APPS AND DAPPS: BLOCKCHAIN DEVELOPMENT FOR IOS

Mark Joselli
PUCPR
mark.joselli@pucpr.br

WHAT'S MONEY?

- Account -> value
- Way to exchange stuff -> acceptability
- Reservation of value -> not perishable

AND A DIGITAL CURRENCY?

- Money that only are exchangeable digitally
  - Facebook Gold, Digital Gold, Bitcoin…
- And also: Electronic Payment Authorization (Credit cards)

MONEY

"something generally accepted as a medium of exchange, a measure of value, or a means of payment"

TYPE OF MONEY

- Commodity Money: The commodity itself becomes the money. Examples of commodity money include gold coins, beads, shells, spices, etc.

- Fiat Money: Fiat money gets its value from a government order.

- Fiduciary Money: Fiduciary money depends for its value on the confidence that it will be generally accepted as a medium of exchange (checks, bank notes…)

FIRST TOKENS

- Way to exchange products:
  1 cow for 10kg of carrots;

- Firs coins of metal

ACCOUNTS

- Certified credits for the production;
- Banks as a way to trade;
- Goldsmiths: deposits and promissory notes

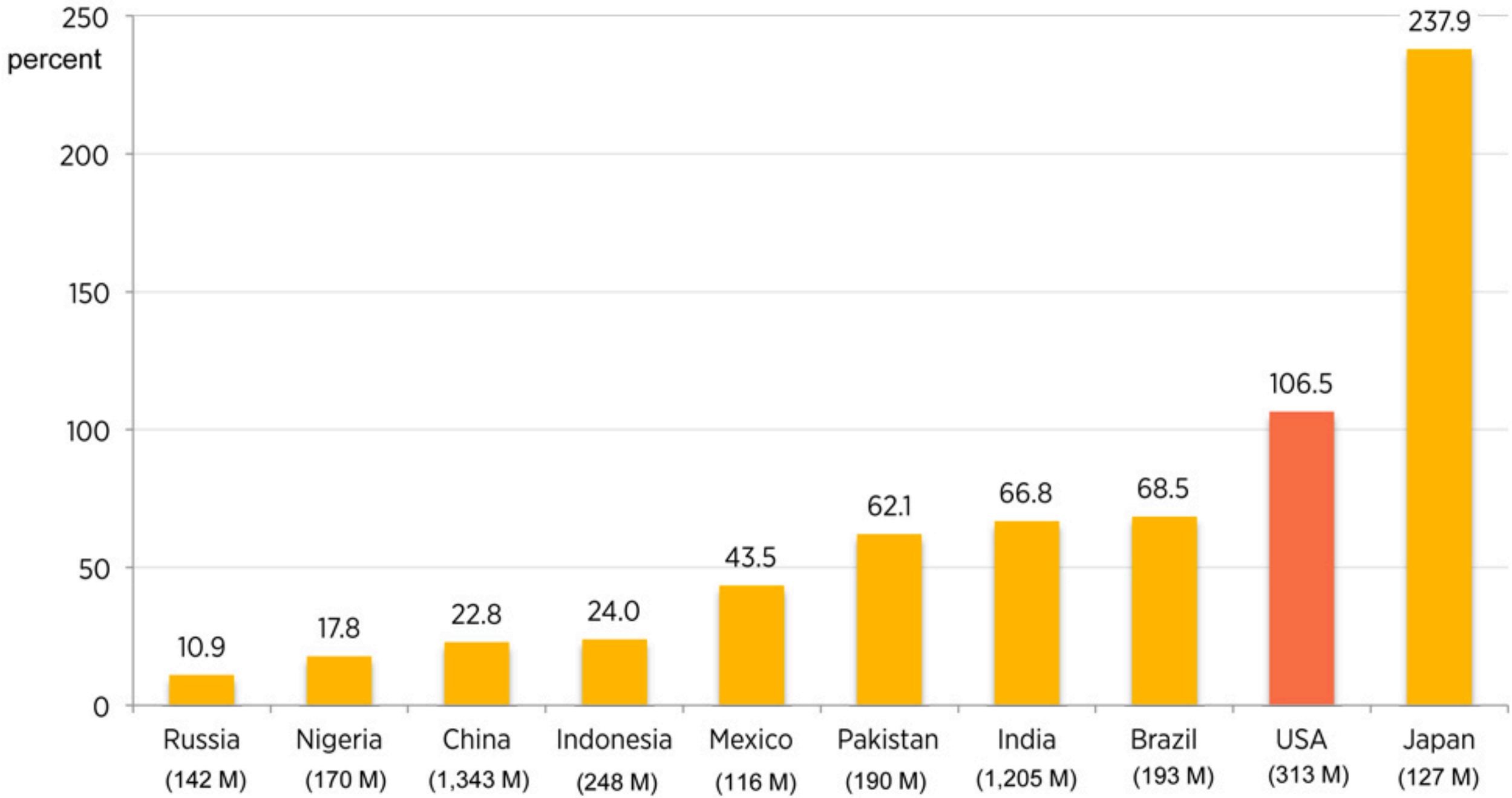
BEGIN OF THE MODERN MONEY

- Notes from private bank
  - Loan based on the money in account;
    - Begin of faction reserve
- Money from the government
  - Support from gold and silver

END OF GOLD STANDARD

- Coins and notes are not reimbursed to gold;
- Exchange market
- Money by Government Decree
  - Supported by the ability to pay the debt
  - Can have inflation and disinflation.

Debt-to-GDP of Most Populous Countries



Source: International Monetary Fund.
Data note: Data for Bangladesh (8th most populous country) unavailable.
Produced by Veronique de Rugy, Mercatus Center at George Mason University.

Open Source Peer-to-Peer Money

INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA

The Economist

OCTOBER 31ST-NOVEMBER 6TH 2015 Economist.com

007 and the spectre of Britain's past

Turkey votes to the sound of bombs

Those ever-creative accountants

America takes the fight to IS

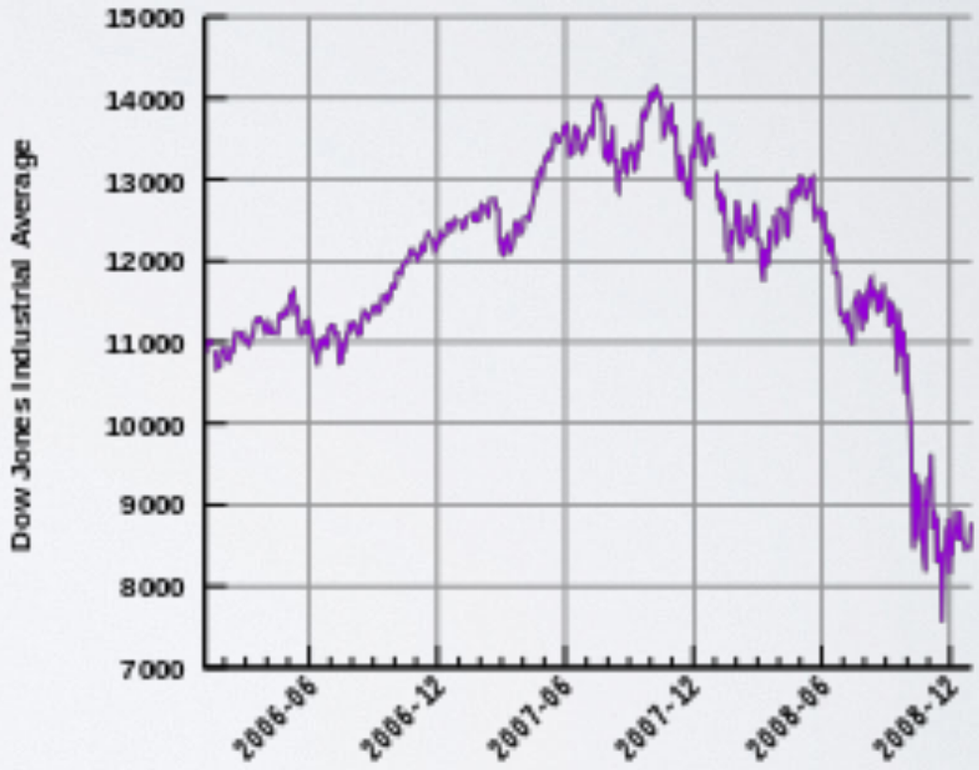
Coywolves: the new superpredator

The trust machine

How the technology behind bitcoin could change the world

2008 CRASH

- It began in 2007 with a crisis in the subprime mortgage market;
- Excessive risk-taking by banks helped to magnify the financial impact globally;
- The banks lost the money from the people (deposits).
- Massive bail-outs of financial institutions by the government with money from the people (taxes).



BITCOIN CREATION

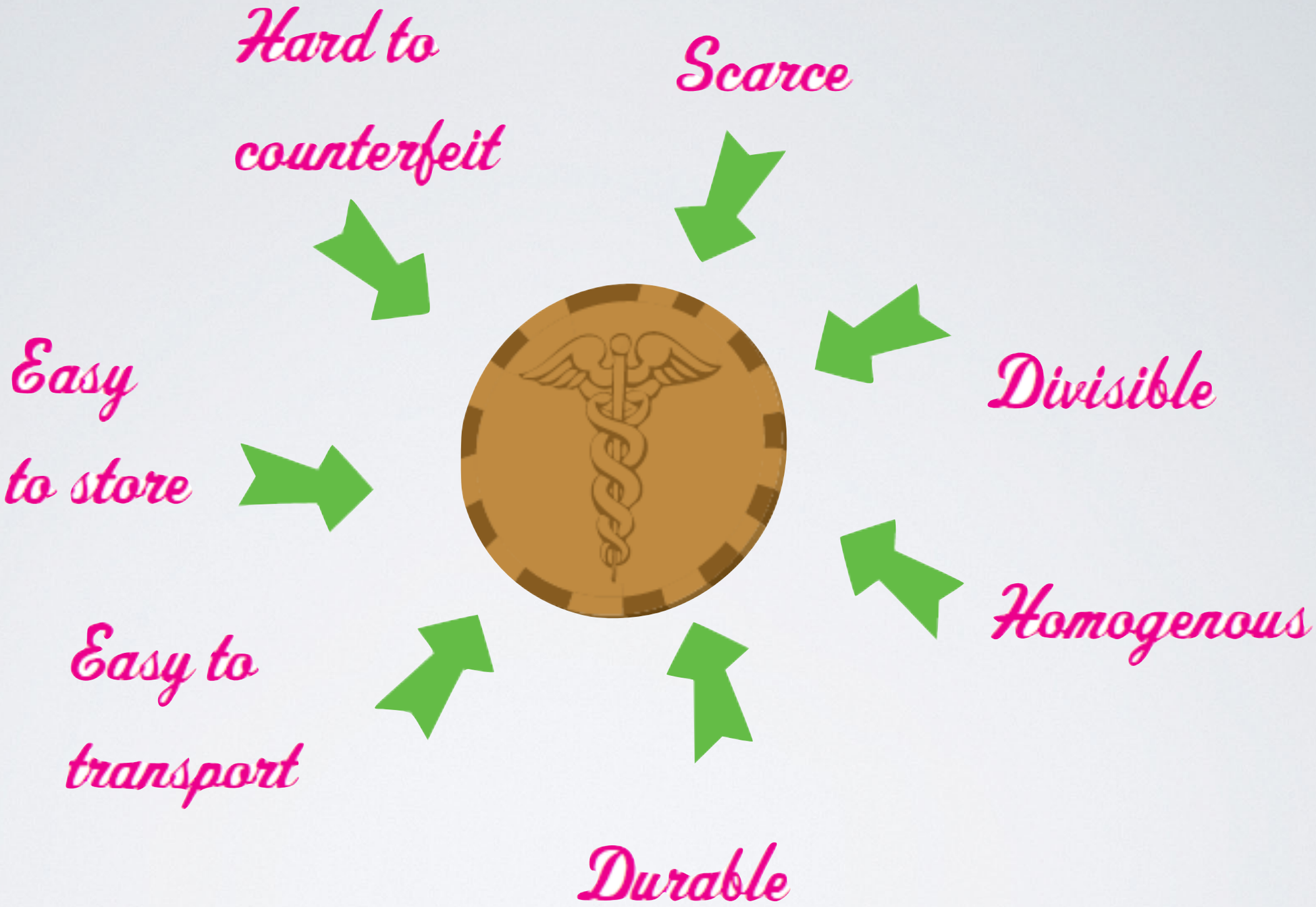
- 31/10/2008, a link to a paper authored by Satoshi Nakamoto titled Bitcoin: A Peer-to-Peer Electronic Cash System was posted to a cryptography mailing list.
- 03/01/2009, the bitcoin network came into existence with Satoshi Nakamoto mining the genesis block of bitcoin (block number 0), with the text:

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

BITCOIN

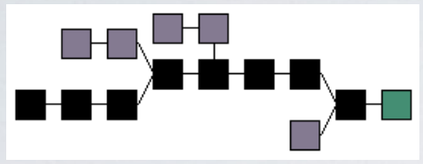
- Digital money
- A way to send and receive bitcoins to addresses
- An Open-source Decentralized Peer-to-peer (P2P) Payment Network
- The security is based on the decentralization and on cryptography

https://www.youtube.com/watch?v=Um63OQz3bjo


Hard to counterfeit
Scarce
Easy to store
Divisible
Easy to transport
Homogenous
Durable

GOOD MONEY

Blockchain



Protocol

Client

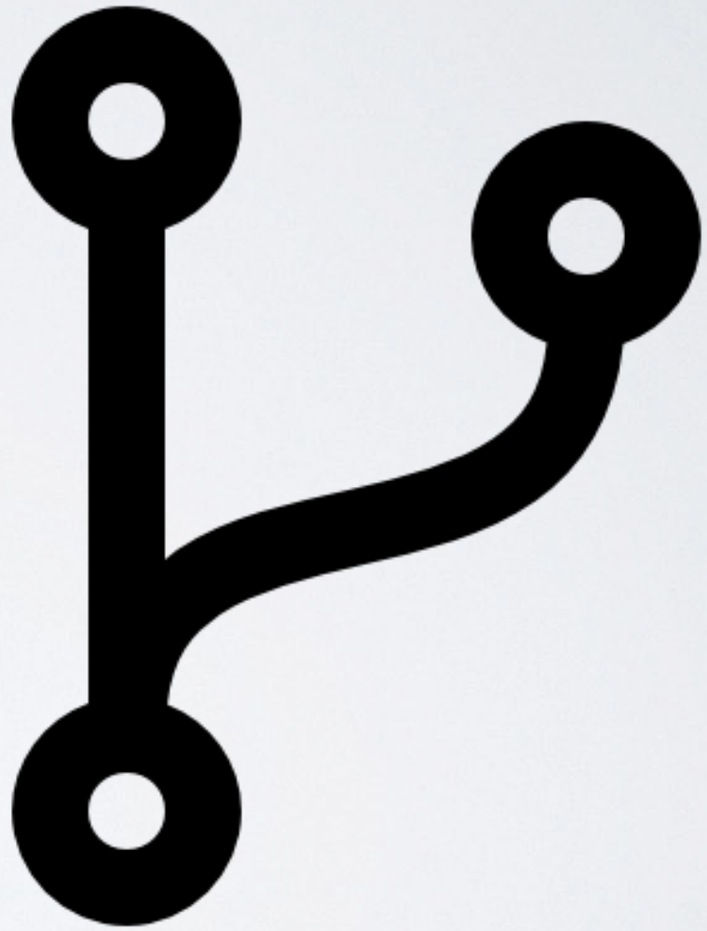
- Network open and decentralized
- Open-source
- Protocol transparent
- Public record of all transactions

