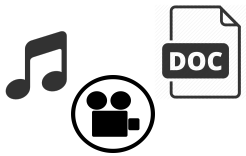
send a photo over the internet



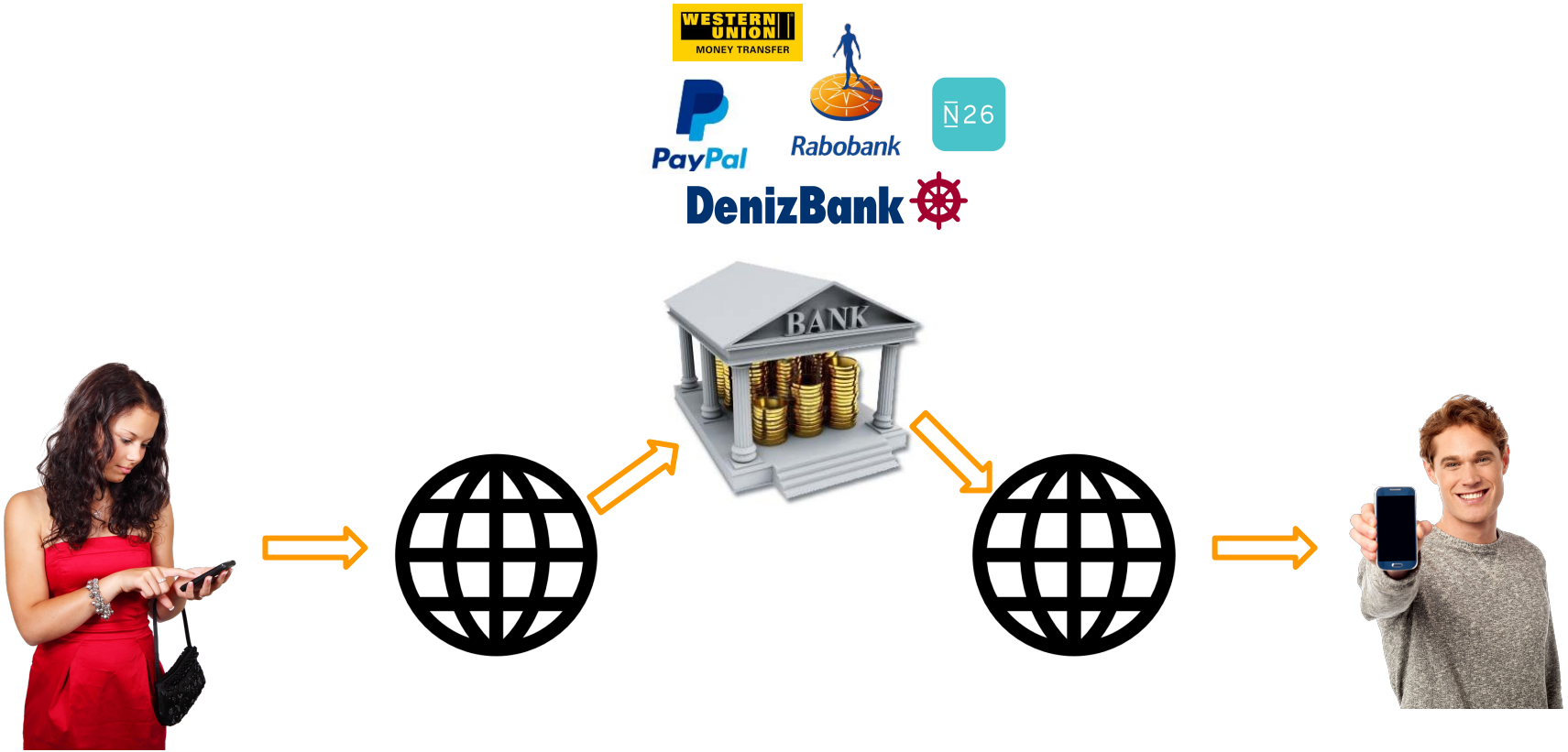




send a photo over the internet



send money over the internet



send money over the internet

billions are excluded

poor people with high risk profiles are internet connected but unbanked: they are banned by banks & financial institutions and cannot send, receive and save money, they cannot purchase and sell online to improve their lives ...

Tapscott, Don & Alex: 'Blockchain Revolution'

in search of the trust protocol

since the 80’s scientists search for digital solutions to solve

- privacy
- security
- inclusion

Financial inclusion

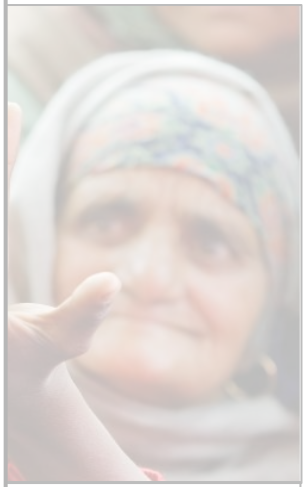
Around 2 billion people don’t use formal financial services and more than 50% of adults in the poorest households are unbanked. Financial inclusion is a key enabler to reducing poverty and boosting prosperity.

in search of the trust protocol

In October 2008 Satoshi Nakamoto published a paper describing the Bitcoin digital currency:

"Bitcoin: A Peer-to-Peer Electronic Cash System"

https://bitcoin.org/bitcoin.pdf



prosperity.

bootstrapping the future

Sathosi Nakamoto's 7 design principles of the blockchain economy

Tapscott, Don & Alex. 'Blockchain Revolution'

1. networked integrity
2. distributed power
3. value as incentive
4. security
5. privacy
6. rights preserved
7. inclusion

bootstrapping the future

Sathosi Nakamoto's 7 design principles of the blockchain economy

Tapscott, Don & Alex. 'Blockchain Revolution'

1. networked integrity

- participants can exchange value directly
- double-spend problem solved

bootstrapping the future

Sathosi Nakamoto's 7 design principles of the blockchain economy

Tapscott, Don & Alex. 'Blockchain Revolution'

2. distributed power

- no single point of control
- no 'middleman' required

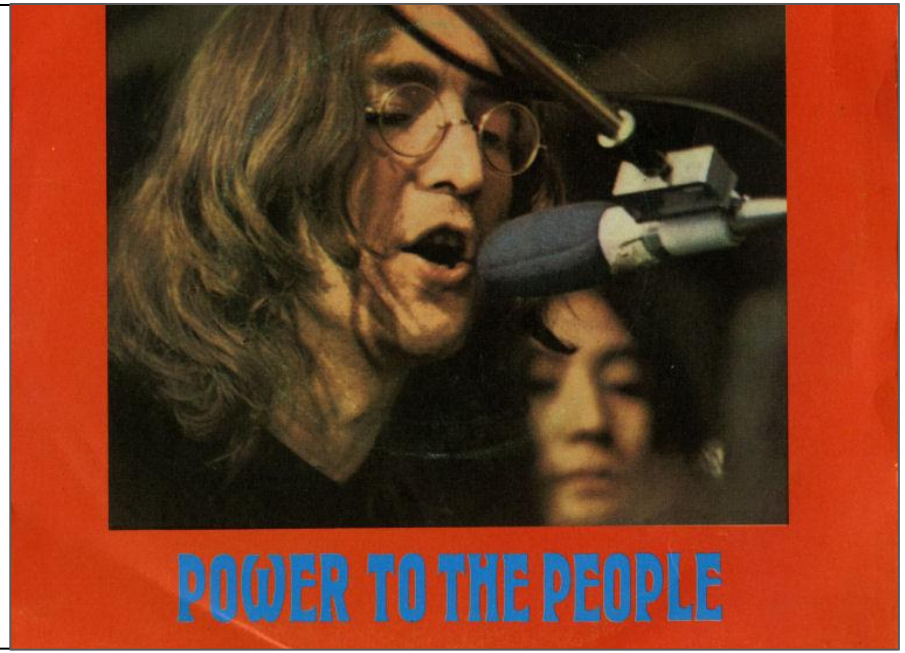
bootstrapping the future

Sathosi Nakamoto's 7 design principles of the blockchain economy

Tapscott, Don & Alex. 'Blockchain Revolution'

