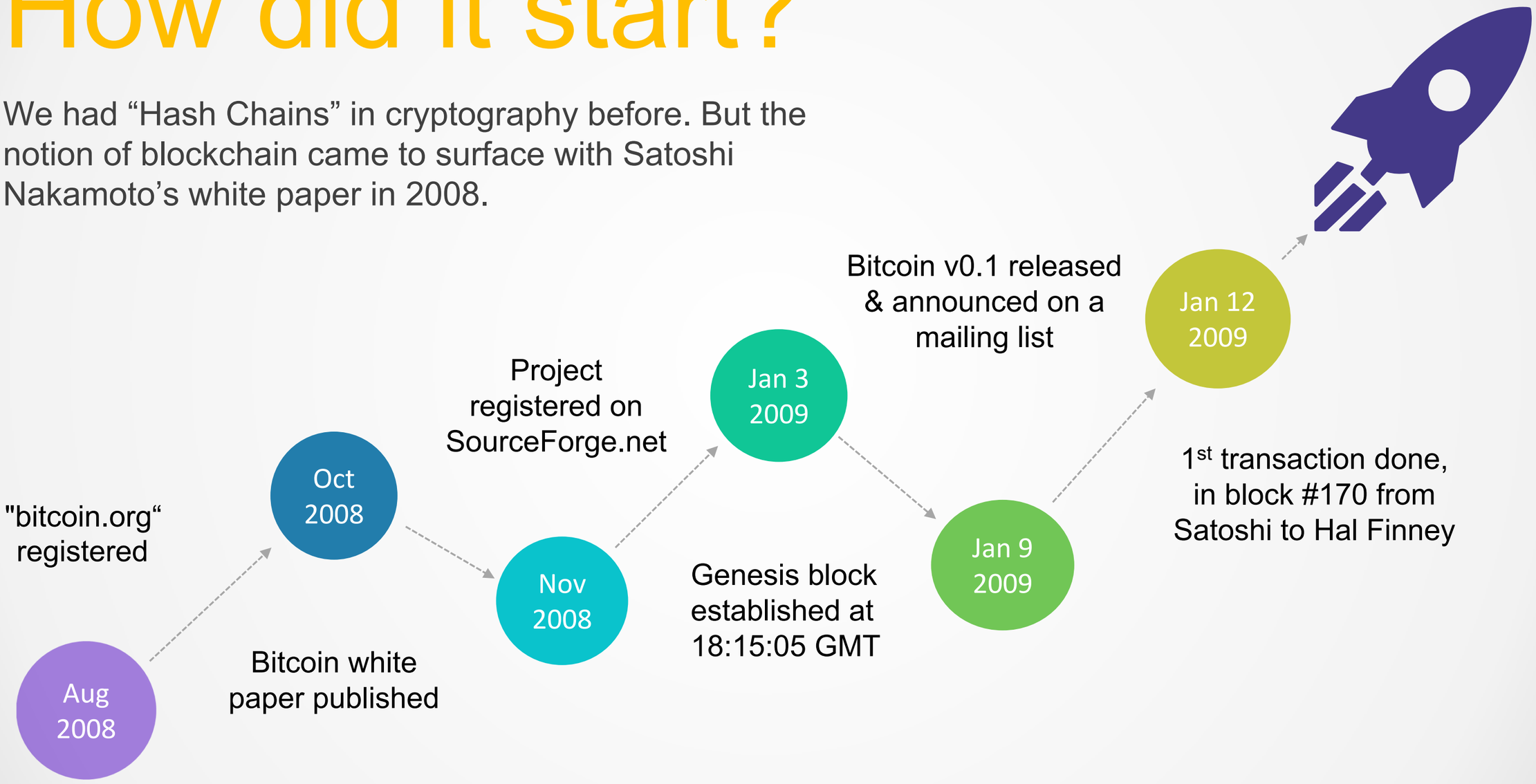
Cryptocurrency and Blockchain Technology

Mohammad Sayad Haghighi, PhD, SMIEEE
Assistant Professor
sayad@ut.ac.ir
University of Tehran, Iran

How did it start?

We had “Hash Chains” in cryptography before. But the notion of blockchain came to surface with Satoshi Nakamoto’s white paper in 2008.



Satoshi's White Paper

Bitcoin: A Peer-to-Peer Electronic Cash System

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

A Free Email Provider

Not even a real name!

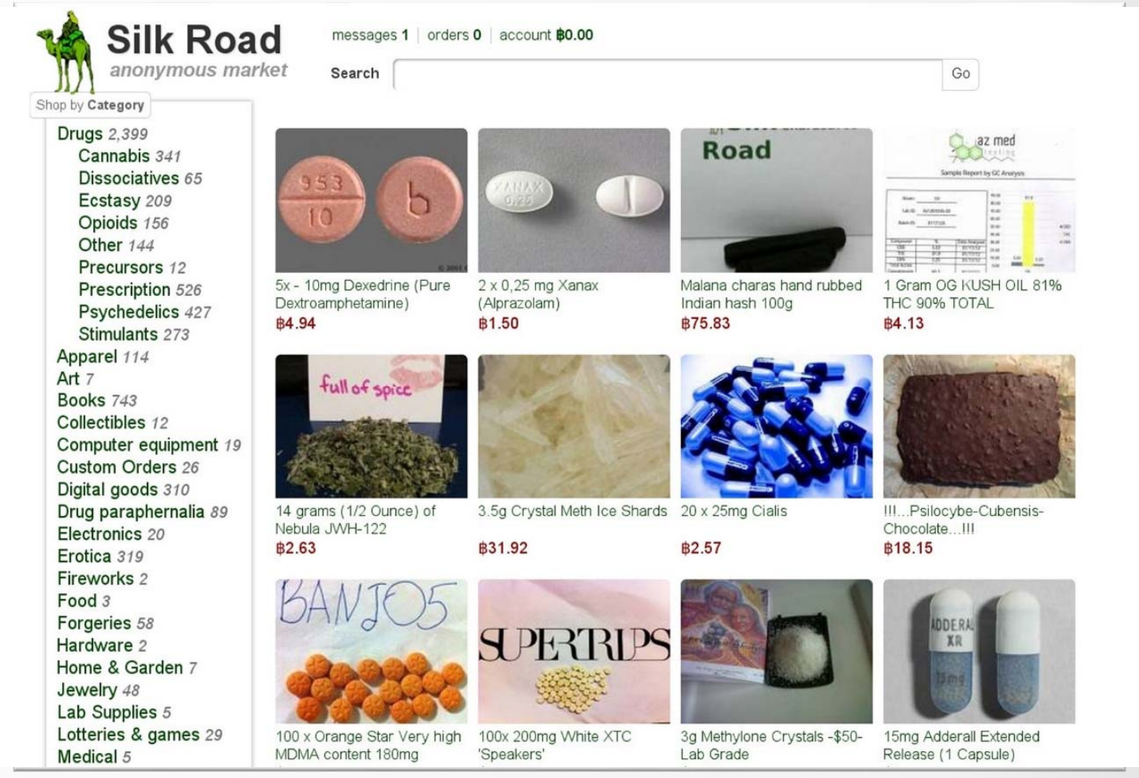
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required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

How did it become famous?

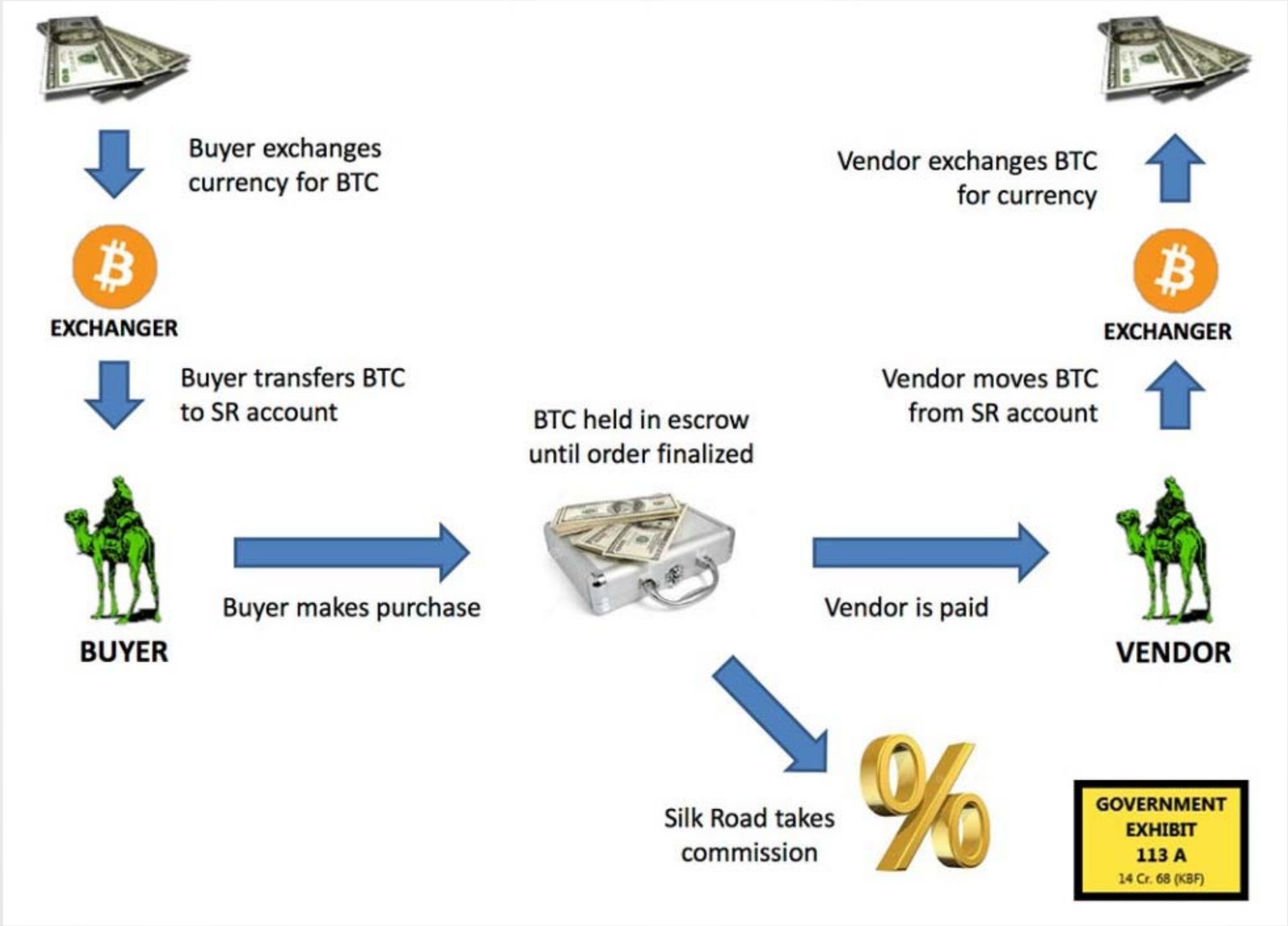
- Silk Road was one of the first online black markets that used Bitcoin and TOR technologies for anonymity.