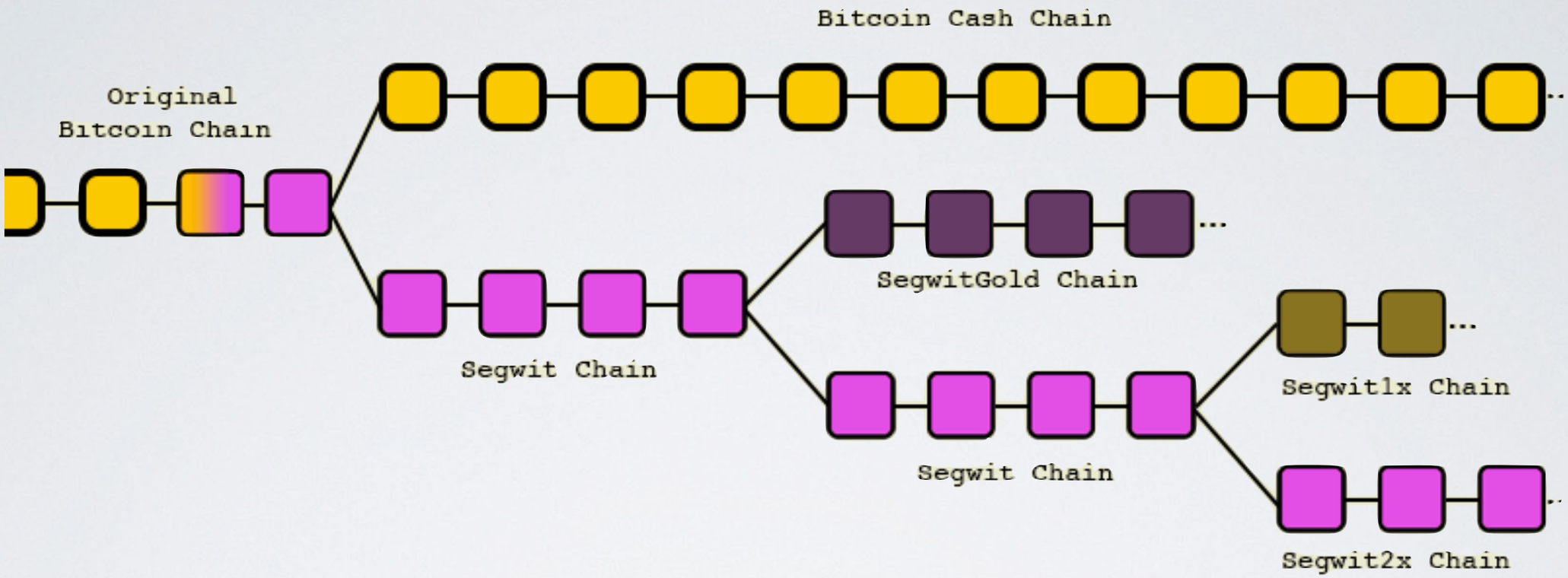
BITCOIN - GOVERNANCE

- An open source community of developers backed by the Bitcoin Foundation.

BITCOIN - DEMOCRATIC

- If someone don't like one of the changes, they are more than welcome to fork the chain and implement their own rules



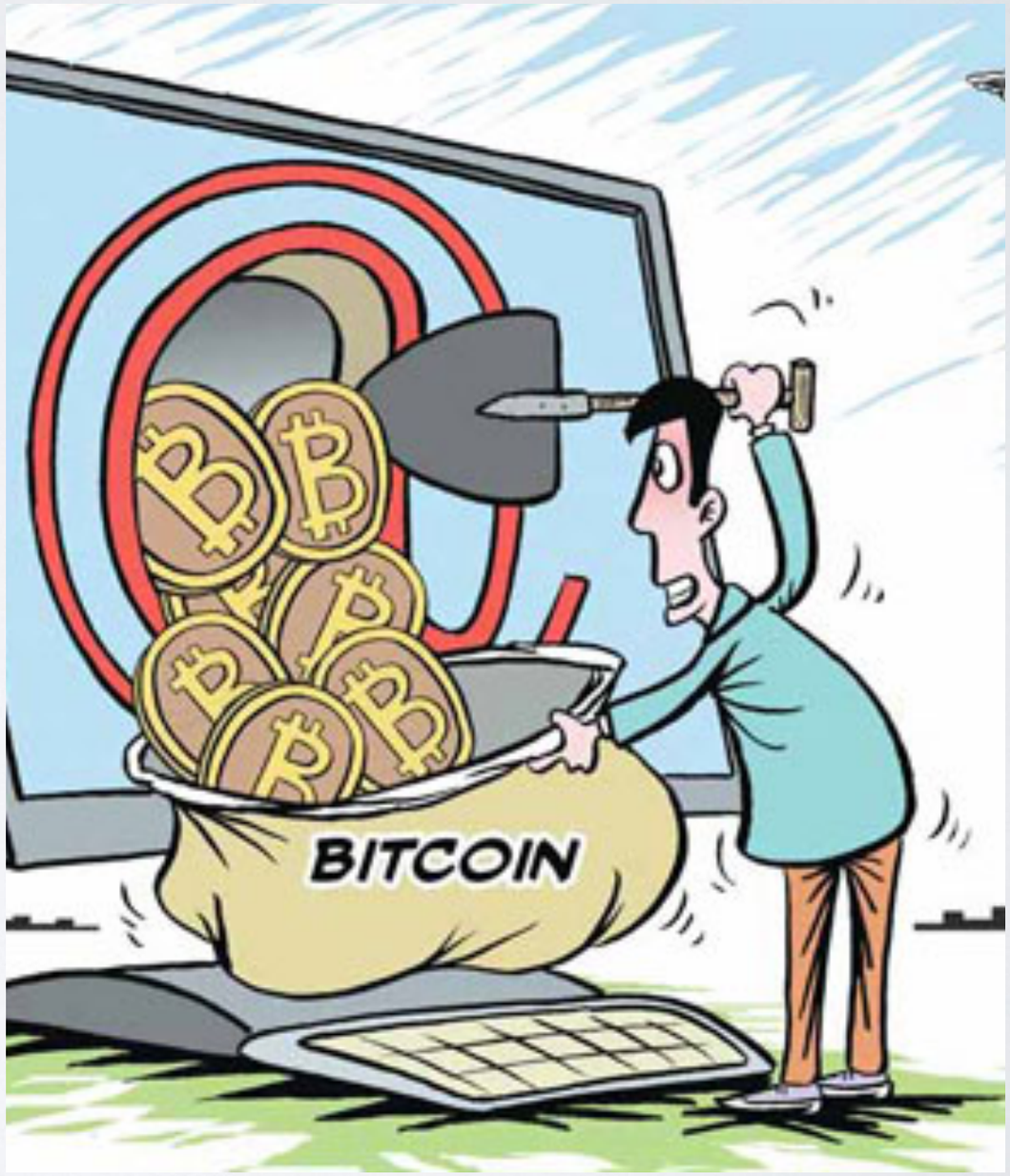


BITCOIN FORKS

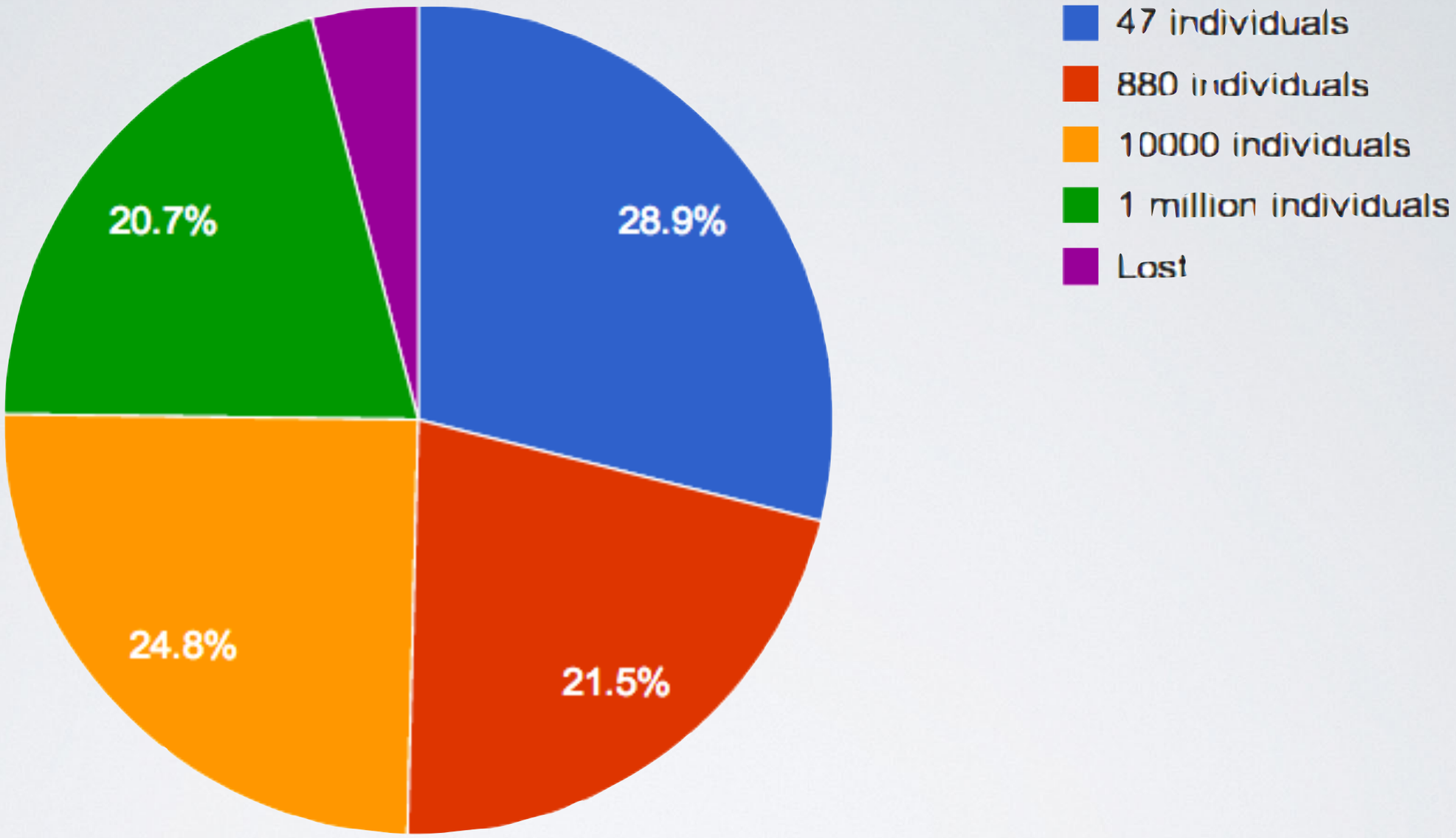
BITCOIN - CREATION

- The bitcoin was meant to be given to the people and not the banks;

- But nowadays are concentrated on few miners.



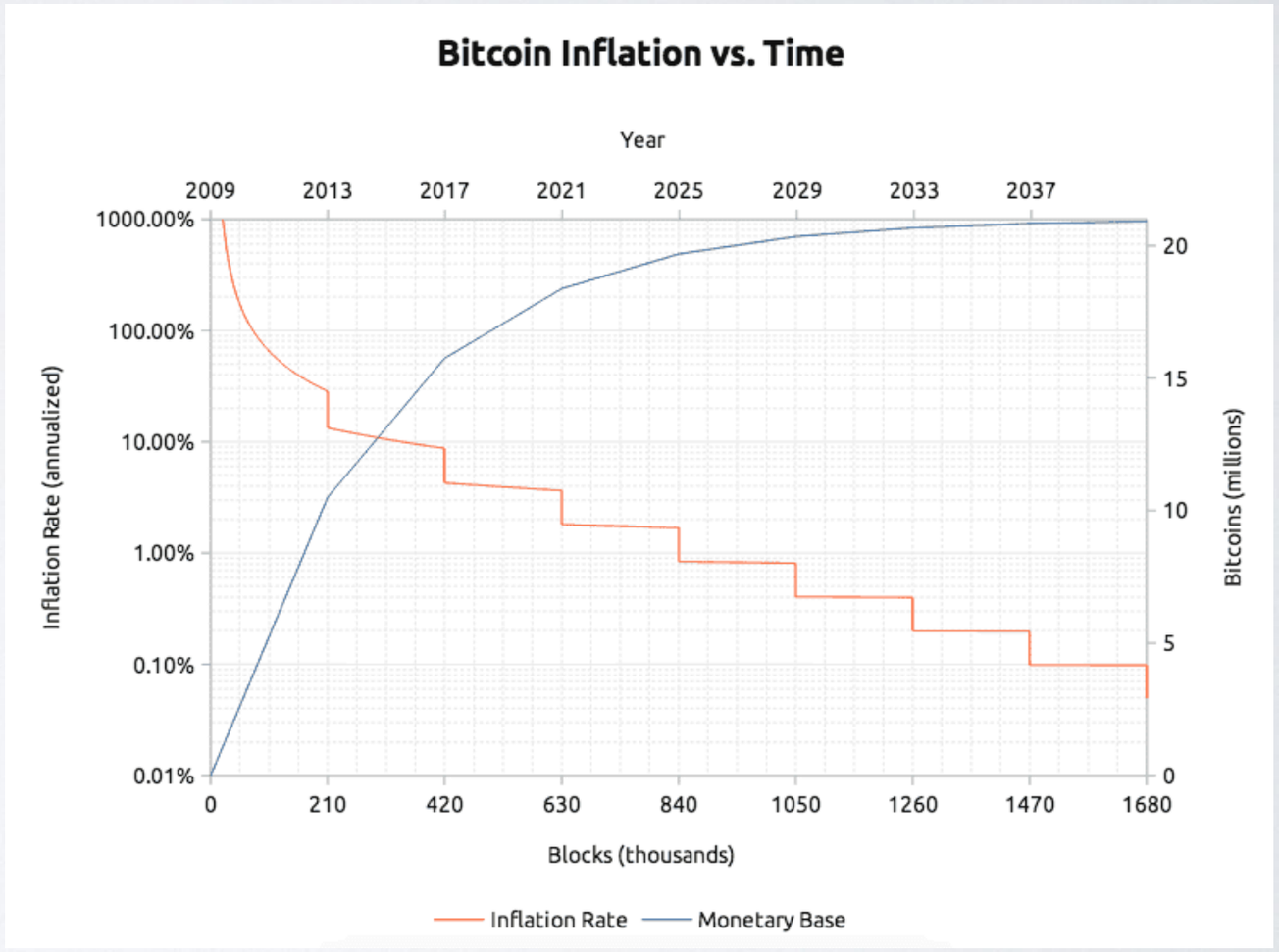
Slices Of The 12 Million Bitcoin Pie



50% OF ALL BITCOINS ARE CONCENTRATED IN 1000 PERSONS

BITCOIN - DEFLATIONARY

- Deflationary by design - money supply cannot be manipulated
- It is fixed at 21 million coins, each divisible up to 8 decimal



BITCOIN - WIKIPEDIA

- Bitcoin (BTC) is a cryptocurrency, a form of electronic cash.
- It is a decentralized digital currency without a central bank or single administrator that can be sent from user-to-user on the peer-to-peer bitcoin network without the need for intermediaries.
- Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain.
- Bitcoins are created as a reward for a process known as mining.
- They can be exchanged for other currencies, products, and services.