3. value as incentive

- reward those who work on it
- no concentration of power
- selfish actions will benefit the system



bootstrapping the future

Sathosi Nakamoto's 7 design principles of the blockchain economy

Tapscott, Don & Alex. 'Blockchain Revolution'

4. security

- cryptography is a must - opting out is no option
- hack proof

bootstrapping the future

Sathosi Nakamoto's 7 design principles of the blockchain economy

Tapscott, Don & Alex. 'Blockchain Revolution'

5. privacy

- people should control their own data
- no honeypots of personal data

bootstrapping the future

Sathosi Nakamoto's 7 design principles of the blockchain economy

Tapscott, Don & Alex. 'Blockchain Revolution'

6. rights preserved

- ownership is transparent
- you can't trade what isn't yours

bootstrapping the future

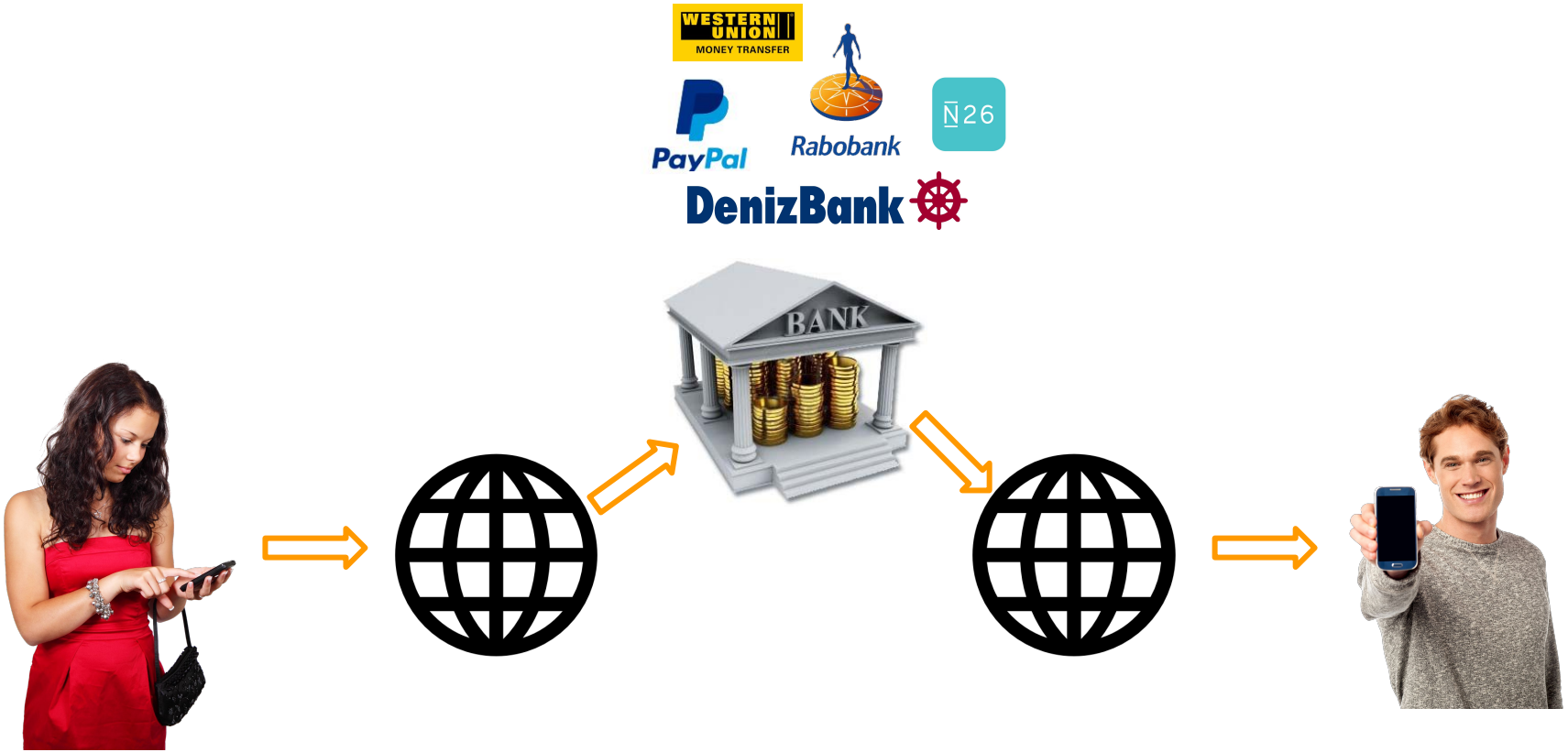
Sathosi Nakamoto's 7 design principles of the blockchain economy

Tapscott, Don & Alex. 'Blockchain Revolution'

7. inclusion

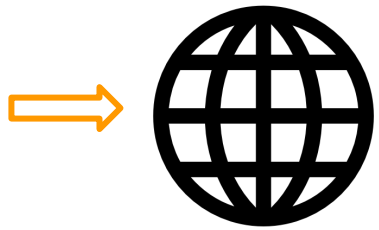
- access for everyone
- simplified payment verification (SPV)

send money over the internet



send money over the internet

no 3rd party needed



send money over the internet

no 3rd party needed

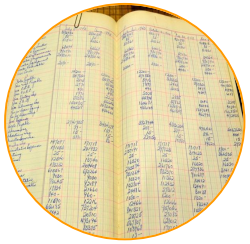
send money over the internet

no 3rd party needed

blockchain

“what the internet is for information is the blockchain for value”

key characteristics



ledger

chronological

ever growing

distributed

immutable

disintermediated

consensus

secure

single source of truth

transparant

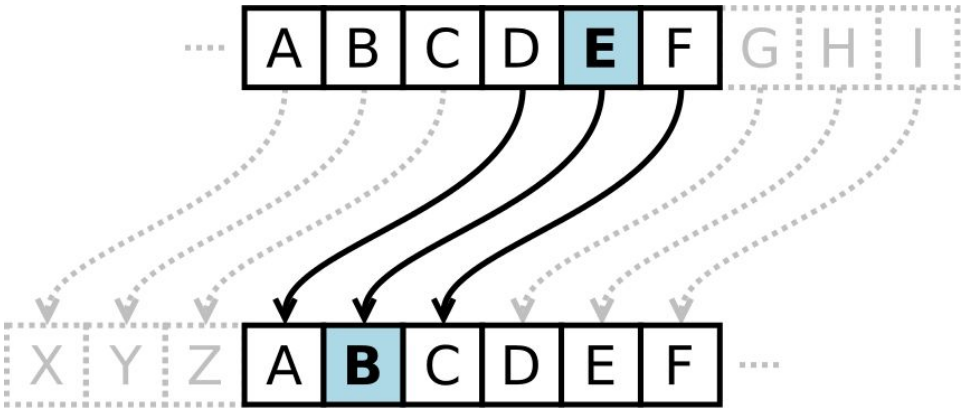
where did the asset came from

how changed the ownership over time

final

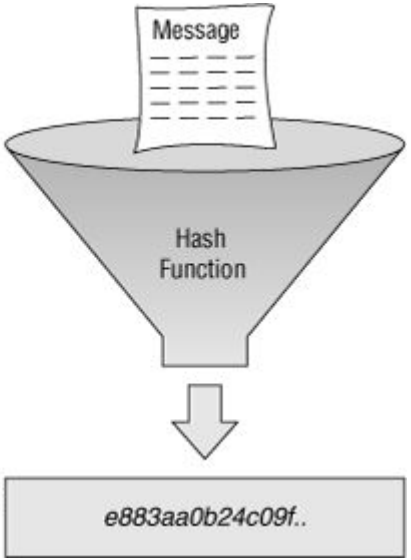
one place to go to determine the ownership of an asset or the completion of a transaction