- Silk Road was shut down in 2013 and the admin (Ross Ulbricht) was arrested. He was sentenced to life in prison!

- Not all the credit for Bitcoin's fame goes to Silk Road. The 2017's price surge was also a big shot.



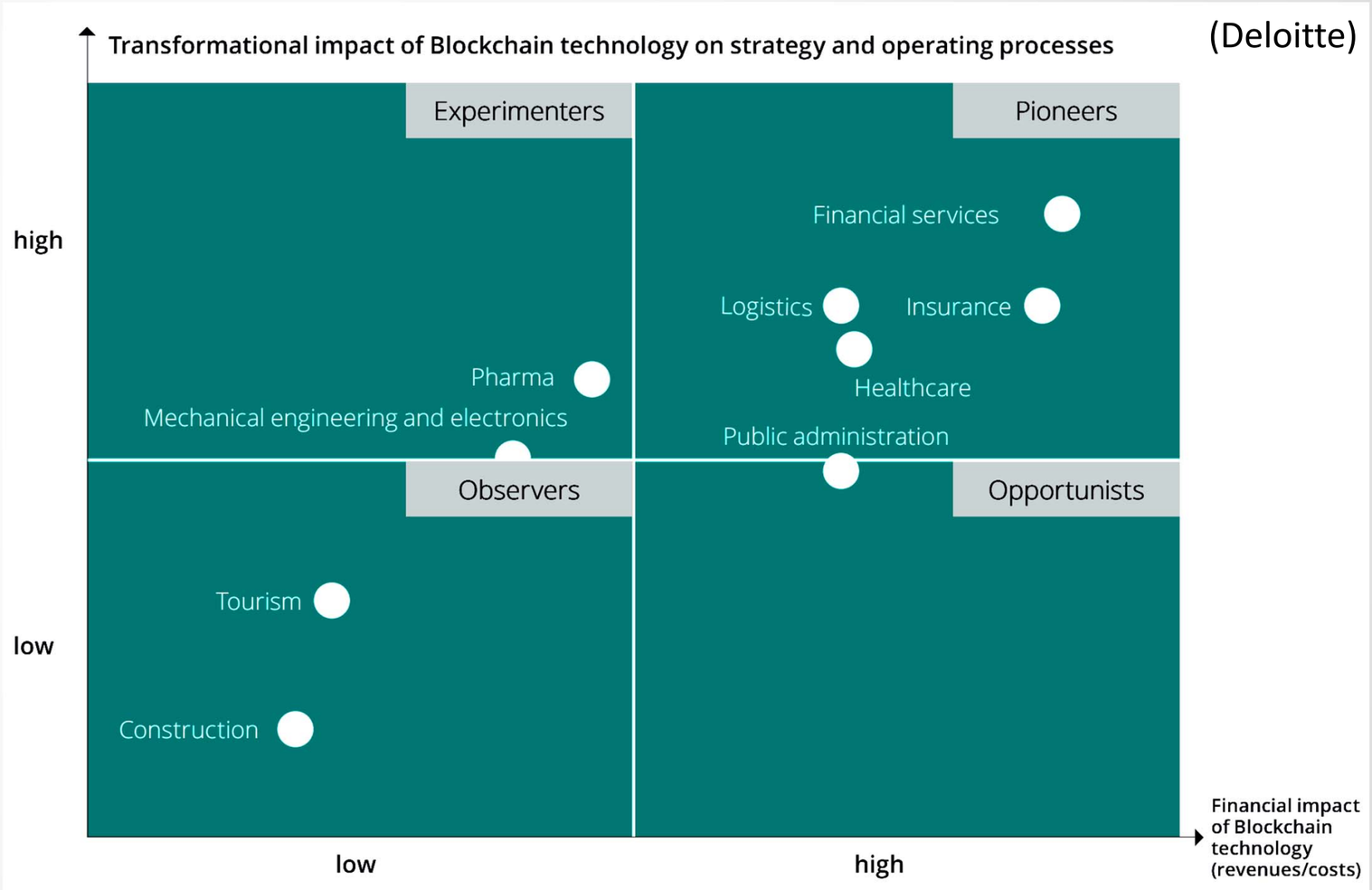
Silk Road's Money Flow



Bitcoin's Relationship with Blockchain

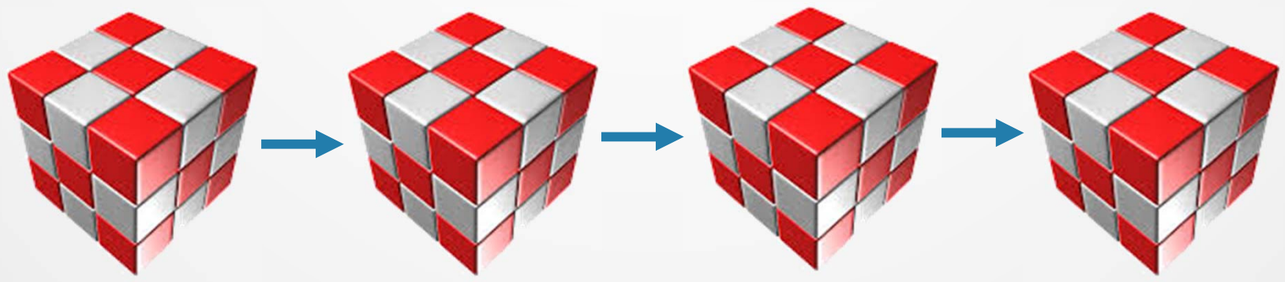
- Bitcoin is one of the many cryptocurrencies, in fact, the 1st one.
- Bitcoin was built upon the Blockchain technology.
- Bitcoin is anonymous. Not all blockchains are like that.
- Blockchains have numerous other applications too.

(Deloitte)



So, what is blockchain?

Blockchain is a secure transaction ledger database (initially made to facilitate currency exchanges) shared by all the members participating in an established, distributed network of computers. (LSTA)



Bitcoin Example:

Centralized vs Decentralized Ledger

A bank keeps names and account balances
→ We know how much one can spend based on his balance in the trusted bank.

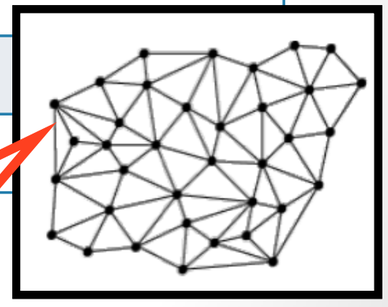
Ledger

Alice	5.3
Bob	100
Frank	700
Carlos	3
Jane	1.3
Charlie	4.645
Scott	.00000001
Kristin	1

Ledger

Alice
Bob
Frank
Carlos
Jane
Charlie
Scott

Transaction
Alice →2B → Bob
Bob →1B → Frank
…



Instead of balance, everybody can get a copy of the transaction records. So, everybody can verify if someone has got money and where it has come from.

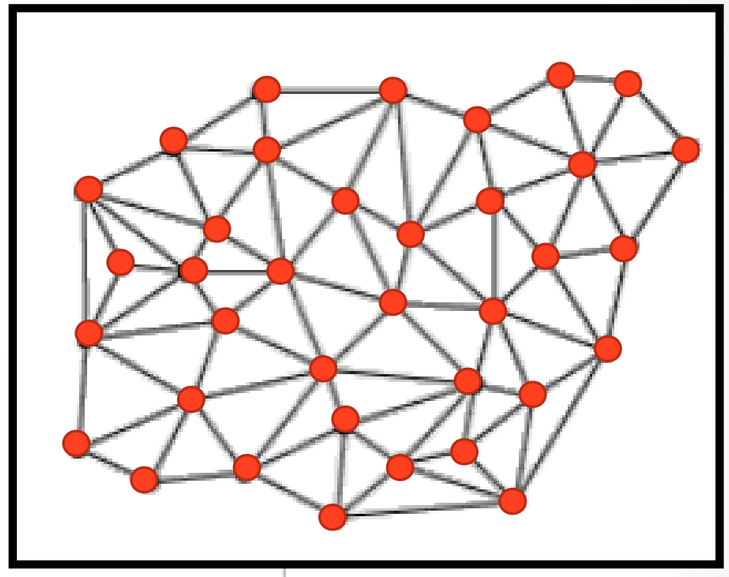
Transferring Money (animated)

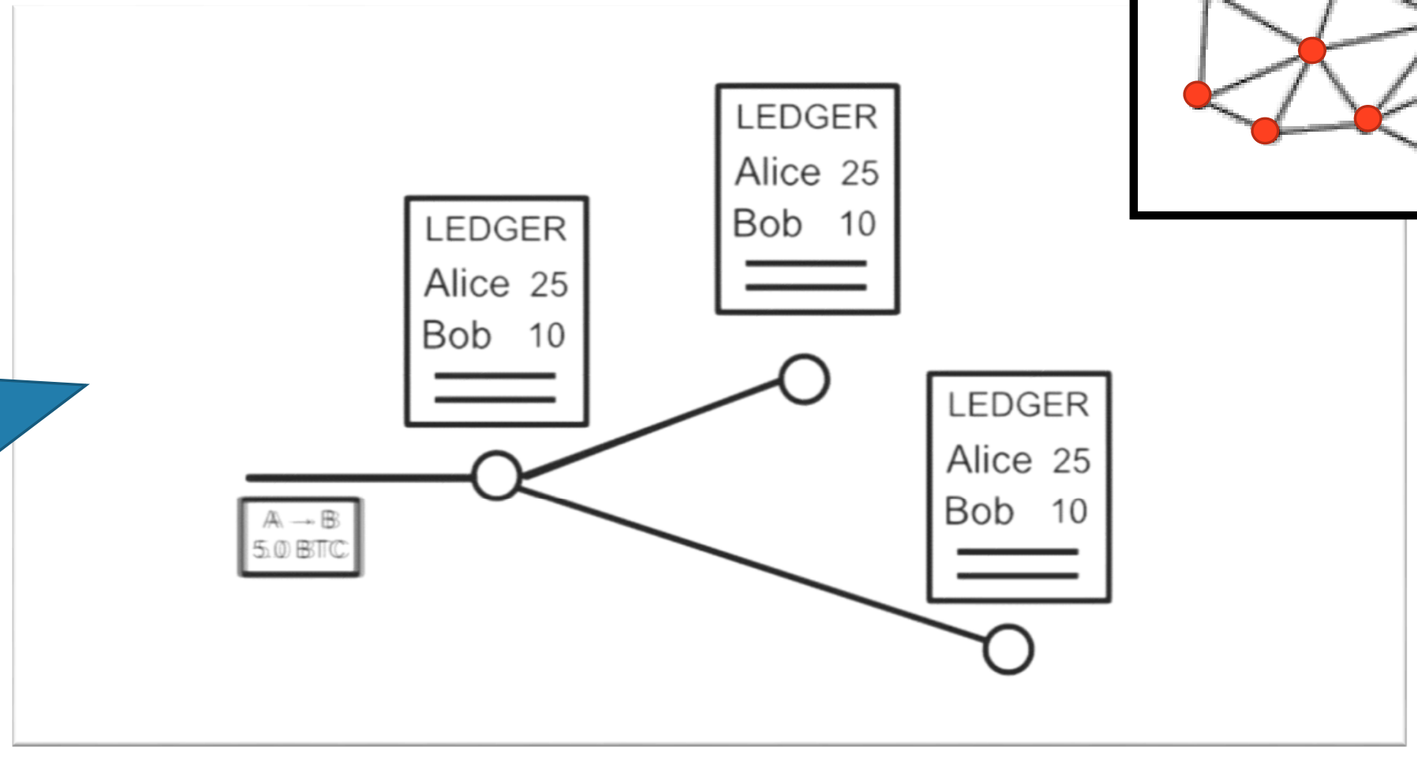
- Alice wants to give Bob 5 bitcoins:

  Alice → Bob 5.0 BTC

- She puts this transaction on a file and sends it to everybody she knows, and those will forward the transaction to everybody they know, and so on.

