

# BLOCKCHAIN

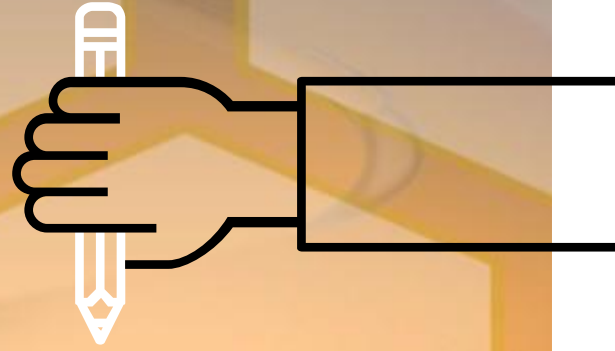
**Scott C.-H. Huang**

Department of Electrical Engineering and Institute of Communications Engineering  
National Tsing Hua University  
[chuang@ee.nthu.edu.tw](mailto:chuang@ee.nthu.edu.tw)

# Outlines

- Introduction to Blockchain
- Introduction to Bitcoin
- Overview of Blockchain
- Overview of Cryptocurrency
- Different cryptocurrencies
- Application of Blockchain
- Smart Contracts

What is  
blockchain?





The blockchain is an **incorruptible digital ledger** of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.

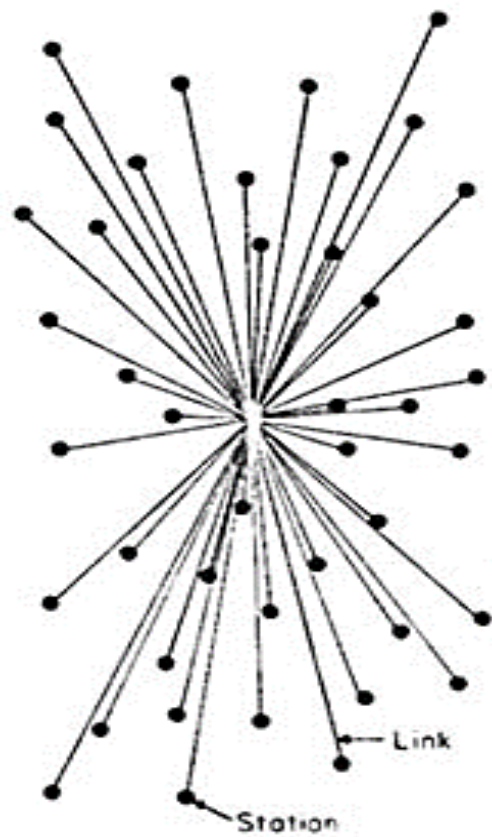
Don & Alex Tapscott, authors Blockchain Revolution (2016)



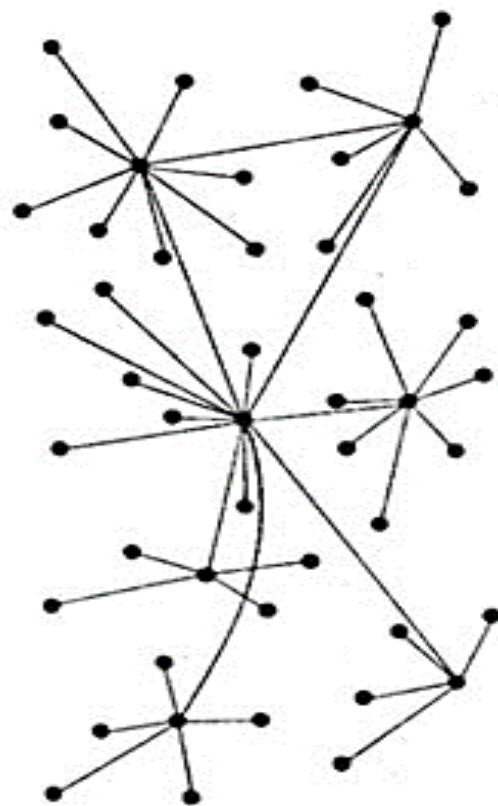


# Blockchain & Distributed Ledgers

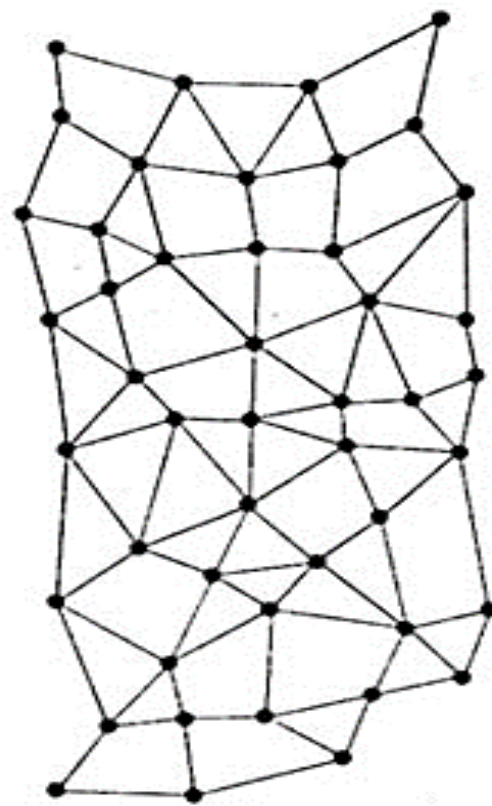
- **Blockchain**
  - The technology behind cryptocurrencies.
  - Analogous to the TCP/IP Protocol that is the foundation of the internet
- **Blockchain are Distributed Ledgers**
  - Ledgers are historically centralized and private
  - Blockchains are Decentralized or Distributed



CENTRALIZED  
(A)



DECENTRALIZED  
(B)



DISTRIBUTED  
(C)

# History of blockchain

When we talk about “**Blockchain**”, we will always mention ...