WHAT IS THE VALUE OF MONEY?

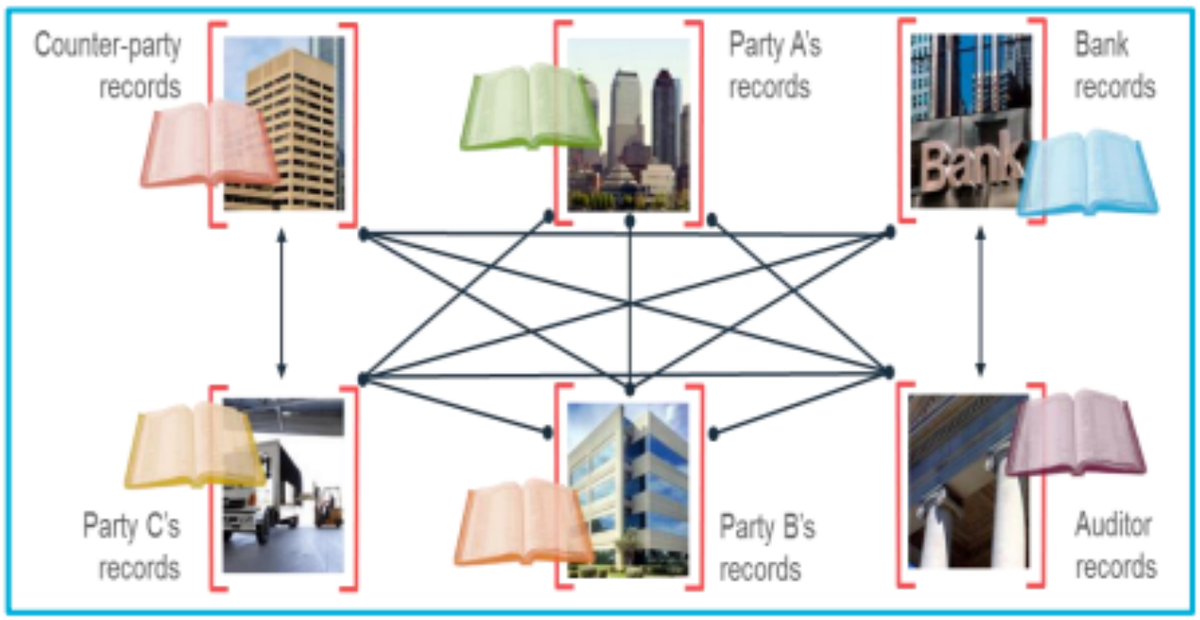
MONEY X BITCOIN

- Money in the past would like to be gold;
- Money nowadays has more value then gold, since it is more accepted.
- Any kind of money has its value based on thrust that they can trade it latter.

What's the difference with Blockchain?

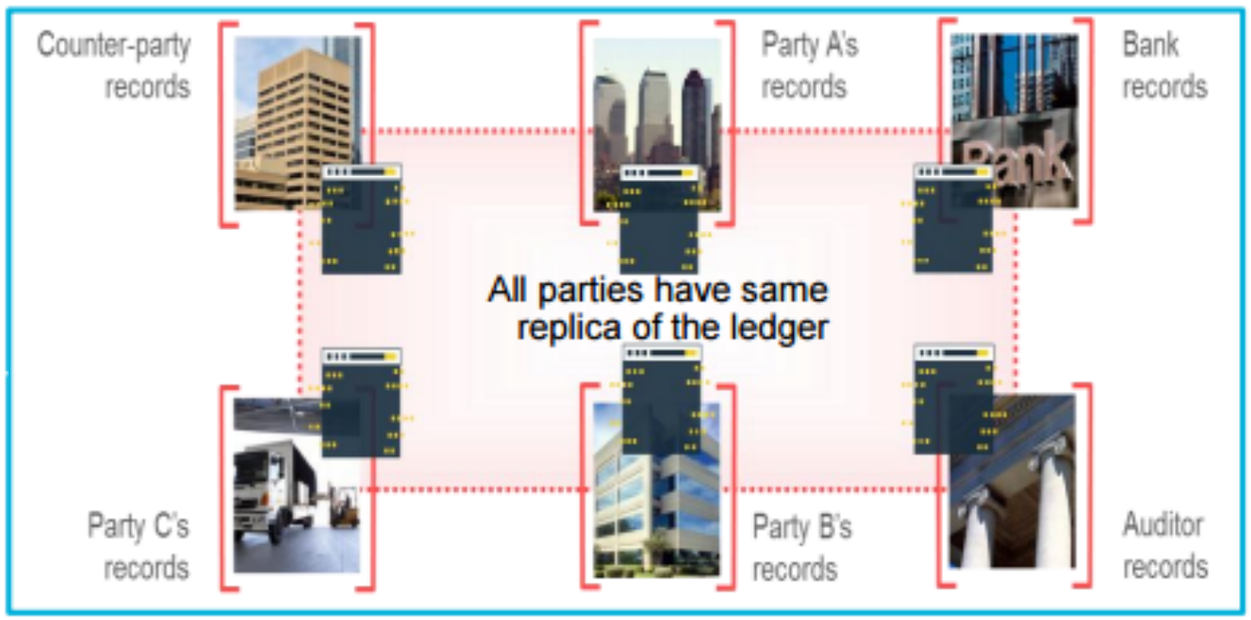
What?

Without Blockchain



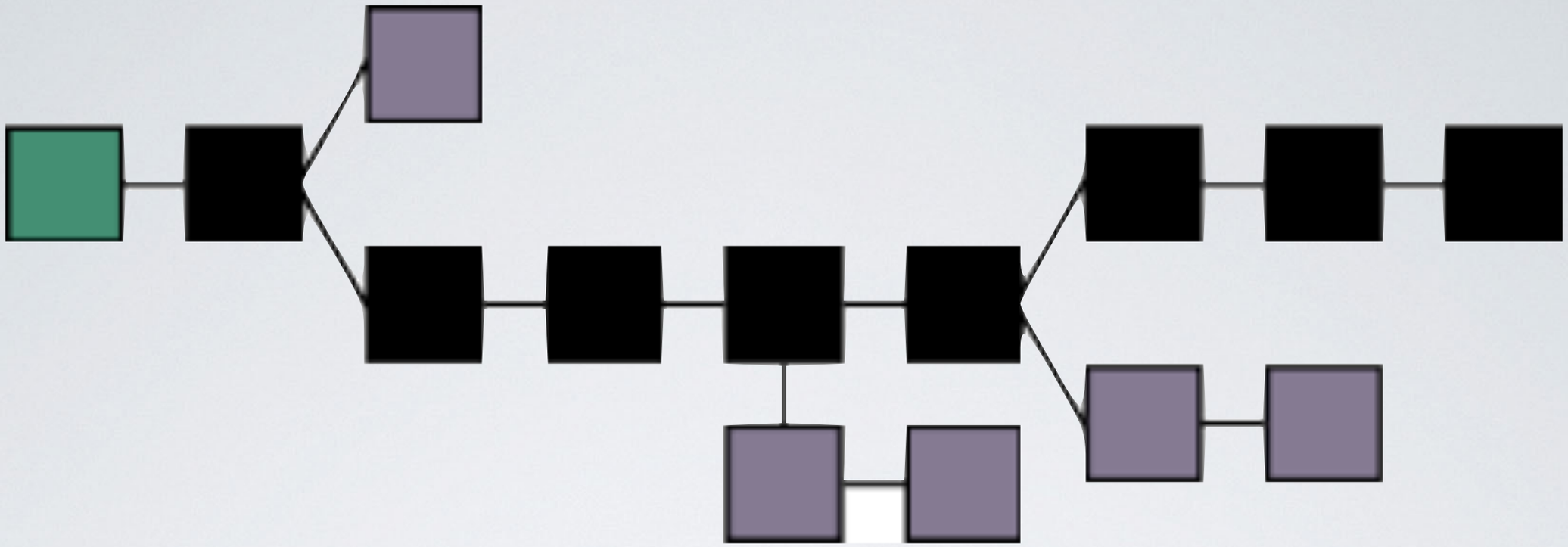
Inefficient, expensive, vulnerable

With Blockchain

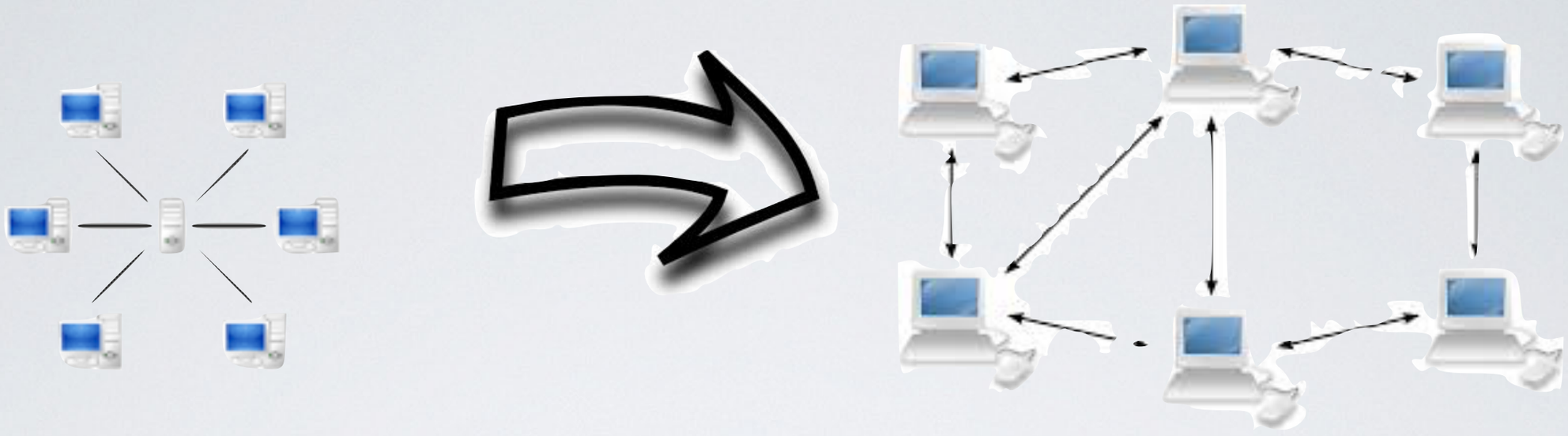


Consensus, provenance, immutability, finality

outthink your limits



- A blockchain is a time-stamped, non-repudiable database that contains the entire logged history of transactions on the system.
- Each transaction processor on the system maintains their own local copy of this database and the consensus formation algorithms enable every copy to stay in sync.



- Blockchain networks are peer-to-peer networks.
- Open blockchain networks are permissionless
  - any client can sync to the network and begin to participate.

HOW DOES IT WORKS?

- The block chain is the fundamental data structure of the Bitcoin protocol.
- It is a single data structure (like a table or hash map) where participants validade and synchronize.
- This allows them to know who owns what.
- Anyone can change it by send bitcoins to someone else.
- Other users (miners) mathematically check the transaction to ensure its validity.

- It's essentially an accounting ledger:
    1. 5/10/18 Mark found : $15.00 (Mining)
    2. 5/10/18 Mark -> Fabio : $10.00
    3. 5/10/18 Maicris -> Mark : $4.00

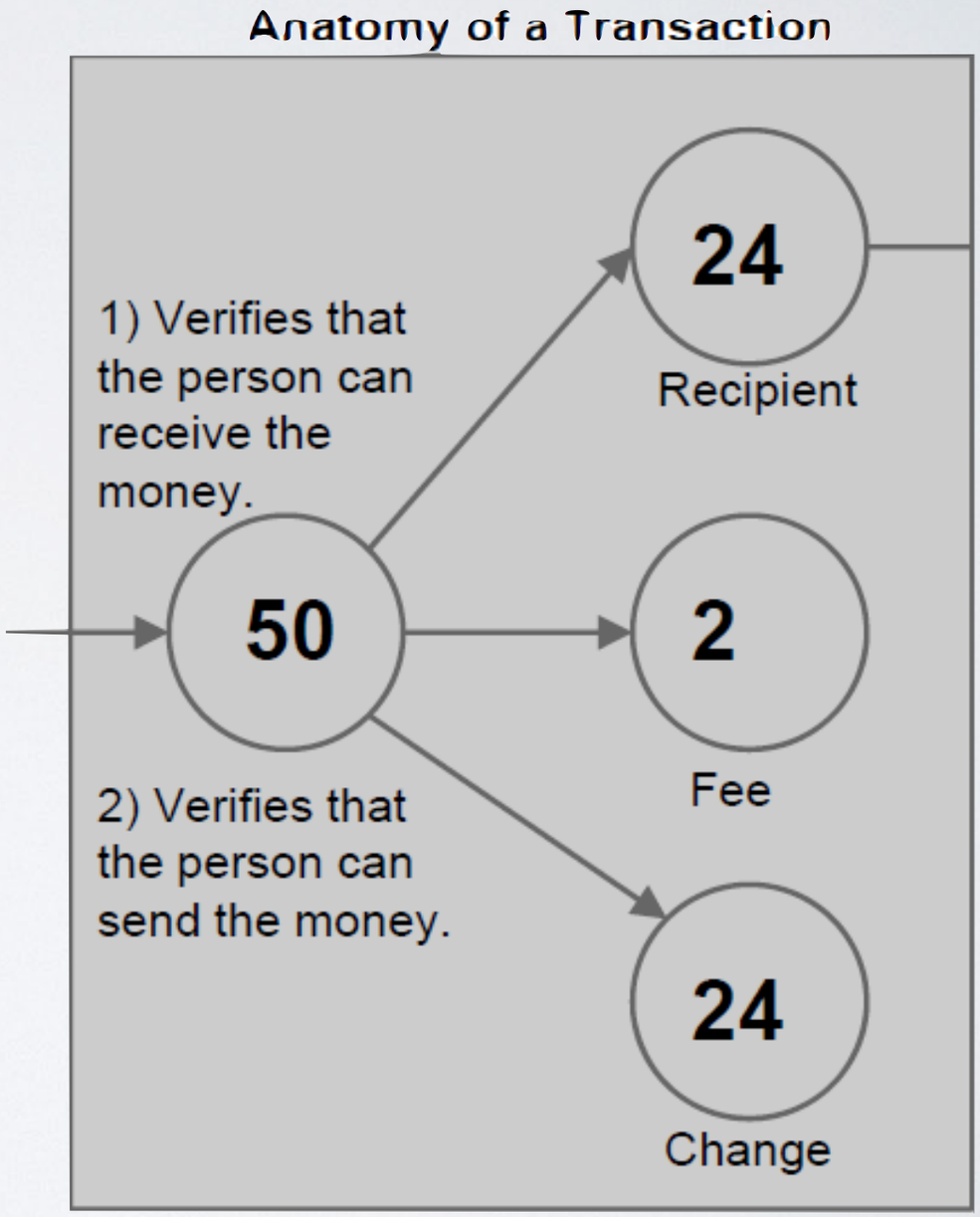
- How much money does Mark have in his wallet?
    - Mark had $15, then gave $10 to Fabio, then received $4 from Maicris. Mark has $9 (15-10+4) now.