How transactions are flooded



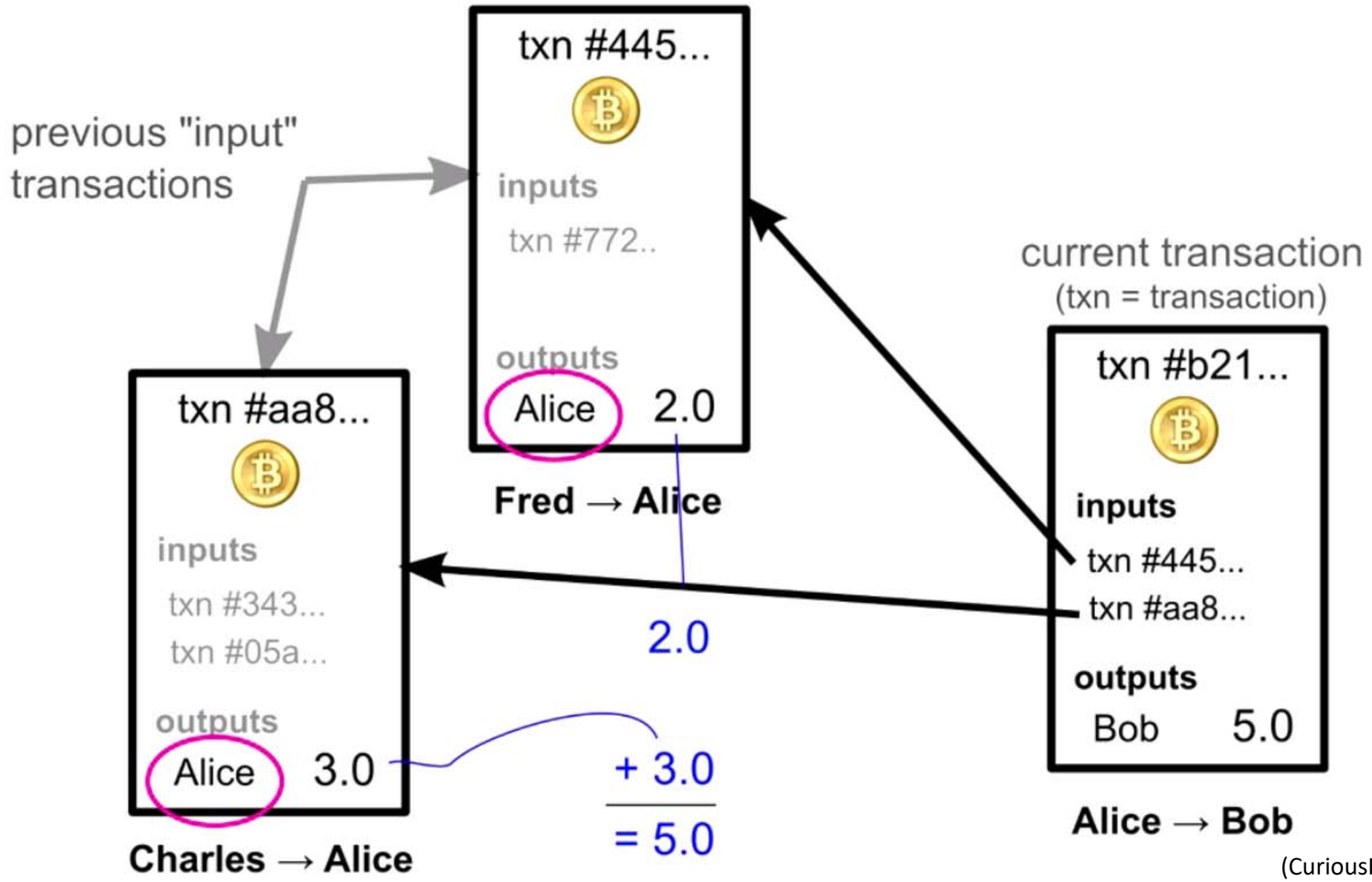


Here, we have shown a ledger by balances for simplicity. It is the transactions list in practice.

(CuriousInvestor)

How does Alice Prove she has the Money to Spend?

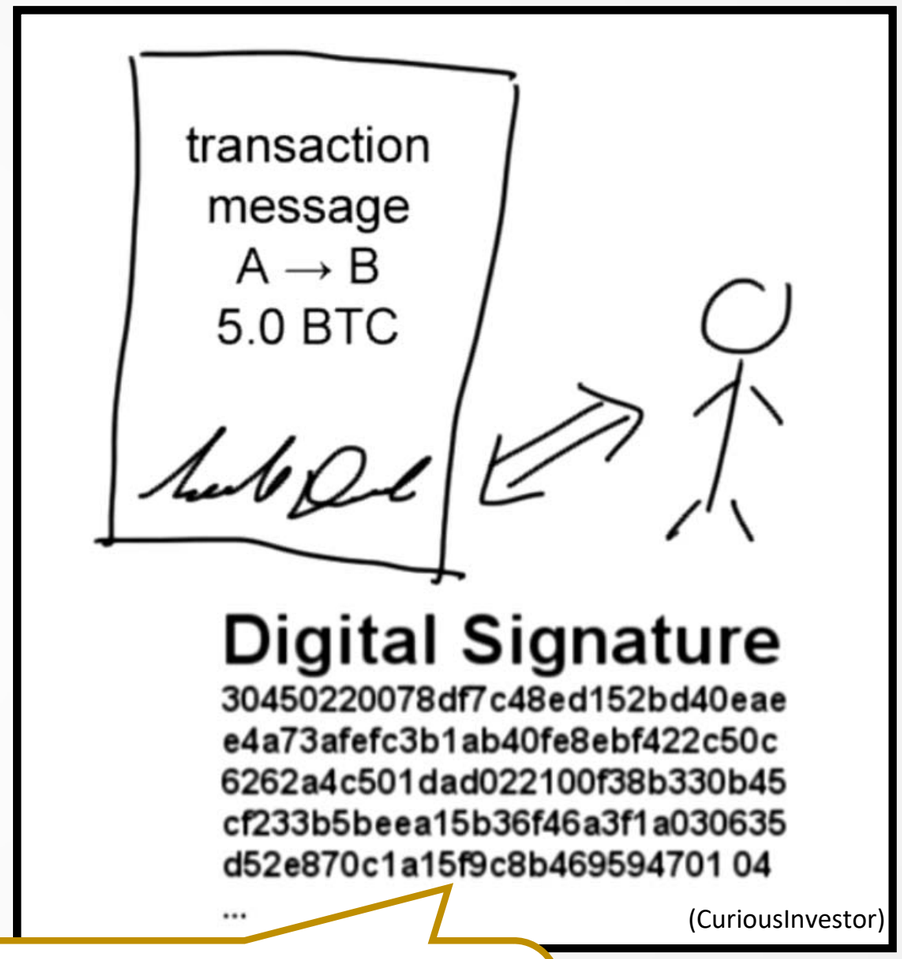
- There is no balance!
- Instead, she mentions the previous (input) transactions.
- Everybody can verify (by signatures) that she has received 5 bitcoins (from Charles and Fred).



(CuriousInvestor)

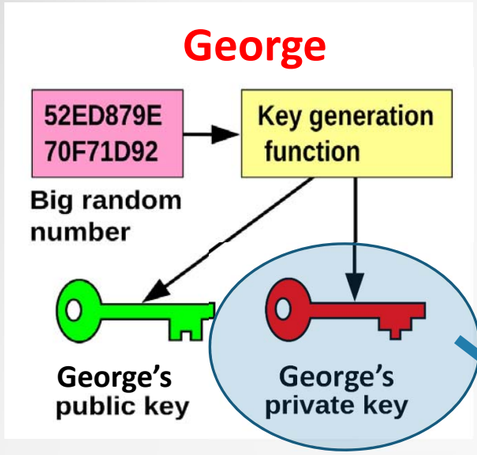
Transaction Protection

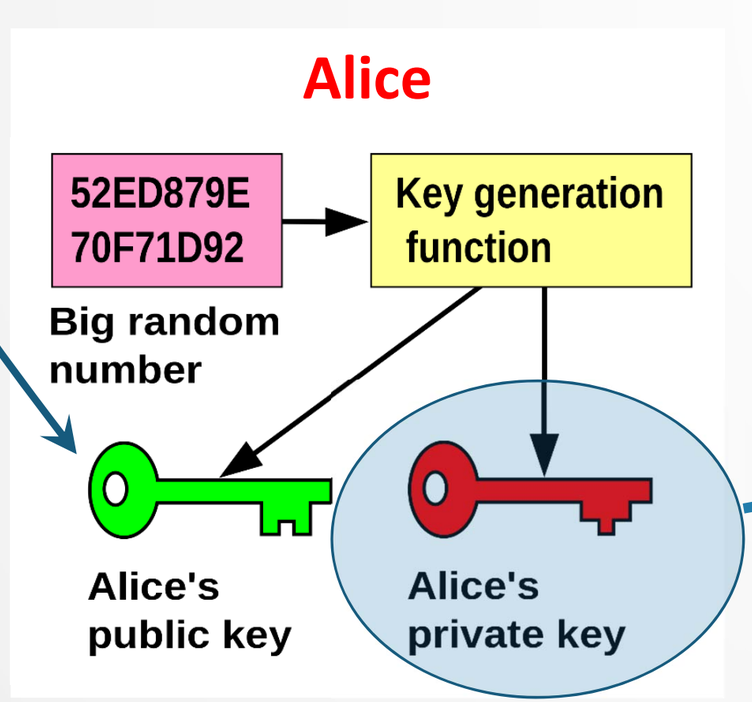
- How do the people make sure that it was actually “A” who did the transaction?
  - By Digital Signature!
  - When you’re paid, the money is sent to your public key.
- You may spend the money by signing another transaction using the private key corresponding to that public key.