# BITCOIN

- Real world Problem
  - transaction fee
  - barrier for currency exchange
- The possible approach to solve these problems is the original idea of Bitcoin.



**Bitcoin** was firstly created according to the idea from **Satoshi Nakamoto** (中本聰) who published the paper named “**A Peer-to-Peer Electronic Cash System**” in 2009 which contained the idea of Blockchain.

- Peer-to-peer network
- Proof of work
- Digital signatures

# Nick Szabo

- American computer scientist



# Craig Steven Wright

- Australian computer scientist and businessman.
- Was the CEO of Hotwire Preemptive Intelligence Group (Hotwire PE)









# Bitcoin Whitepaper

## 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



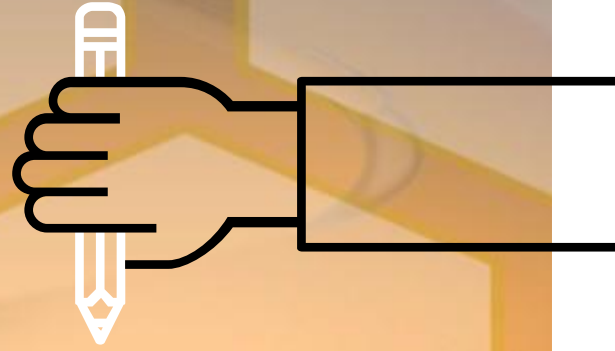
# Bitcoin

A digital money created to make the new payment procedure. It is used on **decentralized peer-to-peer payment network**. This technique required every user in this network to store the transactions (blocks) to keep the network working *without a central authority (Middlemen)*.

# Features of Bitcoin

- Nominal transaction fee's paid to the network
  - Same cost to send \$.01 as \$1,000,000
- Consensus driven – no central authority
- Counterfeit resilient
  - Cannot add coins arbitrarily
  - Cannot be double-spent

# Blockchain Contributor



# Who is the contributor in Blockchain network?

- Users
- Miners

# What are miners doing?

Principally everybody can be a miner. Since a decentralized network has no authority to delegate this task, a cryptocurrency needs some kind of mechanism to prevent one ruling party from abusing it. Imagine someone creates thousands of peers and spreads forged transactions. The system would break immediately.

So, Satoshi set the rule that the miners need to invest some work of their computers to qualify for this task. In fact, they have to find a hash – a product of a cryptographic function – that connects the new block with its predecessor. This is called the Proof-of-Work. In Bitcoin, it is based on the SHA 256 Hash algorithm.



# How Blockchains Work: Maintenance

- ▷ The individuals who maintain and update the Blockchain are “miners,” and they are paid a reward
- ▷ The Miners process transactions by:
  - Solving a complex mathematical problem
  - Sending transactions to other nodes to be verified.

