CORVINUS
UNIVERSITY of
BUDAPEST

CORVINUS
FINTECH
CENTER

Blockchain in supply chain management and protection of digital content

Tuan Trinh

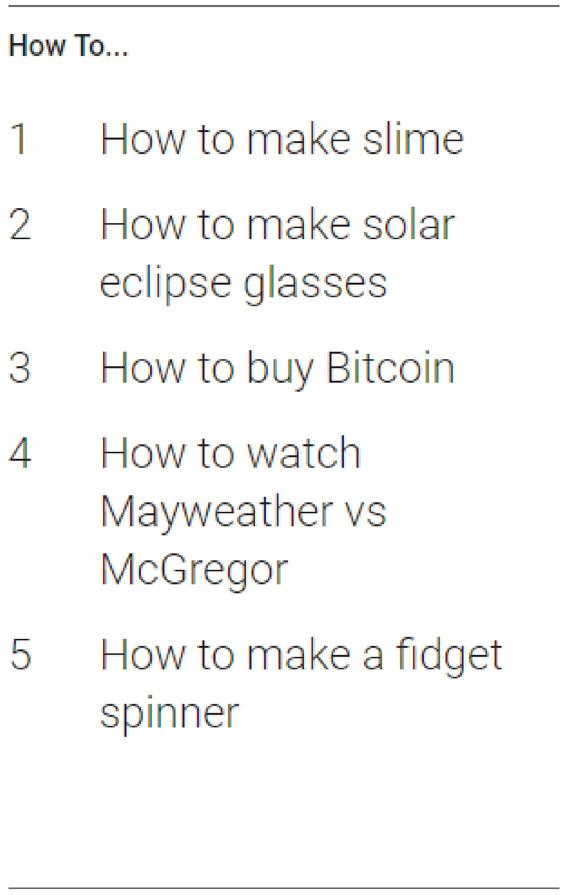
Head of Corvinus Fintech Center

Director of FinTech Working Group, Hungarian ICT Association (IVSZ)

Member of the Advosory Board of NISCI

Hanoi, NISCI AB meeting, August 2, 2018

Most Google-searched items of 2017



How To...

1 How to make slime

2 How to make solar eclipse glasses

3 How to buy Bitcoin

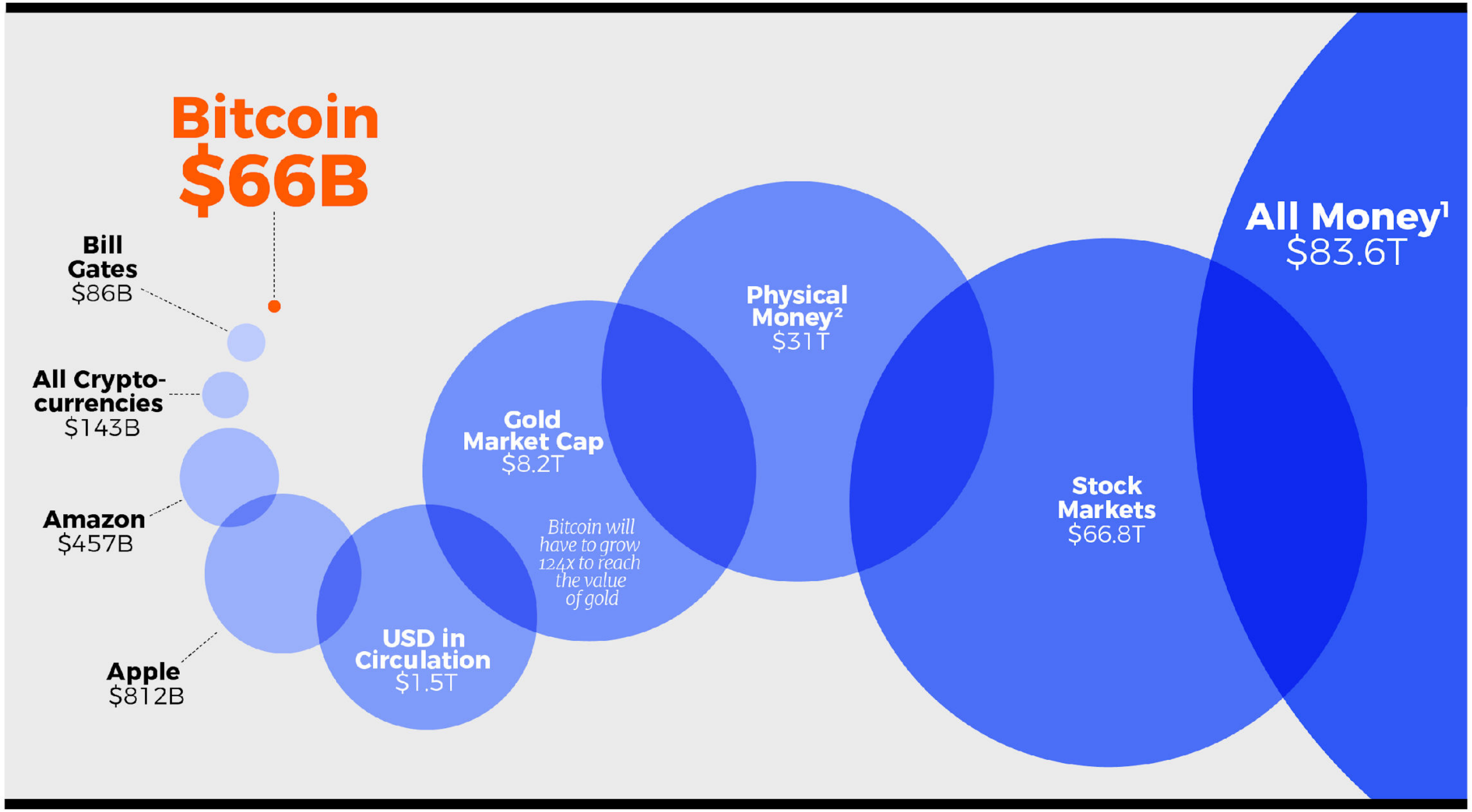
4 How to watch Mayweather vs McGregor

5 How to make a fidget spinner

Bitcoin in Perspective

The market share for cryptocurrencies can grow a lot more

August 2017



Sources:
https://howmuch.net/articles/worlds-money-in-perspective
https://coinmarketcap.com
https://www.forbes.com
https://www.federalreserve.gov
https://www.cia.gov

[1] **All Money** = money in any form including bank or other deposits as well as notes and coins.

[2] **Physical Money** = money in forms that can be used as a medium of exchange, generally notes, coins, and certain balances held by banks.

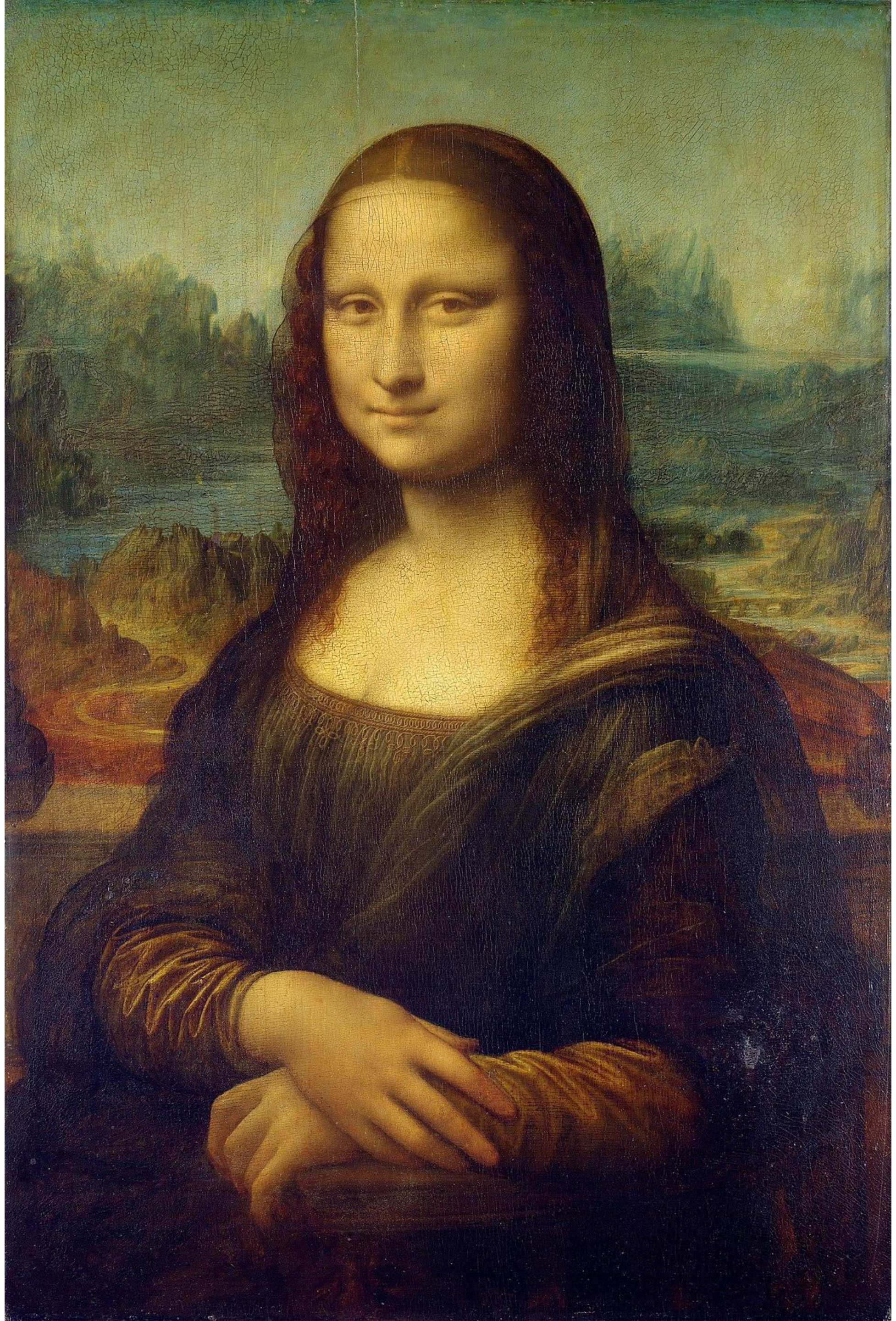
BITCOINIRA

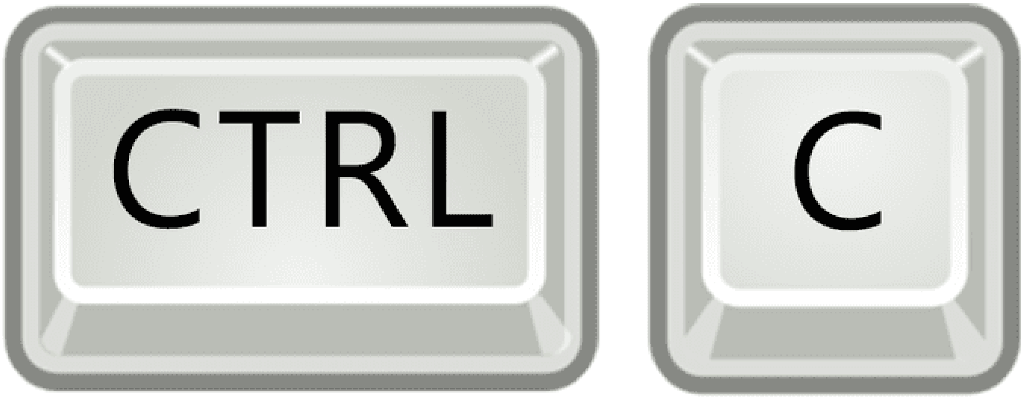
🇻🇳

202,6 billion USD (2016)