TRANSACTIONS

- Input contains

1. A public key that belongs to the redeemer of the output transaction.

2. An ECDSA hash over a hash of the transaction.



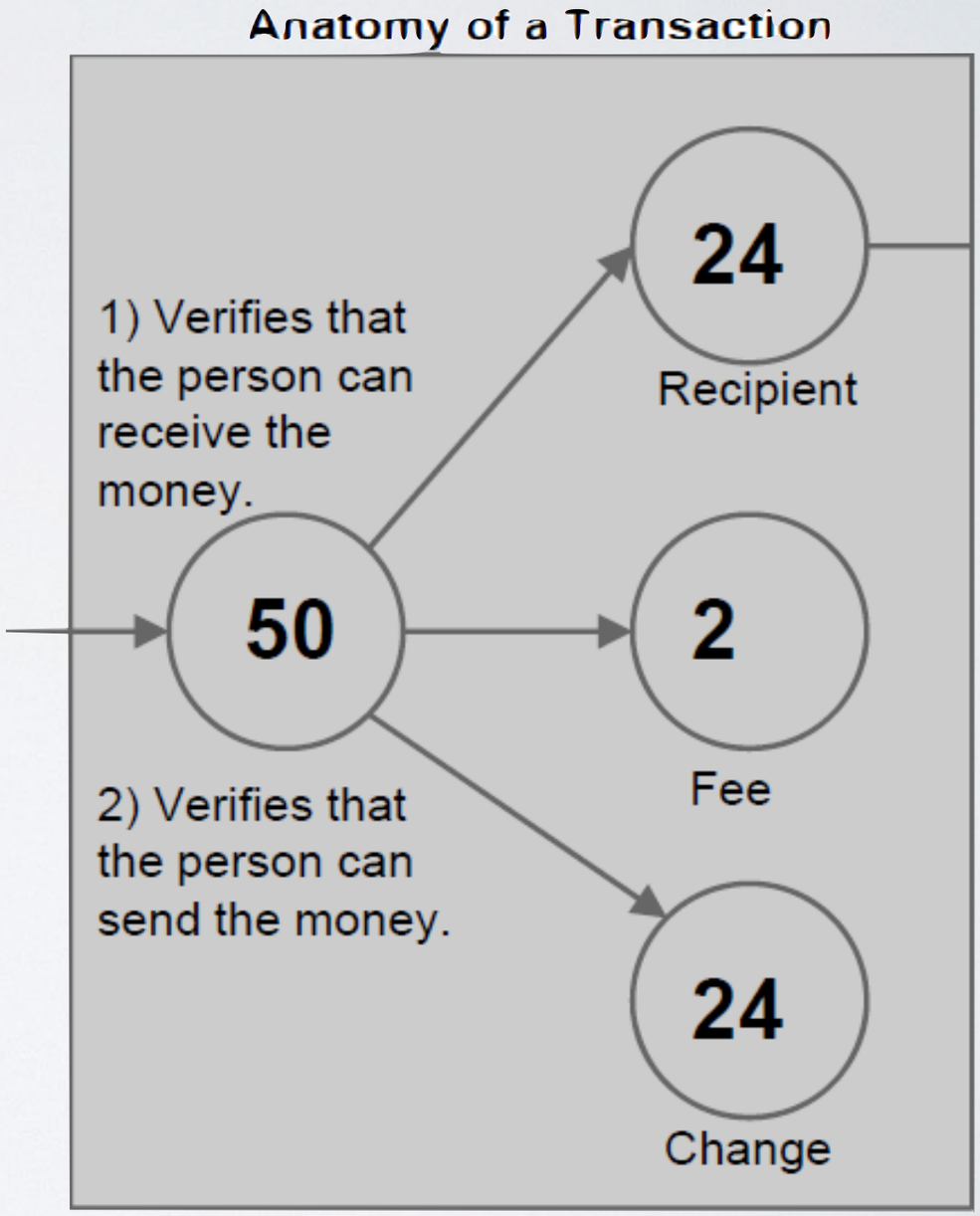
TRANSACTIONS

- Output contains

1. The actual amount being sent to the recipient.

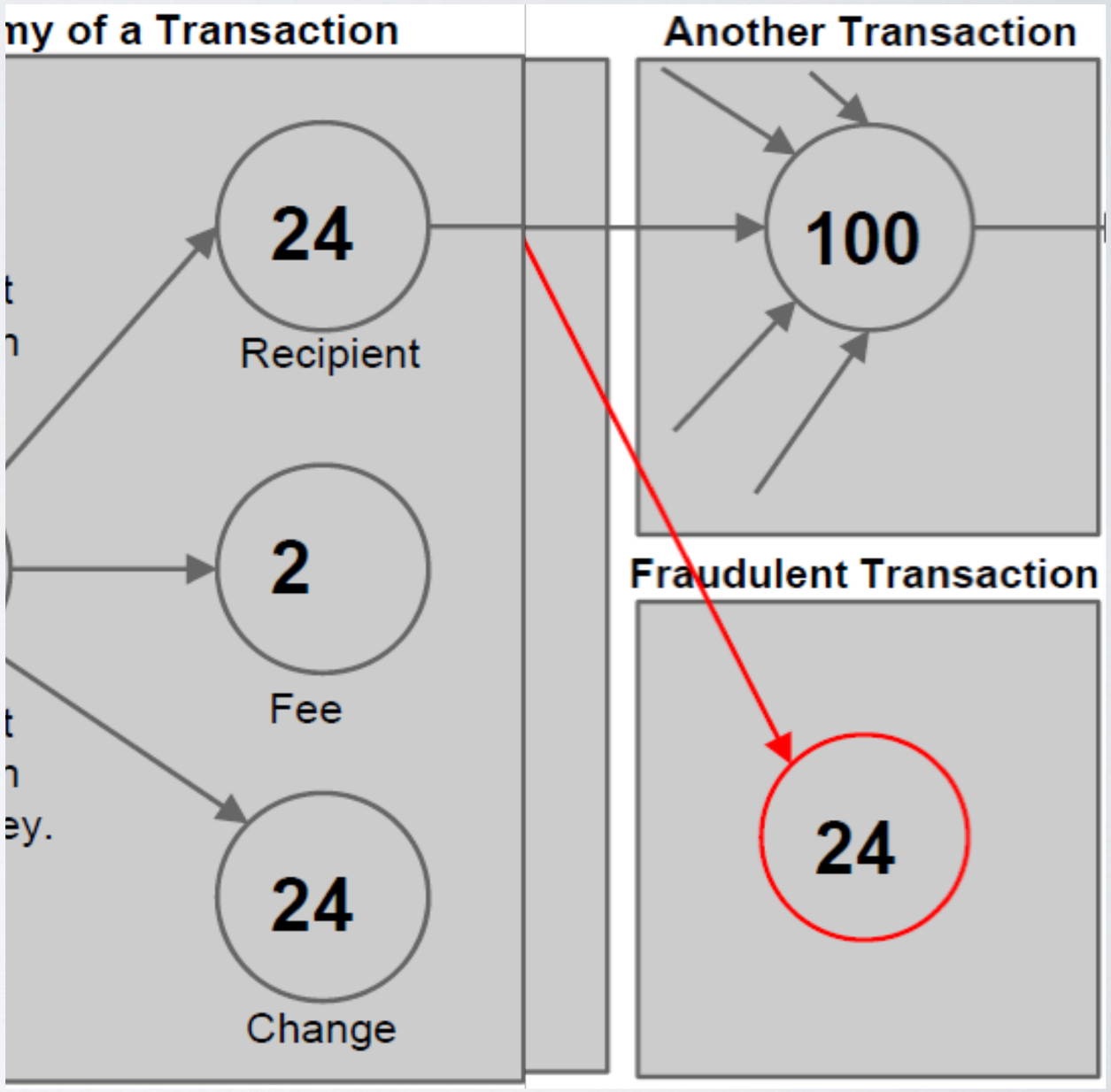
2. The change amount being sent back to the original sender (if any)

3. The voluntary transaction fee attached to the output (if any).



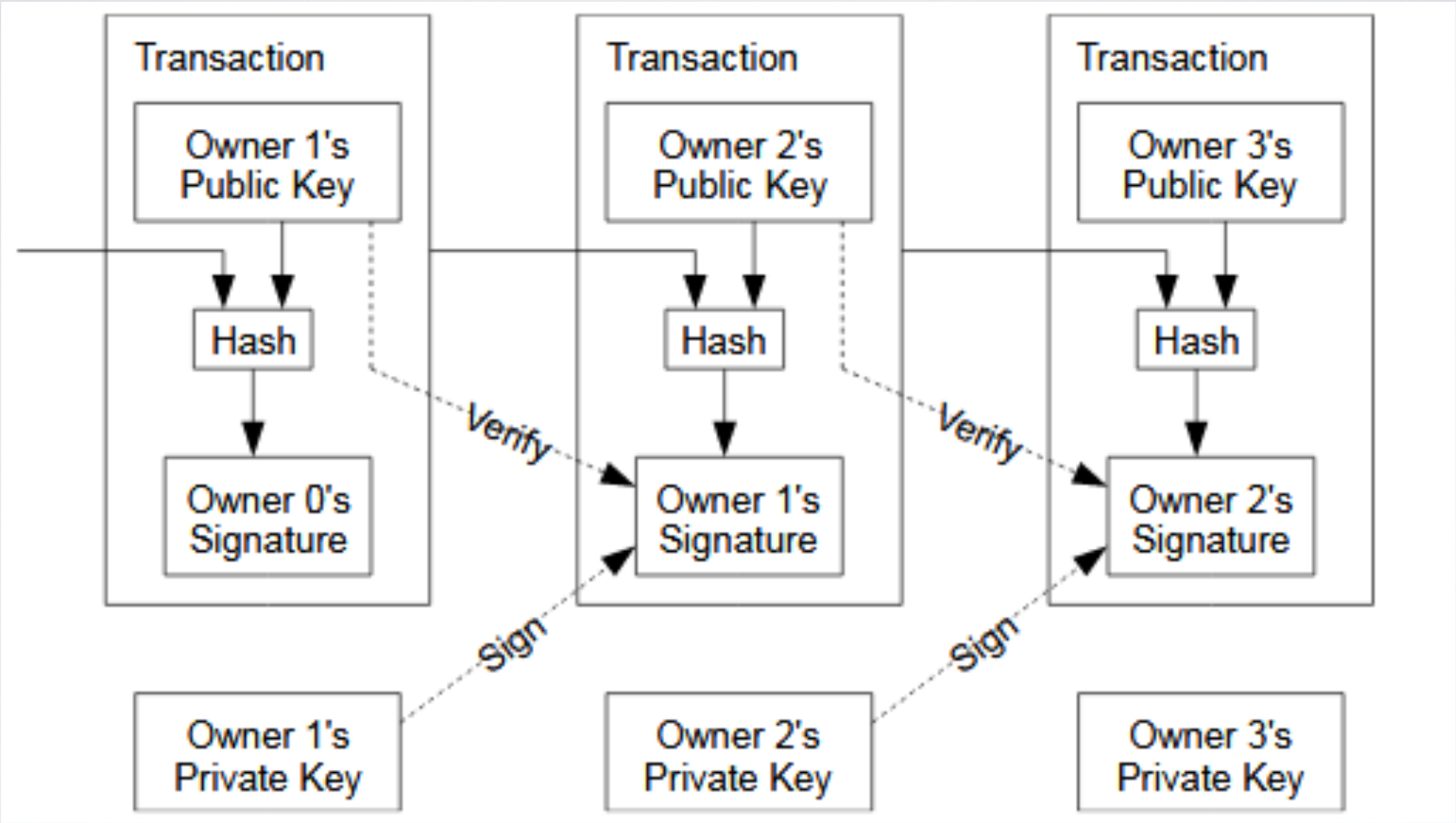
TRANSACTIONS

- The block chain prevents the double spend attack
- by giving other nodes the power to verify that transaction inputs were not already spent somewhere else.



DOUBLE SPEND

- Bitcoin solves the so-called "double spending problem" with digital products.
- For example, if I have an mp3 file or an e-book on my computer, I can copy this file thousands of times freely and upload it to thousands of different people.
- For a digital currency, the possibility of unlimited copying would mean a rapid hyperinflationary death.
- Bitcoin solves this by maintaining a P2P network and recording each transaction in a single blockchain call.
- If I send 1 bitcoin from my bitcoin address to my friend John. The bitcoins network registers this transaction in the block chain and I no longer have possession of that bitcoin.
- The coin "changed" from my bitcoins portfolio to John's wallet



TRANSACTIONS IN ACTION

MINING

MINING

- Miners collect the transactions in the network in large sets called blocks
    - Ex: "Alice pays Karim 10 bitcoins" and "Liam pays Sofia 8.3 bitcoins".
- These blocks are tied together in a continuous, authoritative record called blockchain,
    - which does not allow any conflicting transactions.
- And it lets you know with absolute certainty which transactions are reliable (No Double Spending!).

HASHING

- To understand mining, you need to understand what a hash function is.
- Simply put, a hash function gets an input and creates an apparently random output,
- but the output is consistent every time you run the function on a particular input,
- and it is very difficult to determine an input, considering only the output.

BLOCKCHAIN

- Bitcoin ensures that there is only one block chain, making blocks really difficult to produce.
    - miners have to calculate a cryptographic hash of the block that satisfies certain criteria
    - The difficulty is one of the criteria for the hash that is adjusted based on the frequency blocks being created
- They also carefully validate all transactions that go into their blocks
- Successful miners are rewarded with bitcoins.

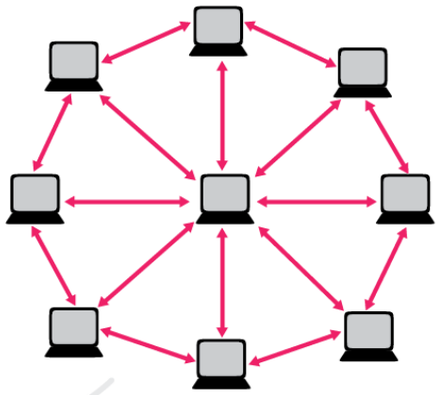
FRAUD PREVENTION

- Users can rely on the blockchain that was harder to produce
- The longer the chain "wins"
- If there was a "fake" blockchain competing with the real ones
  - the fraudster would have to do as much work as the rest of the network to make his block chain seem so reliable
- The intense work required to find blocks through hashing protects the network against fraud

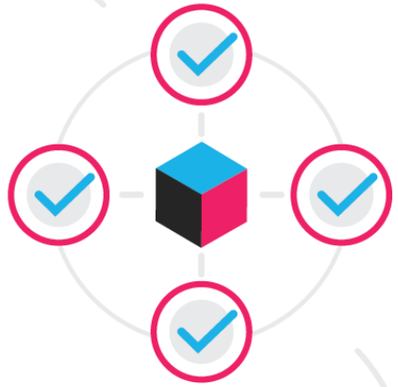
MINING STEPS

1. Collects network transactions
2. Validate them (not allowing conflicted transactions)
3. Put them in larger blocks
4. Computes cryptographic hashes until you find a hash "good enough to count"
5. Then sends the block to the network, adding it to the blockchain and gaining a reward in return

Someone requests a transaction.