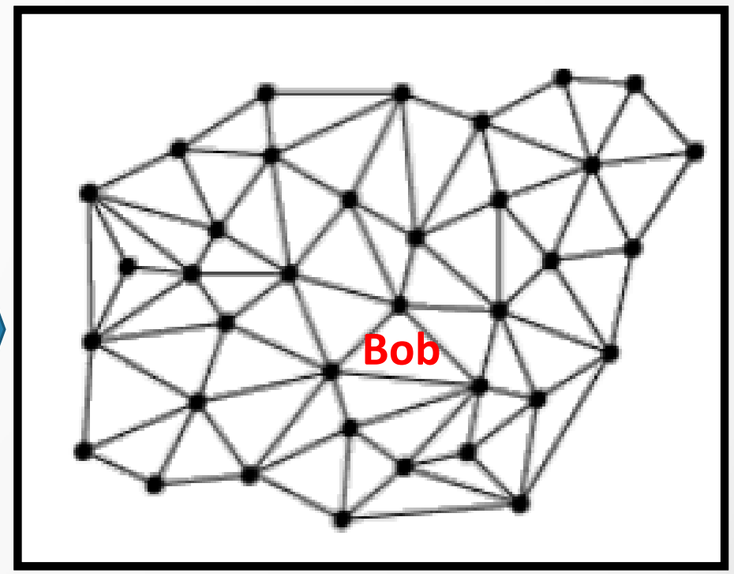
You don’t send someone the money. You actually send it to his public key!

How the Transactions are Protected by Key Pairs and Digital Signature



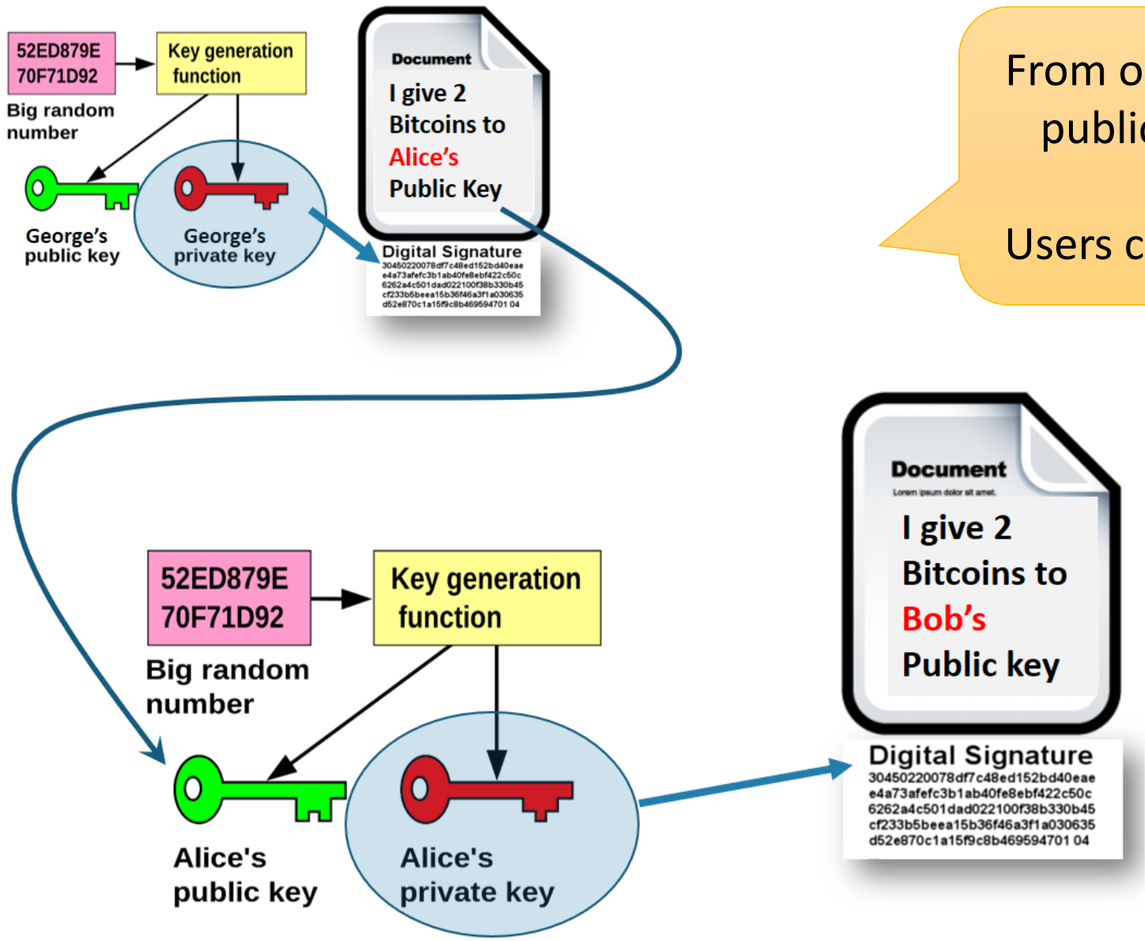


Everyone will know about this transaction then



Anonymity

Anonymity is achieved by not binding the key pairs to their owners' true identity.



From outside, it is as if a bunch of public keys are doing business with each other.
Users can have multiple key pairs.

A Real Transaction

Every transaction has a signature to verify

Previous transactions that prove A has 139.616 BTC

Inputs

Previous output (index)	Amount	From address	Type	ScriptSig
eb38f77560ca...:1	8	1P9SgqzjFWgWVAuZBFwimNPV7LuuaJpgTj	Address	30450220078df7c48ed152bd...eaee4a73afefc31 044760639da2c0d6158484e1a4dab332fefc4bb5
b912994fca58...:1	0.03	18Mk65wV1E5kCVHFShvUTU6zt4yVFKM5Ft	Address	304502204e877fc5ca3783e165052e64c4788dd 04769bbfc55cbd412784e024c8624f8c4f42d7cb
58379d94fe85...:15	1	1G4hfnM2ufAPEECdawg5gtvUTBB2PxvLr2	Address	3044022075d23fd4a8004866777210f51f46c96 046dd45b37fe3ff33f1563458cfbdfb7f922d1b4a
fc9d1cd1c2ac...:1	130	1LpQVnJSMgqqibQBGZwbobdX2Ghn9YWyC7	Address	3046022100a65a188b89a4e5ae2eaa5ba387503 04ba81a1a538c5ddf7e0c76884497ab522456b9
7b6f7d4a521c...:1	0.55357267	16Kb6XppHUbjgmYQDpRyxz9jNE9Az5Xvcb	Address	3045022100eeb76e61abe62d38fd462eafd1d11f 04f4fa1d3e26f3e7058038871a31b8bf63fd127f6
544097a30e09...:0	0.03270607	1JnsDx1g6c757z8AnJUemj46YQgCTw54QN	Address	3045022100859df2ced47493e86a849cce10615 04de257fe6490bd16188be6d06ca7b34816fa4b

+

139.616

Outputs

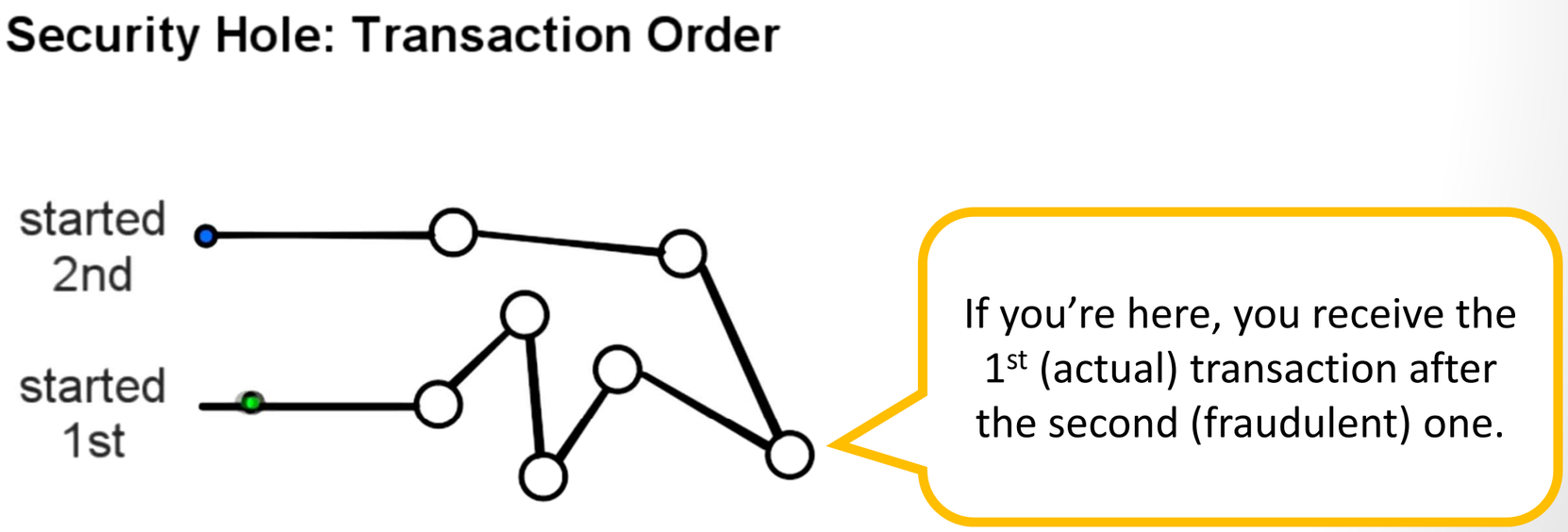
Commission

back to sender

Index	Redeemed at input	Amount	To address	Type	ScriptPubKey
0	8baaca27d158... 0.011	0.01071174	1F7BgzQbyWTWzEMUKNzzLdjkbjaQT9K96m	Address	OP_DUP OP_HASH160 9abd2e0c0a63dea36b75c3128fe15d82f274e394 OP_EQUALVERIFY OP_CHECKSIG
1	1bb973b4ccc8... 139.606	139.605567	1NT2zFMa11NiCZydt4kqgXRZPf3iS6ZPGZ	Address	OP_DUP OP_HASH160 eb471d7a903e538cb94c1f2faf20eaadad8479af OP_EQUALVERIFY OP_CHECKSIG

A Security Concern

Due to the network topology, a money can be spent twice and the 2nd transaction is accepted first! Therefore, the 1st transaction (which was real) can be deemed fraudulent and double spending.