cryptography



hash

a one-way algorithm to generate a cryptographic key

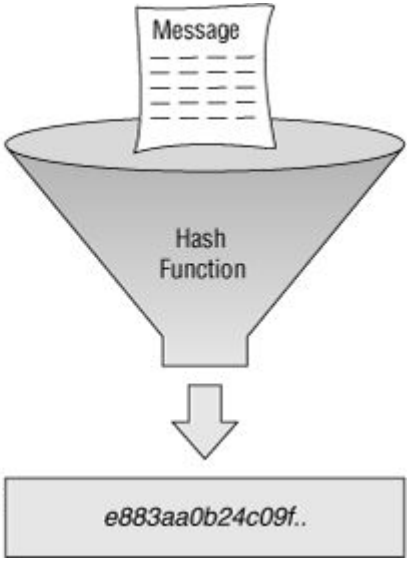


Data: Peter Langela
1962-03-09
Deventer

Hash: 4e456c6a96e1ec0440026081721e6006bc98546c3f4c2aaf8417c599704169e3

hash

a one-way algorithm to generate a cryptographic key



Peter Langela
1962-03-09
Deventer

Data: Peter Langela
1962-03-09
Deventer

Hash: 4e456c6a96e1ec0440026081721e6006bc98546c3f4c2aaf8417c599704169e3

X

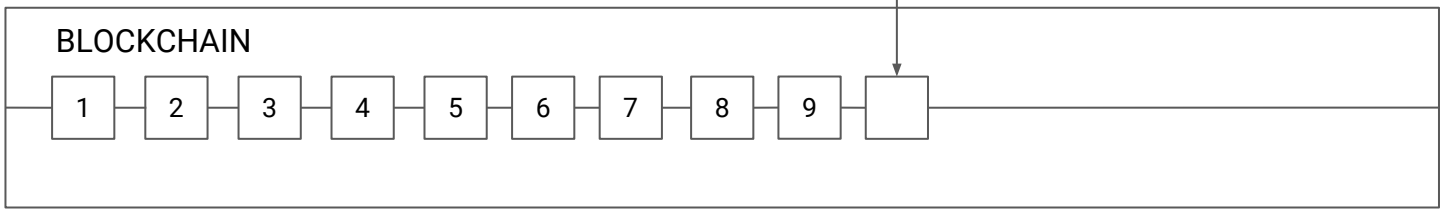
4e456c6a96e1ec044002608
1721e6006bc98546c3f4c2a
af8417c599704169e3

basic block structure

Block:	# 8
Nonce:	46943
Data:	
Prev:	000012fa9b916eb9078f8d98a7864e697ae83ed54f5
Hash:	0000c3756ee71b0422c44e9b784b63a21e931ba0494

Block:	# 9
Nonce:	1969
Data:	
Prev:	0000c3756ee71b0422c44e9b784b63a21e931ba0494
Hash:	00005ca784cbfb3238a9bdb0dd46ecc3a8474813e0e

Block:	# 10
Nonce:	45113
Data:	peter -> karin 100 karin -> inge 50 peter -> inge 50 inge -> peter 75
Prev:	00005ca784cbfb3238a9bdb0dd46ecc3a8474813e0e
Hash:	000012457cd1747a55aa672cb9e5a9884c21b17021e



basic block structure

sequence number →

number used once →

the data to store →

hash of previous block →

hash of this block →

Block: # 8

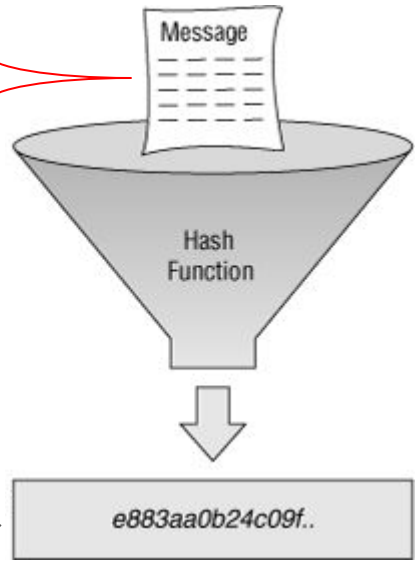
Nonce: 46943

Data:

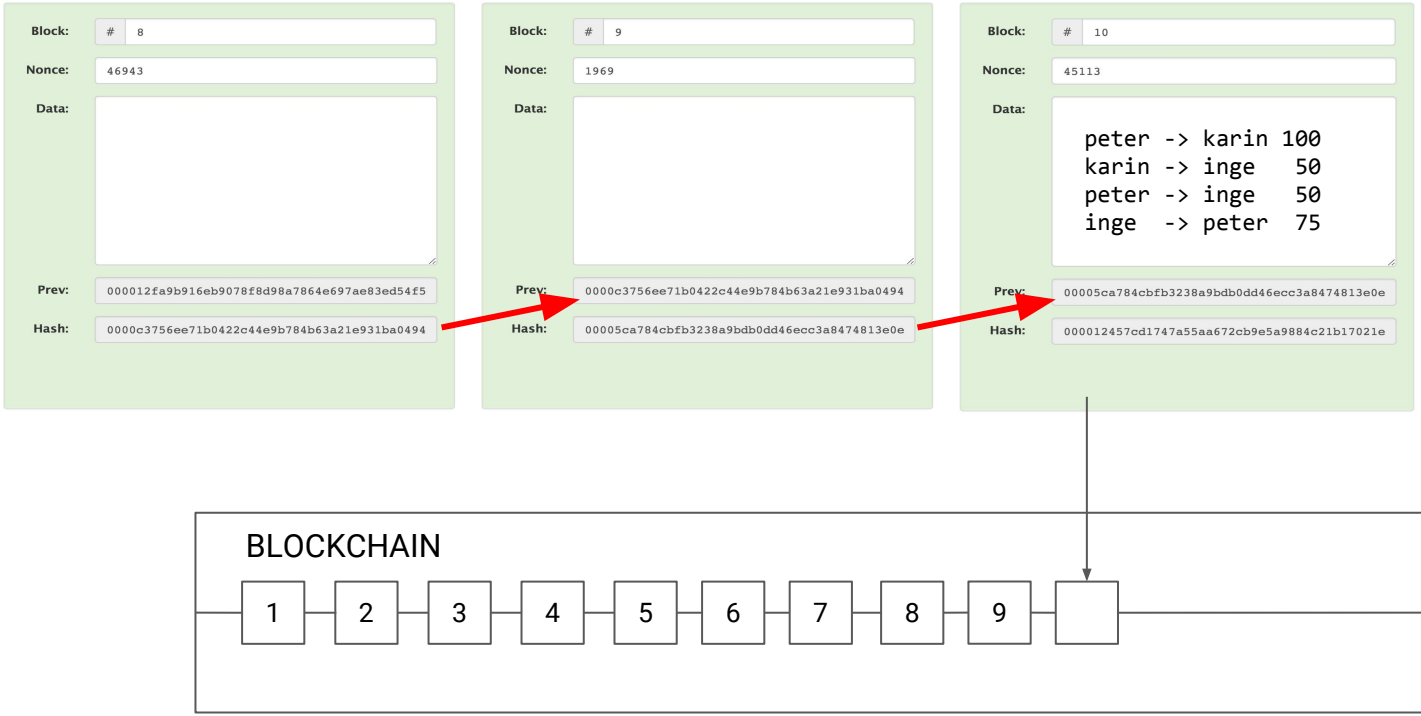
```
peter -> karin 100
karin -> inge   50
peter -> inge   50
inge  -> peter  75
```