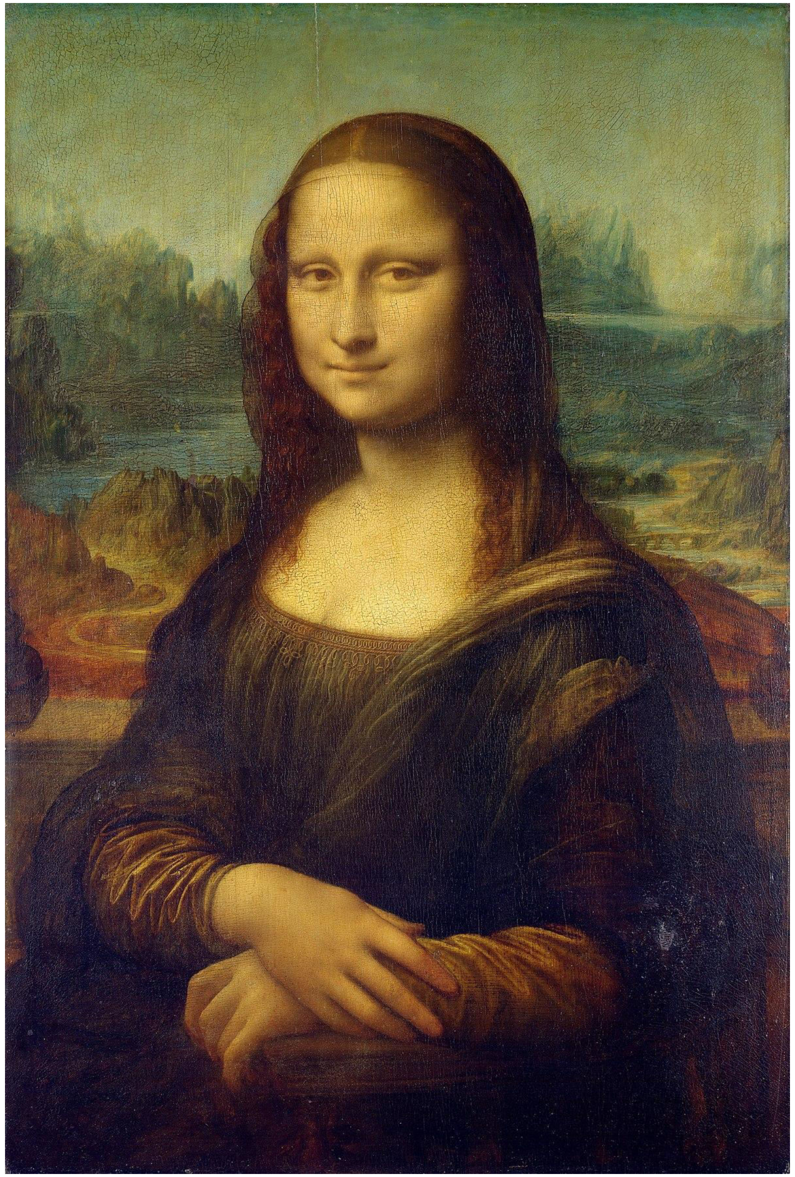
GDP: 🇭🇺

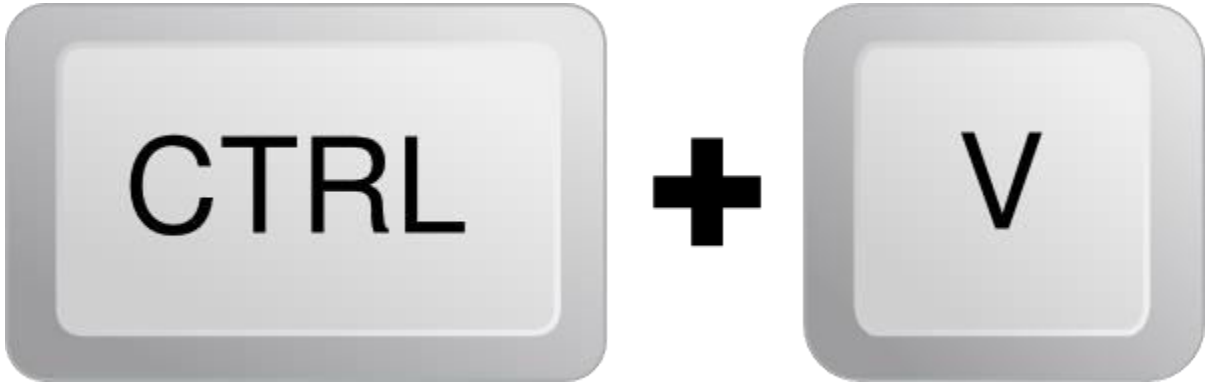
124.3 billion USD (2016)