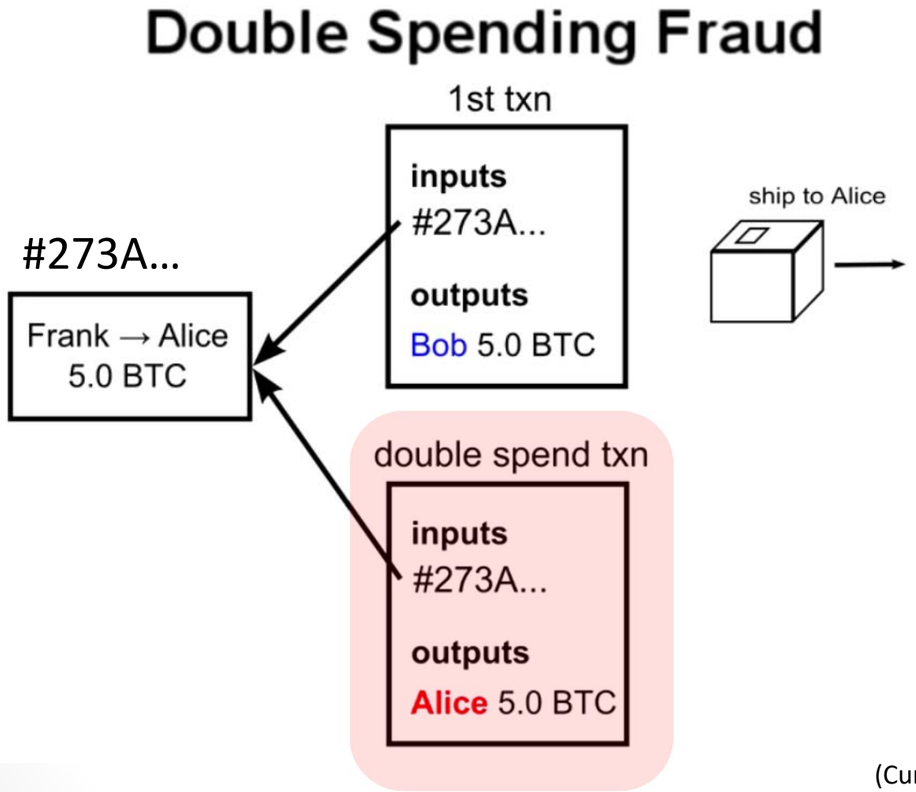


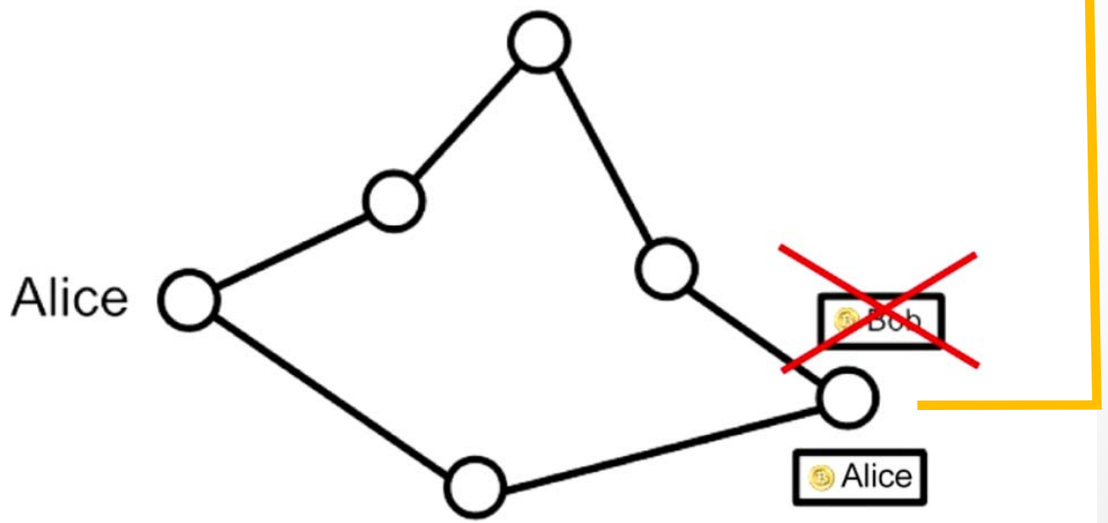
(CuriousInvestor)

Example of Double Spending Fraud

- Alice buys a product from Bob. Right after he ships the item, Alice makes another transaction and gives the money back to herself (using another key pair).

This node wants to deal with Bob, what does he think?



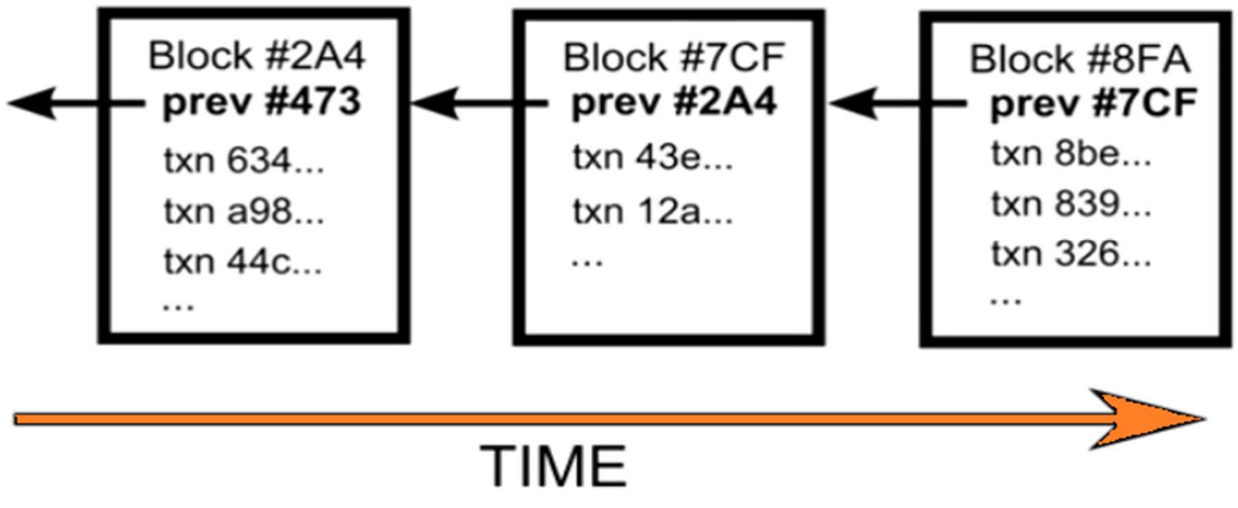


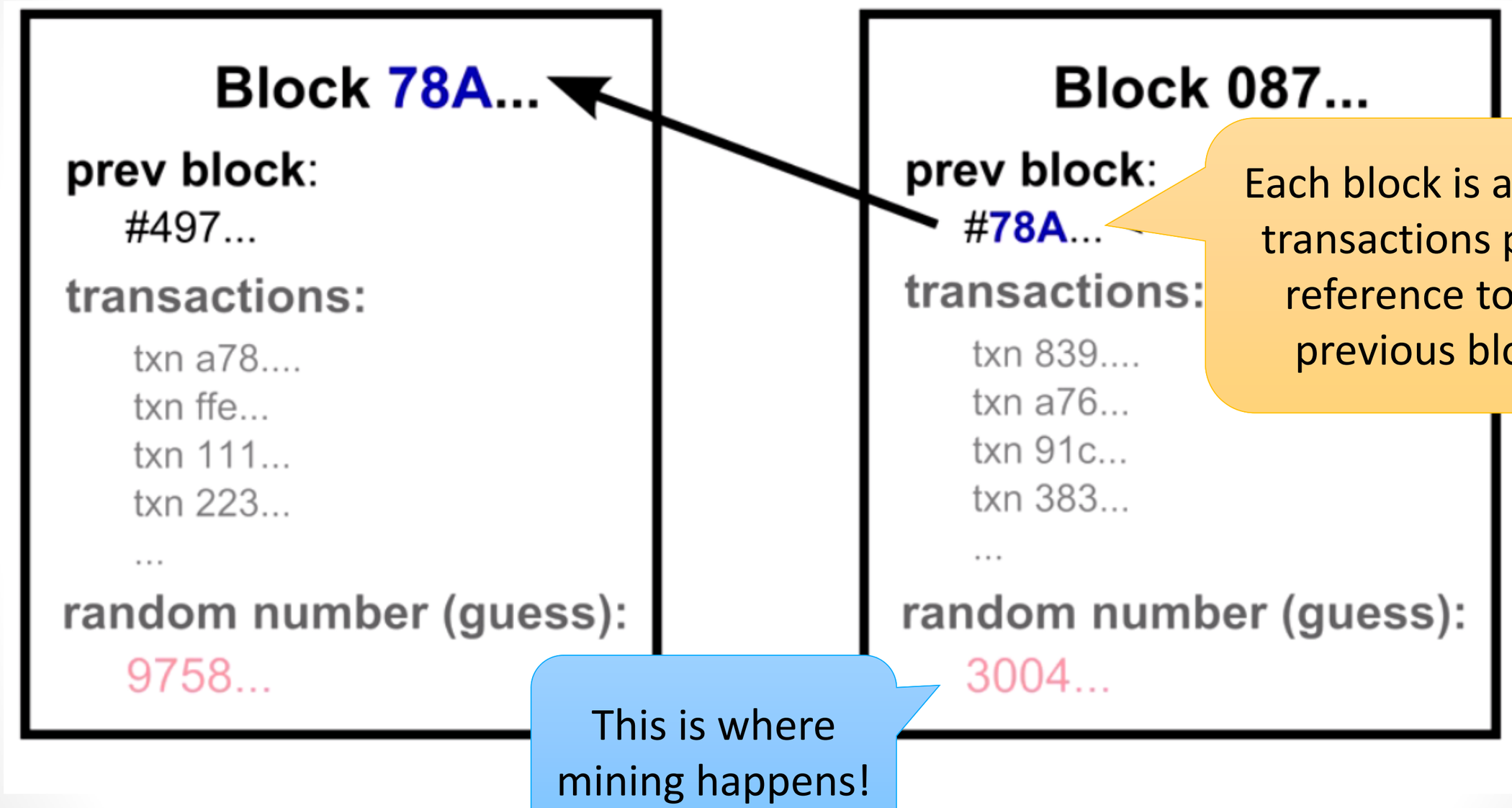
(CuriousInvestor)

Blockchain:
A way to Find the Right Transactions Order

- There will be disagreements in the network whether Alice or Bob owns the money.

- We should find a way to figure out the correct transaction order.
  - That was how **blockchain** was invented.





(Source: CuriousInvestor)

Who Should Make a Block?

A block is made of a set of transactions happened in the same time slot (around 10 mins).