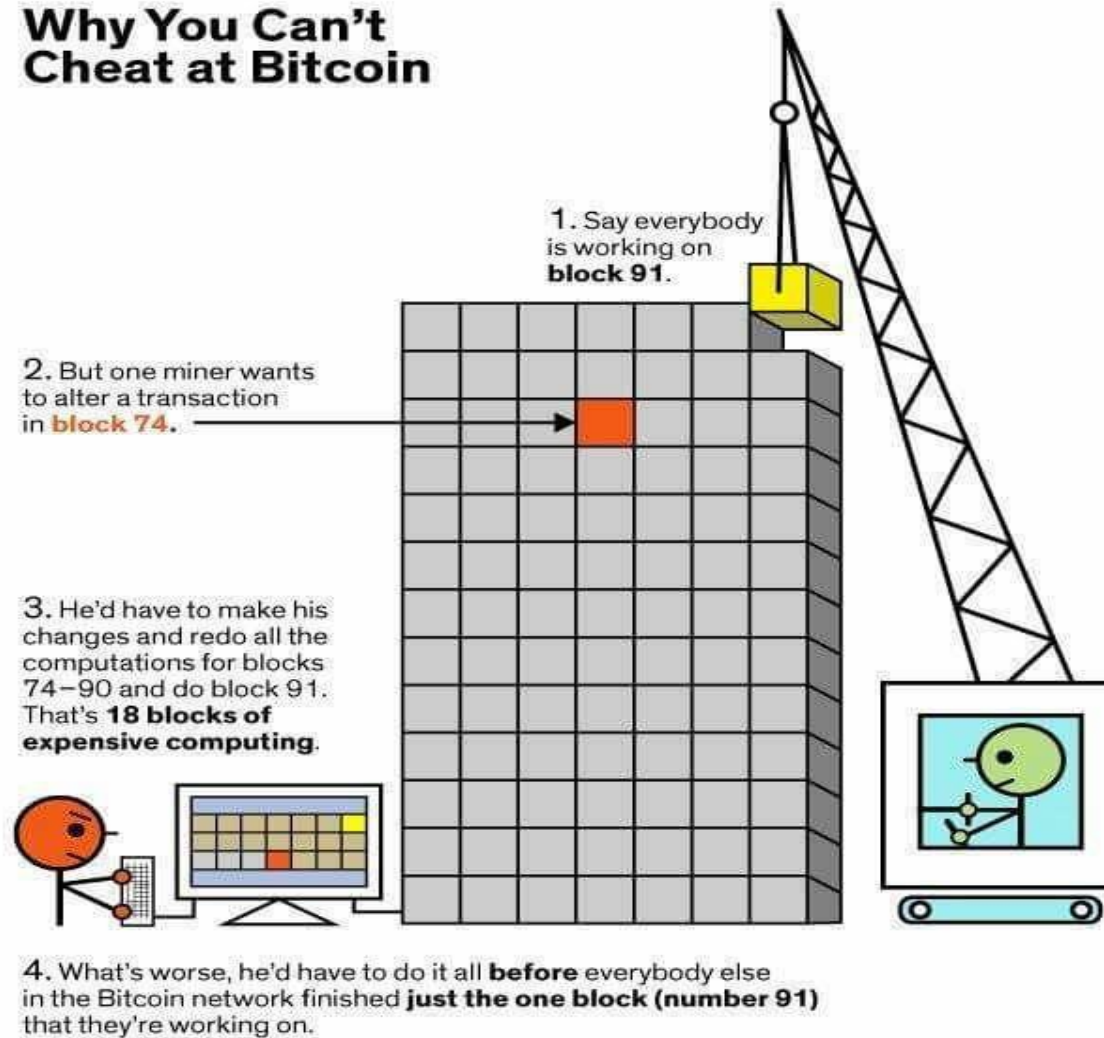
# How Blockchains Work: Hashing

- ▶ When all miners agree the problem has been solved correctly, the block is added to the chain and is visible to the entire network
- ▶ The unbroken Hash (seal) confirms that the block, and therefore every block before it, is legitimate

# How Blockchains Work: Hashing (cont.)

- ▶ Recall: Transactions must be validated by other network miners
- ▶ Miners incentivized to add “valid” transactions via a reward; invalid transactions are rejected, and thus, no reward is given

## Why You Can't Cheat at Bitcoin



# Pseudo Anonymous

- ▶ Using public key cryptography, specifically Elliptic Curve Cryptography due to its key strength and shorter keys
- ▶ Transactions are sent to public key “addresses”