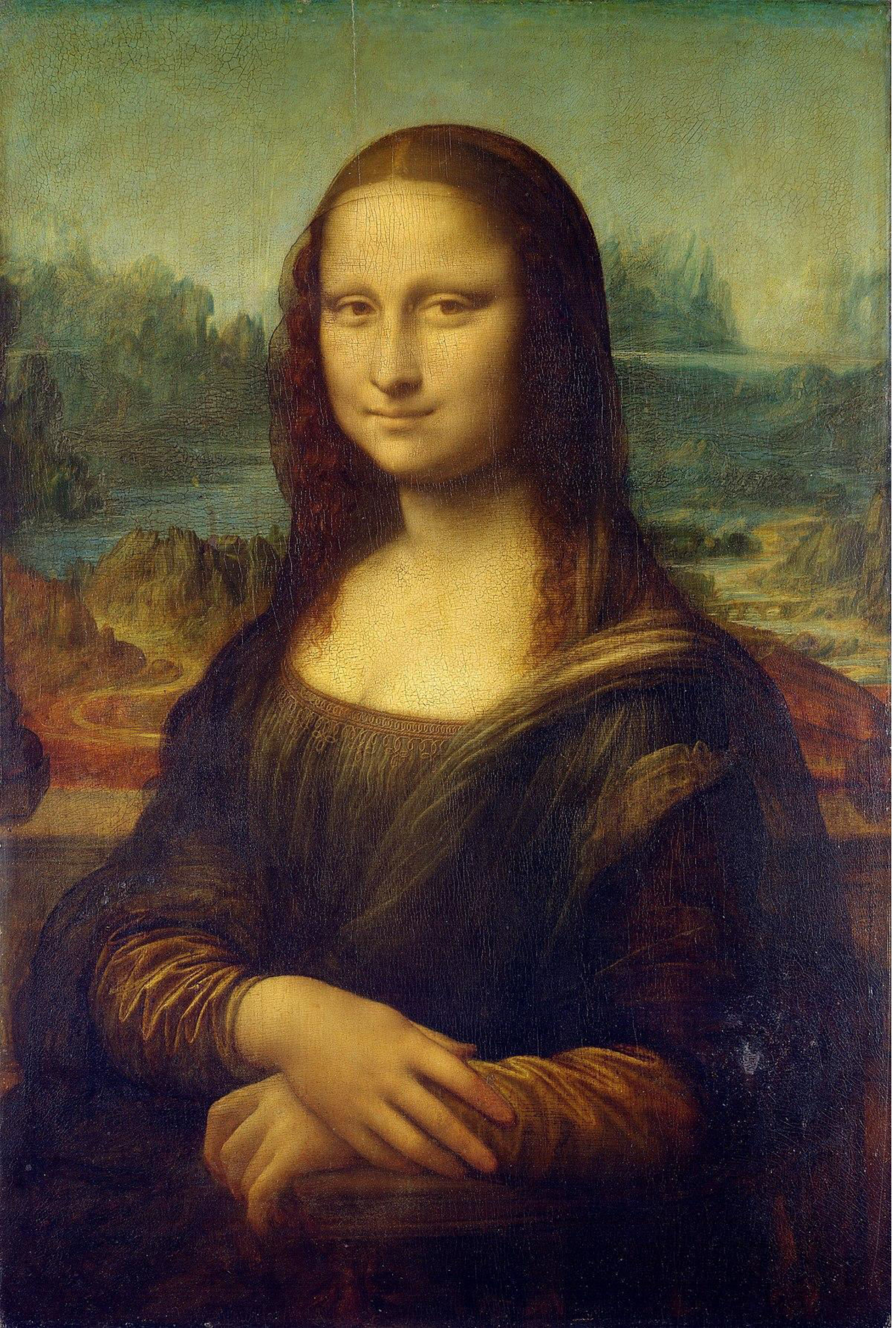


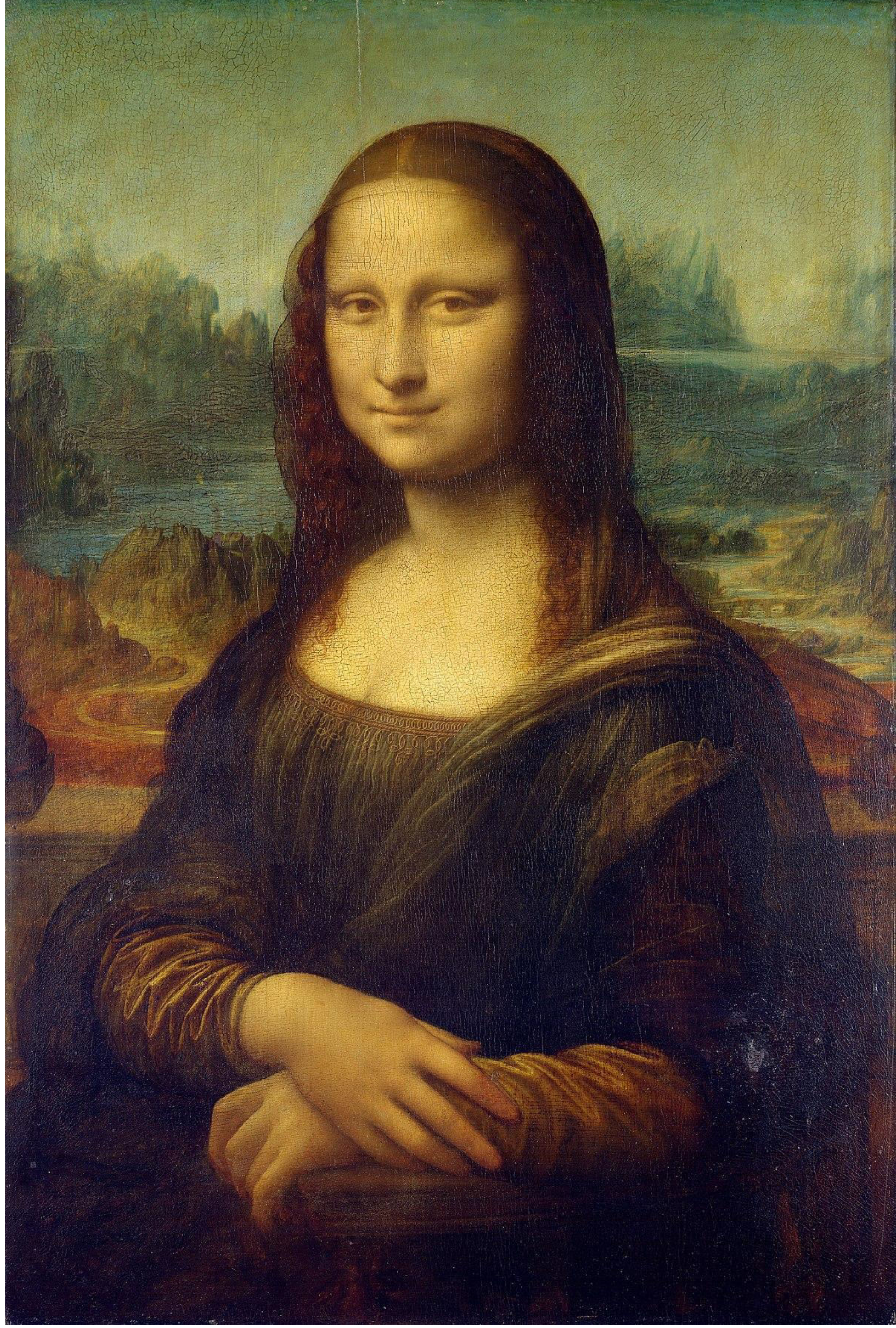
CTRL
C



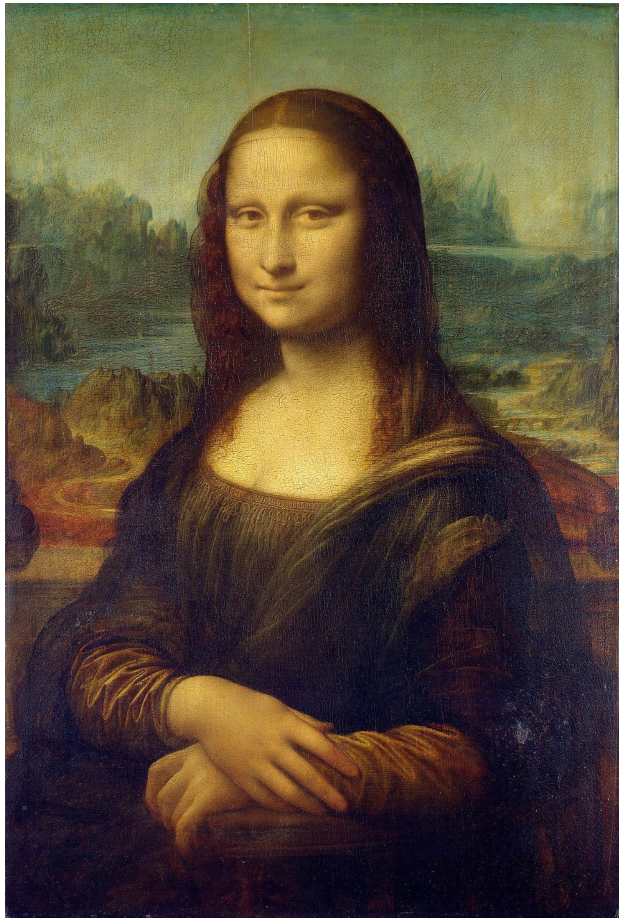


CTRL
+
V



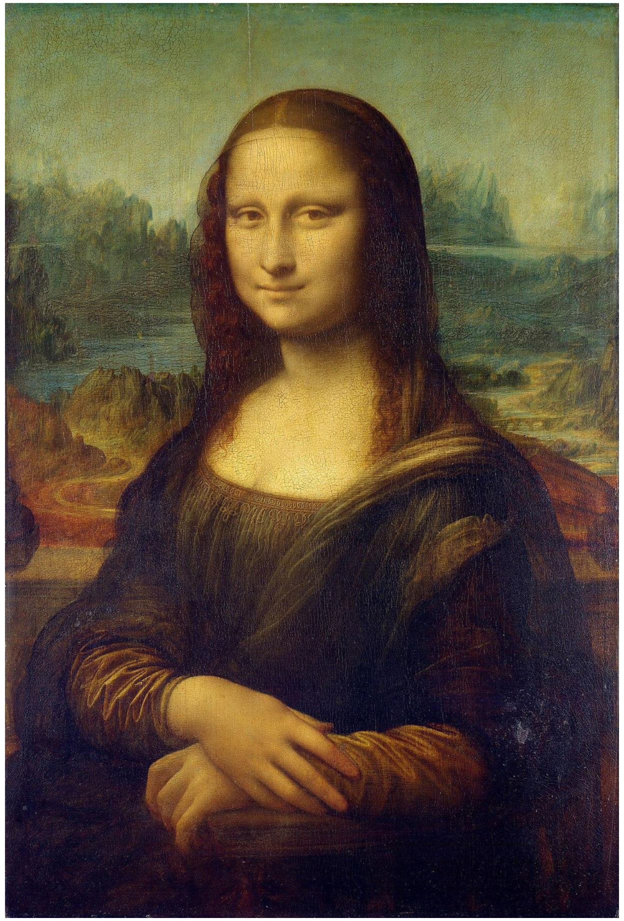


$=?



„On permanent display at The Louvre museum in Paris, the Mona Lisa was assessed at **US$100 million** on December 14, 1962. Taking inflation into account, the 1962 value would be around **US$790 million** in 2016.”

Source: Wikipedia



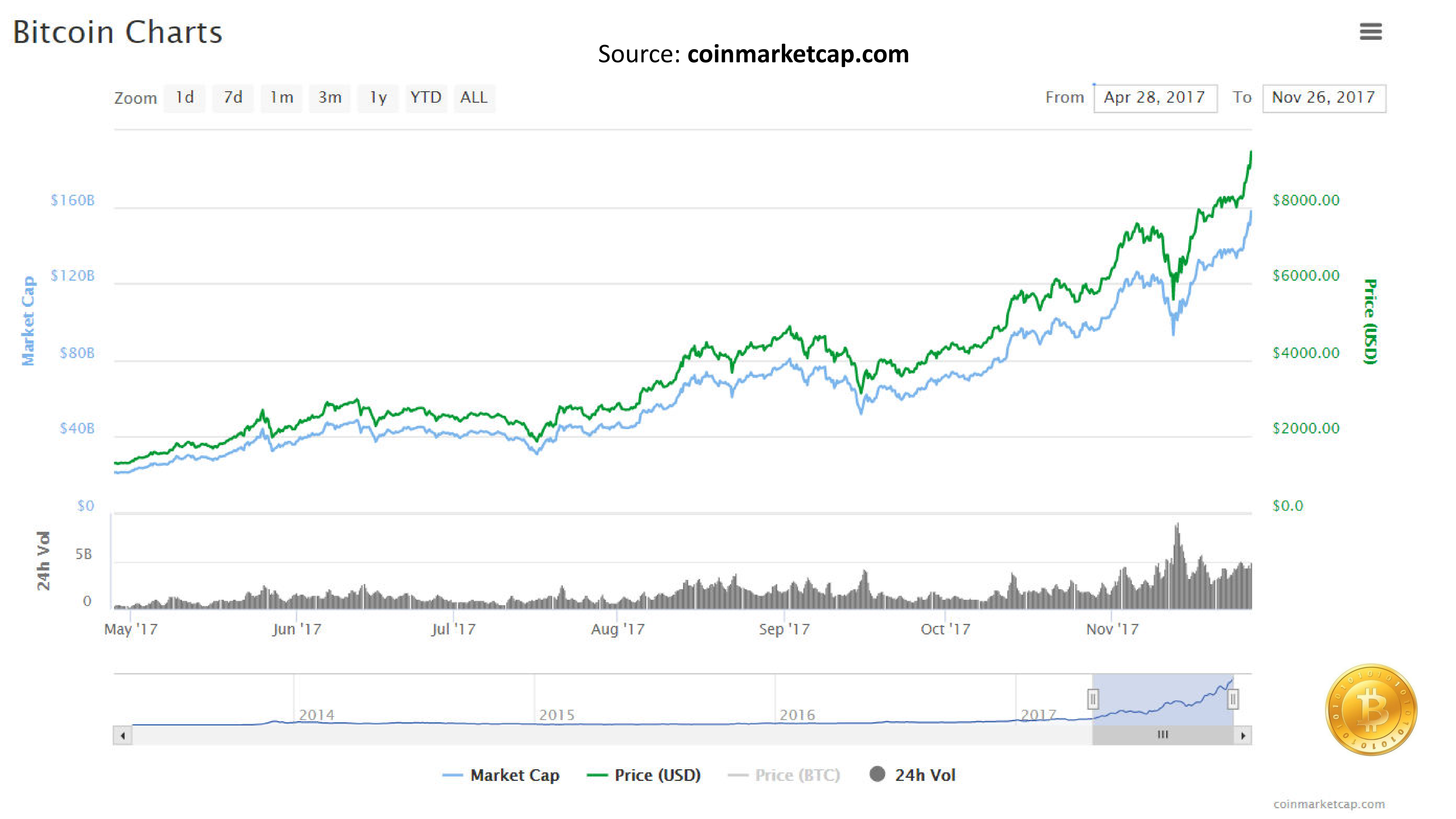
G

$=0

“**BITCOIN** is a remarkable **cryptographic achievement** and the ability to create **something that is not duplicable** in the digital world has enormous value ”

Eric Schmidt

CEO of Google



Bitcoin Charts

Source: **coinmarketcap.com**

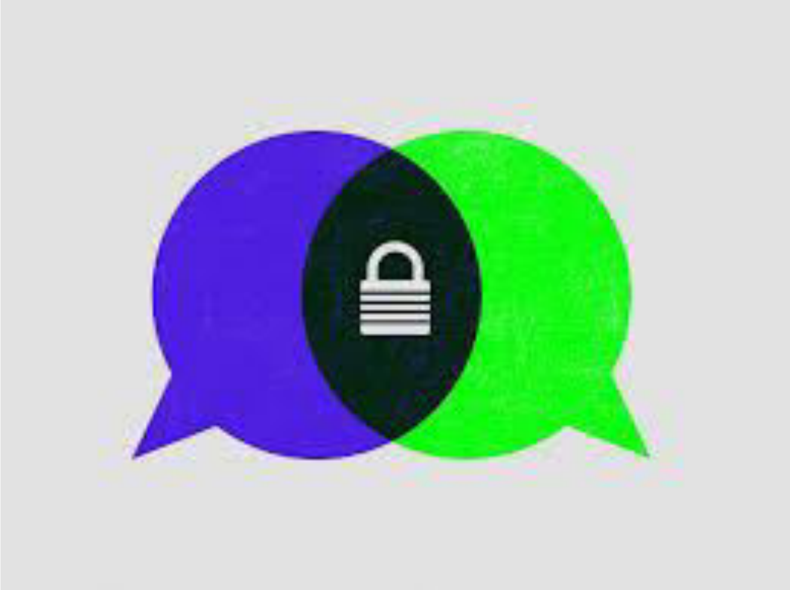
From Apr 28, 2017 To Nov 26, 2017

Blockchain Phone

SIRIN LABS

Blockchain Phone

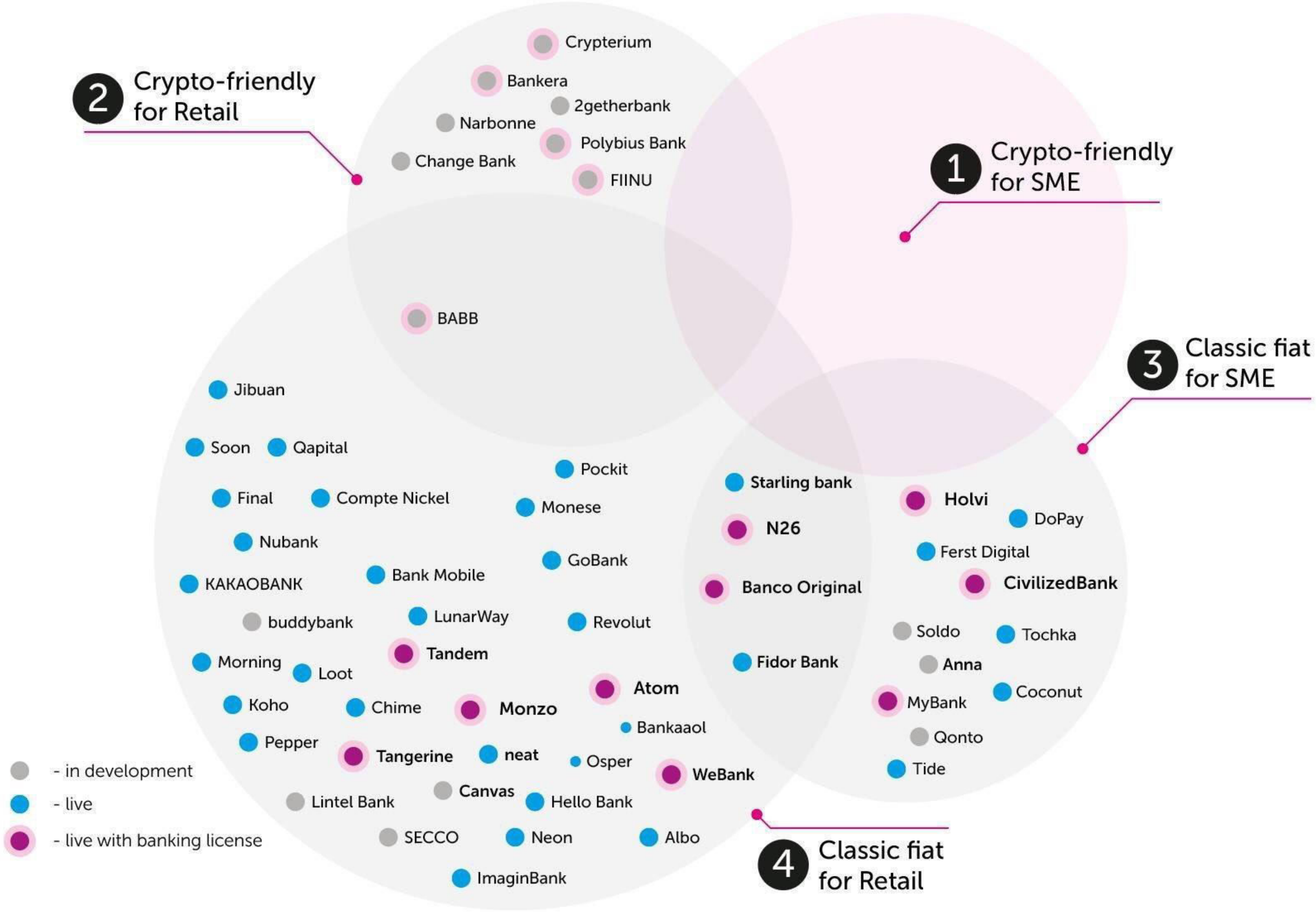
„A mobile phone that fully secure and safe enough to hold cryptographic coins”



- Sirin operating system
- Crypto wallets
- Securing exchange access
- Behavioral-based instrusion prevention system
- Physical security switch
- Blockchain-based tamper proof

Blockchain Phone

Overview of neobanks' universe



Analysis provided by: Life.SREDA venture capital | Based on Blockchain Fund | ARIVAL