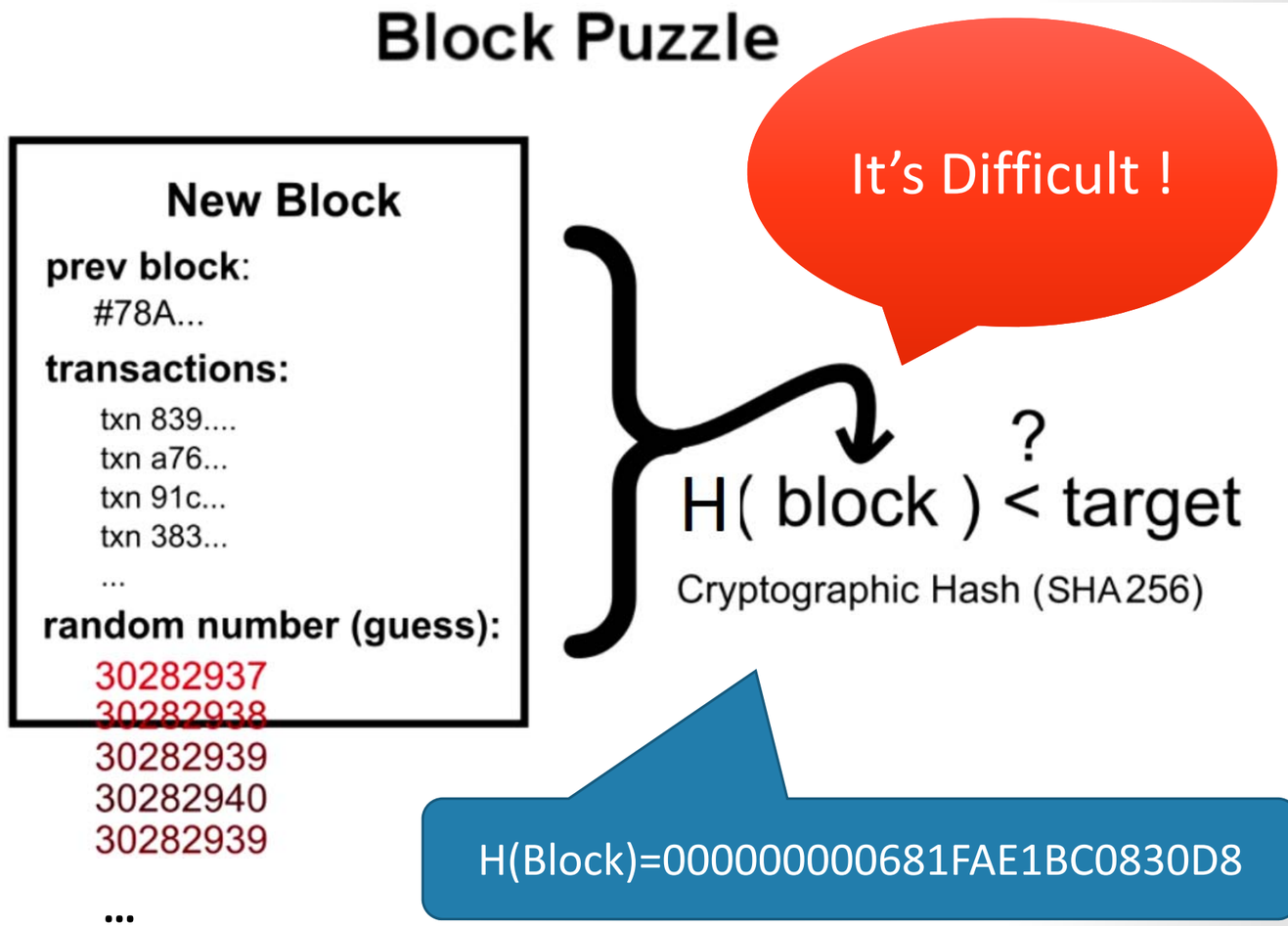
- In PoW, any node can create a block, and by creating the block, makes the transactions permanent (along the branch).
- To make a block, the node must solve a hard mathematical puzzle.

(CuriousInvestor)

Mining !

To make a block, one has to add a number to the transaction data in a way that the puzzle is solved.

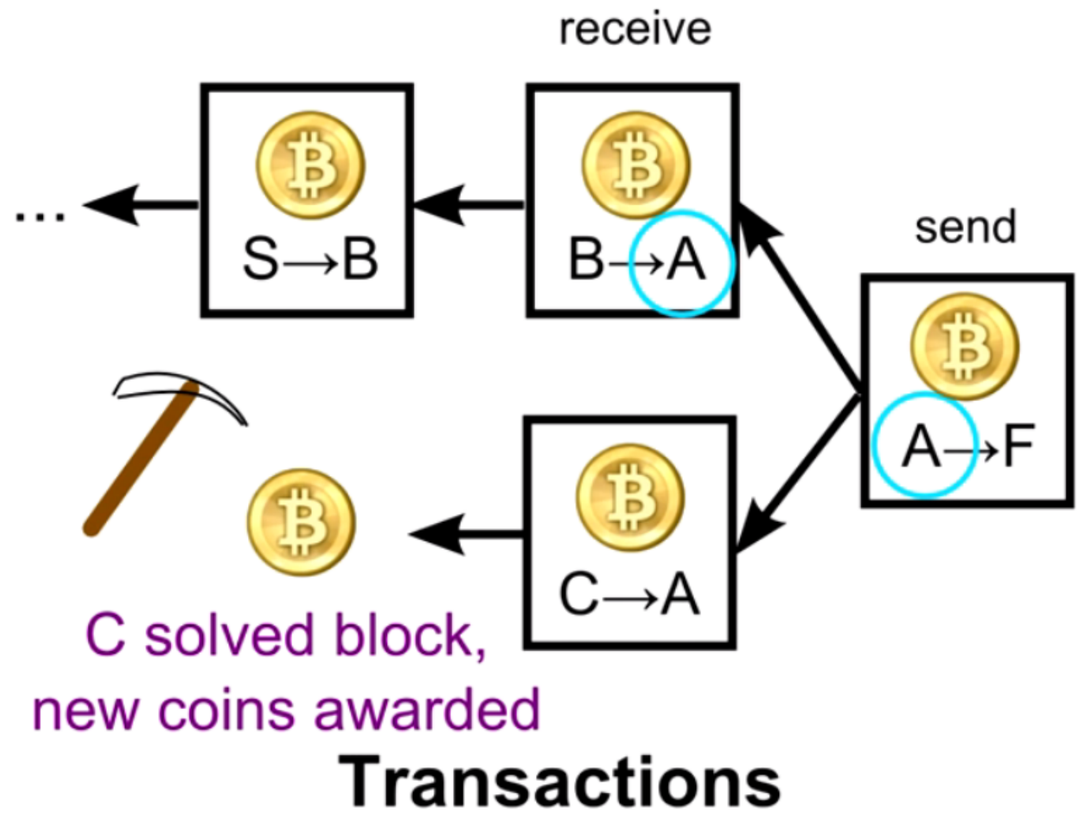
It Bitcoin, the puzzle is finding a hash function value that it is smaller than a target threshold.



Mining (Cont.)

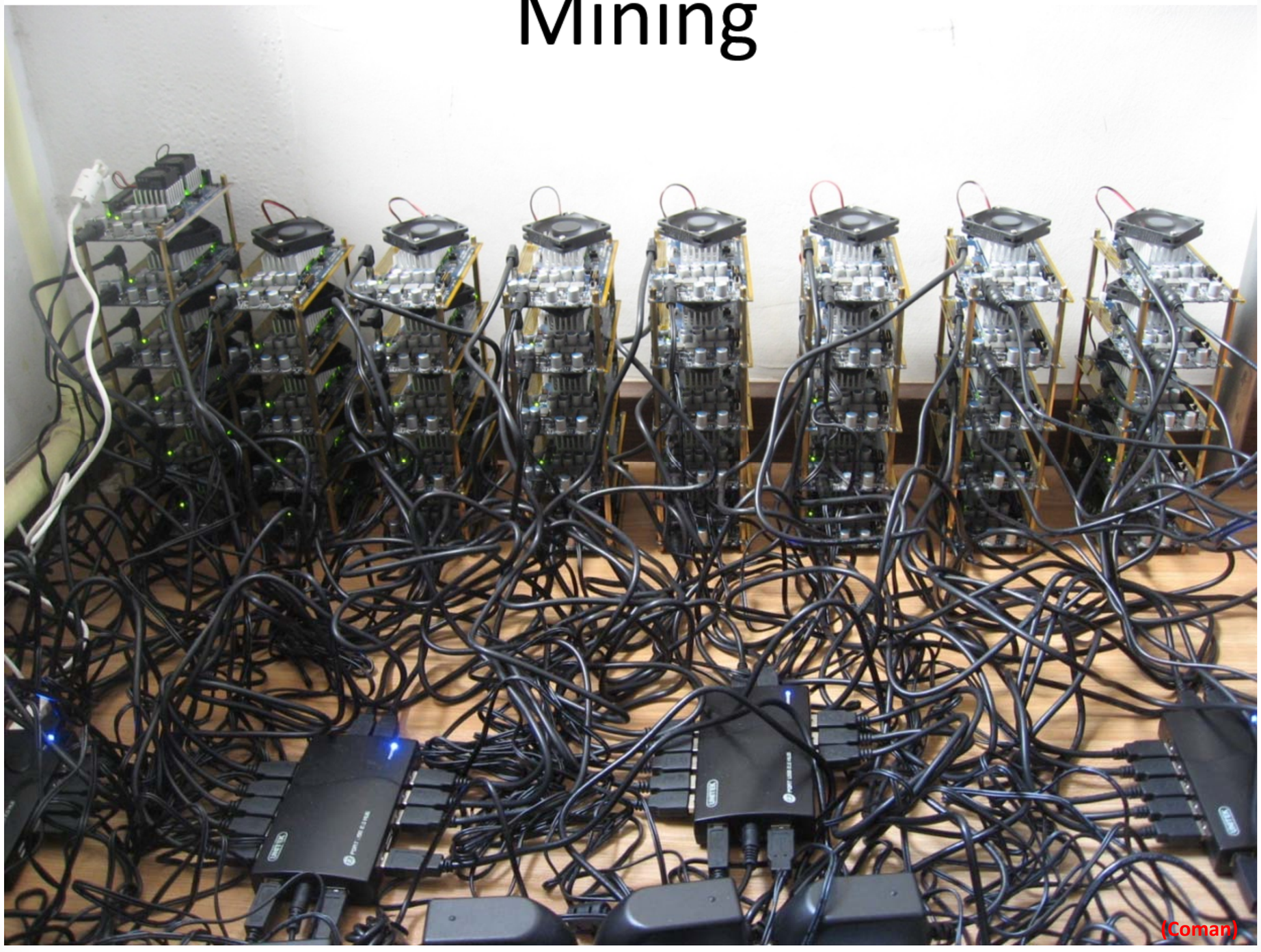
- **Why should people do this?**
  - There's an incentive! **That's how money is created!**

Initially the reward was 50 Bitcoins. Every 4 years, the reward is divided by 2. Now (2018) if you solve one block, you get 12.5 bitcoins.