Prev: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5

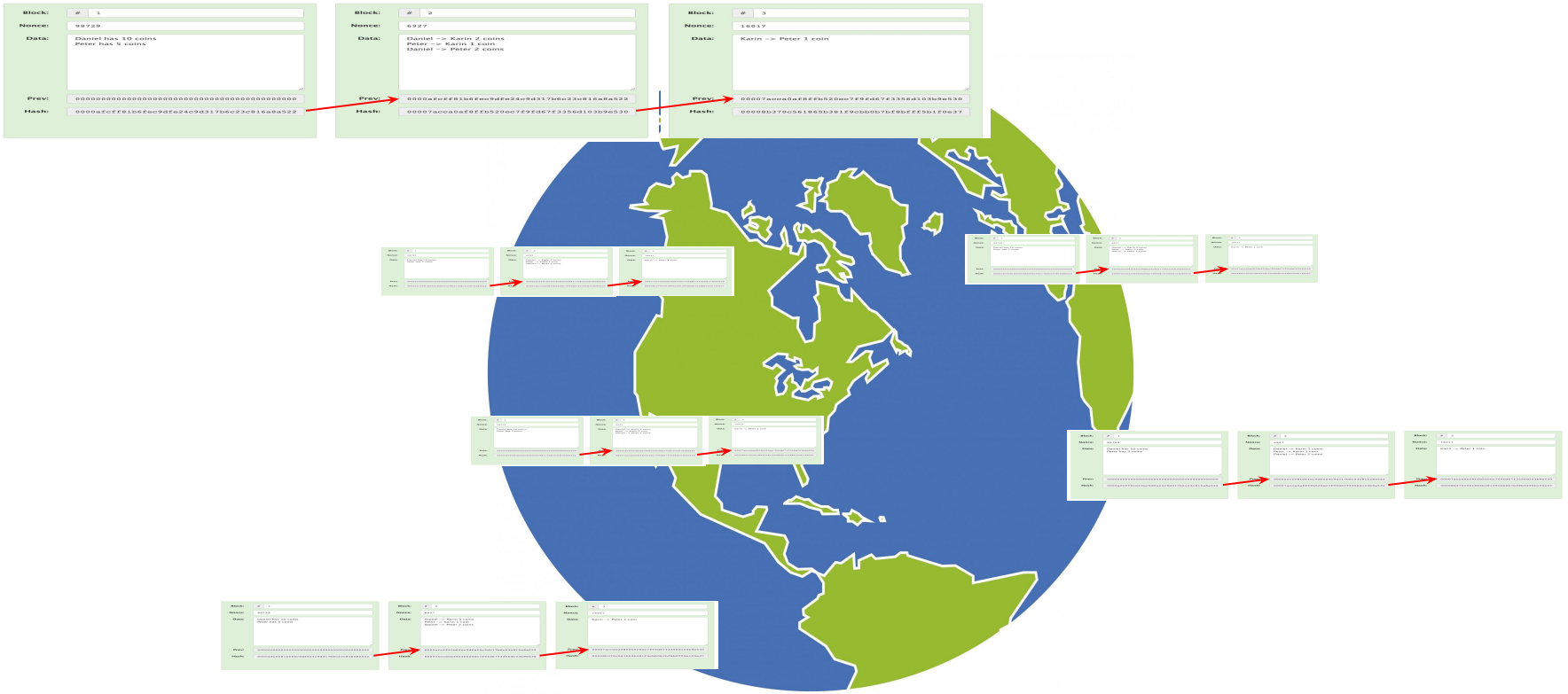
Hash: 0000c3756ee71b0422c44e9b784b63a21e931ba0494



basic block structure



distributed chain of blocks



distributed chain of blocks

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Thu Mar 15 2018 11:18:09 GMT+0100 (CET).

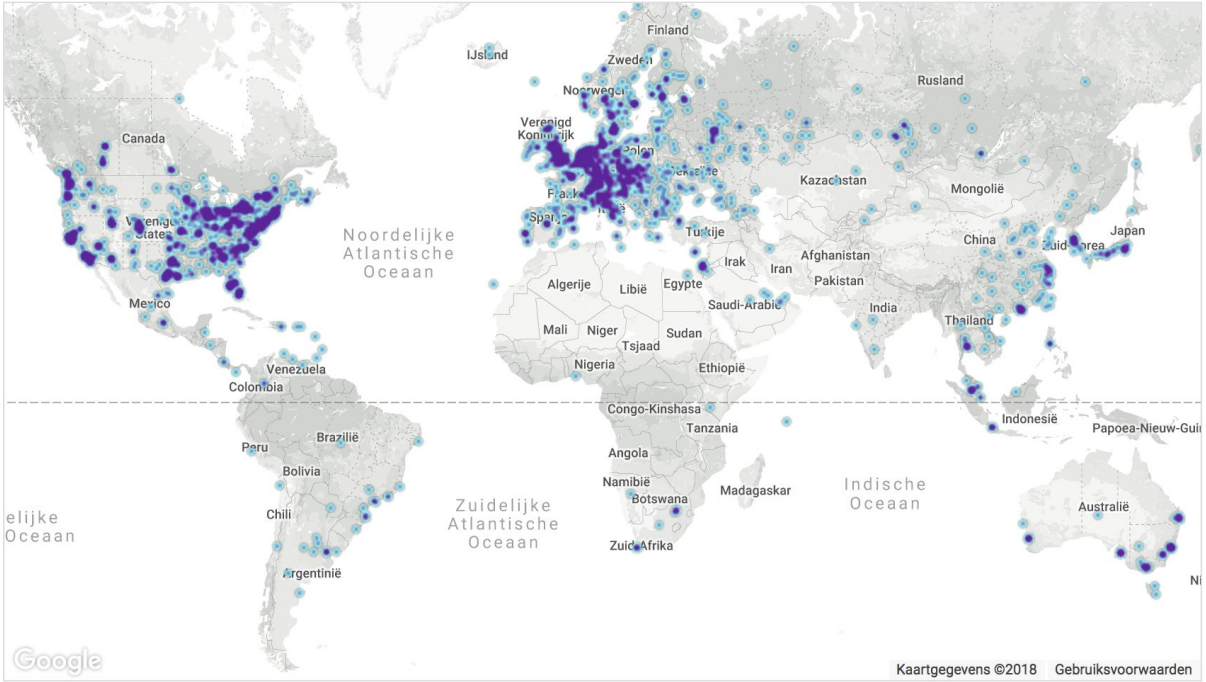
12236 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2694 (22.02%)
2	China	2322 (18.98%)
3	Germany	1962 (16.03%)
4	France	702 (5.74%)
5	Netherlands	482 (3.94%)
6	United Kingdom	405 (3.31%)
7	Canada	396 (3.24%)
8	Russian Federation	359 (2.93%)
9	n/a	288 (2.35%)
10	Singapore	235 (1.92%)

More (101) »