End of Story #1

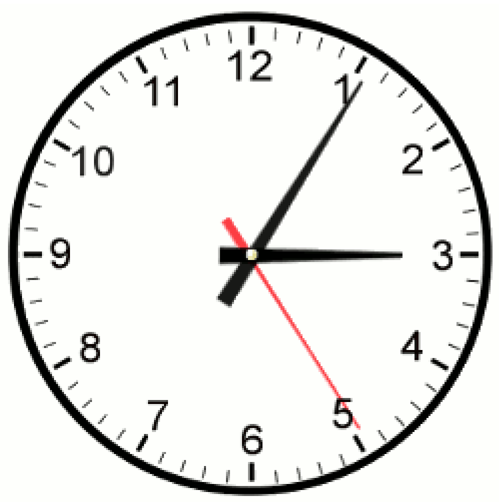
Story #2

10007*71249 =

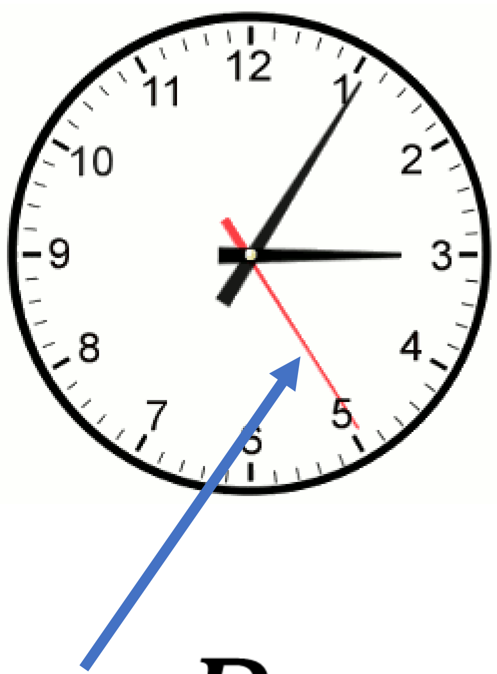
10007*71249 =712988743

8633=?*?

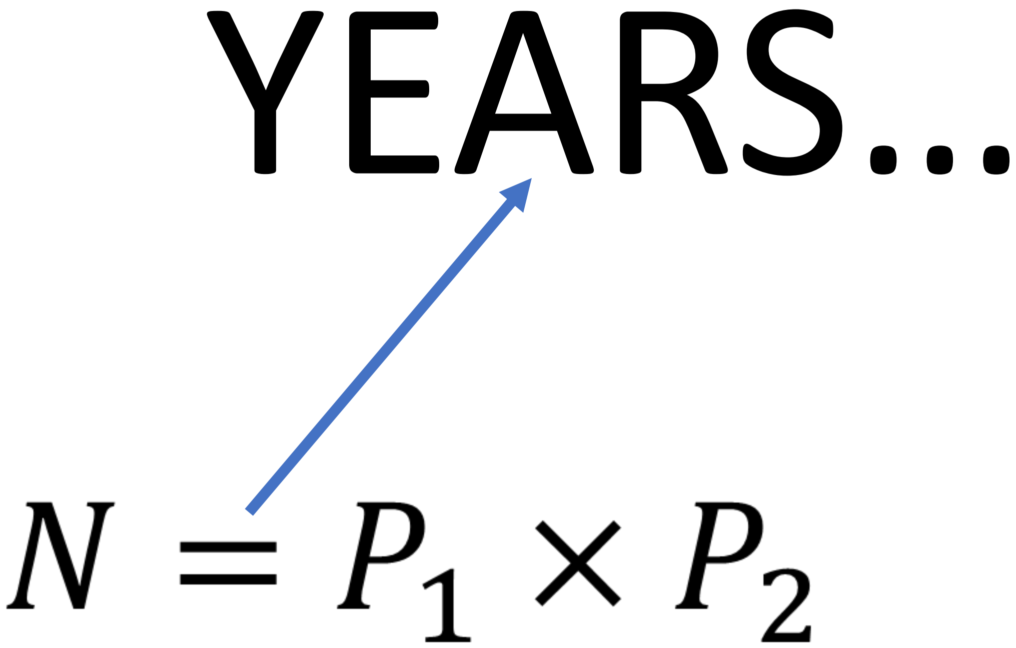
8633=89*97



$$P_1 \times P_2 = N$$



$$P_1 \times P_2 = N$$



YEARS...

$$N = P_1 \times P_2$$

Public Address

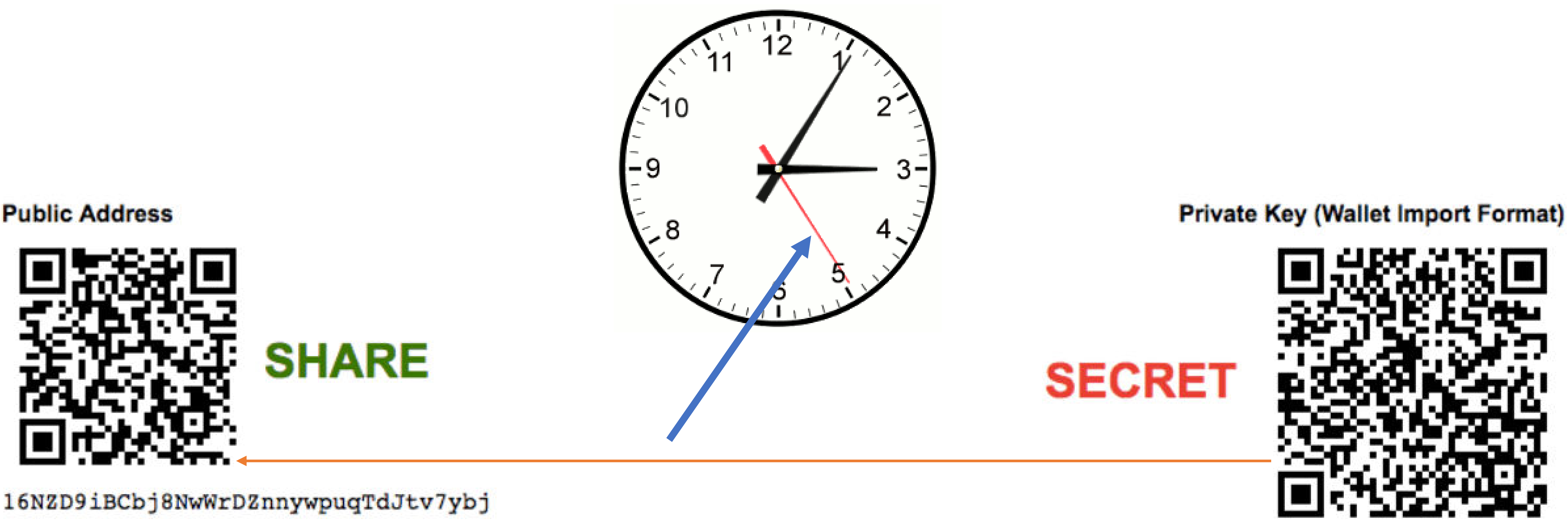
SHARE

16NZD9iBCbj8NwWrDZnnywpuqTdJtv7ybj

Private Key (Wallet Import Format)

SECRET

5JAG4cZ2JzQMezBd53zTHp7urRrqC75GG7f5vaEuXgyFfH3DiSg



Public Address

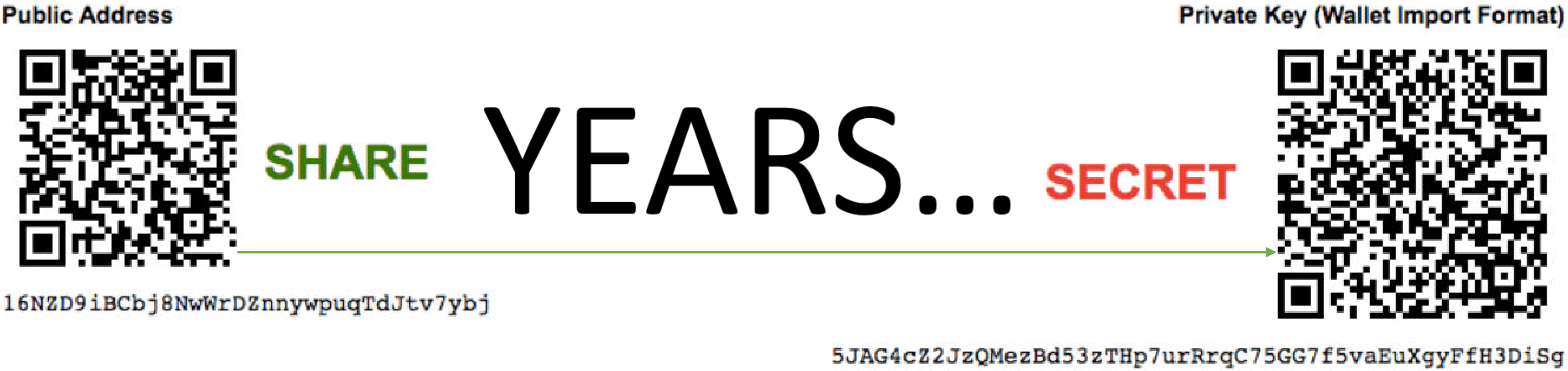
SHARE

16NZD9iBCbj8NwWrDZnnywpuqTdJtv7ybj

Private Key (Wallet Import Format)

SECRET

5JAG4cZ2JzQMezBd53zTHp7urRrqC75GG7f5vaEuXgyFfH3DiSg



Public Address

Private Key (Wallet Import Format)

SHARE

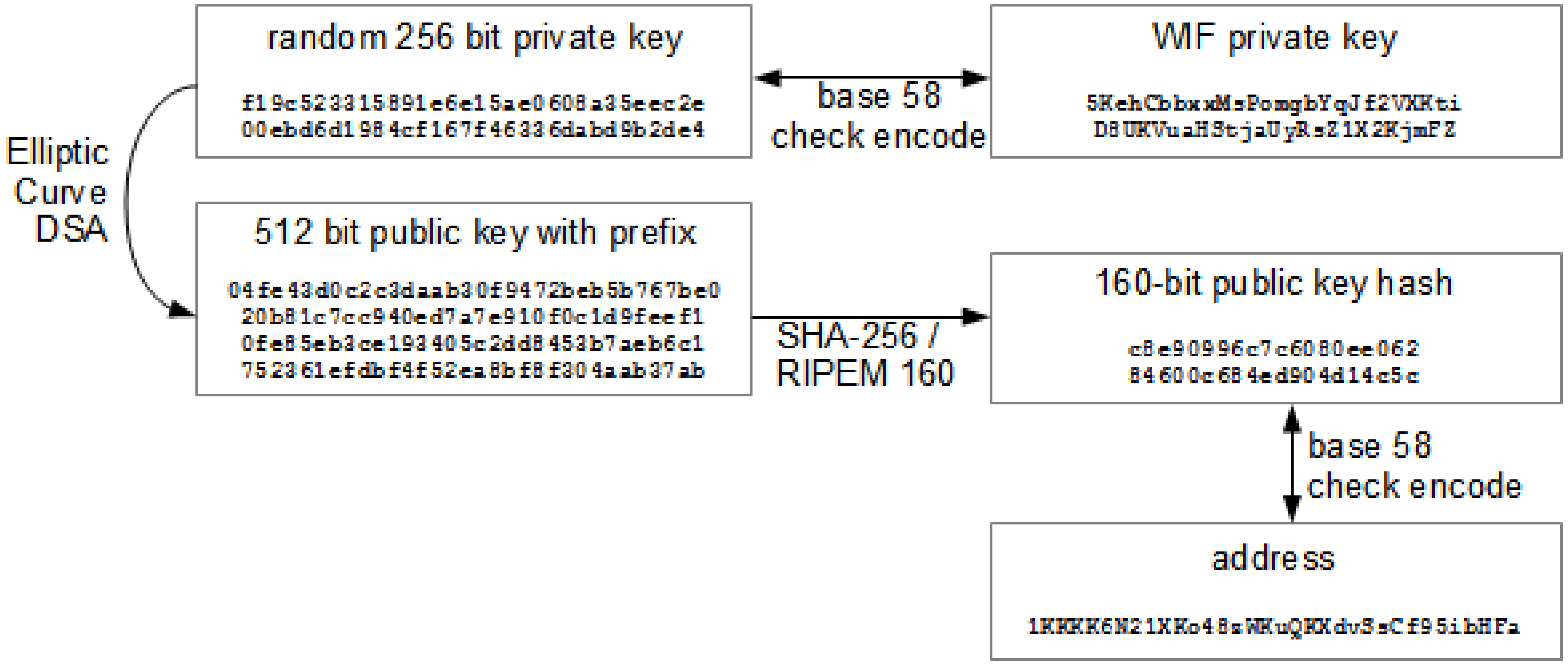
YEARS...