The requested transaction is broadcast to a **P2P network consisting of computers, known as nodes.**



Validation

The network of nodes **validates the transaction and the user's status using known algorithms.**

A verified transaction can involve **cryptocurrency,** contracts, records, or other information.

cryptocurrency

Has no intrinsic value in that is not redeemable for another commodity such as gold.

Has no physical form and exists only in the network.

Its supply is not determined by a central bank and the network is completely decentralized.

Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger,**

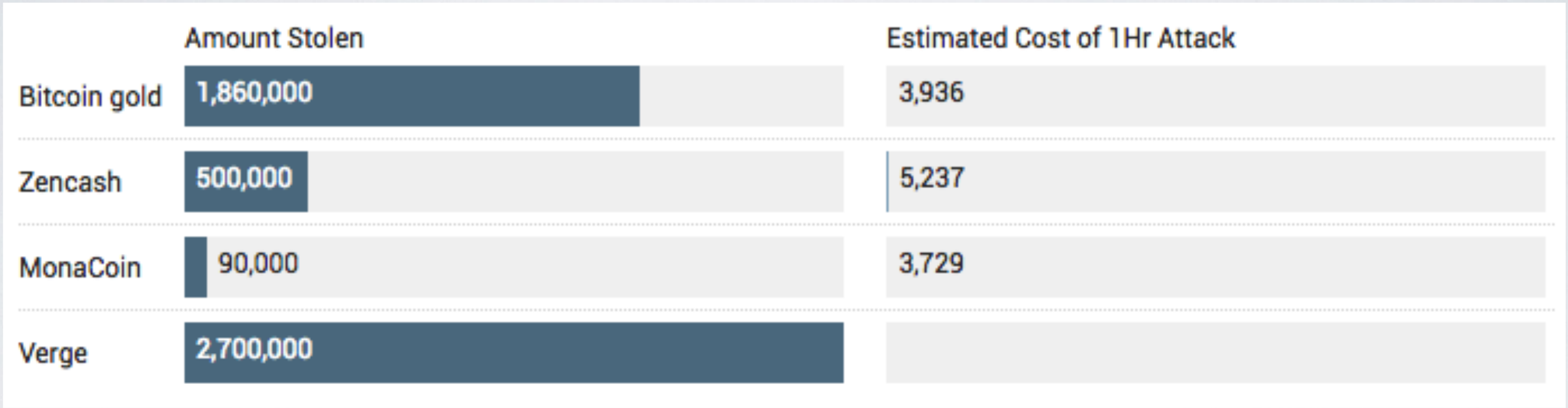
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

The transaction is complete.

51% ATTACK

- An attacker with> 50% power can hash
    - spend double: reverse transactions that it sends while it's in control
    - Prevent some or all transactions from gaining any confirmations
    - Prevent some or all other generators from getting any generations
    - https://www.crypto51.app/

SUCCESSFUL 51% ATTACKS



WHY BITCOIN

- Bitcoin can be used to buy goods anonymously (not anymore).
- Bitcoin is not bound by any country or subject to regulation.
- Advantages for small businesses because at Bitcoin there are no credit card fees or chargebacks (but have fees and long confirmation time).
- Some people buy bitcoins as an investment, hoping they will increase their value.
- This is one of the reasons for price instability

WHY NOT BITCOIN

- Portfolio Vulnerable to Robbery
- Hacks
- No regulation (yet)
- Denial of Service Attacks (DoS)
- Illegal content in the block chain
- Bitcoins are concentrate in the hand of a few
- Market manipulations
- Energy consumption
- Tulip mania

ENERGY CONSUMPTION

- An area of heavy criticism has to do with the vast amount of energy needed to process and store transactions, especially as the use of blockchain technology increases

- Miners in Bitcoin's blockchain network are seeking 450 billion trillion solutions per second in efforts to validate transactions by using substantial amounts of computer power

- Note that there are also opportunities to decentralize the energy grid

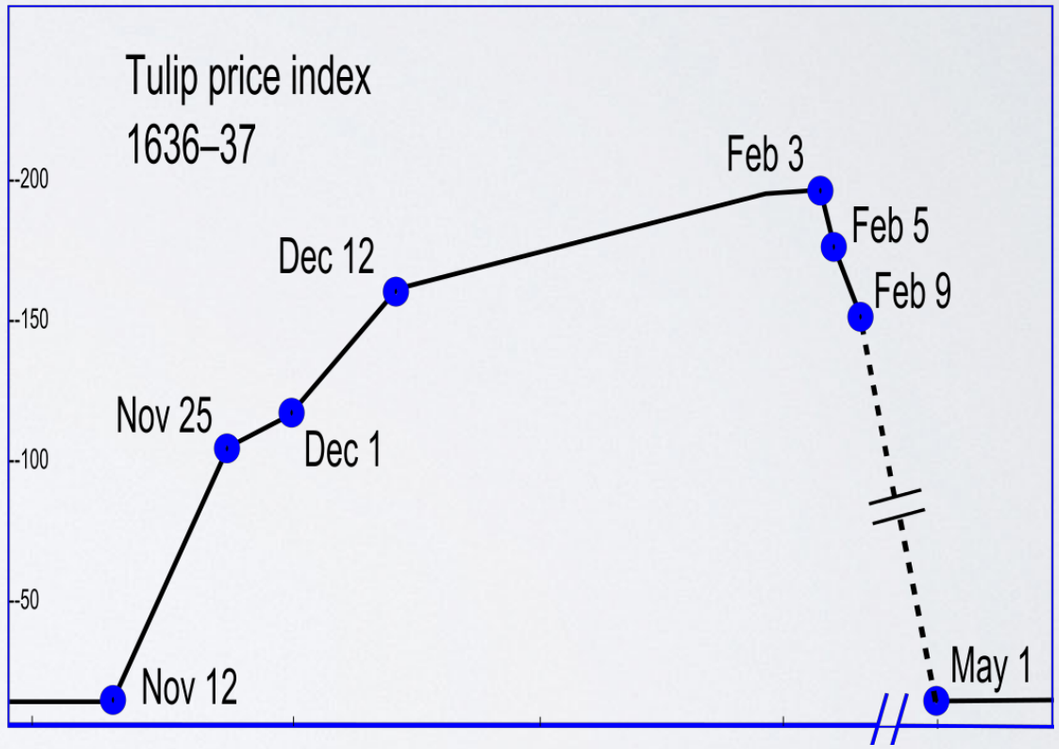
- Resources wasted: Mining with Bitcoin wastes enormous amounts of energy ($ 15 million / day)

TULIP MANIA

- Tulip mania was a period in which contract prices for some bulbs of tulips reached extraordinarily high levels

- and then dramatically collapsed in February 1637.

- It is generally considered the first recorded speculative bubble.

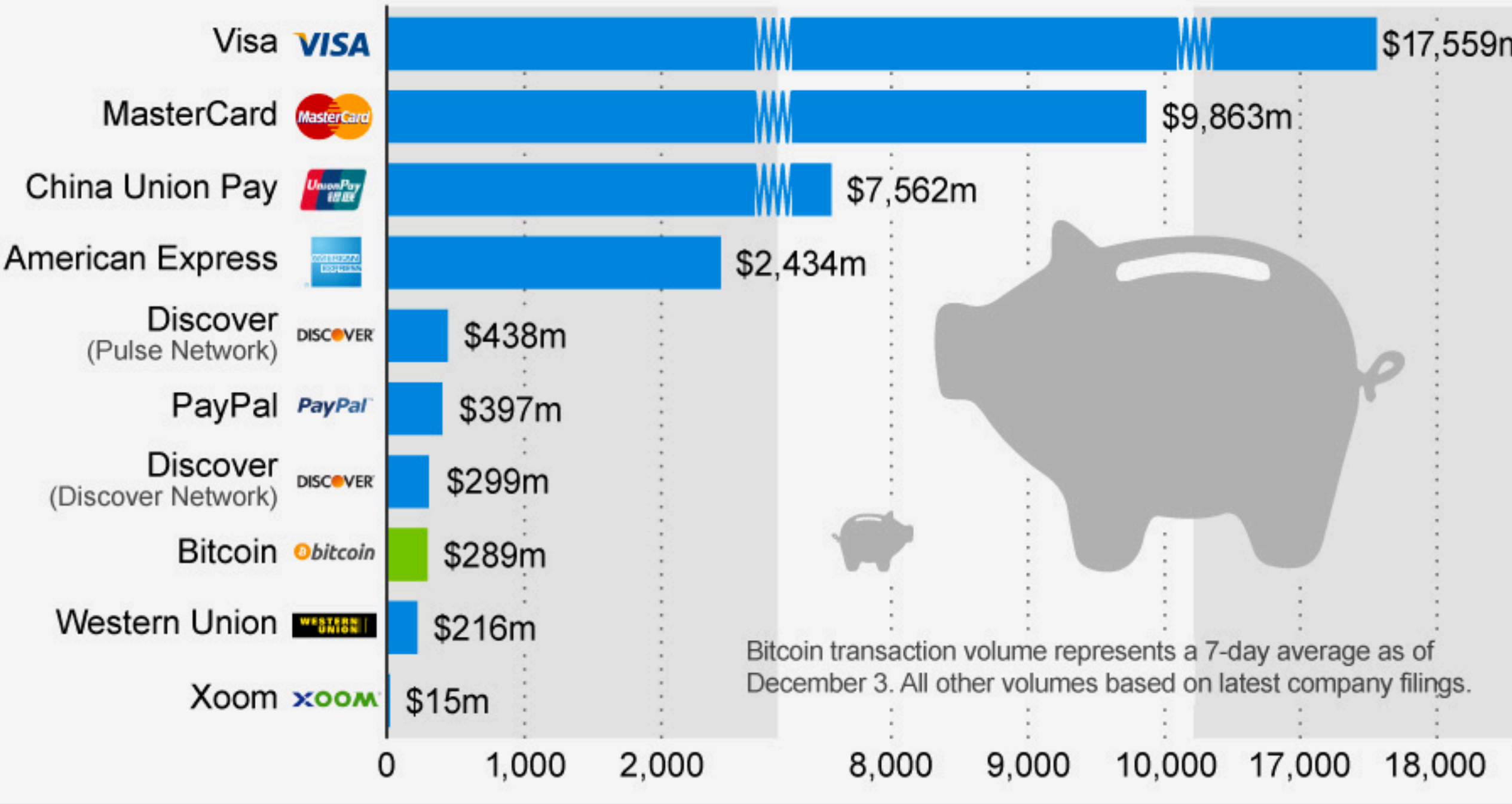


POSSIBILITIES

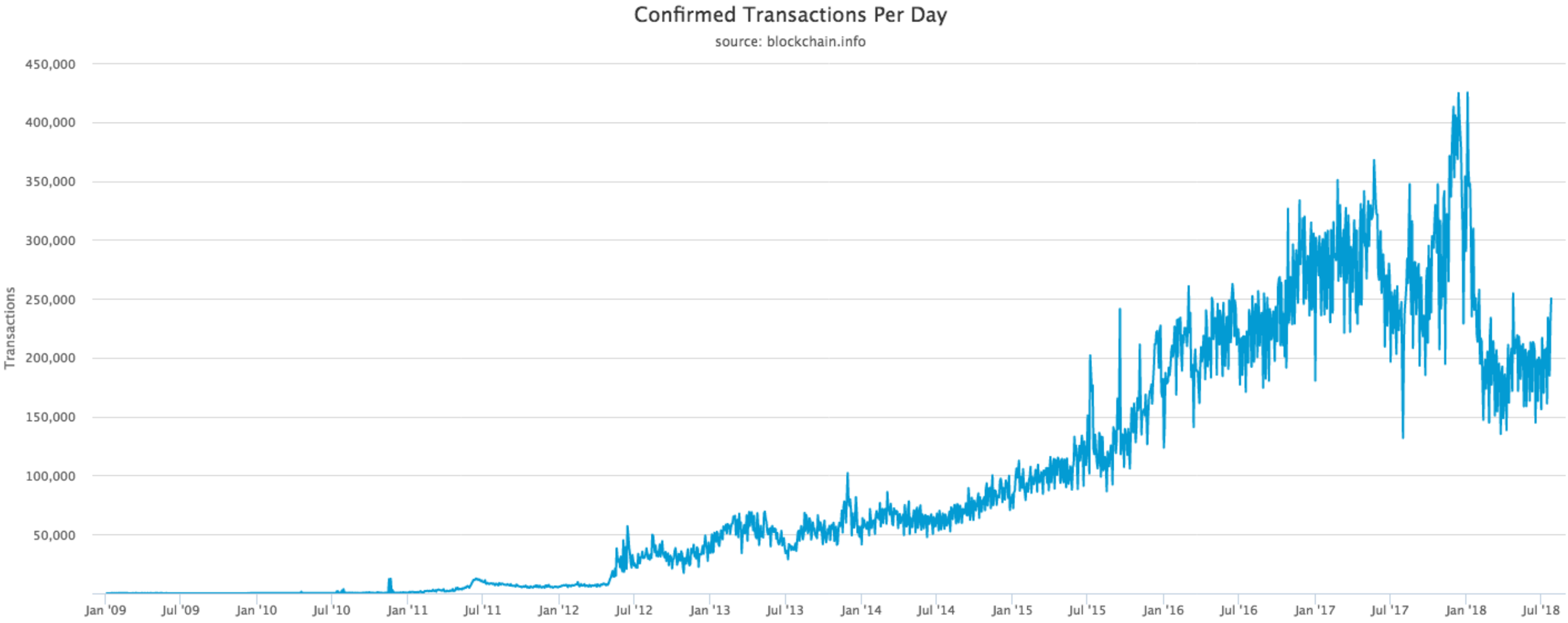
- End of national currencies (and government plans to take your money)
- End of Banks (and their abuse taxes)
- The end of predatory lending
- The end of IRF
- The end of the voting booth
- The end of payment orders
- Anyone with a cell phone can act as a bank