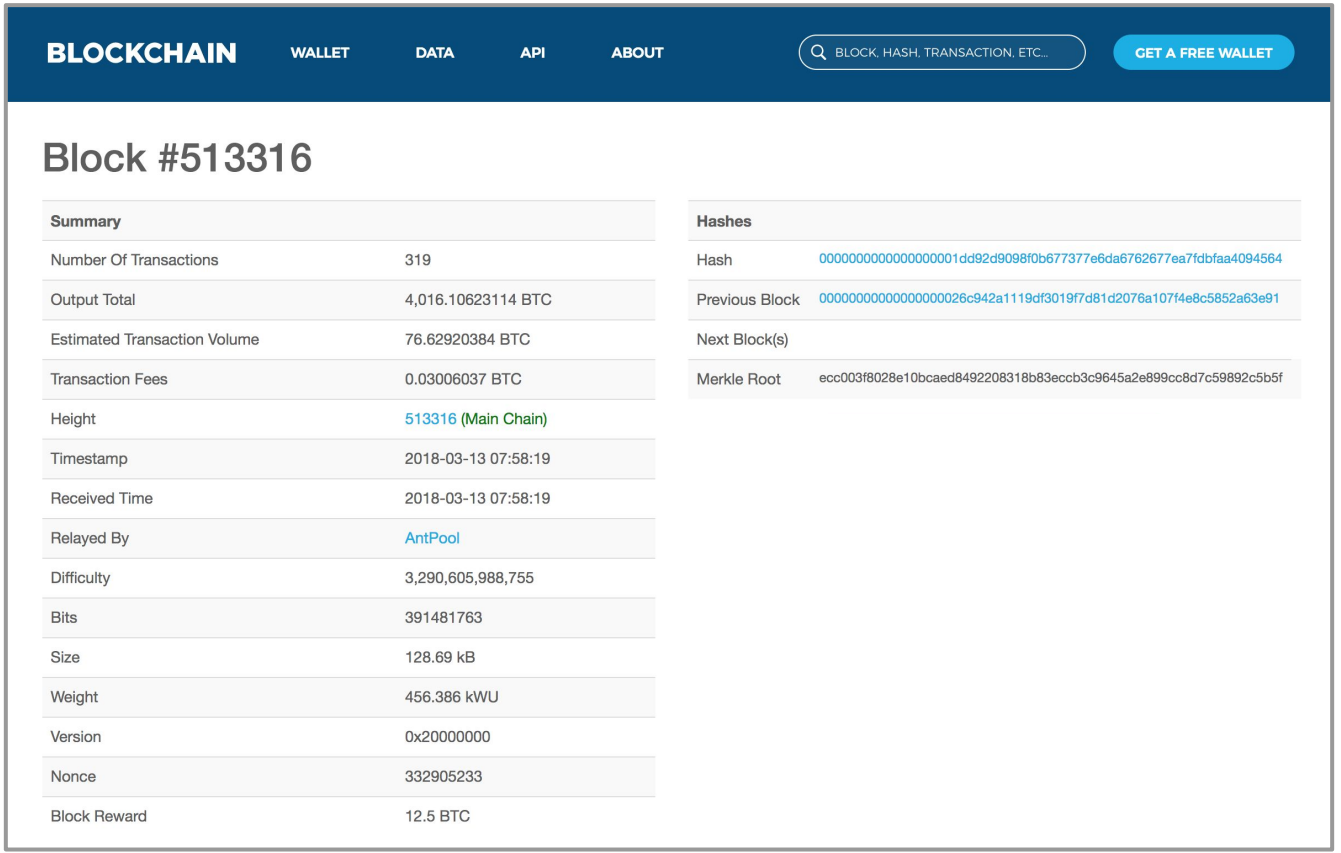


Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

https://bitnodes.earn.com

blockchain.info



Block #513316

Summary	
Number Of Transactions	319
Output Total	4,016.10623114 BTC
Estimated Transaction Volume	76.62920384 BTC
Transaction Fees	0.03006037 BTC
Height	513316 (Main Chain)
Timestamp	2018-03-13 07:58:19
Received Time	2018-03-13 07:58:19
Relayed By	AntPool
Difficulty	3,290,605,988,755
Bits	391481763
Size	128.69 kB
Weight	456.386 kWU
Version	0x20000000
Nonce	332905233
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000001dd92d9098f0b677377e6da6762677ea7fdbfaa4094564
Previous Block	00000000000000000026c942a1119df3019f7d81d2076a107f4e8c5852a63e91
Next Block(s)	
Merkle Root	ecc003f8028e10bcaed8492208318b83eccb3c9645a2e899cc8d7c59892c5b5f

addresses & keys

Address

public key to which transactions can be sent

public key
(like a bank account)

1MZ8srBWA1FiMZmhJR4pAZ2pS4GHVHWvDN

private key(s)
(like a password)

9WSMsn3tsu9kiRgZYfpA2zhxVTYsLnvMiij
S7B2zdZ5Qyf1K1TBApNrJXdRqhkXfwYP3

wallet

collection of private keys that correspond to addresses;

a private key is necessary to spend from an address;

wallet-id: 940f97d0-1a0c-4abc-93f7-c3aef3809b4a

public keys	private keys	balance
1MZ8srBWA1FiMZmhJR4pAZ2pS4GHVHWvDN	9WSMsn3tsu9kiRgZYfpA2zhxVTYsLnvMiijS7B2zdZ5Qyf1K1TBApNrJXdRqhkXfwYP3	BTC 0.2455872
1MZ8srBWA1FiMZmhJR4pAZ2pS4GHVHWvDN	9WSMsn3tsu9kiRgZYfpA2zhxVTYsLnvMiijS7B2zdZ5Qyf1K1TBApNrJXdRqhkXfwYP3	BTC 0.005455
1MZ8srBWA1FiMZmhJR4pAZ2pS4GHVHWvDN	9WSMsn3tsu9kiRgZYfpA2zhxVTYsLnvMiijS7B2zdZ5Qyf1K1TBApNrJXdRqhkXfwYP3	BTC 1.0555321
1MZ8srBWA1FiMZmhJR4pAZ2pS4GHVHWvDN	9WSMsn3tsu9kiRgZYfpA2zhxVTYsLnvMiijS7B2zdZ5Qyf1K1TBApNrJXdRqhkXfwYP3	BTC 0.45099882
1MZ8srBWA1FiMZmhJR4pAZ2pS4GHVHWvDN	9WSMsn3tsu9kiRgZYfpA2zhxVTYsLnvMiijS7B2zdZ5Qyf1K1TBApNrJXdRqhkXfwYP3	BTC 9.00004421
1MZ8srBWA1FiMZmhJR4pAZ2pS4GHVHWvDN	9WSMsn3tsu9kiRgZYfpA2zhxVTYsLnvMiijS7B2zdZ5Qyf1K1TBApNrJXdRqhkXfwYP3	BTC 0.1052519
		total: BTC 10,86286923

Bitcoin & Satoshi

Satoshi

smallest unit of the bitcoin currency

1 Satoshi	= 0.00000001 ฿	
10 Satoshi	= 0.00000010 ฿	
100 Satoshi	= 0.00000100 ฿	= 1 Bit / µBTC (you-bit) microbitcoin
1,000 Satoshi	= 0.00001000 ฿	
10,000 Satoshi	= 0.00010000 ฿	
100,000 Satoshi	= 0.00100000 ฿	= 1 mBTC (em-bit) millibitcoin
1,000,000 Satoshi	= 0.01000000 ฿	= 1 cBTC (bitcent) centibit
10,000,000 Satoshi	= 0.10000000 ฿	= 1 dBTC decibit
100,000,000 Satoshi	= 1.00000000 ฿	

alt coins vs tokens

alt coins

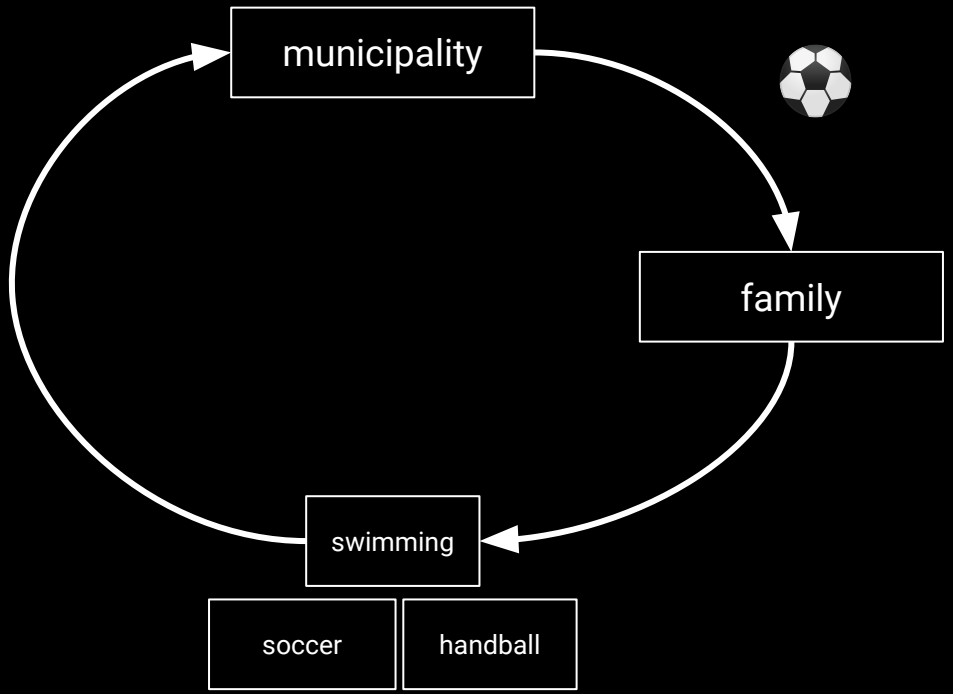
- alternative cryptocurrency coins
- either a variant (fork) of Bitcoin or have their own blockchain
- examples: Namecoin, Litecoin, Bitcoin Cash