SECRET

16NZD9iBCbj8NwWrDZnnywpuqTdJtv7ybj

5JAG4cZ2JzQMezBd53zTHp7urRrqC75GG7f5vaEuXgyFfH3DiSg

Bitcoin Keys



random 256 bit private key

f19c523315891e6e15ae0608a35eec2e
00ebd6d1984cf167f46336dabd9b2de4

base 58
check encode

WIF private key

5KehCbbxxMsPomgbYqJf2VXKti
D8UKVuaHStjaUyRsZ1X2KjmFZ

Elliptic
Curve
DSA

512 bit public key with prefix

04fe43d0c2c3daab30f9472beb5b767be0
20b81c7cc940ed7a7e910f0c1d9feef1
0fe85eb3ce193405c2dd8453b7aeb6c1
752361efdbf4f52ea8bf8f304aab37ab

SHA-256 /
RIPEM 160

160-bit public key hash

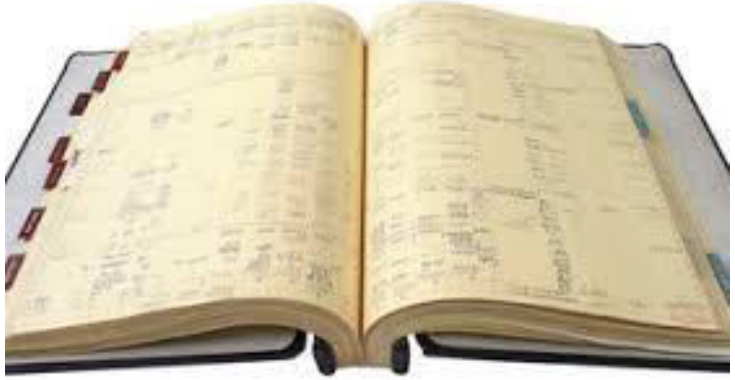
c8e90996c7c6080ee062
84600c684ed904d14c5c

base 58
check encode

address

1KKKK6N21XKo48zWKuQKXdvSsCf95ibHFa

It all begins with the ledger



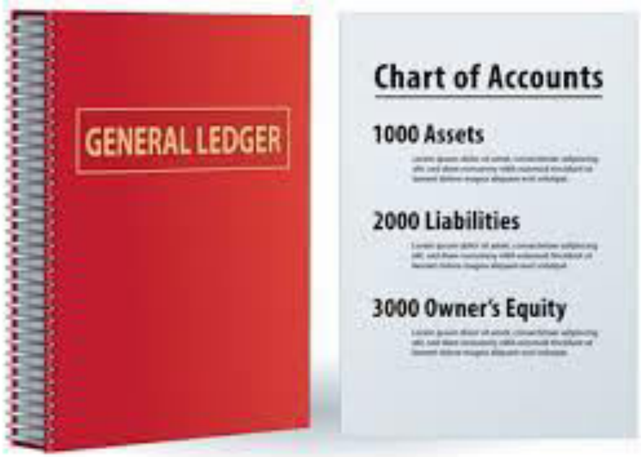
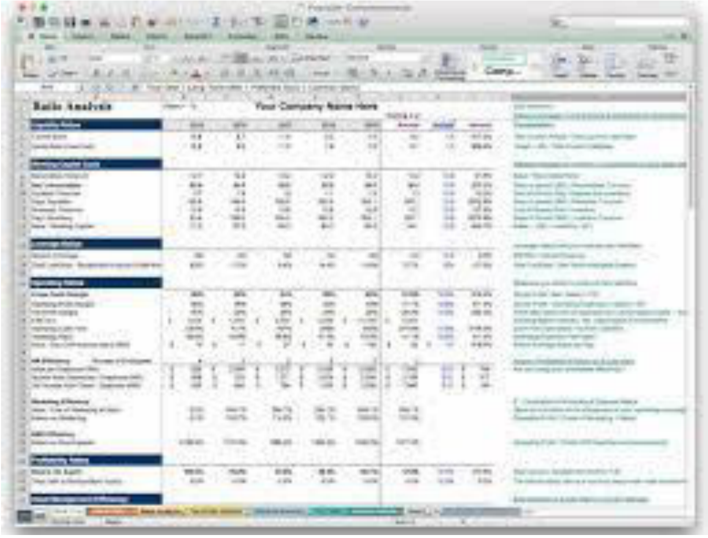