1AjYPi8qryPCJu6xgdJuQzVnWFXLmxq9s3

1Give4dbry2pyJihnpqV6Urq2SGEhpsz3K

d39b0c4653b982e9aee616003db410e75868f61054656e044f0cdedbb6e77342

2015-01-13 16:23:53

1G5kvbP33mMwgtSTHpwAJe86xWKBwUHSV4

1HKBEEHryiuBd8Fp9Skhui6YGnLYNB3hQZ

1pob2EUuE1r7PjpMceubopkSWnrkSivY5



1JqFCQNCJr16rb4h3J2SvDg5ic5UejEPwi

14DaDziYJCD4h8GQ3nbh8bx244Fc9Fc13J

2.103973 BTC

0.01000001 BTC

2.11397301 BTC



# Addresses are like Accounts

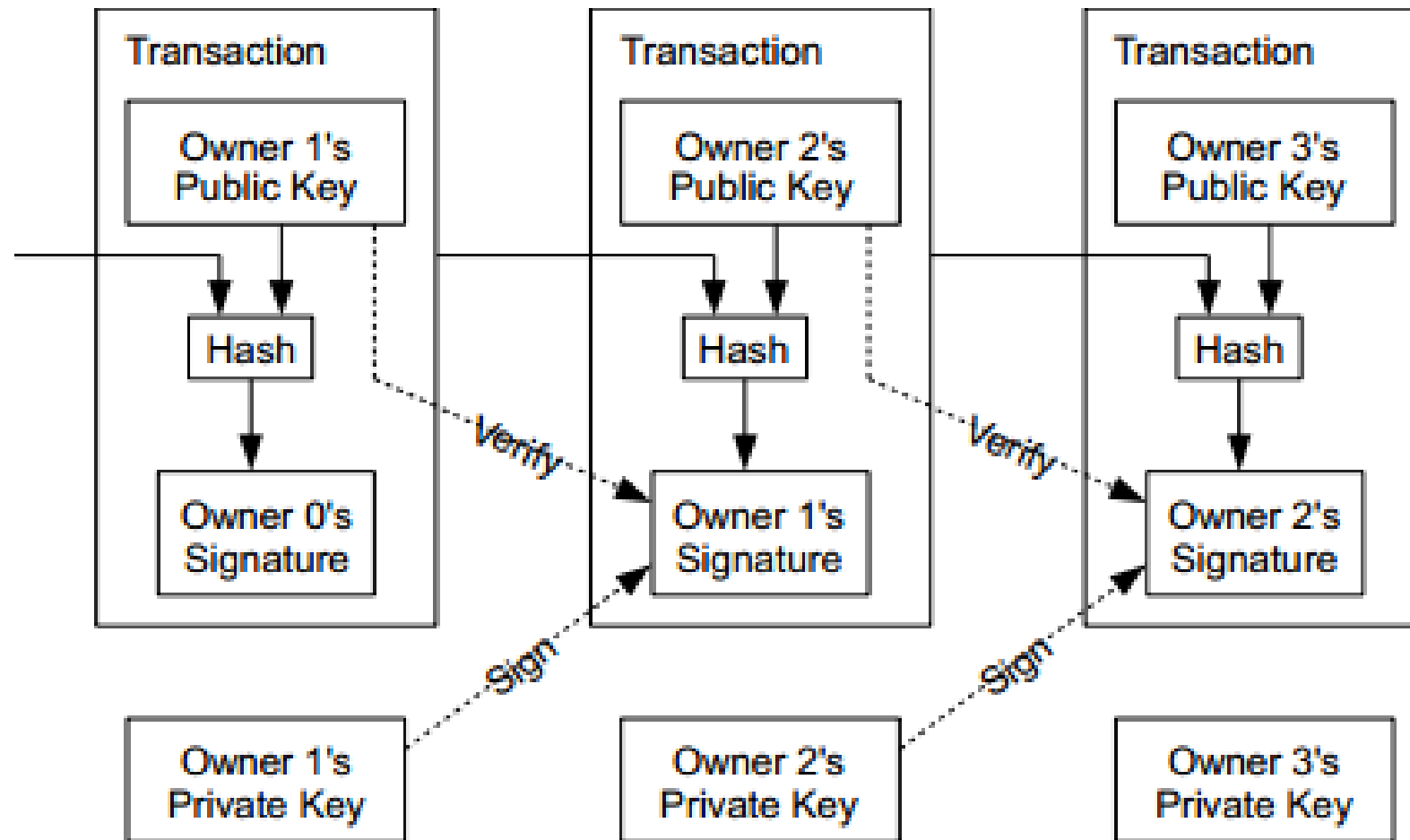
- ▶ The wallet listens for transactions addressed to any of its public keys and in theory is the only node that is able to decrypt and accept the transfer
- ▶ “Coins” are “sent” by broadcasting the transaction to the network which are verified to be viable and then added to a block
- ▶ Keys can represent a MULTI-SIG address that requires a N of M private keys in order to decrypt the message

# Public Ledger

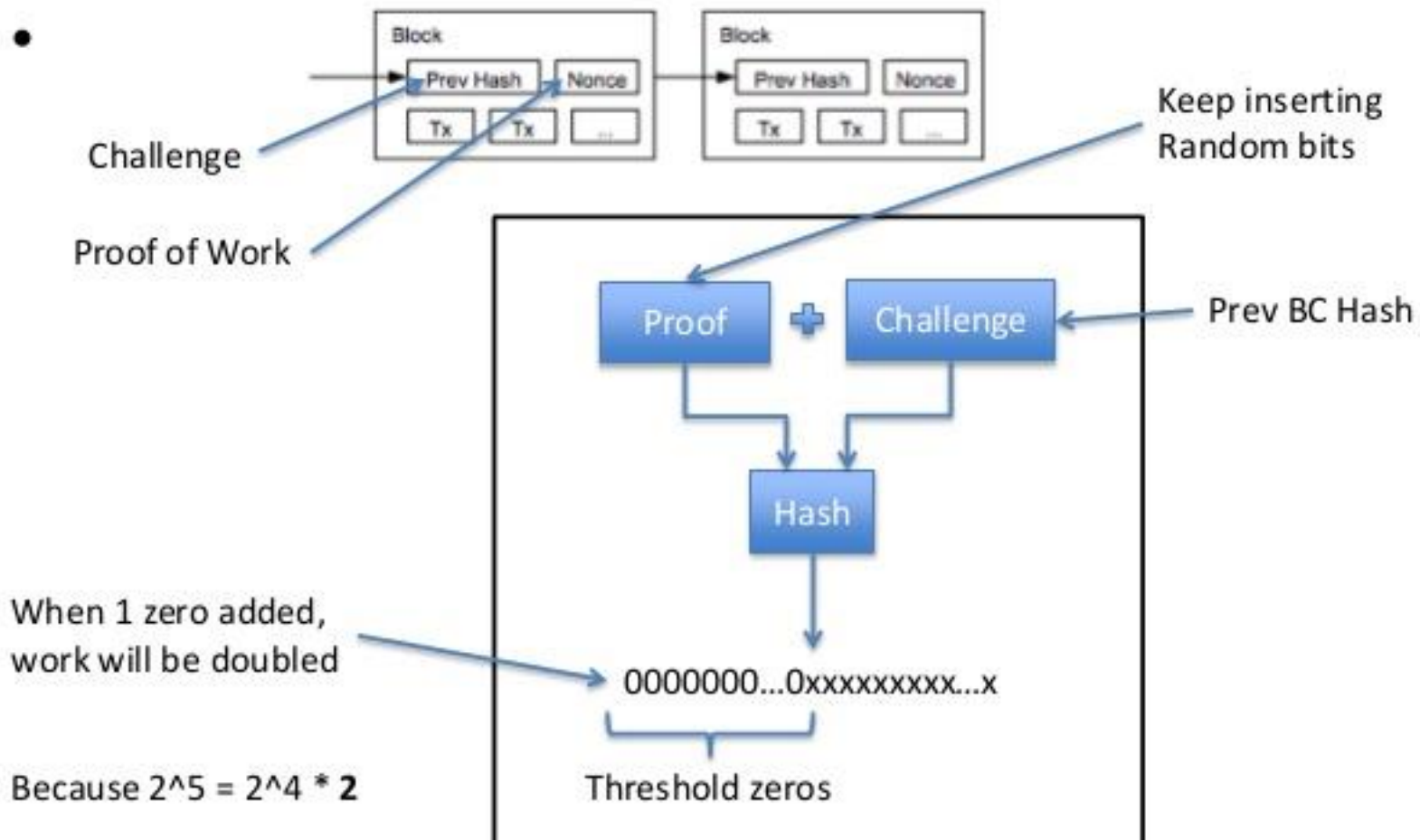
- ▶ Every *viable* transaction is stored in a public ledger
- ▶ Transactions are placed in blocks, which are linked by SHA256 hashes.
- ▶ <https://blockchain.info>