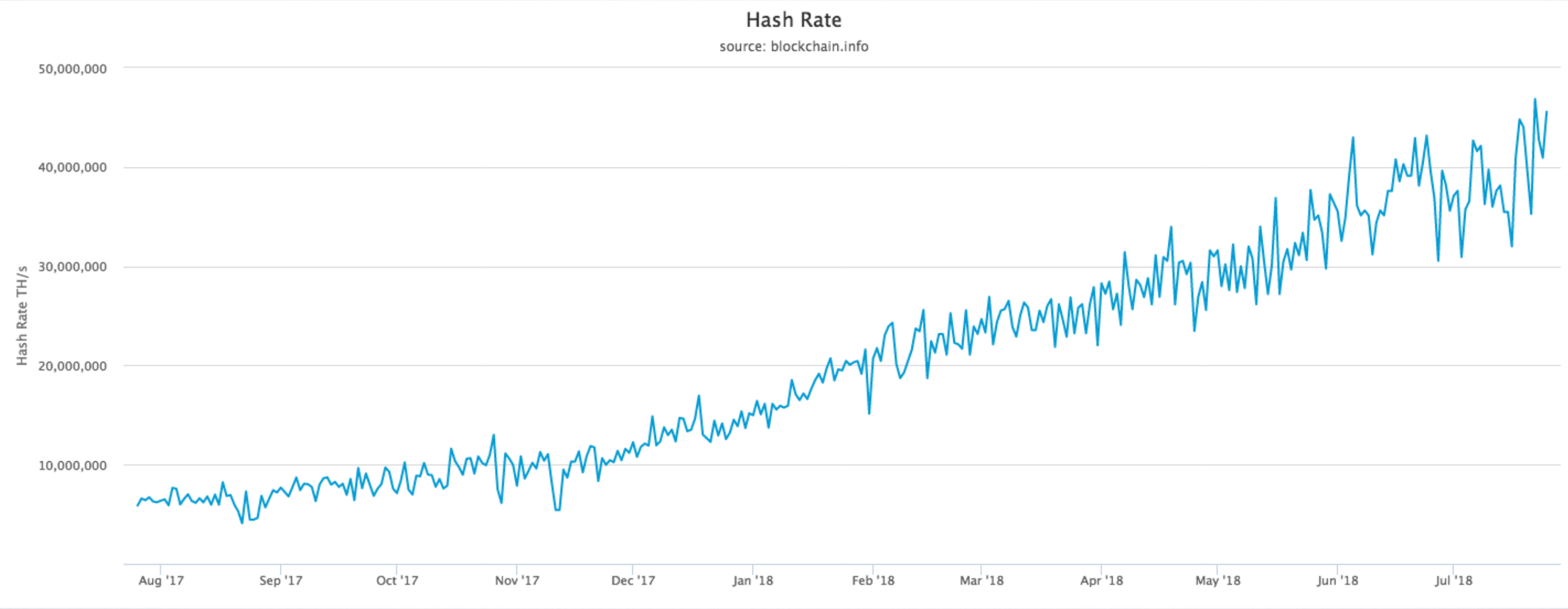
How Bitcoin Activity Stacks Up Against Other Payment Networks

Average daily transaction volume of selected payment networks (in million U.S. dollars)

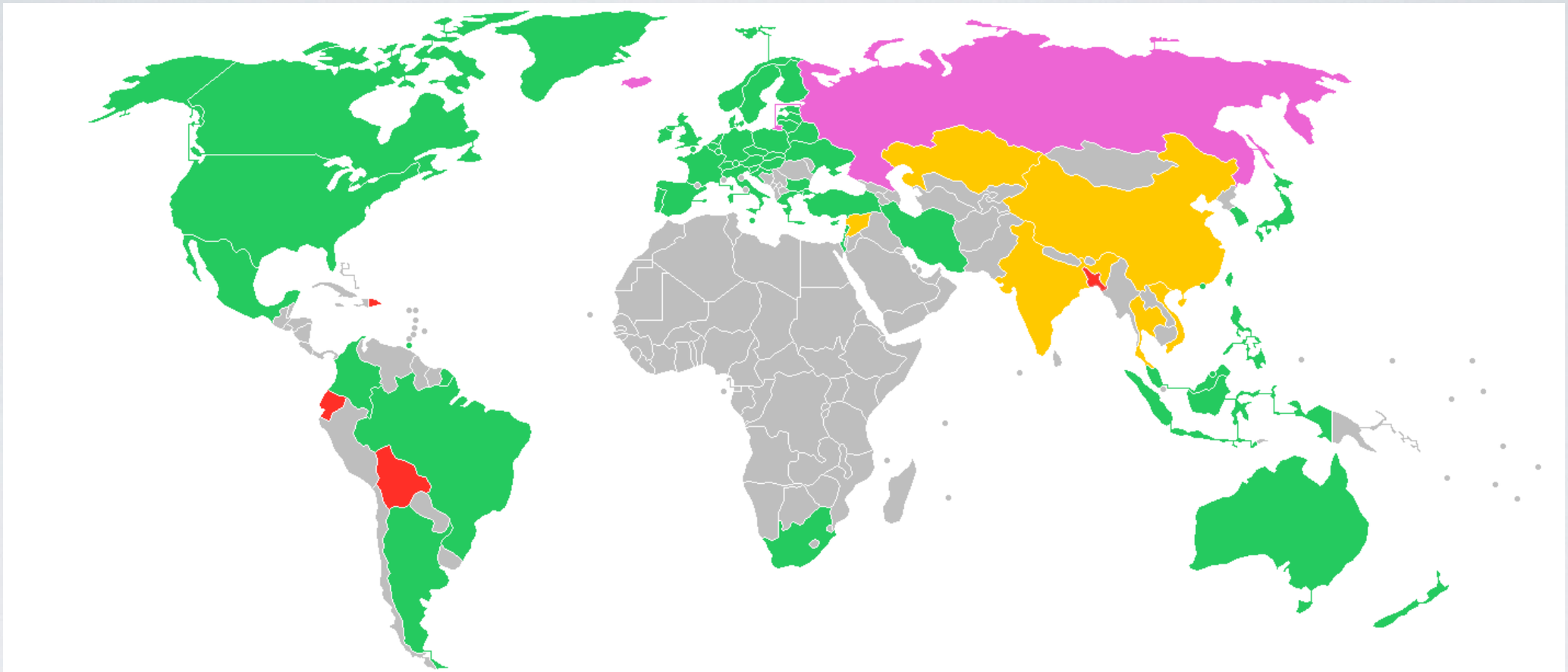


Source: Coinometrics


Confirmed Transactions Per Day
source: blockchain.info
Transactions
450,000
400,000
350,000
300,000
250,000
200,000
150,000
100,000
50,000
Jan '09
Jul '09
Jan '10
Jul '10
Jan '11
Jul '11
Jan '12
Jul '12
Jan '13
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
Jan '17
Jul '17
Jan '18
Jul '18


Hash Rate
source: blockchain.info
Hash Rate TH/s
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
Aug '17
Sep '17
Oct '17
Nov '17
Dec '17
Jan '18
Feb '18
Mar '18
Apr '18
May '18
Jun '18
Jul '18


Market Price (USD)
source: blockchain.info
USD
22,500
20,000
17,500
15,000
12,500
10,000
7,500
5,000
2,500
Jan '09
Jul '09
Jan '10
Jul '10
Jan '11
Jul '11
Jan '12
Jul '12
Jan '13
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
Jan '17
Jul '17
Jan '18
Jul '18



LEGALITY

2	Ethereum	$48,153,443,418	$477.06	$1,588,420,000	100,937,495 ETH	0.50%	
3	XRP	$18,080,457,201	$0.459879	$188,618,000	39,315,683,476 XRP *	-0.60%	
4	Bitcoin Cash	$14,402,226,598	$834.49	$580,286,000	17,258,738 BCH	-0.15%	
5	EOS	$7,702,915,690	$8.60	$621,283,000	896,149,492 EOS *	0.17%	
6	Stellar	$6,097,836,041	$0.324917	$187,685,000	18,767,365,329 XLM *	0.21%	
7	Litecoin	$5,001,983,379	$86.87	$272,513,000	57,581,957 LTC	-0.46%	
8	Cardano	$4,415,872,727	$0.170319	$77,473,100	25,927,070,538 ADA *	-1.09%	
9	IOTA	$2,886,236,451	$1.04	$42,523,600	2,779,530,283 MIOTA *	5.10%	
10	Tether	$2,511,201,913	$1.00	$2,660,620,000	2,507,140,346 USDT *	0.42%	
11	TRON	$2,490,663,391	$0.037882	$185,072,000	65,748,111,645 TRX *	1.35%	
12	Monero	$2,297,669,536	$141.30	$29,724,000	16,261,161 XMR	0.21%	
13	NEO	$2,243,930,000	$34.52	$80,969,200	65,000,000 NEO *	0.57%	
14	Dash	$2,033,845,016	$247.53	$137,089,000	8,216,593 DASH	0.45%	
15	Ethereum Classic	$1,767,381,725	$17.11	$181,955,000	103,320,612 ETC	3.04%	
16	NEM	$1,644,489,000	$0.182721	$10,169,900	8,999,999,999 XEM *	0.78%	
17	VeChain	$1,427,910,282	$2.57	$7,849,350	554,545,494 VEN *	30.49%	
18	Tezos	$1,322,588,690	$2.18	$2,532,330	607,489,041 XTZ *	4.44%	
19	Binance Coin	$1,273,659,496	$13.34	$53,571,400	95,512,523 BNB *	3.51%	
20	OmiseGO	$1,010,500,351	$7.21	$36,007,000	140,245,398 OMG *	0.86%	

OTHERS INTERESTING PROJECTS

- Brave browser– BAT Secure Desktop and Mobile Browser
- Oyster storage – PRL Cloud storage
- NapoleonX – Decentralized prediction market
- Nexo –Lending Platform
- Dent – Mobile data lending
- Steemit– Blockchain-based rewards blogging platform
- view.ly– Crypto-decentralized video platform
- Bitbay– Decentralized marketplace
- Bounty0x– Decentralized bounty hunting platform
- Golem– Computing power shared machine learning, rendering, computing power
- Nebula– Decentralized AI Blockchain

TOKENS

- A wider use is supported by the digital infrastructure introduced by Bitcoin, they are represented by "tokens".

- A "token" can be defined as a "scarce digital asset based on the underlying technology inspired by Bitcoin."

- Tokens can use similar code bases, but different blockchain databases.

- The Ethereum was inspired by Bitcoin, but has its own blockchain and was designed to be more programmable. Tokens can be issued at the top of the blockchain Ethereum.

- Token buyers are buying private keys, which are similar to the API keys, but can be transferred to other parties without the consent.

3 LEVELS OF BLOCKCHAIN

1. Storage for digital records

2. Exchanging digital assets (called tokens)

3. Running Smart Contracts

- Basic rules - Terms and conditions registered in the code

- Distributed network performs contract and monitors compliance

- Results are automatically validated without third parties

SMART CONTRACTS

- Consensus protocols are critical to determining the sequence of actions resulting from the contract code.

- This allows you to negotiate everything using peer-to-peer, from renewable energy to automated reservations of hotel rooms.

WHAT ARE SMART CONTRACTS?

- They are computer protocols that facilitate, verify or reinforce the negotiation or execution of a contract or make a contractual clause unnecessary

- It can help to exchange money, property, stocks or anything of value in a transparent and conflict-free manner, avoiding the services of an intermediary

- Set the rules and penalties around a contract in the same way as a traditional contract, but also automatically impose those obligations (code is law)

Average Settlement Time By Transaction Type

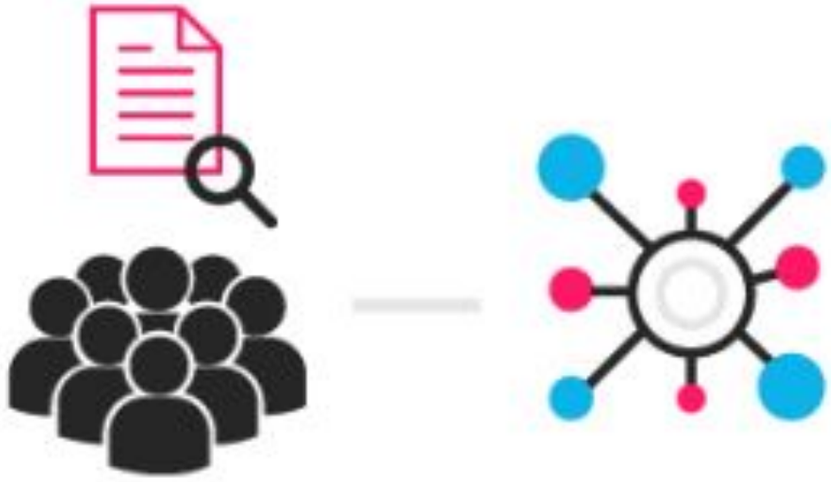
1

An option contact between parties is written as code into the blockchain. The individuals involved are anonymous, but the contact is the public ledger.