tokens

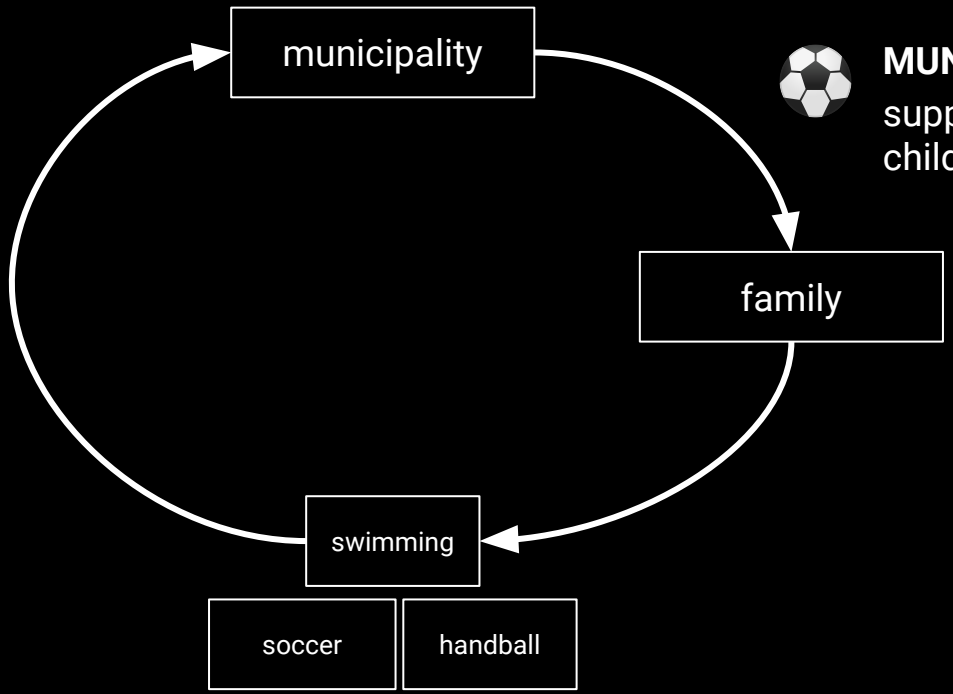
- representation of a particular asset or utility
- usually resides on top of another blockchain
- created and distributed through an ICO
- examples: Ethereum, Power Ledger, IOTA

cryptocoins

example: crypto sport token

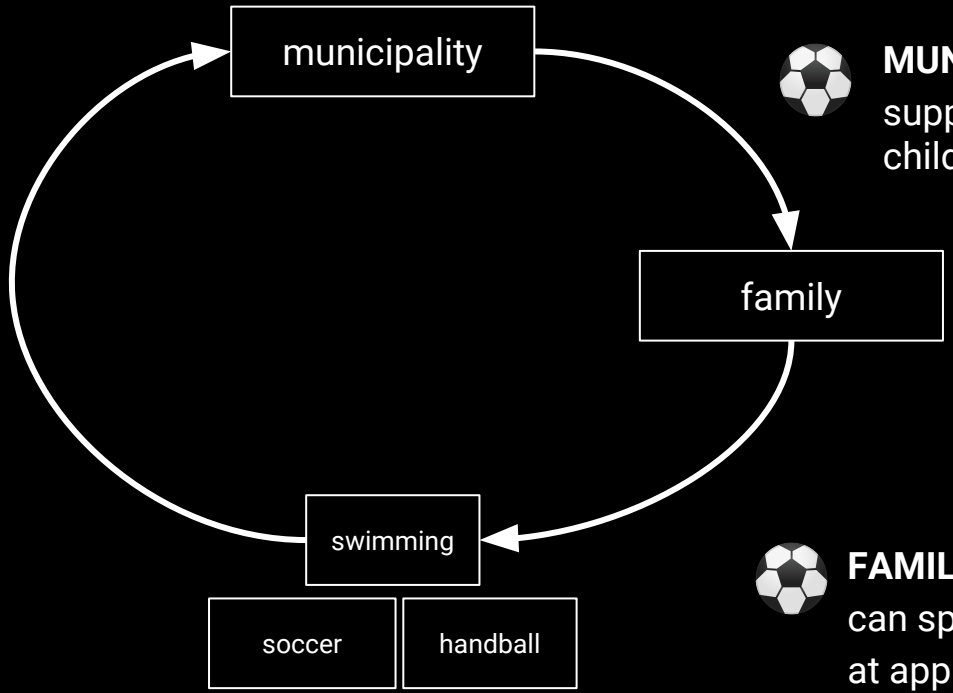


example: crypto sport token



MUNICIPALITY
support poor families assuring children can do sport activities

example: crypto sport token

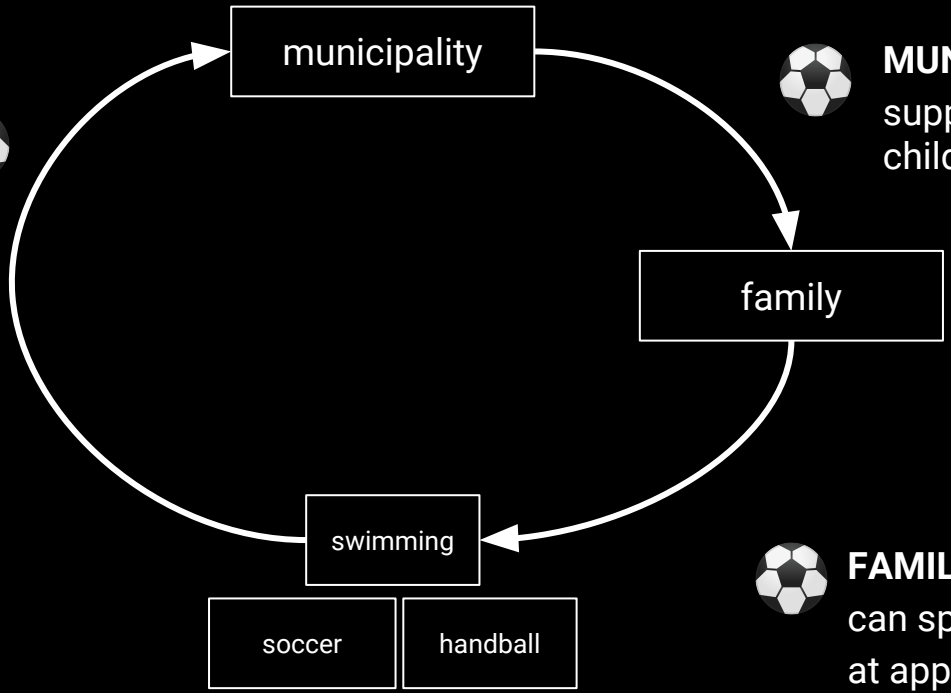


MUNICIPALITY
support poor families assuring children can do sport activities

FAMILY
can spent crypto sport token only at approved sport organizations

example: crypto sport token

SWIMMING CLUB
can pay rent for swimming pool with crypto sport token to municipality