# Transaction Confirmation

- ▶ Having a transaction provisionally accepted into a candidate block signals that the network has verified that the inputs were viable
- ▶ Every new block accepted into the chain after the transaction was accepted is considered a confirmation
- ▶ Coins are not considered mature until there have been 6 confirmations (basically an hour assuming a 10 minute block cadence)
- ▶ New Coins created by the mining process are not valid until about 120 confirmations
- ▶ This is to assure that a node with more than 51% of the total hash-power does not pull off fraudulent transactions

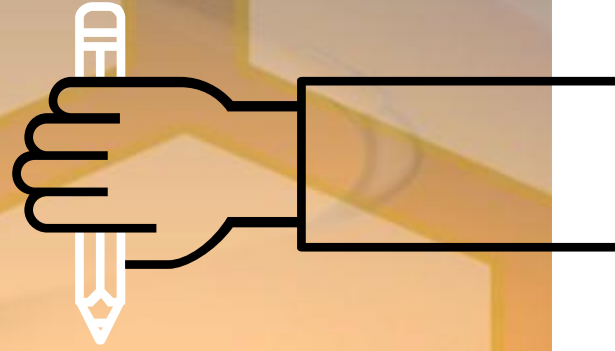


# Proof of Work



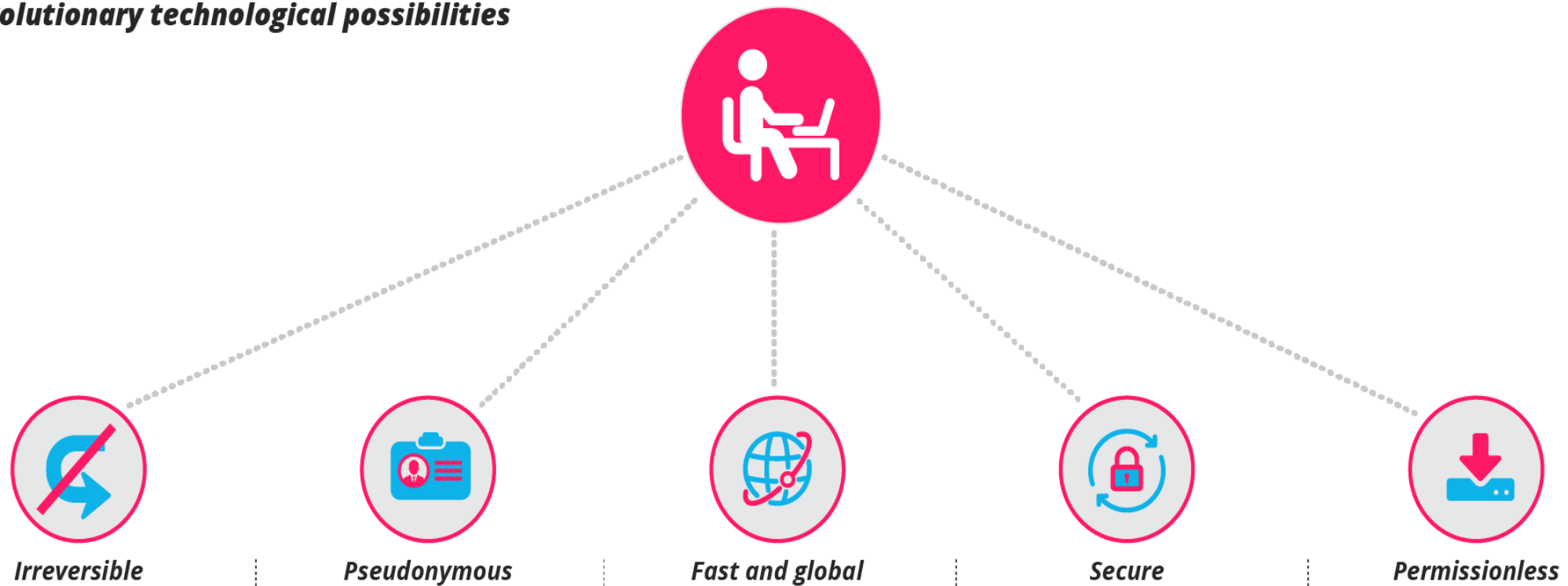


# Transaction Properties



# Transaction properties

***Cryptocurrency opens the door for revolutionary technological possibilities***



Ref: <https://blockgeeks.com/guides/what-is-cryptocurrency>

# Transaction properties

**Irreversible:** After confirmation, a transaction can't be reversed. By nobody. And nobody means nobody. Not you, not your bank, not the president of the United States, not Satoshi, not your miner. Nobody. If you send money, you send it. Period. No one can help you, if you sent your funds to a scammer or if a hacker stole them from your computer. There is no safety net.