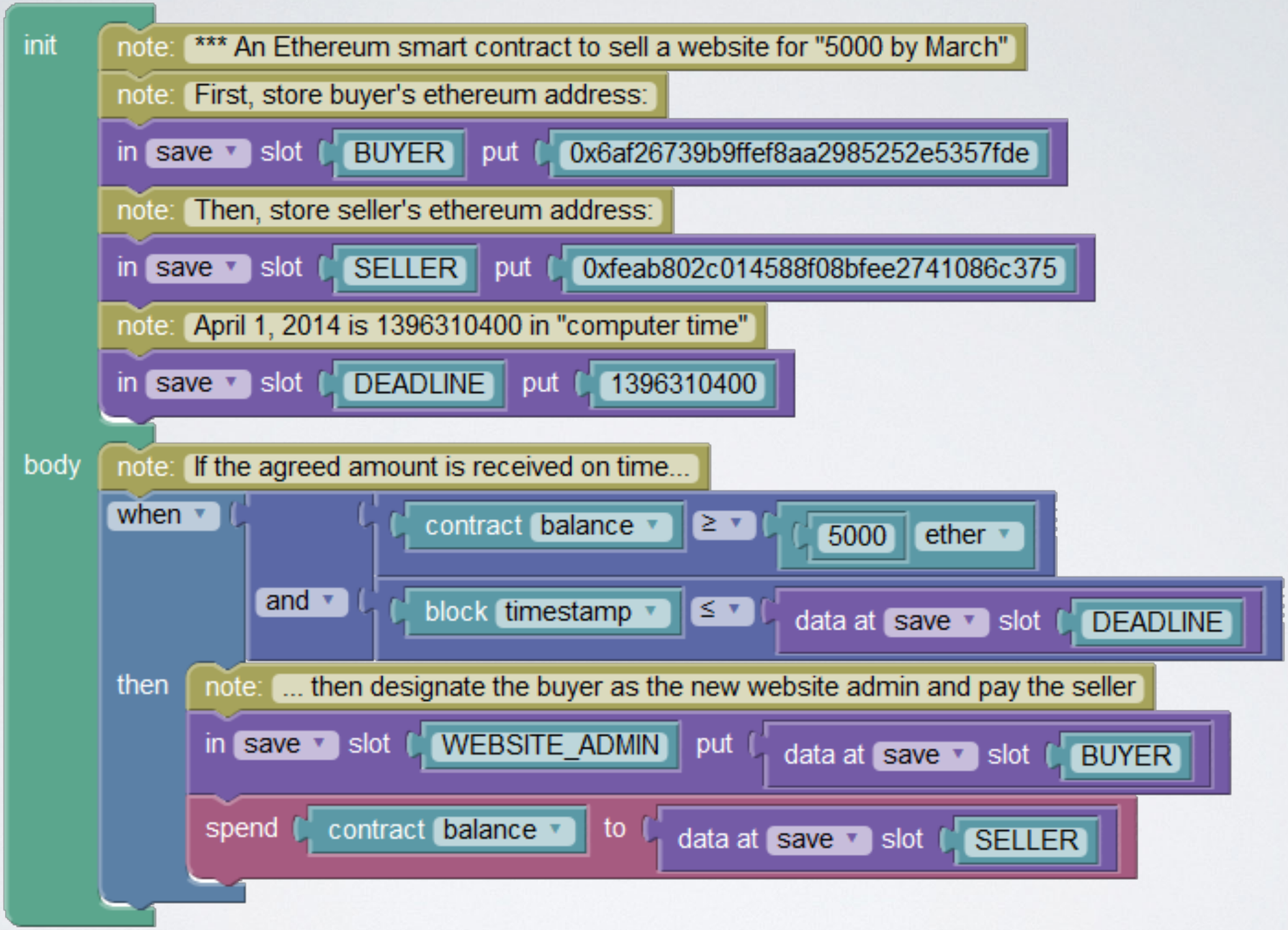
2

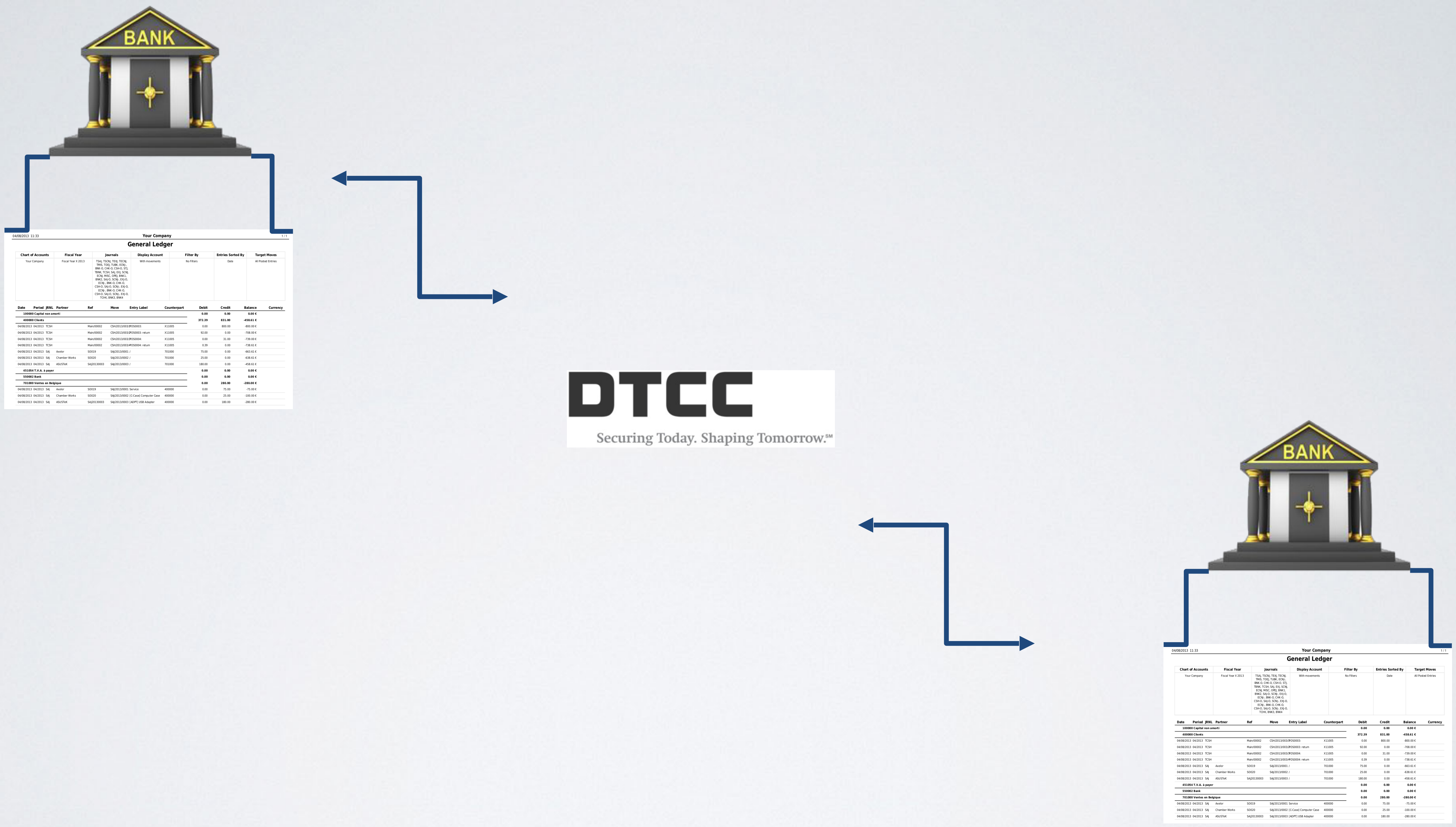
A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

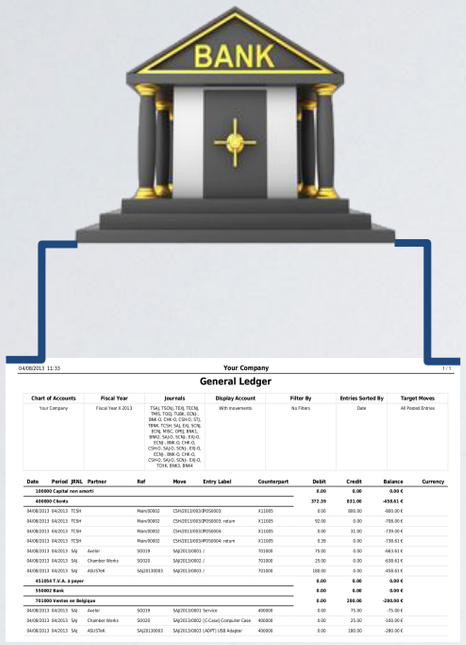
3



Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions


init
note: *** An Ethereum smart contract to sell a website for "5000 by March"
note: First, store buyer's ethereum address:
in save slot BUYER put 0x6af26739b9ffef8aa2985252e5357fde
note: Then, store seller's ethereum address:
in save slot SELLER put 0xfeab802c014588f08bfee2741086c375
note: April 1, 2014 is 1396310400 in "computer time"
in save slot DEADLINE put 1396310400
body
note: If the agreed amount is received on time...
when
contract balance ≥ 5000 ether
and
block timestamp ≤ data at save slot DEADLINE
then
note: ... then designate the buyer as the new website admin and pay the seller
in save slot WEBSITE_ADMIN put data at save slot BUYER
spend contract balance to data at save slot SELLER


BANK
Your Company
General Ledger
DTCC
Securing Today. Shaping Tomorrow.
BANK
Your Company
General Ledger



04/08/2013 11:33 — Your Company — 1 / 1

General Ledger

Chart of Accounts	Fiscal Year	Journals	Display Account	Filter By	Entries Sorted By	Target Moves
Your Company	Fiscal Year # 2013	TSAJ, TSCN), TCH), TSC(N), TMS), TOJ), TUBK, ECN) , BNK-O, CHK-O, CSH-O, ST), TRNK, TCSH, SAJ, EXJ, SCN), ECN, MISC, OPEJ, BNK-O, CHK-O, CSH-O, ST), ECN) , BNK-O, CHK-O, CSHO, SAJ-O, SCN), EXJ-O, ECN) , BNK-O, CHK-O, CSHO, SAJO, SCN), EXJ-O, TCH, BNKO, BNKK	With movements	No Filters	Date	All Posted Entries

Date	Period	JRNL	Partner	Ref	Move	Entry Label	Counterpart	Debit	Credit	Balance	Currency
100000 Capital non amorti								**0.00**	**0.00**	**0.00 €**	
400000 Clients								**372.39**	**831.08**	**-458.61 €**	
04/08/2013	04/2013	TCSH			Main/00002	CSH/2013/003/POS0003	X11005	0.00	880.00	-880.00 €	
04/08/2013	04/2013	TCSH			Main/00002	CSH/2013/003/POS0003 return	X11005	92.00	0.00	-788.00 €	
04/08/2013	04/2013	TCSH			Main/00002	CSH/2013/003/POS0004	X11005	0.00	31.00	-739.00 €	
04/08/2013	04/2013	TCSH			Main/00002	CSH/2013/003/POS0004 return	X11005	0.39	0.00	-738.61 €	
04/08/2013	04/2013	SAJ	Axelor		SO019	SAJ/2013/0001 /	701000	75.00	0.00	-663.61 €	
04/08/2013	04/2013	SAJ	Chamber Works		SO020	SAJ/2013/0002 /	701000	25.00	0.00	-638.61 €	
04/08/2013	04/2013	SAJ	ASUSTeK		SAJ/2013/0003	SAJ/2013/0003 /	701000	180.00	0.00	-458.61 €	
411054 T.V.A. à payer								**0.00**	**0.00**	**0.00 €**	
550002 Bank								**0.00**	**0.00**	**0.00 €**	
701000 Ventes en Belgique								**0.00**	**288.00**	**-288.00 €**	
04/08/2013	04/2013	SAJ	Axelor		SO019	SAJ/2013/0001 Service	400000	0.00	75.00	-75.00 €	
04/08/2013	04/2013	SAJ	Chamber Works		SO020	SAJ/2013/0002 (C-Case) Computer Case	400000	0.00	25.00	-100.00 €	
04/08/2013	04/2013	SAJ	ASUSTeK		SAJ/2013/0003	SAJ/2013/0003 (ADPT) USB Adapter	400000	0.00	180.00	-280.00 €	

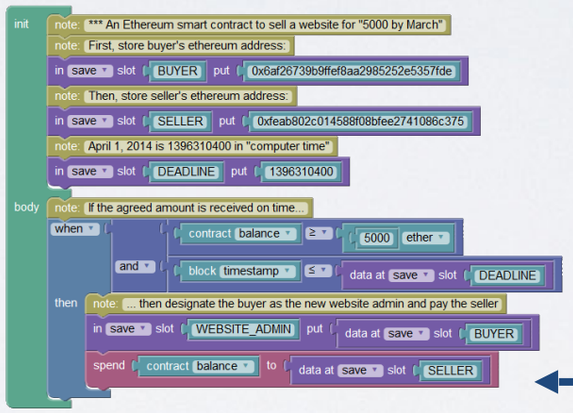
```
init
    note: *** An Ethereum smart contract to sell a website for "5000 by March"
    note: First, store buyer's ethereum address:
    in save slot BUYER put 0x6af26739b9ffef8aa2985252e5357fde
    note: Then, store seller's ethereum address:
    in save slot SELLER put 0xfeab802c014588f08bfee2741086c375
    note: April 1, 2014 is 1396310400 in "computer time"
    in save slot DEADLINE put 1396310400
body
    note: If the agreed amount is received on time...
    when
        contract balance ≥ 5000 ether
        and
        block timestamp ≤ data at save slot DEADLINE
    then
        note: ... then designate the buyer as the new website admin and pay the seller
        in save slot WEBSITE_ADMIN put data at save slot BUYER
        spend contract balance to data at save slot SELLER
```

04/08/2013 11:33 — Your Company — 1 / 1

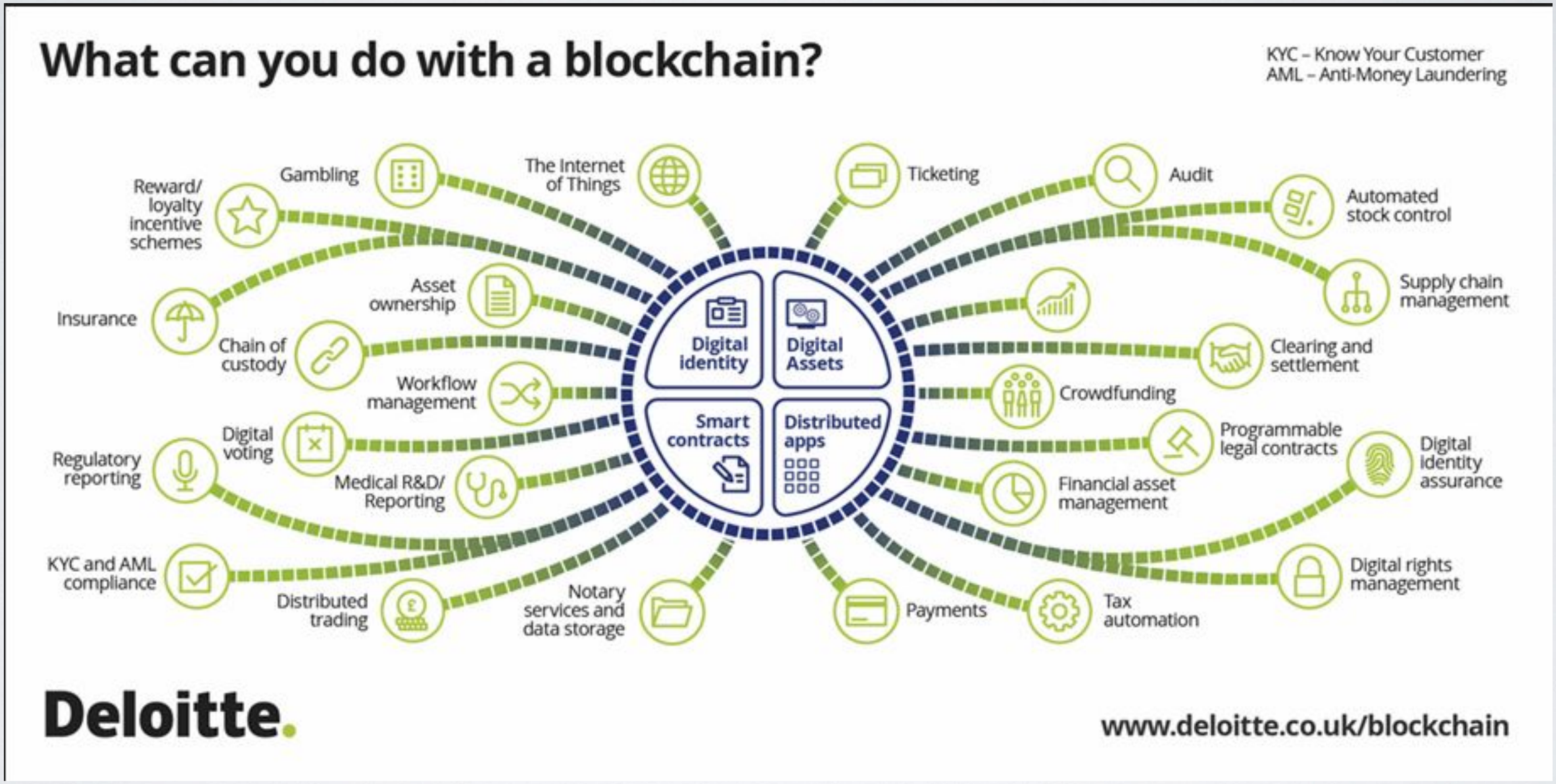
General Ledger

Chart of Accounts	Fiscal Year	Journals	Display Account	Filter By	Entries Sorted By	Target Moves
Your Company	Fiscal Year # 2013	TSAJ, TSCN), TCH), TSC(N), TMS), TOJ), TUBK, ECN) , BNK-O, CHK-O, CSH-O, ST), TRNK, TCSH, SAJ, EXJ, SCN), ECN, MISC, OPEJ, BNK-O, CHK-O, CSH-O, SAJ-O, SCN), EXJ-O, ECN) , BNK-O, CHK-O, CSHO, SAJO, SCN), EXJ-O, TCH, BNKO, BNKK	With movements	No Filters	Date	All Posted Entries