Chart of Accounts

1000 Assets

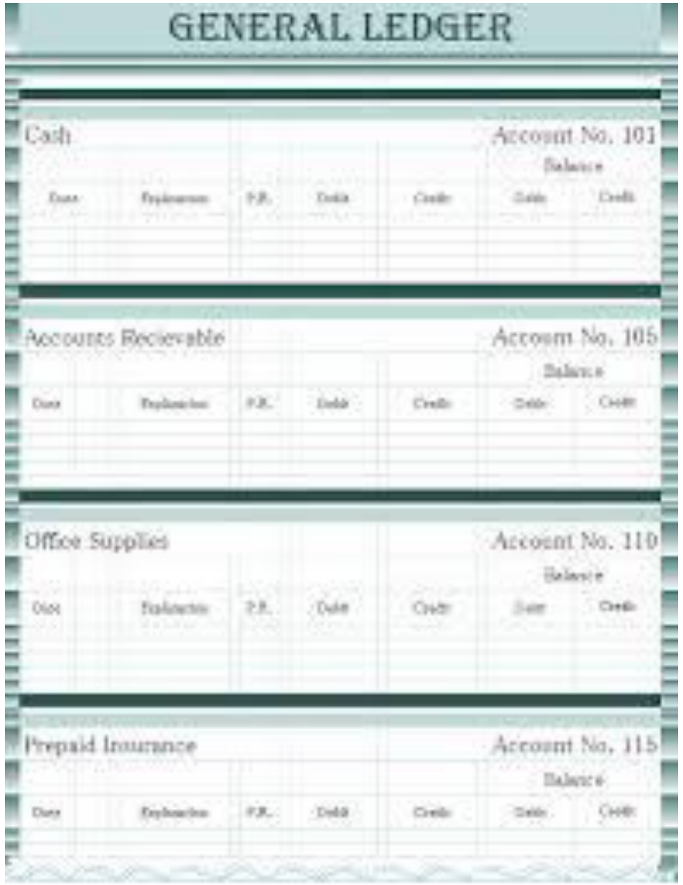
2000 Liabilities

3000 Owner's Equity



Ratio Analysis

Your Company Name Here



GENERAL LEDGER

Cash Account No. 101

					Balance	
Date	Explanation	P.R.	Debit	Credit	Debit	Credit

Accounts Recievable Account No. 105

					Balance	
Date	Explanation	P.R.	Debit	Credit	Debit	Credit

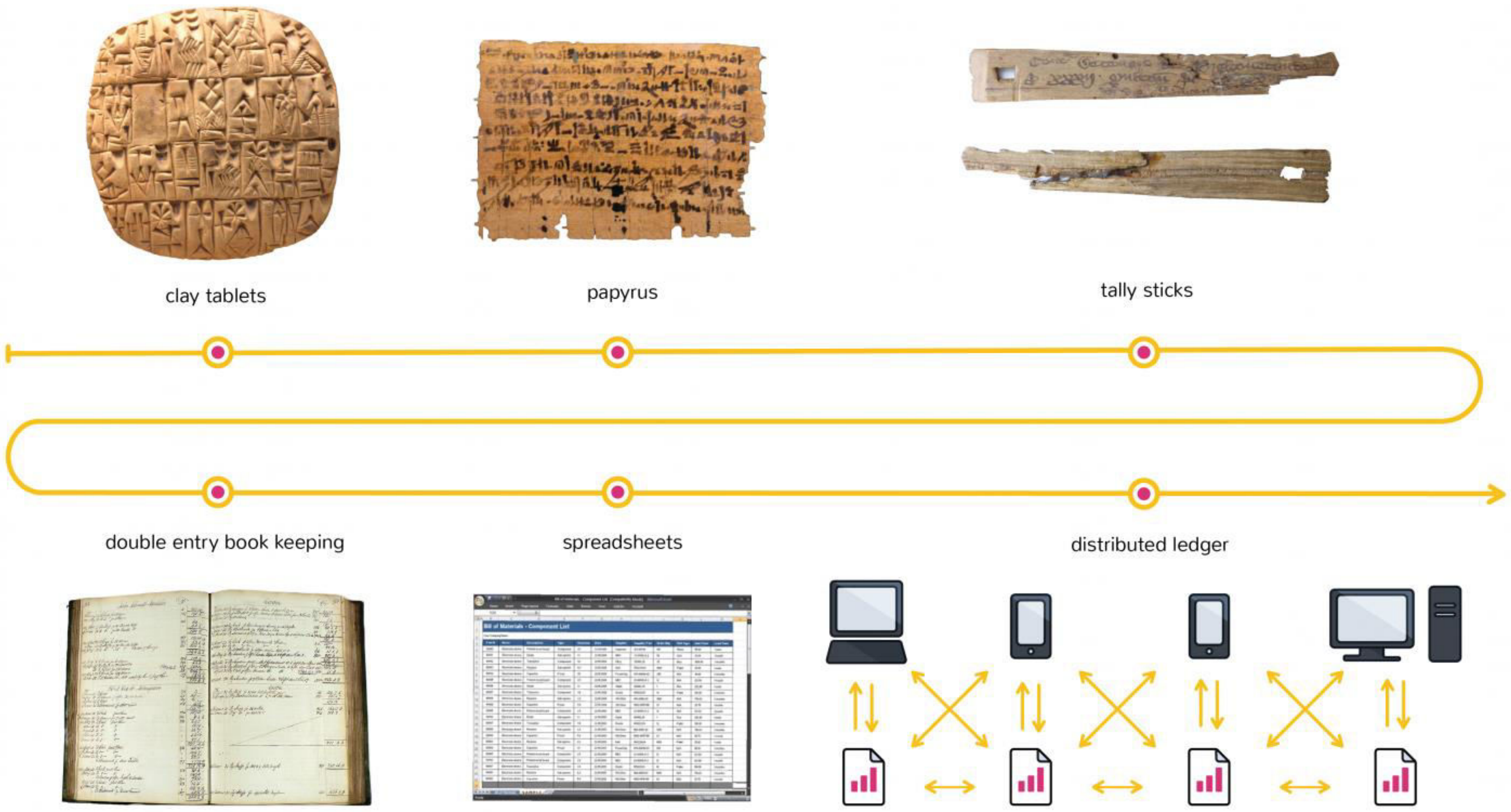
Office Supplies Account No. 110

					Balance	
Date	Explanation	P.R.	Debit	Credit	Debit	Credit

Prepaid Insurance Account No. 115

					Balance	
Date	Explanation	P.R.	Debit	Credit	Debit	Credit

From Clay Tablets to Distributed Ledger



clay tablets

papyrus

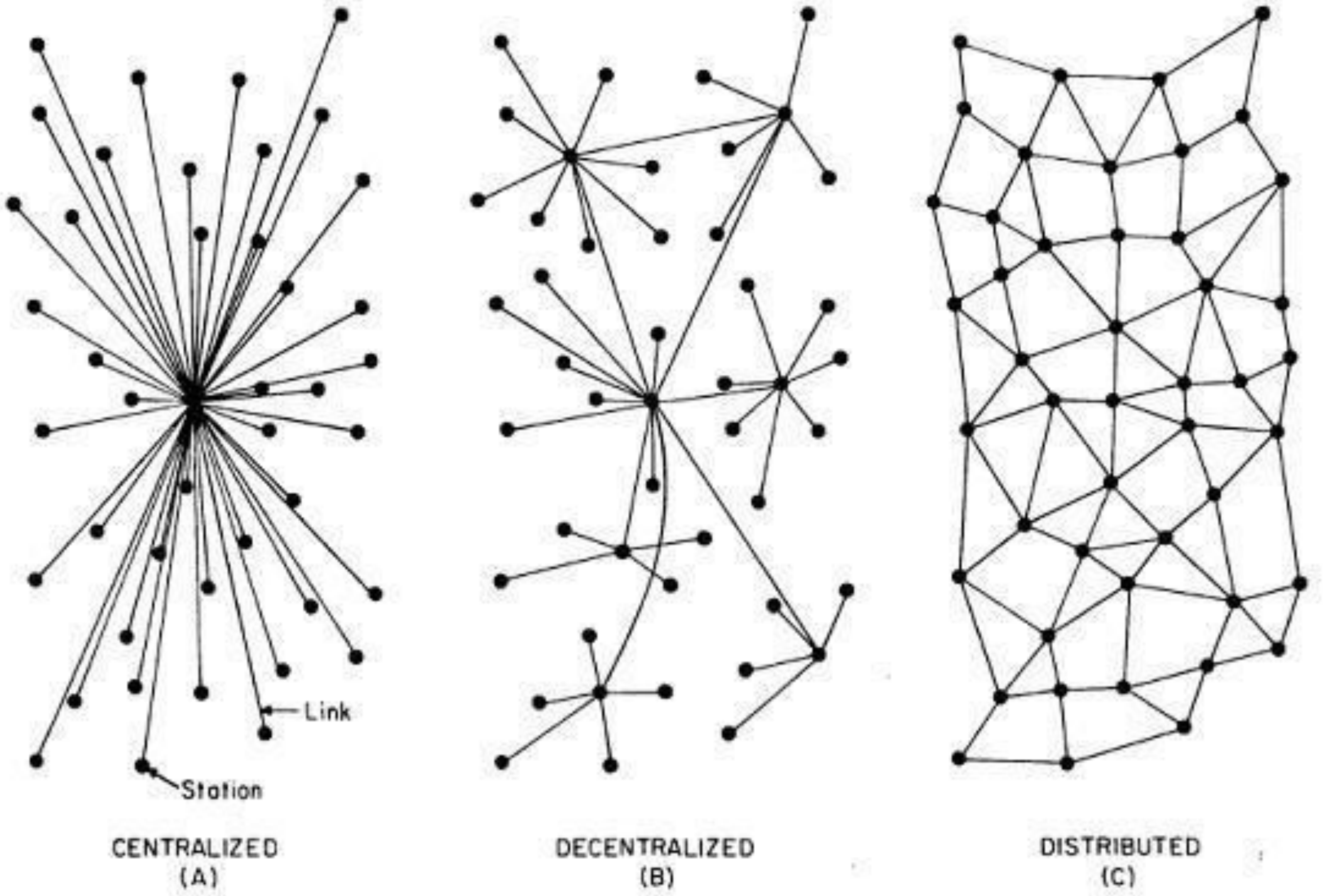
tally sticks

double entry book keeping

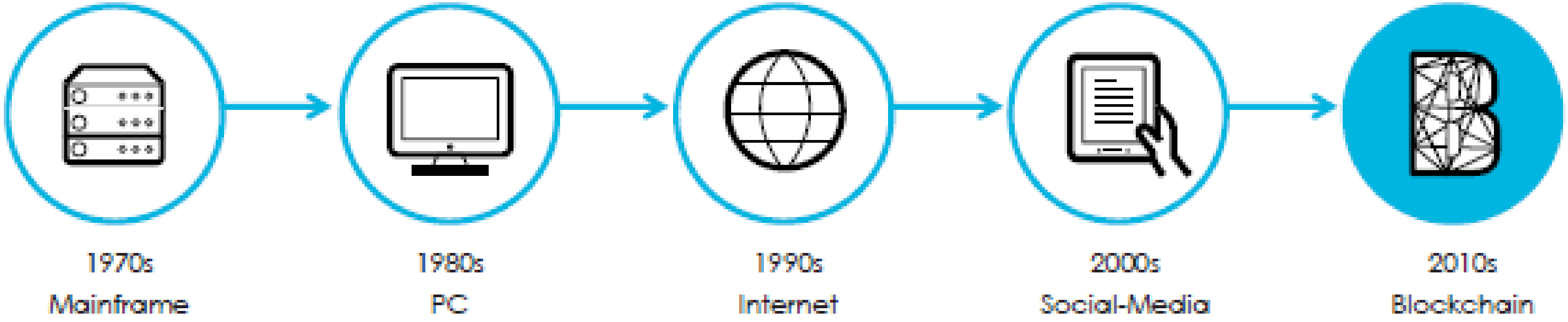
spreadsheets

distributed ledger

(R)Evolution?

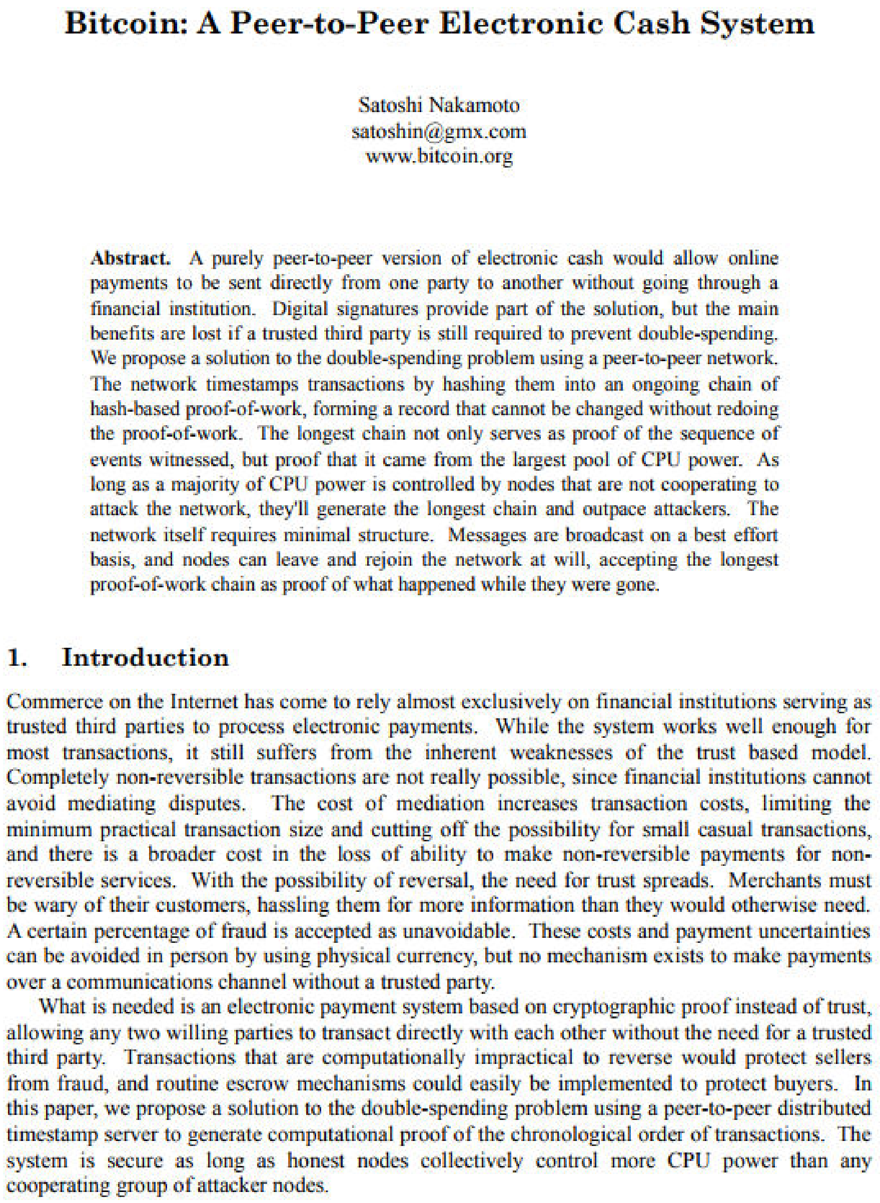


(R)Evolution


1970s
Mainframe
1980s
PC
1990s
Internet
2000s
Social-Media
2010s
Blockchain

Satoshi Nakamoto’s White Paper (2008)

1. Immutable & distributed data stores
   - GFS (Google File System), HDFS (Hadoop Distributed File System)
   - NoSQL, CouchDB,…
2. Peer-to-Peer network
   - Napster, KaZaa, BitTorent,…
3. The AAA of security (Authenticity, Authorization, Accountability)
   - Public Key Infrastructure (PKI), e.g. „RSA”
   - Digital signature, hash functions, Merkle tree,…
4. Fault-tolerant system design & game theory
   - Byzantine fault tolerance
   - PoW, PoS, 51% rule, …
5. Genesis block & chain



Bitcoin: A Peer-to-Peer Electronic Cash System

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

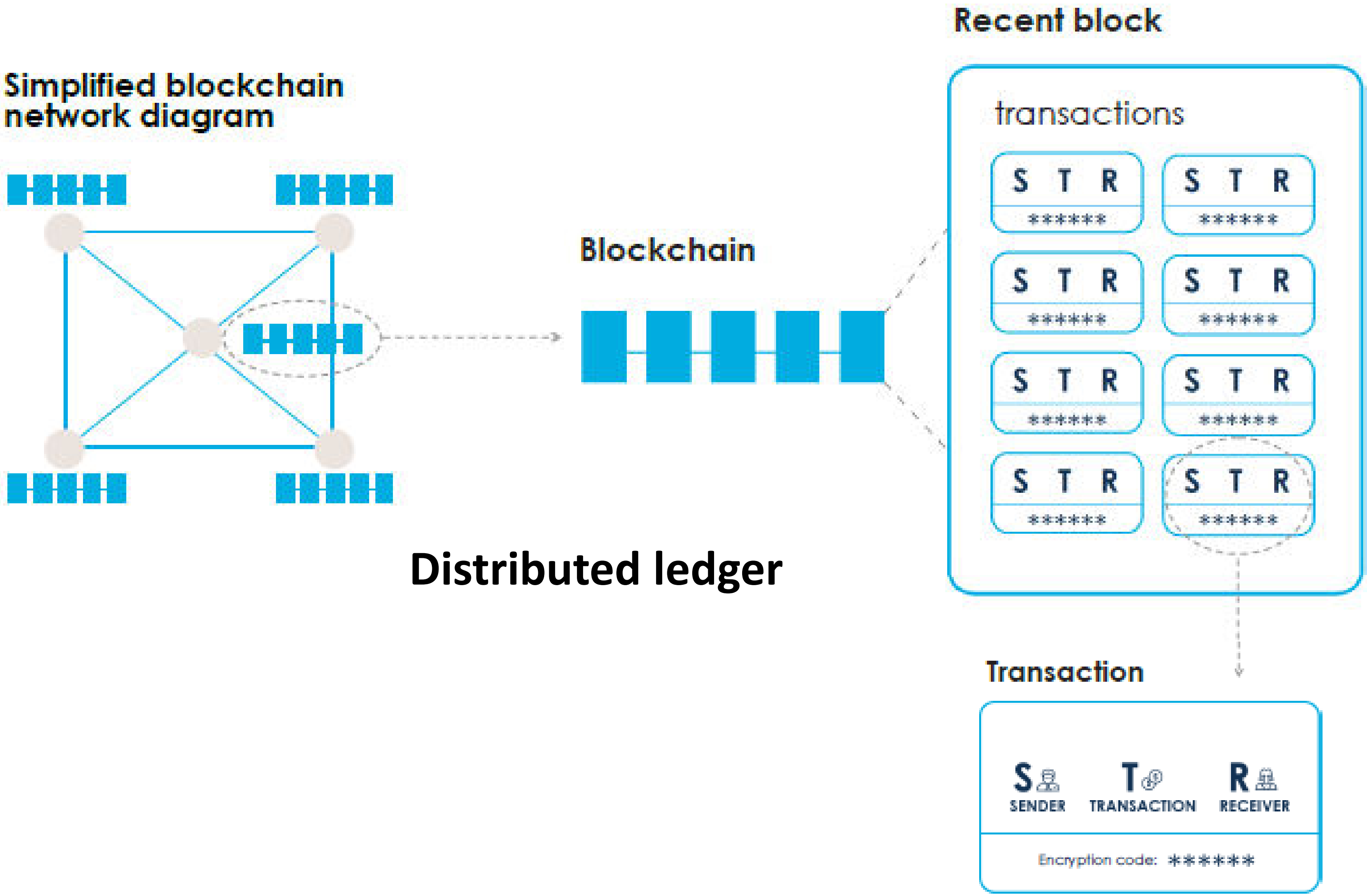
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