# Transaction properties

**Pseudonymous:** Neither transactions nor accounts are connected to real-world identities. You receive Bitcoins on so-called addresses, which are randomly seeming chains of around 30 characters. While it is usually possible to analyze the transaction flow, it is not necessarily possible to connect the real world identity of users with those addresses.



# Transaction properties

**Fast and global:** Transaction are propagated nearly instantly in the network and are confirmed in a couple of minutes. Since they happen in a global network of computers they are completely indifferent of your physical location. It doesn't matter if I send Bitcoin to my neighbor or to someone on the other side of the world.





# Transaction properties

**Secure:** Cryptocurrency funds are locked in a public key cryptography system. Only the owner of the private key can send cryptocurrency. Strong cryptography and the magic of big numbers makes it impossible to break this scheme. A Bitcoin address is more secure than Fort Knox.



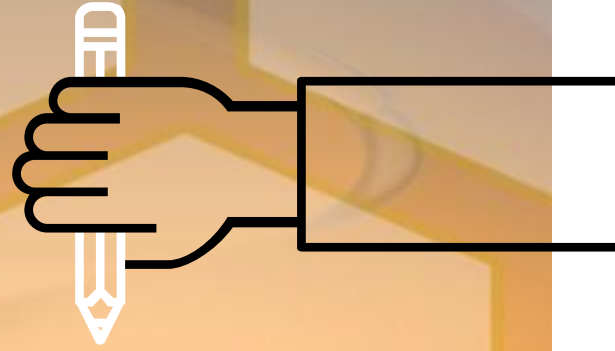


# Transaction properties

**Permissionless:** You don't have to ask anybody to use cryptocurrency. It's just a software that everybody can download for free. After you installed it, you can receive and send Bitcoins or other cryptocurrencies. No one can prevent you. There is no gatekeeper.



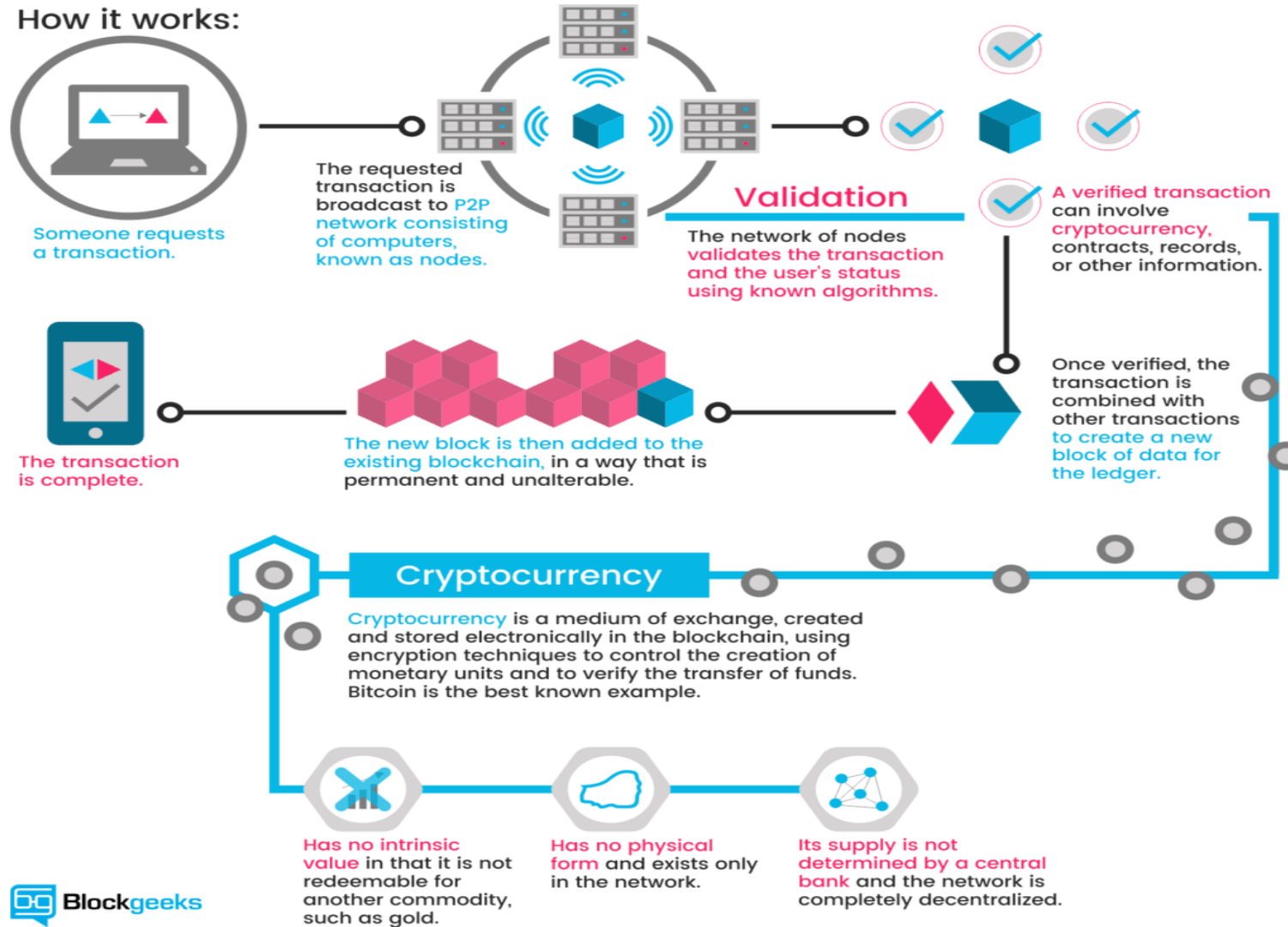
# What is Cryptocurrency?