Date	Period	JRNL	Partner	Ref	Move	Entry Label	Counterpart	Debit	Credit	Balance	Currency
100000 Capital non amorti								**0.00**	**0.00**	**0.00 €**	
400000 Clients								**372.39**	**831.08**	**-458.61 €**	
04/08/2013	04/2013	TCSH			Main/00002	CSH/2013/003/POS0003:	X11005	0.00	880.00	-880.00 €	
04/08/2013	04/2013	TCSH			Main/00002	CSH/2013/003/POS0003: return	X11005	92.00	0.00	-788.00 €	
04/08/2013	04/2013	TCSH			Main/00002	CSH/2013/003/POS0004:	X11005	0.00	31.00	-739.00 €	
04/08/2013	04/2013	TCSH			Main/00002	CSH/2013/003/POS0004: return	X11005	0.39	0.00	-738.61 €	
04/08/2013	04/2013	SAJ	Axelor		SO019	SAJ/2013/0001 /	701000	75.00	0.00	-663.61 €	
04/08/2013	04/2013	SAJ	Chamber Works		SO020	SAJ/2013/0002 /	701000	25.00	0.00	-638.61 €	
04/08/2013	04/2013	SAJ	ASUSTeK		SAJ/2013/0003	SAJ/2013/0003 /	701000	180.00	0.00	-458.61 €	
411054 T.V.A. à payer								**0.00**	**0.00**	**0.00 €**	
550002 Bank								**0.00**	**0.00**	**0.00 €**	
701000 Ventes en Belgique								**0.00**	**288.00**	**-288.00 €**	
04/08/2013	04/2013	SAJ	Axelor		SO019	SAJ/2013/0001 Service	400000	0.00	75.00	-75.00 €	
04/08/2013	04/2013	SAJ	Chamber Works		SO020	SAJ/2013/0002 (C-Case) Computer Case	400000	0.00	25.00	-100.00 €	
04/08/2013	04/2013	SAJ	ASUSTeK		SAJ/2013/0003	SAJ/2013/0003 (ADPT) USB Adapter	400000	0.00	180.00	-280.00 €	


init
note *** An Ethereum smart contract to sell a website for "5000 by March"
note First, store buyer's ethereum address:
in save slot BUYER put 0x6af26739b9ffef8aa2985252e5357fde
note Then, store seller's ethereum address:
in save slot SELLER put 0xfeab802c014588f08bfee2741086c375
note April 1, 2014 is 1396310400 in "computer time"
in save slot DEADLINE put 1396310400
body
note If the agreed amount is received on time...
when
contract balance ≥ 5000 ether
and
block timestamp ≤ data at save slot DEADLINE
then
note ... then designate the buyer as the new website admin and pay the seller
in save slot WEBSITE_ADMIN put data at save slot BUYER
spend contract balance to data at save slot SELLER

USE CASES


What can you do with a blockchain?
KYC – Know Your Customer
AML – Anti-Money Laundering
Reward/ loyalty incentive schemes
Gambling
The Internet of Things
Ticketing
Audit
Automated stock control
Insurance
Asset ownership
Supply chain management
Chain of custody
Digital identity
Digital Assets
Clearing and settlement
Workflow management
Crowdfunding
Digital voting
Smart contracts
Distributed apps
Programmable legal contracts
Regulatory reporting
Medical R&D/ Reporting
Financial asset management
Digital identity assurance
KYC and AML compliance
Distributed trading
Notary services and data storage
Payments
Tax automation
Digital rights management
Deloitte.
www.deloitte.co.uk/blockchain

ethereum

The World Computer - Open Source Peer-to-Peer Applications

ETHEREUM

- Ethereum is a decentralized platform that executes smart contracts: applications that run exactly as scheduled without any chance of downtime, censorship, fraud, or third-party interference.

- These applications run on a custom blockchain, an extremely powerful shared global infrastructure that can move value and represent ownership of the property.

- This allows developers to create markets, store debt records or promises, move funds according to past instructions (such as a will or a future contract), and many things that have not yet been invented, all without an intermediary or counterparts risk .

ENTERPRISE
ETHEREUM
ALLIANCE

OUR VISION

Be an open source standard, not a product

Address enterprise deployment requirements

Evolve in tandem with advances in public Ethereum

Leverage existing standards

OUR MISSION

A clear roadmap for enterprise features and requirements

Robust governance model and accountability, clarity around IP and licensing models for open source technology

Resources for businesses to learn about Ethereum and leverage this groundbreaking technology to address specific industry use cases

ETHER

- Ether is the fuel for the Ethereum network.
- Ether is a necessary element - a fuel - to operate the Ethereum distributed application platform.
- It is a form of payment made by platform customers for the machines that perform the requested operations, serving as the incentive that ensures that developers write quality applications and that the network remains healthy.
- The total supply of ether and its emission rate were decided by the donations collected in the pre-sale of 2014.
- Developers wishing to create applications that will use the Ethereum blockchain need ether.
- Users who want to access and interact with smart contracts in the Ethereum blockchain also need ether.

ERC-20

- ERC (Ethereum Request for Comments) is an official protocol for making suggestions to improve the Ethereum network;
    - 20 - is the unique identification number of the offer.
- Tokens that meet these specifications are known as ERC-20 tokens and are actually smart contracts for the system
- The ERC-20 standard defines a set of rules that must be met in order for a token to be accepted and capable of interacting with other tokens on the network.
- The tokens themselves are block assets, which can have value, and can be sent and received like any other cryptomade of Ethereum blocks.

ERC-721

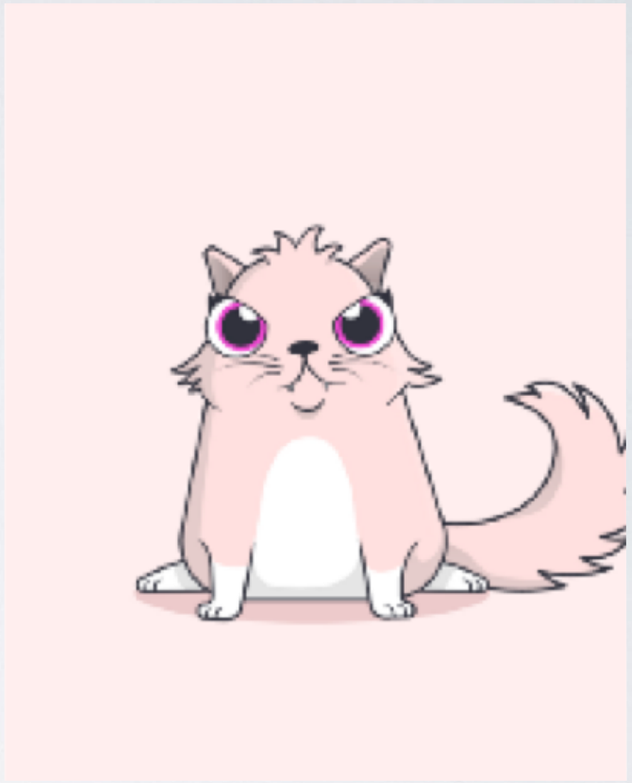
- ERC-721 is an open, free standard that describes how to create non-fungible or exclusive coins in the Ethereum blockchain.

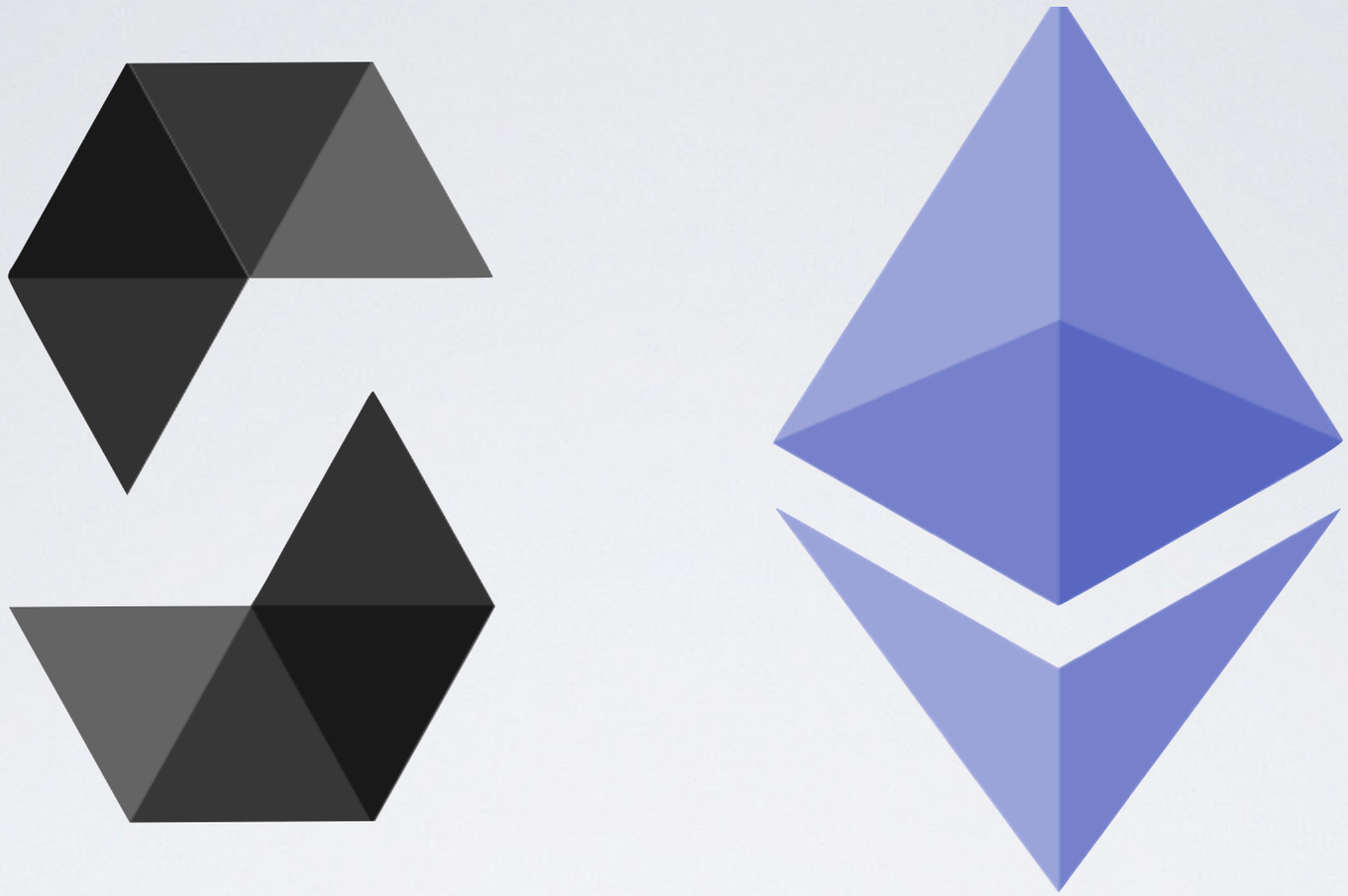
- While most tokens are fungible (each token is the same as any other token), ERC-721 tokens are all unique.

- Think of them as rare and unique collectibles.

CRYTOKITTIES

- CryptoKitties is a virtual blockchain based game developed by Axiom Zen that allows players to buy, collect, play and sell various types of virtual cats.
- It represents one of the first attempts to deploy blockchain technology for recreational and leisure purposes.
- The popularity of the game in December 2017 congested the Ethereum network, causing it to reach a record of transactions and slow significantly.
- On March 20, 2018, it was announced that CryptoKitties would be dismantled in its own company and raised $ 12 million from various venture capital firms and angel investors.
- In December 2017, a CryptoKitty was sold for $ 100,000.



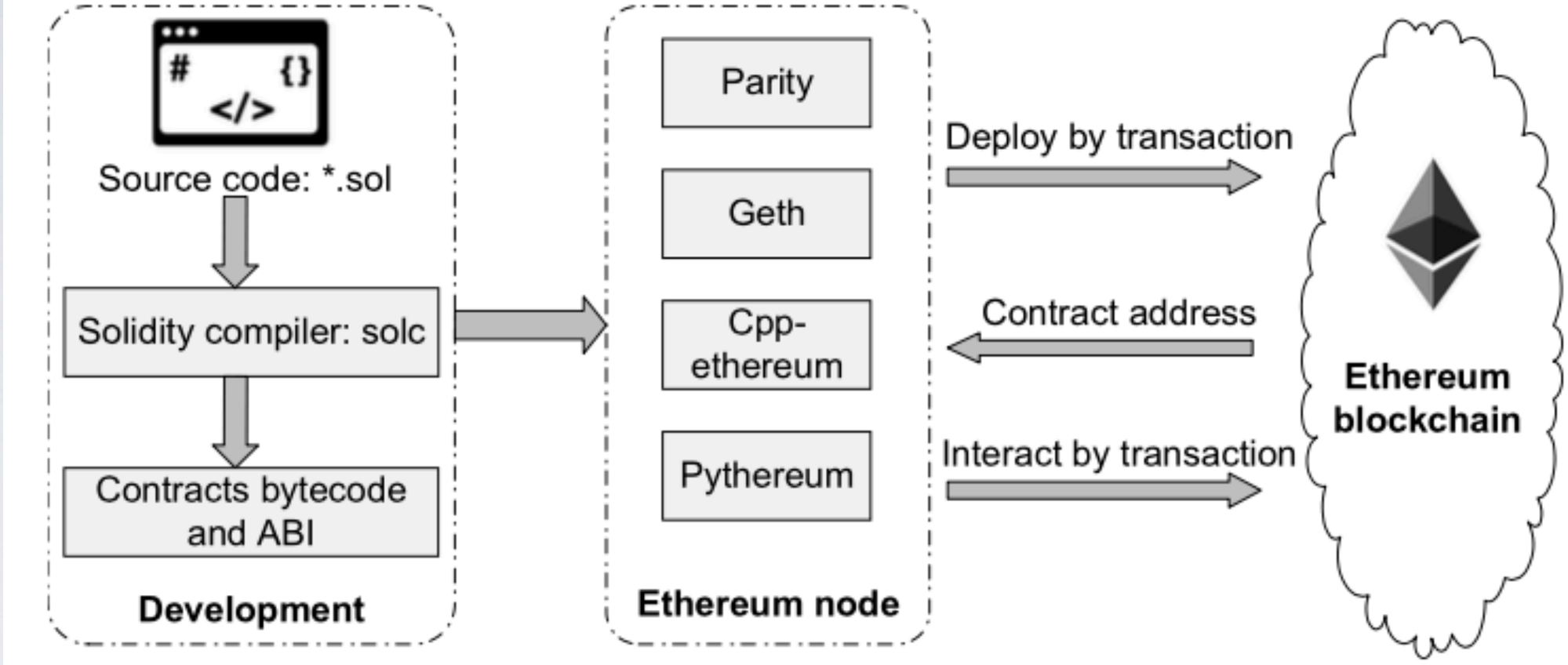


SOLIDITY

Language to create smart contracts

SOLIDITY

- High-Level Object-Oriented Language for Smart Contracts
- Solidity was initially proposed in August 2014 by Gavin Wood
- Solidity allows programming in Ethereum, a blockchain-based virtual machine
- Solidity is a programming language with static typing
- A Contract programming language that has similarities to Javascript and C
- Specific features of the contract include modifier (guard) clauses, event notifiers, and custom global variables.
- Solidity is compiled to bytecode which is executable in EVM



SMART CONTRACT DEPLOYMENT

IOS APPS

- Creation of a token and an economy (that can be shared between games/apps);
- Allowing payment in cryptocurrencies;
- Creation of unique itens (that can also be traded and shared between games/apps);
- Creation of smart contracts to automatize of services and also transparency;

PRACTICAL EXAMPLE

- Creating a Smart contract
- Creating an iOS App to interact with the contract
- Code:
  - https://github.com/mjoselli/ETH_iOS_workshop

MINICHALLENGE EXAMPLE

- Big Idea: Blockchain
- Essential Question: How can the blockchain change peoples live?
- Challenge: Develop an App that use the blockchain to help people?