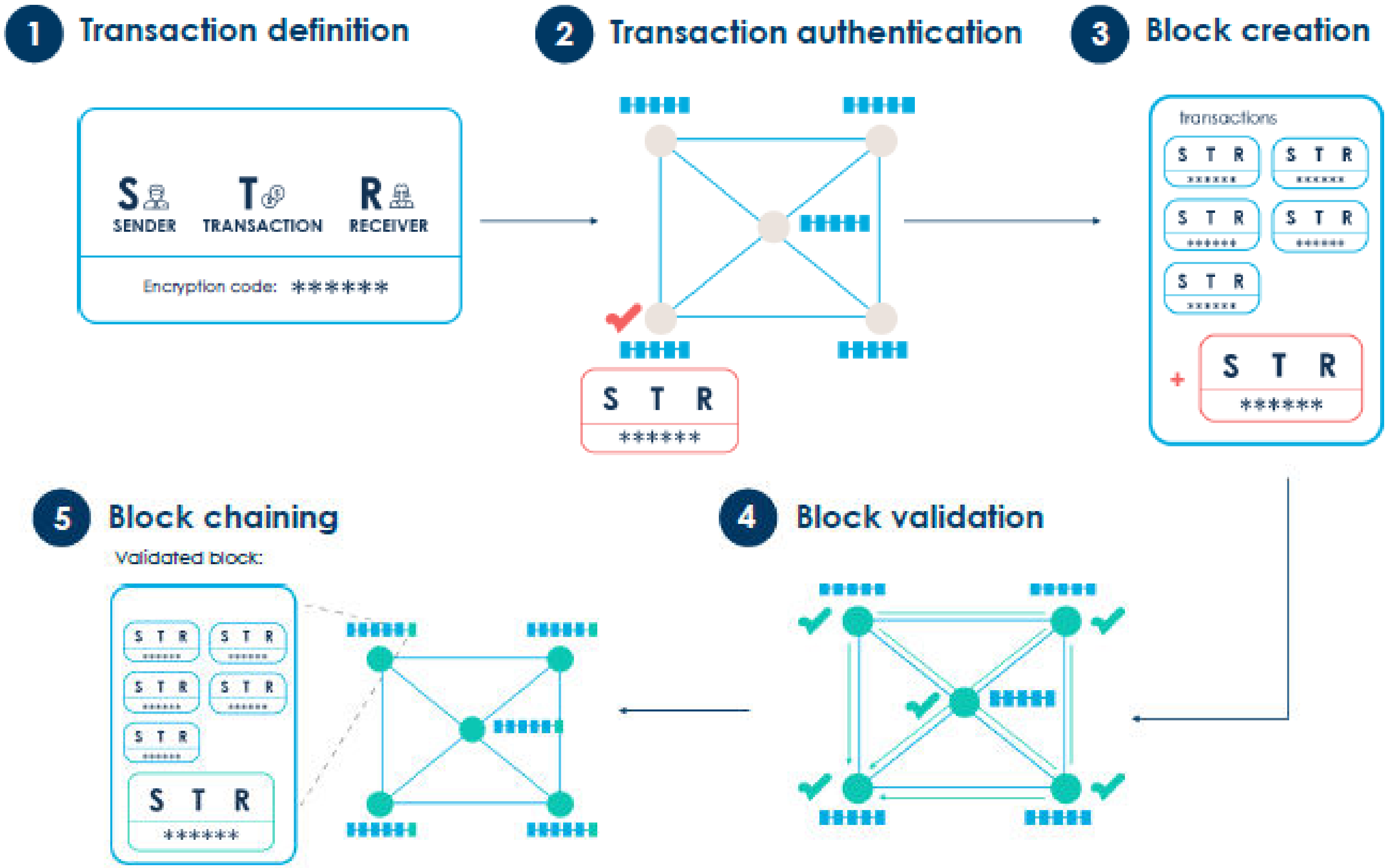
1. Introduction

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 avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

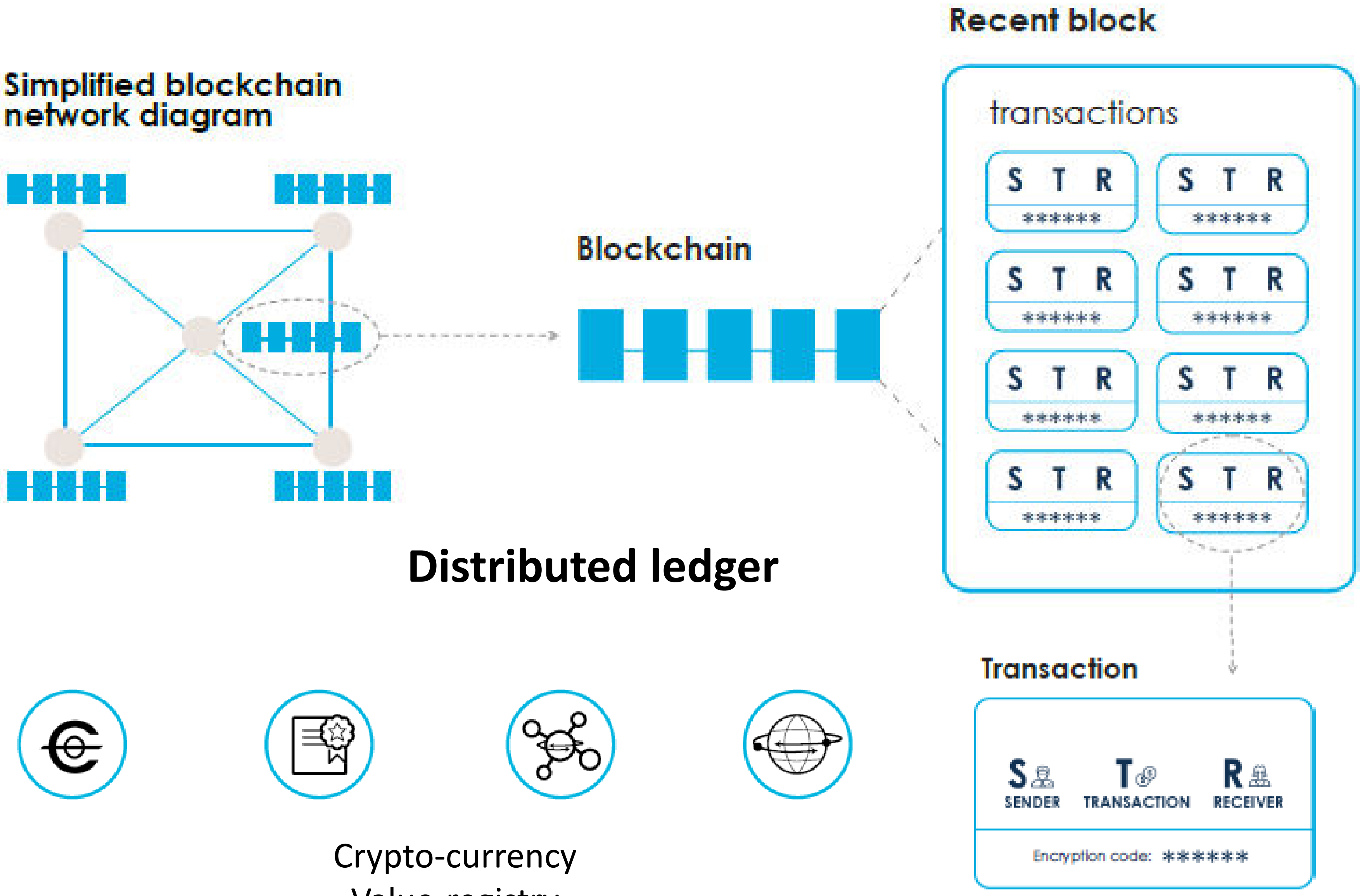
Distributed ledger





- **Concensus** from the majority of the network
- “Bitcoin mining”

Distributed ledger



Crypto-currency
Value-registry
Value-ecosystem
Value-web

Meanwhile in Australia...

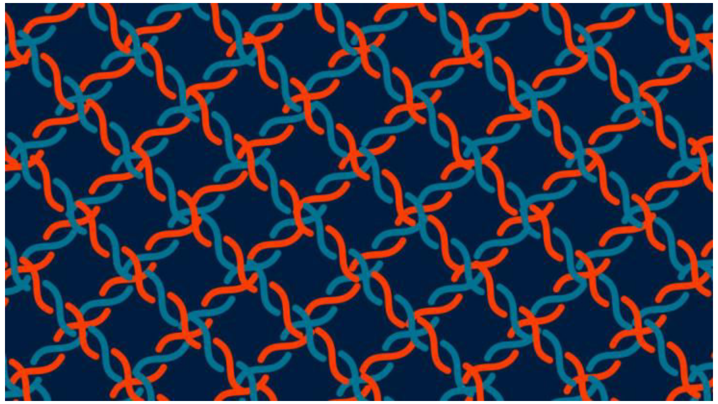
CBHGROUP

agridigital

2017: Sweden Land Registry on blockchain

Blockchain & Global Supply Chain

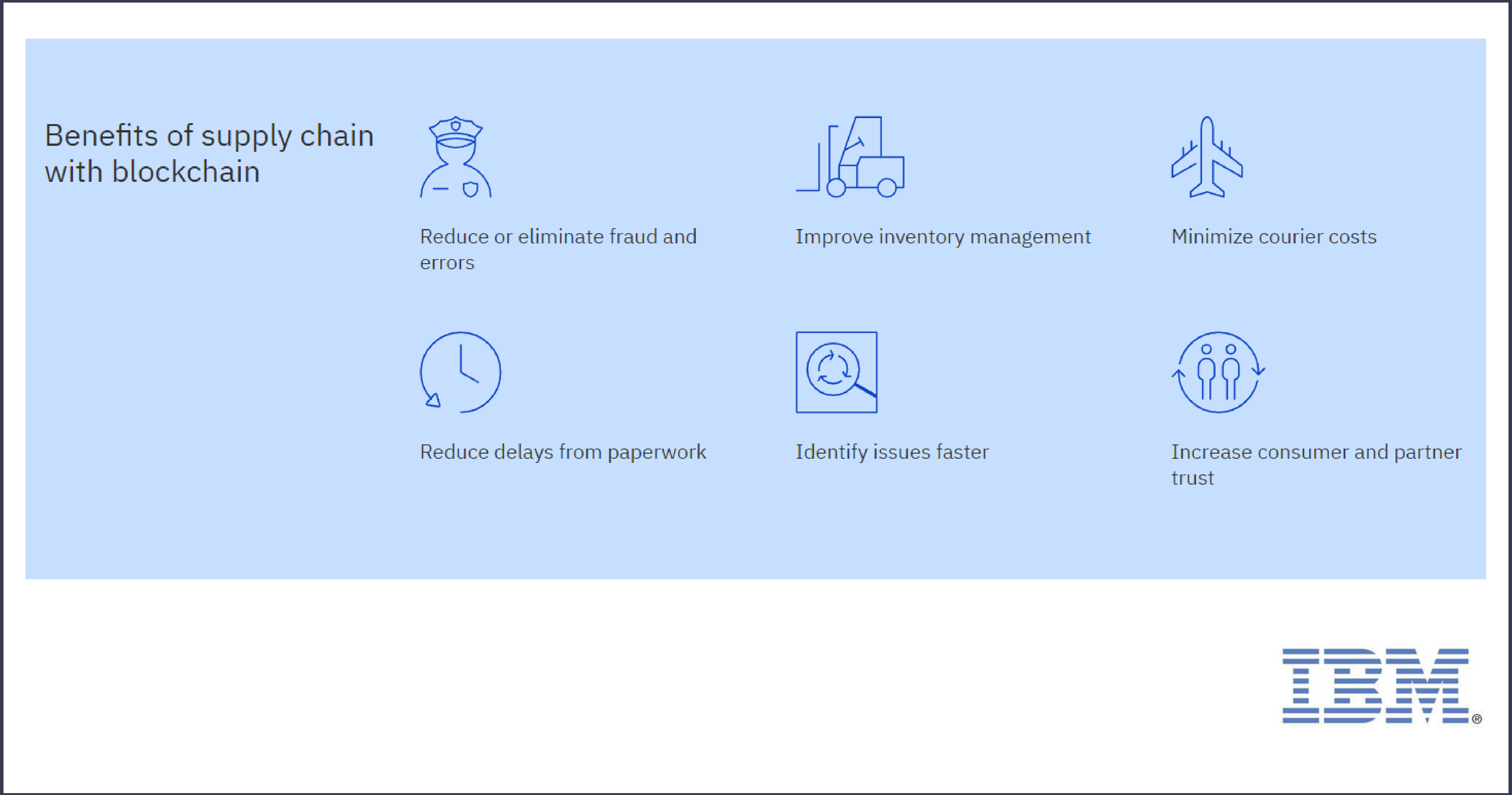
- The E.coli outbreak at Chipotle Mexican Grill outlets in 2015, 55 customers left ill
  - The restaurant chain’s reputation.
  - Sales plummeted, and Chipotle’s share price dropped 42%, to a three-year low
- Using a blockchain to transfer title and record permissions and activity logs so as to **track the flow of goods and services** between businesses and across borders
- Legal challenges