# What is Cryptocurrency?

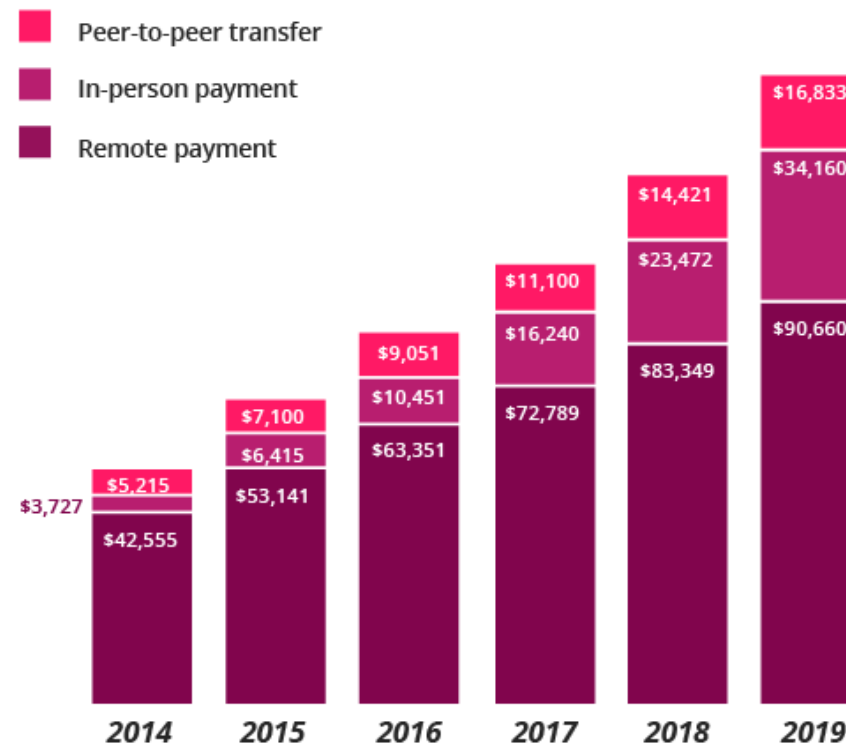
“A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.”

## How it works:



# Cryptocurrencies: Dawn of a new economy

***US mobile payments are expected to hit \$142 billion by 2019***



# Cryptocurrencies: Dawn of a new economy



## ***Peer-to-peer***

"Peer-to-peer" transfer occur when one person pays another person using a mobile device. The device uses either a preloaded app or a browser-based app to initiate, authenticate, and transfer funds



## ***In-person***

"In-person" purchases are initiated using a mobile device where the buyer and seller are in-person, usually at a brick-and-mortar retail location where the product/ service is immediately delivered.



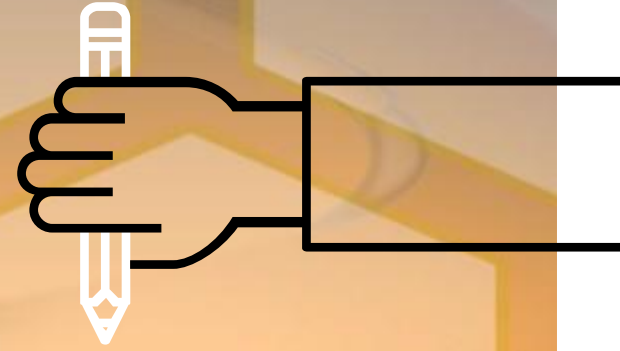
## ***Remote***

"Remote" payments are made when a buyer purchases goods or services using a mobile device, but the buyer is not physically present with the seller and the good are not immediately delivered(as with eCommerce).