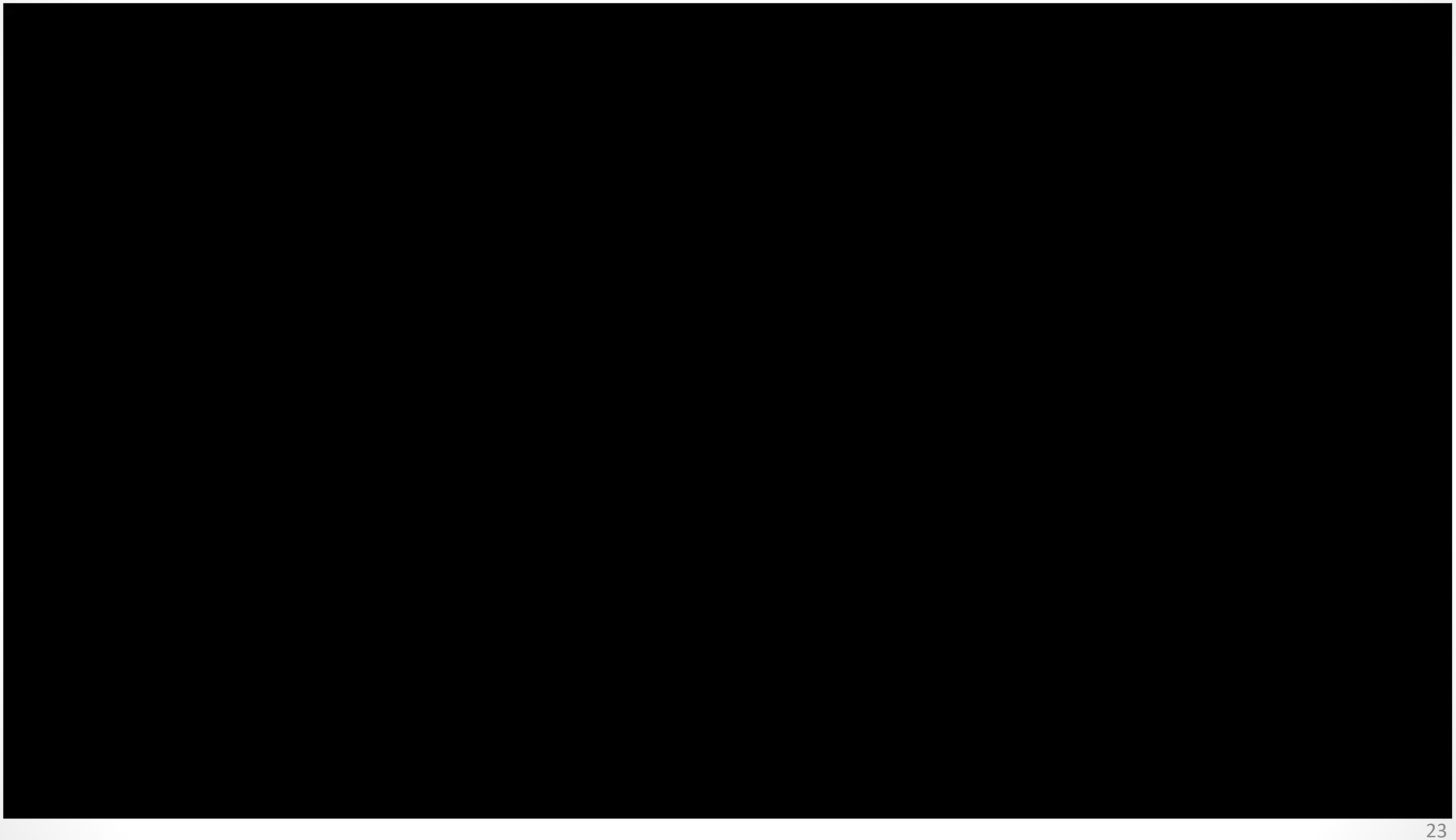
(CuriousInvestor)

Mining



(Coman)

Live Transactions on my Phone (on May 24, 2016) – blockchain.info



Bitcoin is not Alone

- There are plenty of other cryptocurrencies
  - Monero
  - Litecoin
  - Zcash
  - Ripple
  - IOTA (based on tangles)
  - …

- But Ethereum opened a new chapter in blockchains in 2013.

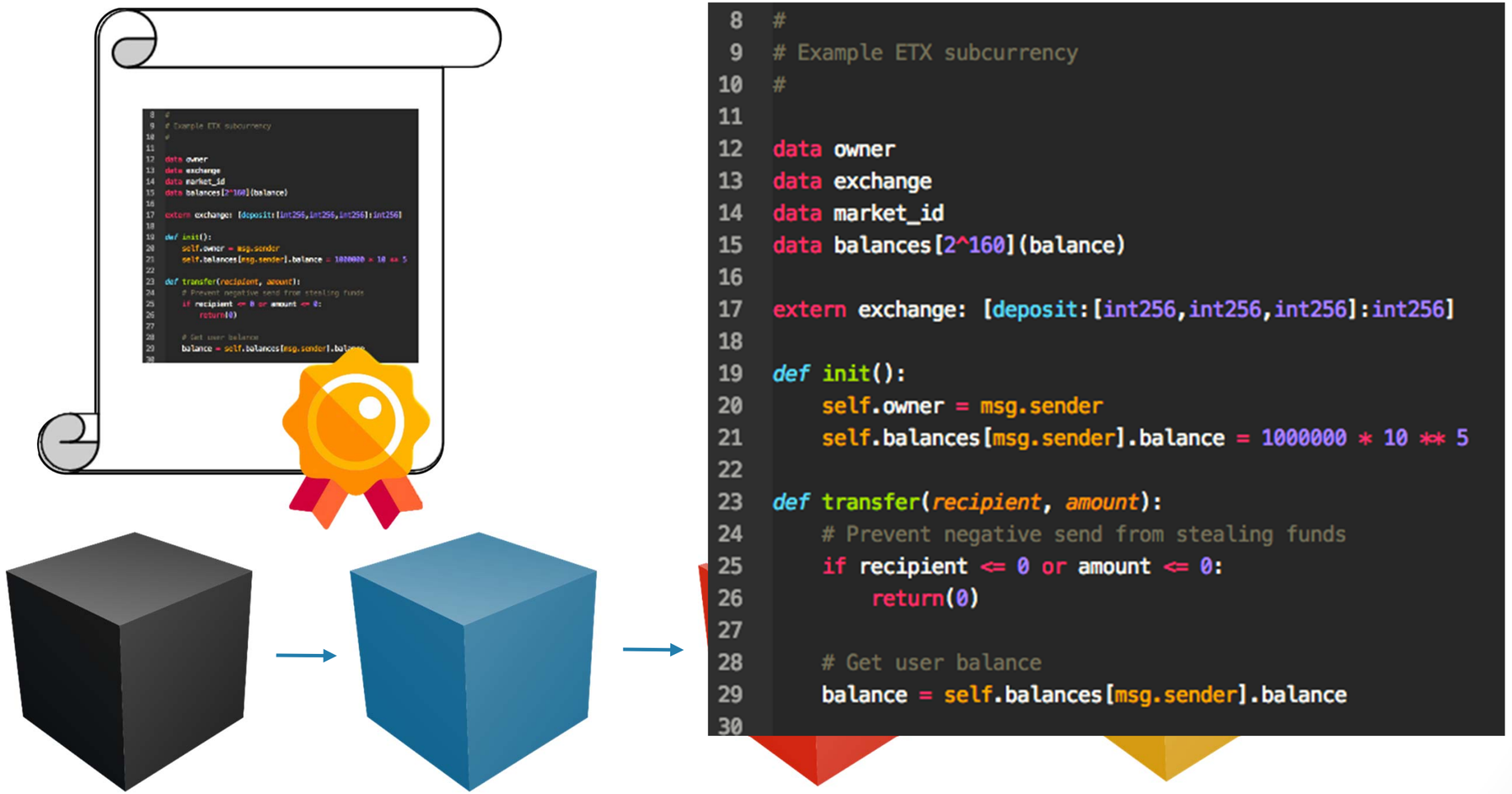
Ethereum

Ethereum's idea was conceived by Vitalik Buterin in 2013. But it went live in 2015.

He wanted to generalize the idea of blockchains, and mixed it with programming. That's how "Smart Contract" was born.

What is a Smart Contract? (animated)

- It’s a piece of computer program, stored in blockchain.



Crowdsourcing with Smart Contracts

In Ethereum, you can interact with smart contracts as well as human beings (2 account types).

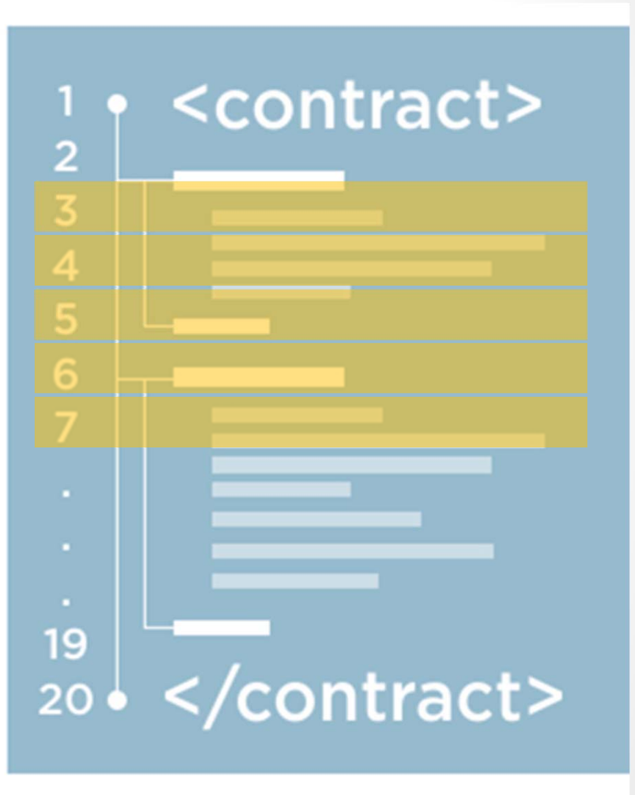
We can write a smart contract (program) that collects money for a project. Programs can have if/then.

If the collected money ≥ T , then
{
Transfer money to the team
}
else
{
refund the money
}

(Source: Savjee)

How are the Blocks Verified?

- Similar to Bitcoin, everybody receives a copy of the smart contract (program) as well as all the other interactions done with it.