Harvard Business Review

Challenges with supply chain management

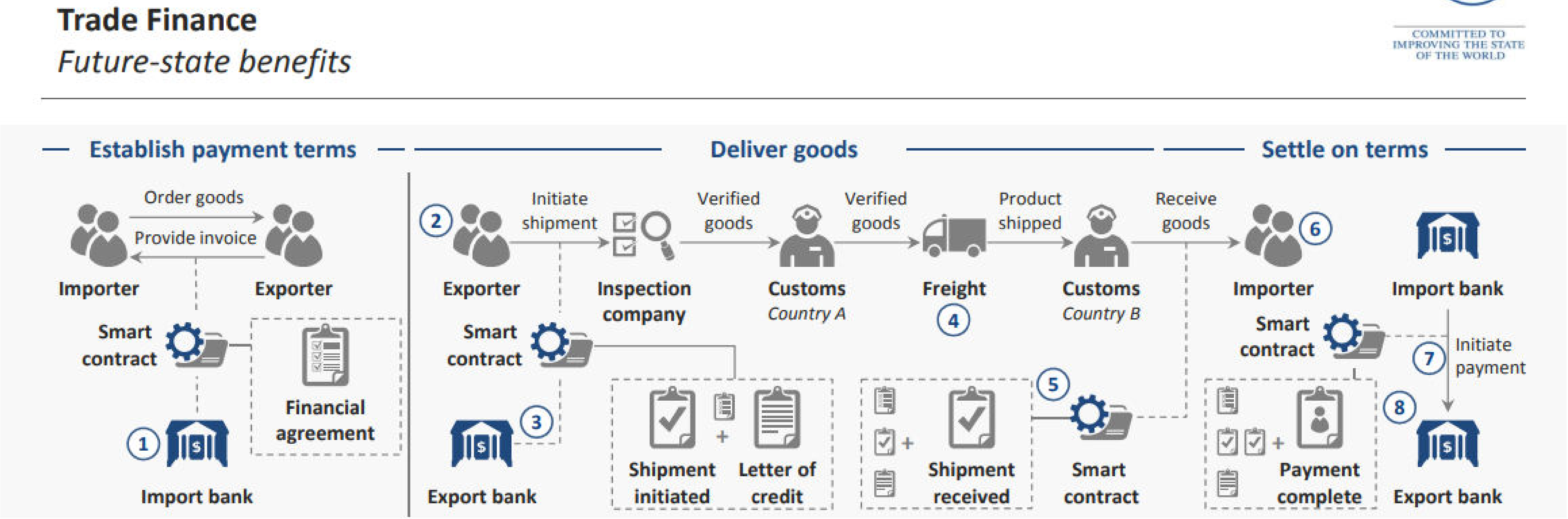
- Complexity (from local trade in the past to global trade)
  - the supply chain can span over hundreds of stages
  - multiple geographical (international) locations
  - a multitude of invoices and payments
  - have several individuals and entities involved
  - and extend over months of time
- Transparency (or lack of)
  - Trust and ethical issues as well
- Efficiency
  - Current supply chain management can be highly inefficient as vendors and suppliers try to connect the dots on who needs what, when and how.



Benefits of supply chain with blockchain

- Reduce or eliminate fraud and errors
- Improve inventory management
- Minimize courier costs
- Reduce delays from paperwork
- Identify issues faster
- Increase consumer and partner trust

Trade Finace enhanced by Smart Contracts on Blockchain



1. Real-time review
2. Transparent factoring
3. Disintermediation
4. Reduced counter party risk

5. Decentralized contract execution
6. Proof of ownership
7. Automated settlement and reduced transaction fee
8. Regulatory transparency

Value registry

- Public ledger to register physical assets
- Challenges of traditional document validation models
  - Relying on central authorities for storing and validating documents
  - Risks include transfer, breach, and deterioration
- Blockchain-based solution
  - Signature and timestamp associated with a document are stored in the blockchain
  - To register ownership of an asset, a transaction is created with a reference to the physical asset
  - This information is stored on a Blockchain record, holding roughly 40 bytes of data
  - The owner of the **private key** to to that public record is then registered as the owner of that asset

Examples

- Factom for Land Registry for the government of Honduras
- Sweden Land Registry on blockchain

Potential usecases of blockchain in agriculture

Food safety

Traceability

Transaction costs

Agri-trade finance

Opening new market

Logistics

Smart contracts

AGRILEDGER

ripe.io
Blockchain of Food

agridigital

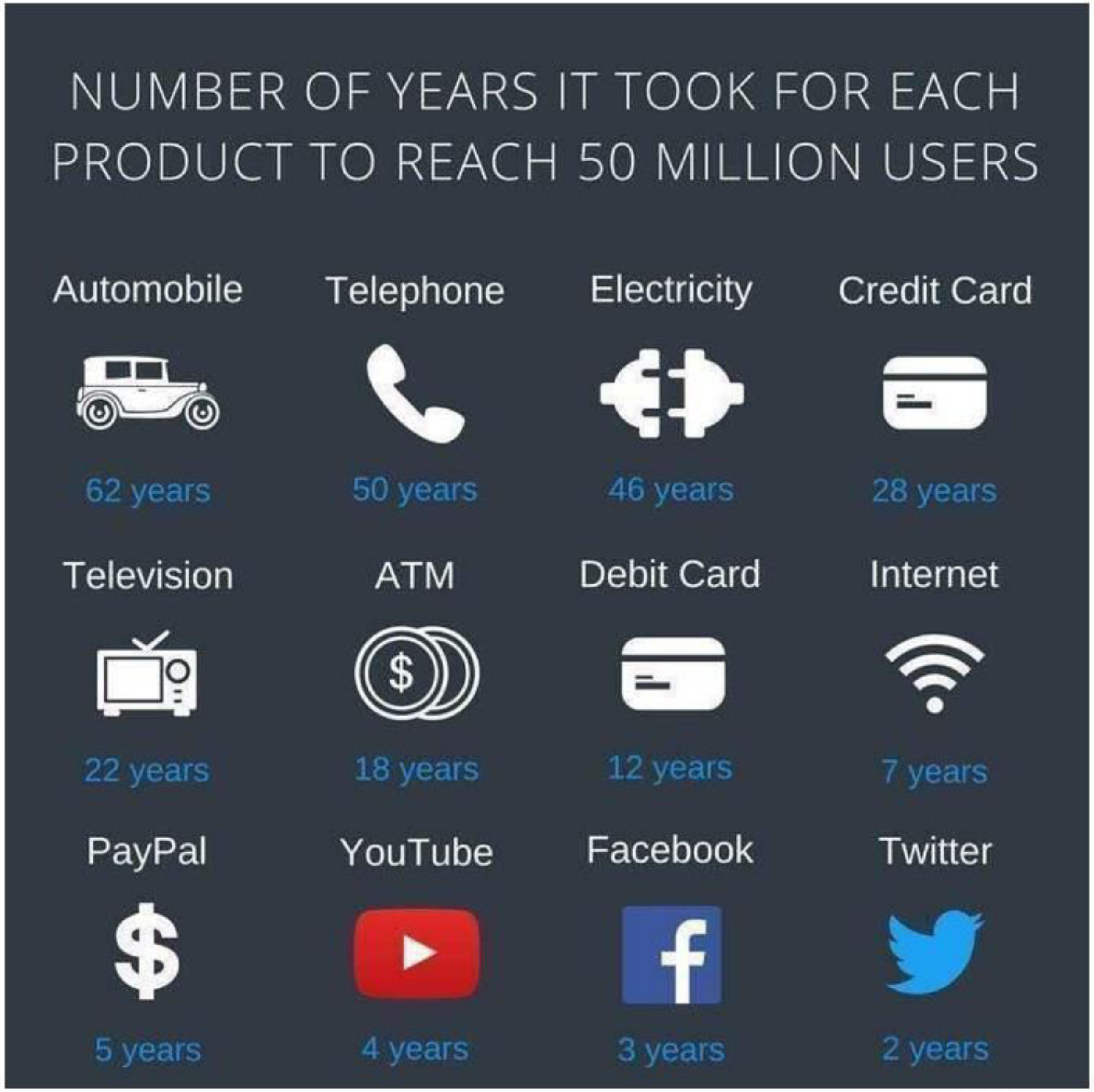
TE-FOOD

ICO

“Blockchain will do for transactions what the Internet did for information”

MIT Technology Review

10 years, and NOBODY has come up with a REALISTIC use for blockchain



NUMBER OF YEARS IT TOOK FOR EACH PRODUCT TO REACH 50 MILLION USERS

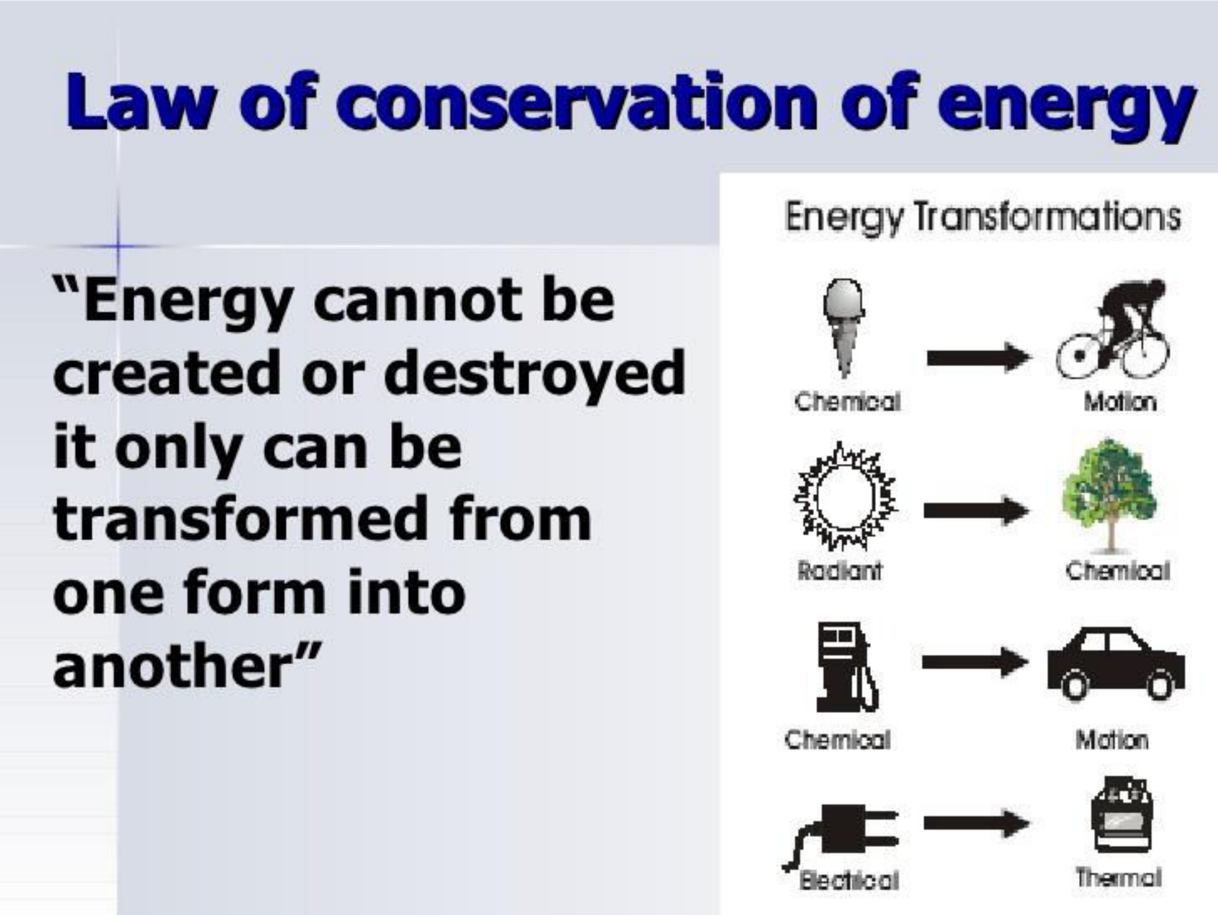
Automobile	Telephone	Electricity	Credit Card
62 years	50 years	46 years	28 years
Television	ATM	Debit Card	Internet
22 years	18 years	12 years	7 years
PayPal	YouTube	Facebook	Twitter
5 years	4 years	3 years	2 years

THE WALL STREET JOURNAL.

Angry Birds did this in a space of 35 days!

> “Processing a bitcoin transaction consumes more than 5,000 times as much energy as using a Visa credit card.”

IEEE SPECTRUM



Law of conservation of energy

"Energy cannot be created or destroyed it only can be transformed from one form into another"

Energy Transformations
Chemical
Motion
Radiant
Chemical
Chemical
Motion
Electrical
Thermal

Source: CBSE Lectures

2018

2018 and beyond

Equilibrium state

CORVINUS
FINTECH
CENTER

Spirits of Innovation