*Source: Forrester research, "US mobile payments forecast, 2014 to 2019" November 17, 2014*



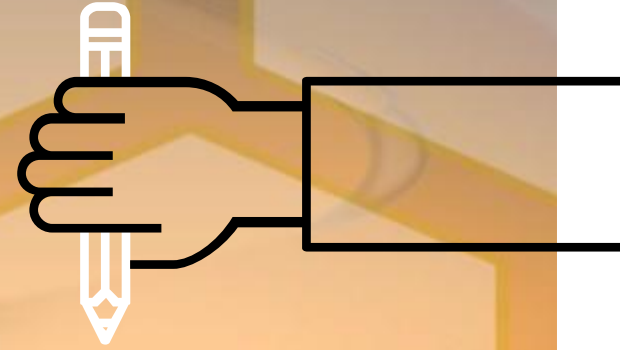
# Cryptocurrencies



# Different cryptocurrencies (updated: 2019/11/05)

1	 Bitcoin BTC	NT\$283,412.04	+1.58%	NT\$5.1T	<a href="#">Trade</a>
2	 Ethereum ETH	NT\$5,616.39	+1.53%	NT\$609.2B	<a href="#">Trade</a>
3	 XRP XRP	NT\$9.08	+2.61%	NT\$393.3B	<a href="#">Trade</a>
4	 Bitcoin Cash BCH	NT\$8,791.09	+0.39%	NT\$159.2B	<a href="#">Trade</a>
5	 Litecoin LTC	NT\$1,868.48	+4.89%	NT\$118.9B	<a href="#">Trade</a>
6	 EOS EOS	NT\$104.44	+5.18%	NT\$98.1B	<a href="#">Trade</a>
7	 Stellar Lumens XLM	NT\$2.4431	+16.53%	NT\$48.8B	<a href="#">Trade</a>
8	 Chainlink LINK	NT\$80.35	+0.15%	NT\$28.1B	<a href="#">Trade</a>
9	 Dash DASH	NT\$2,203.41	+1.75%	NT\$20.1B	<a href="#">Trade</a>
10	 Tezos XTZ	NT\$27.54	+4.59%	NT\$18.2B	<a href="#">Trade</a>

# Applications of Blockchain



# Applications of blockchain

- e-wallet
- Smart contract
- Database system
  - Traceability of agriculture and food supply chain

# Smart Contracts

- Self-automated computer programs that can carry out the terms of any contract
- Mostly based on objective conditions precedent
  - “If, then” criteria



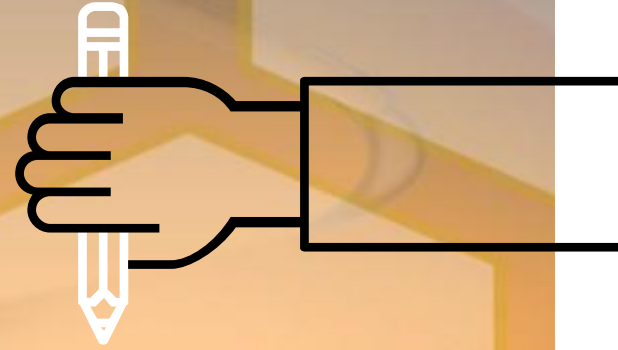
# Smart Contracts (cont.)

- Variables: Readily Verifiable Data
- Oracles: Reliable sources
  - Social Security DMF
  - FAA Records
  - National Weather Service
- Crowdsourcing
  - Voting

# Smart Contracts (cont.)

- Think: Escrow Agreements
  - Money held in escrow until performance is met
  - Once performance is validated, money released
  - Regulated by an unbiased party, which only seeks the objectively “right” answer, devoid of outside influence

# Types of Cryptocurrencies and Uses



# Example of Protocol Tokens



Bitcoin



Ethereum



Litecoin



Bitcoin Cash

# Ethereum.org

*Turing complete contracts on a blockchain.*

- Contracts are the main building blocks of Ethereum.
- A contract is a computer program that lives inside the distributed Ethereum network and has its own ether balance, memory and code.
- Every time you send a transaction to a contract, it executes its code, which can store data, send transactions and interact with other contracts.
- Contracts are maintained by the network, without any central ownership or control.
- Contracts are written in languages instantly familiar to any programmer and powered by Ether, Ethereum's cryptofuel.



# Other Blockchain Applications

- Issuing Stocks and Bonds
- Insurance
- Land Registries
- Supply Chain Integrity

# Consensus Algorithms

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Mixed

# Proof of Work

- Miners check the validity of transactions for a fee
- Wasting lots of energy
- Easier to be controlled by big mining companies
- Anti-ASIC cryptocurrencies

# Proof of Stake

- The idea resembles company shares
- Only those with enough shares can speak in a shareholders' meeting
- The more shares you have, the more influence you have
- To create a block, you need to have some shares. The more the better.



# Coin-Age

- If you possess a coin for 100 days, or you possess 100 coins for a day, you have 100 coin-age.
- More coin-age means more stakes. The one with more stakes is more likely to be selected as the next block creator.
- After a block was created, the possessor's coin-age will be reset to 0.
- There is a limit on the number of days to be counted towards the coin-age.
- Drawback: bad fluidity



# Anti-ASIC Cryptocurrencies

- Evolution of hash algorithms: SHA256 (bitcoin) -> Scrypt (LiteCoin) -> Ethash (Ethereum) -> X11 (Dash) -> X13, X15, X17, X16R...

# Script

- PoW
- It generates lots of pseudorandom data to be computed
- It needs lots of memory
- Used by Litecoin and Dogecoin
- GPU is more efficient in executing Script as compared with CPU
- There is a shortage of strong GPU card towards the end of 2013

# X11

- PoW used in Dash
- Serializing 11 different hash algorithms including
  - BLAKE, Blue Midnight Wish, Grøstl, JH, Keccak, Skein, Luffa, CubeHash, SHAvite-3, SIMD, ECHO (NIST hash competitors)
- Needs lots of memory