MUNICIPALITY
support poor families assuring children can do sport activities

FAMILY
can spent crypto sport token only at approved sport organizations

ex nto sport token

SWIMMING CLUB
can pay rent for swimming pool with crypto sport token to municipality

MUNICIPALITY
support poor families assuring children can do sport activities

amily

FAMILY
can spent crypto sport token only at approved sport organizations

Home › Voorpagina Groningen › Start 'Kindpakket' op De Noordster

Voorpagina Groningen

Start 'Kindpakket' op De Noordster

9 november 2017

Start 'Kindpakket' op De Noordster

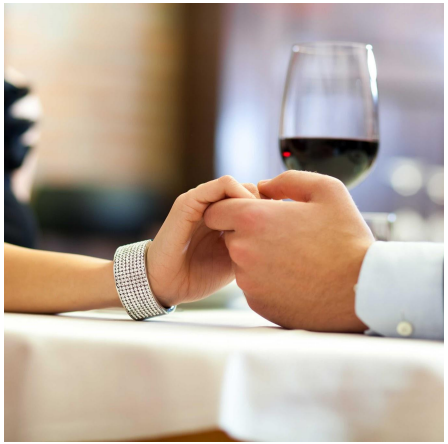
ZUIDHORN – Wethouders Nederveen en Stol hebben vorige week woensdag op De Noordster de aftrap verricht van de uitvoering van het Kindpakket. Het Kindpakket is een budget voor kinderen van ouders met een minimuminkomen. De gemeente Zuidhorn gaat ontvangt vanaf dit jaar de zogenaamde Klijnsma-gelden. In de gemeente Zuidhorn gaat het om ongeveer 150 kinderen, die hiervoor in aanmerking komen. Zij krijgen hiermee de kans mee te doen op sociaal gebied, met sport, culturele activiteiten en op school. De gemeente voert deze landelijke opdracht uit met lokale ondernemers en verenigingen. Om kinderen mee te laten doen aan (sociale) activiteiten, werkt de gemeente ook nauw samen met instanties zoals Stichting Leergeld, Jeugdcultuur- en Jeugdsportfonds en de Vakantiebank. Om de ouders meer keuze te geven is het aanbod uitgebreid tot 12 lokale ondernemers. Het resultaat is een impuls voor de lokale economie omdat een brede groep

types of blockchain

public blockchain

read and write access is not limited - all the users have the same rights - everybody can download a copy

private blockchain



controlled by a single entity that operates the necessary servers, decides who gets access and is responsible for achieving consensus

consortium blockchain

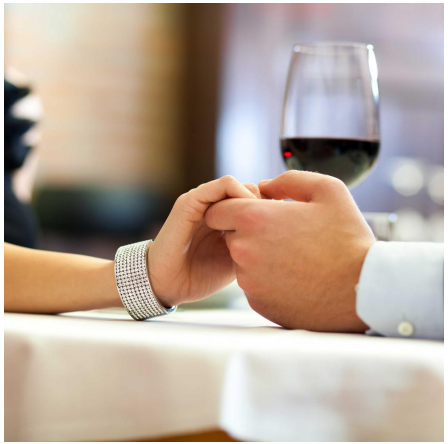
governance is split between two or more entities - consensus controlled by a set of pre-selected nodes

types of blockchain

blockchain

te access is not
he users have
ghts - everybody
ad a copy

private blockchain

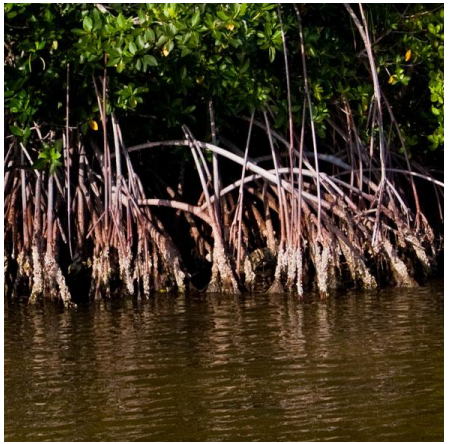


controlled by a single entity that operates the necessary servers, decides who gets access and is responsible for achieving consensus

consortium blockchain

governance is split between two or more entities - consensus controlled by a set of pre-selected nodes

hashgraph



different from blockchain - consensus via gossip protocols - consensus without miners

consensus protocols

proof of work

- define an expensive computer calculation (mining)
- miners compete for the solution
- a reward is given to the first miner who find the solution for the block

proof of stake

- the next block is chosen via a combination of random selection and wealth
- no block reward, only a transaction fee
- no competition, much more effective and sustainable

consensus protocols

proof of stake

- the next block is chosen via a combination of random selection and wealth
- no block reward, only a transaction fee
- no competition, much more effective and sustainable

proof of capacity

- the more hard drive space you have, the better your chance of mining the next block
- the algorithm generates large data sets known as 'plots', which you store on your hard drive
- the more plots the better your chance

blockchain challenges

- no regulations
- privacy
- low transaction rates
- high energy consumption
- complex keys
- lack of developers
- negative image of Bitcoin

Bitcoin vs. Ethereum

- digital money
- a single application - peer to peer electronic payment system
- send ฿ from Peter -> Beau

- world computer - smart contracts
- host and run any application that has been built on it
- send value from Peter -> Beau
  - if Peter’s balance > 5 ETH
  - and if it’s Beau’s birthday

Ethereum - the world computer

code inside the blocks ...

Block: # 1

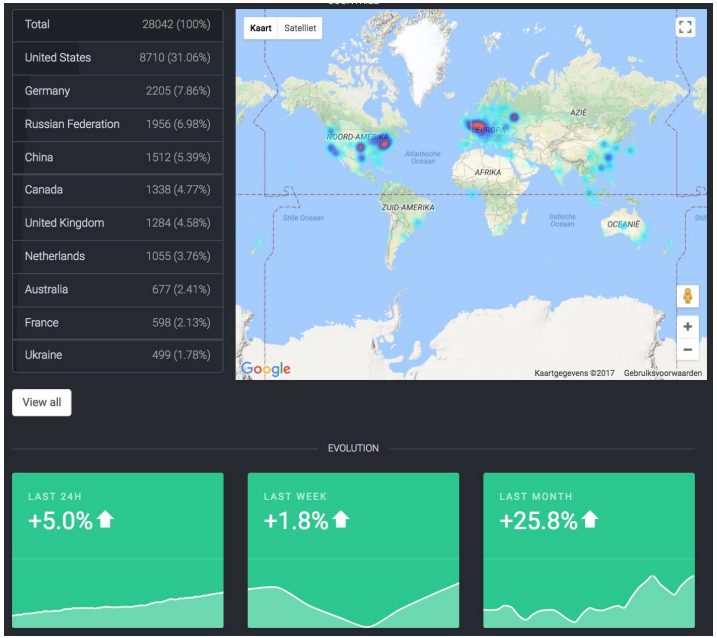
Nonce: 68028

Data:

```
var _greeting = "Hello World!"
var greeterContract = web3.eth.contract(greeterCompiled.greeter.info.abiDefinition);

var greeter = greeterContract.new(_greeting,{from:web3.eth.accounts[0], data: greeterCompiled.greeter.code, gas: 300000},
function(e, contract){
   if(!e) {

      if(!contract.address) {
        console.log("Contract transaction send: TransactionHash: " + contract.transactionHash + " waiting to be mined...");

      } else {
```

Hash: 00004e097624c41ae9aa94b49de0aaf5934f5880d1a3fbb201e5616207652826

Mine



https://www.ethernodes.org
https://etherscan.io

Ethereum - the world computer

What about Smart Contracts?

Smart contracts can account and overwatch the conditions of a contract. The advantage of computers only knowing yes and no comes in handy: Every condition in a contract leads to a decision.

Because of that contracts can be checked automatically with smart contracts. Equipped with the right content and algorithms the encrypted data blocks guarantee the observance of these contracts.