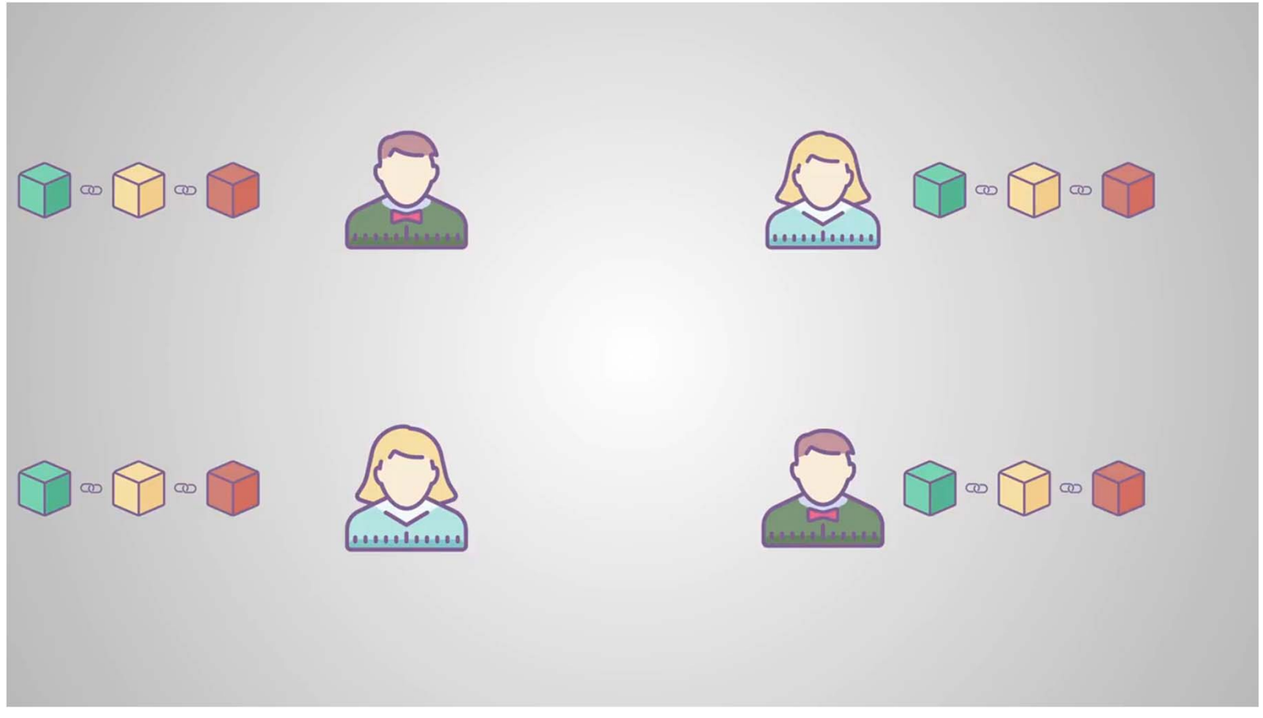


(bitsonblocks.net)

- Each member can run the code on his/her computer and give it the same interactions to find the current state of the contract.

How are the Blocks Verified?

- Again, we can use the blockchain to ease the processing and make sure the interactions are in the correct order.
- We can rely on the miners if we want not to do all the work.



(Savjee)

Some Business Domains Affected

FINANCIAL

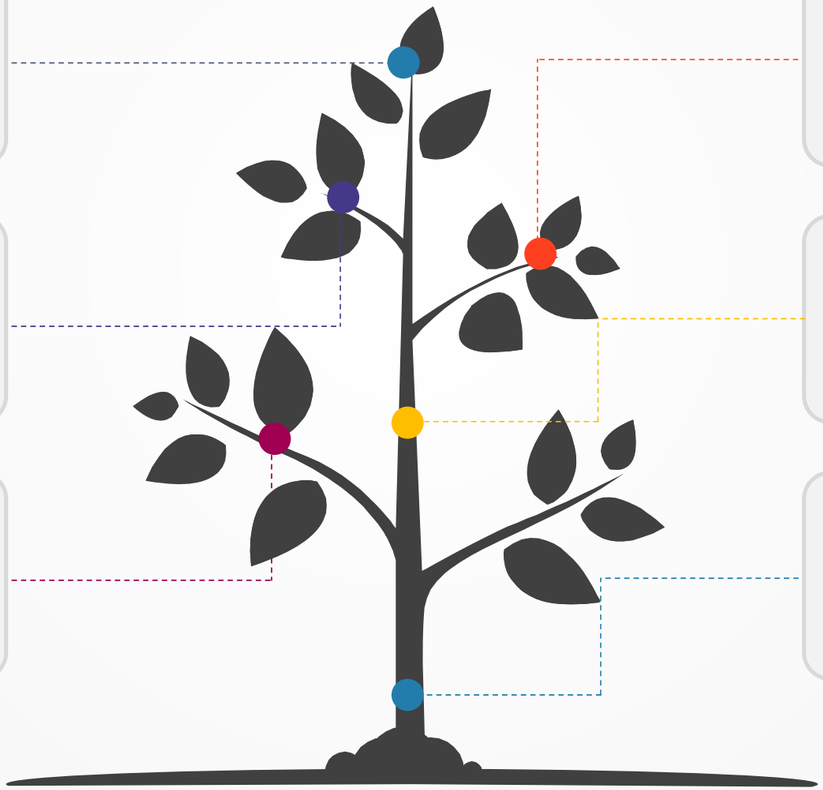
Banking & Payments,
Loans, Gambling, …

INTERNET & CYBERSEC

IoT, Domain Name System,
Trust Management, …

ENERGY

Smart Grid P2P Energy
Exchange, …



OWNERSHIP/COPYRIGHT

Music & Film Industries
Real Estate

SERVICE/GOVERNANCE

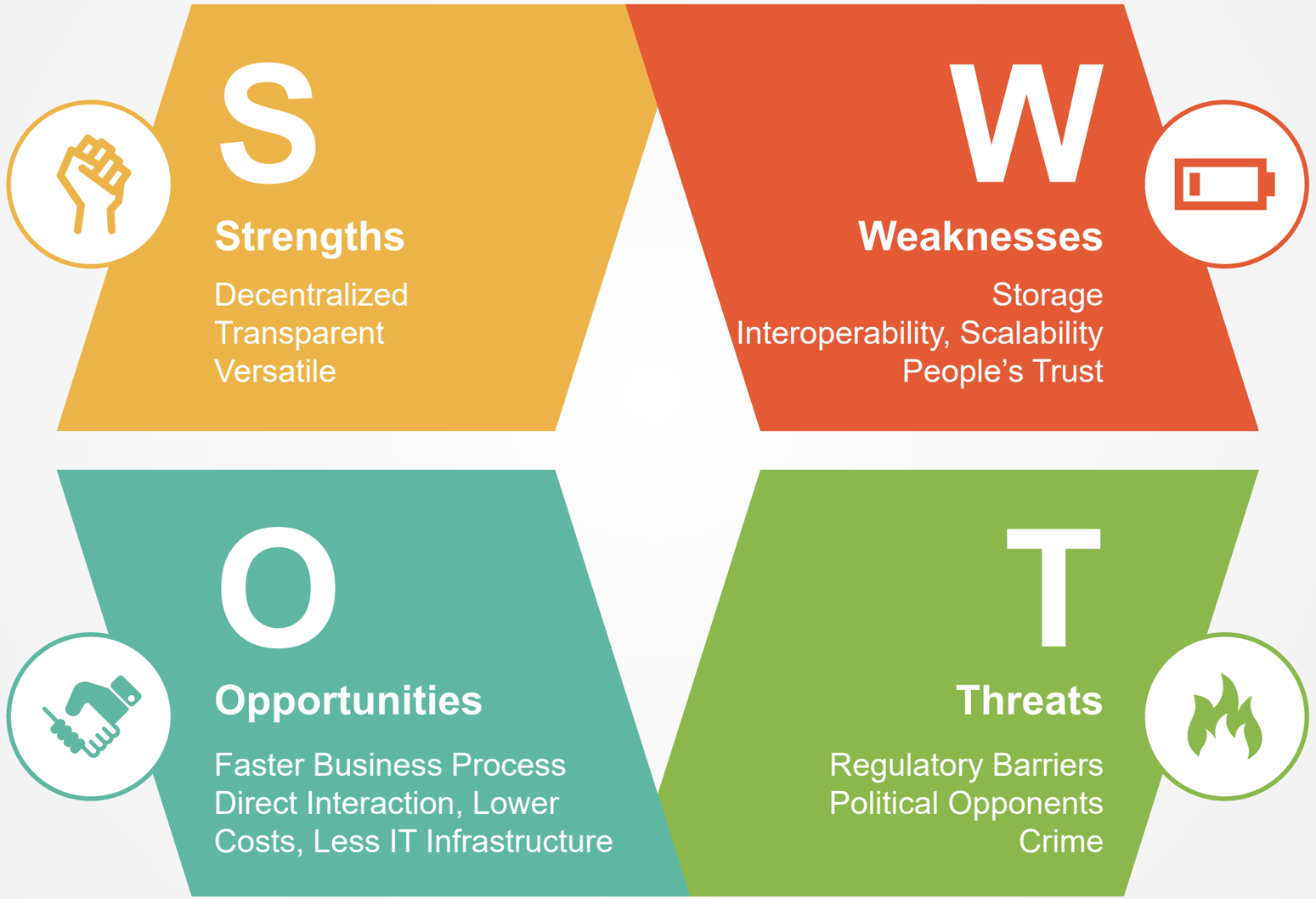
eVoting, Crowdfunding, Charity,
Justice System

INDUSTRY

Supply Chain,
Insurance

Blockchain

Blockchain SWOT Analysis



(Partly from Deutsche Bank Research, Deutsche Bank AG)

Related ITU-T Activities

- **Focus Groups**
  - FG-DPM (Data Processing & Management)
  - FG-DLT (Distributed Ledger Technology)
  - FG-DFC (Digital Currency)
- SG13 – Future Networks (& Cloud)
- SG17 – Security
- SG20 – IoT, Smart Cities & Communities

Some Deliverables on Blockchain in FG-DPM

WG3: Data Sharing, Interoperability and Blockchain

D3.5 **Overview of IoT and Blockchain**	• Provide blockchain overview including basic concepts, key characteristics, various models • Analyze blockchain as a decentralized database solution • Analyze key benefits of using blockchain for IoT in terms of accelerating transaction, reducing costs and building trust • Specify roles of blockchain technique in DPM for IoT and SC&C applications
D3.6 **Bockchain-based Data Exchange and Sharing Technology**	• Identify roles and considerations of blockchain in data exchange and sharing • Identify challenges for blockchain-based data exchange and sharing • Present blockchain operations to support resilience, sharing, and auditable protection of IoT data • Demonstrate how blockchain can change the future of IoT in relation to device identity and data integrity
D3.7 **Using blockchain to improve data management**	• Identify roles and consdierations of blockchain in data management • Identify challenges of blackchain techique to improve data management • Provide detailed operations of blockchain in data management perspectives • Analyze blockchain in the public sector's data management of data as a public good ✓ Case study – blockchain in smart cities • Analyze blockchain in the industry's data management of data as a source of competitive advantage ✓ Case study – blockchain in industrial applications

(SG11 Workshop, 15 November 2017, ITU-T activities on Blockchain)

Thank you