Human mistakes during composition and execution are prevented.

blockchain examples

HEALTH

Mijn Zorg Log

legally certified medical data exchange

ENERGY

Power Ledger

peer-to-peer energy trading platform

LEGAL

Xablu Contracts

solution for shared assets and shared risk

LAND REGISTRY

Lantmäteriet

Swedish land registry utilize blockchain

GAMBLING

SmartBox
First blockchain game machine

TRAVEL

LOCKCHAIN
0% Commissions on Bookings

EDUCATION

BLOCKCERTS
COMPLIANT

SUPPLY CHAIN

skuchain

example: Smart Bill of Lading (B/L)

50+ million
B/L each year

More than 50 million Bill of Lading documents are created each year.

$100
costs per document

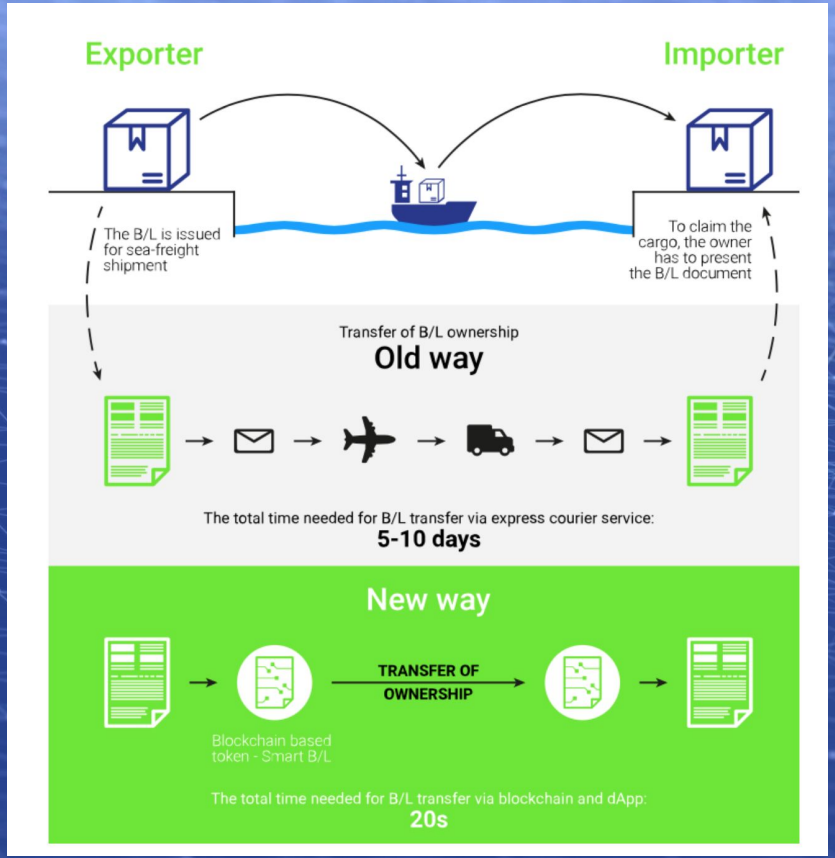
Average Bill of Lading courier costs are $100 per document.

$5 billion
courier costs per year

Companies could save $5 billion per year just on courier costs.

5 to 10
business days

It takes 5 to 10 business days on average for a Bill of Lading to get from its origin to the destination.

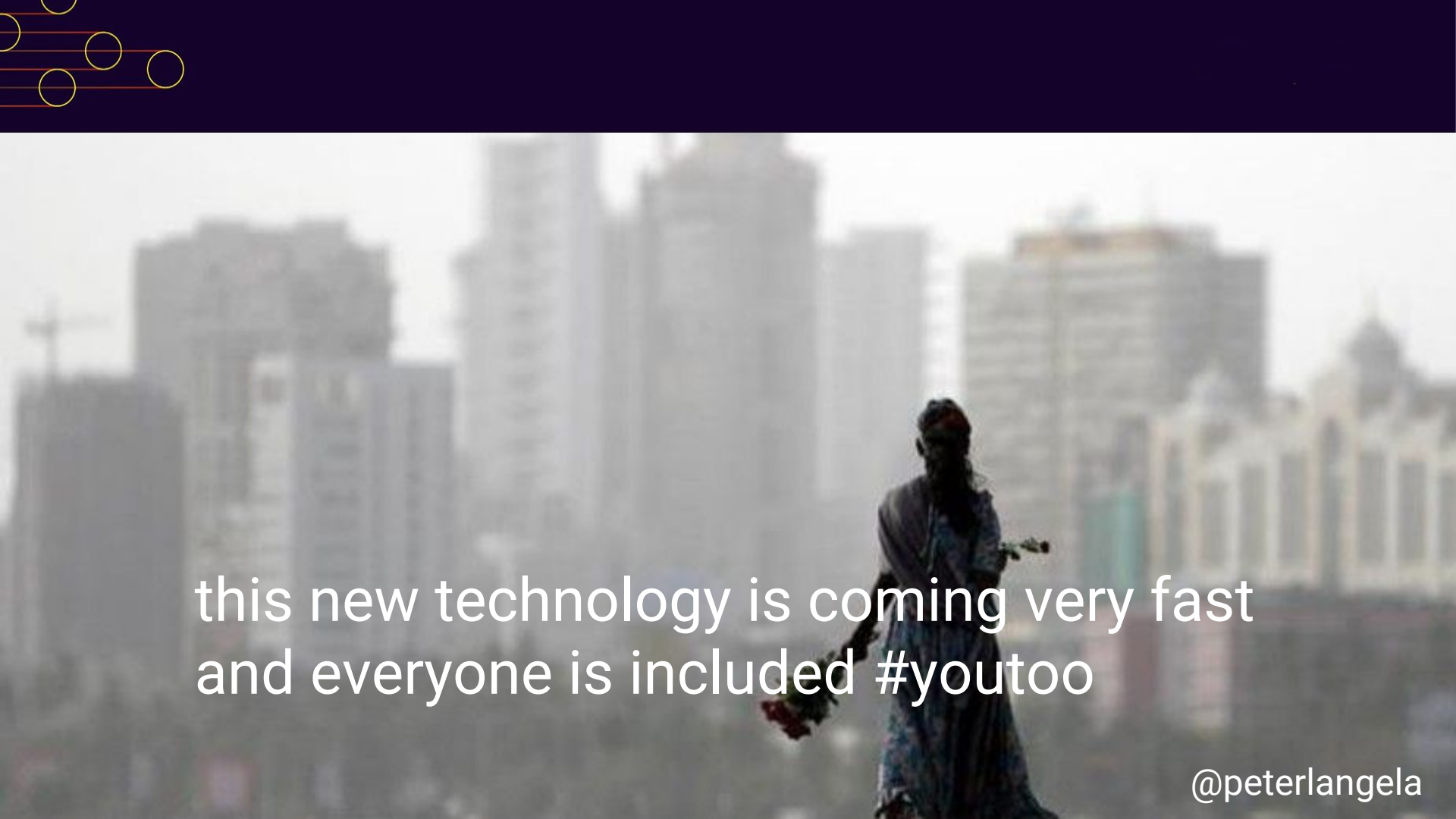


https://cargox.io/solutions/Smart-BL

CargoX

Bosch IoT adaptor XDK110

- universal programmable sensor device for IoT
- 8 built-in sensors
- IOTA MAM (Masked Authenticated Messaging) protocol sensors encrypt entire data streams for secure storage into IOTA blockchain

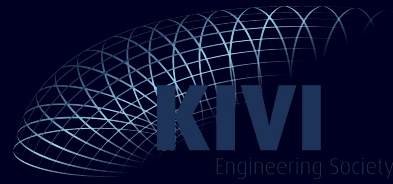

this new technology is coming very fast
and everyone is included #youtoo
@peterlangela

PETER LANGELA

Blockchain Technology Meetup Twente

Meetup

thursday 29th, 2018 16:00
The Gallery, Utwente
Enschede



UNIVERSITY OF TWENTE.

Novel-T
innovate & accelerate