Blockchain Security and Its Business Application Cases

國立政治大學 資訊管理學系
Dept. of Management Information Systems
National Chengchi University

蕭舜文 助理教授
Dr. Shun-Wen Hsiao
hsiaom@nccu.edu.tw

2020.10.23

Guest Lecturer: Shun-Wen Hsiao

- **National Chengchi University**
  - Assistant Professor, 2017~
- **Academic Sinica**
  - Postdoctoral Researcher
- **Carnegie-Mellon University**
  - CyLab, Visiting Scholar
- National Taiwan University
  - Bachelor & Doctoral degree @ Information Management

- Research Interests
  - Cybersecurity & Computer Science
    - Computer Networks, Web Security, Cloud Security
    - Cloud Computing, Computer Virtualization
    - Malware, Forensics, Dynamic and Static Analysis
  - Blockchain and Smart Contract
  - Data Science
    - Data Science for FinTech and Cybersecurity Application

https://sites.google.com/view/mikehsiao/

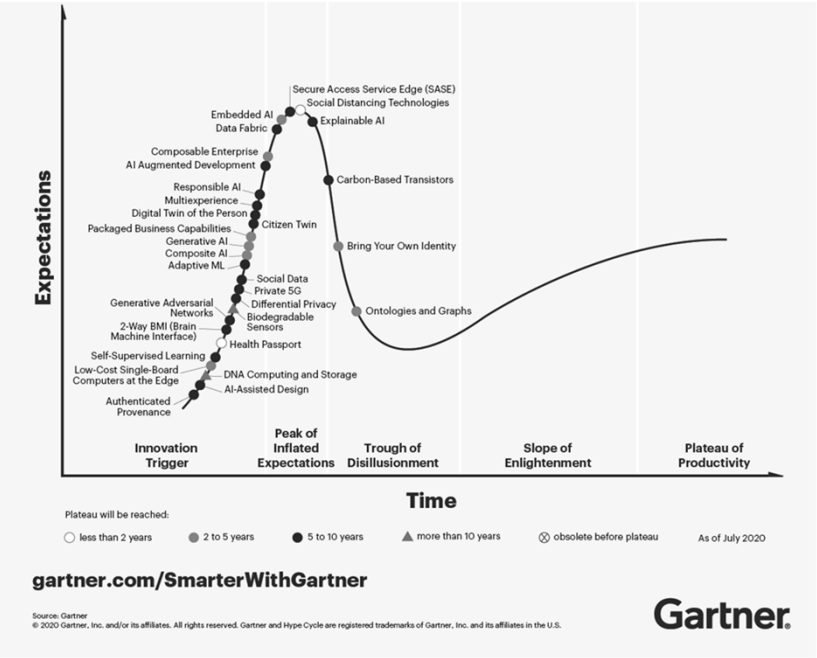
Outline

- **Digital Currency and Blockchain**
  - FinTech, Digital Currency
  - HashCash and Proof-of-Work
  - Distributed Ledger
  - Wallet
  - Blockchain Structure
- **Security and Security Management**
  - What is Security?
  - Risk Assessment
- **Blockchainized Applications and DApp Cases**
  - Smart Contract
  - DApp (Decentralized App)
  - Possible Applications
  - Real-world Cases
  - Adoption or not?

Digital Currency and Blockchain

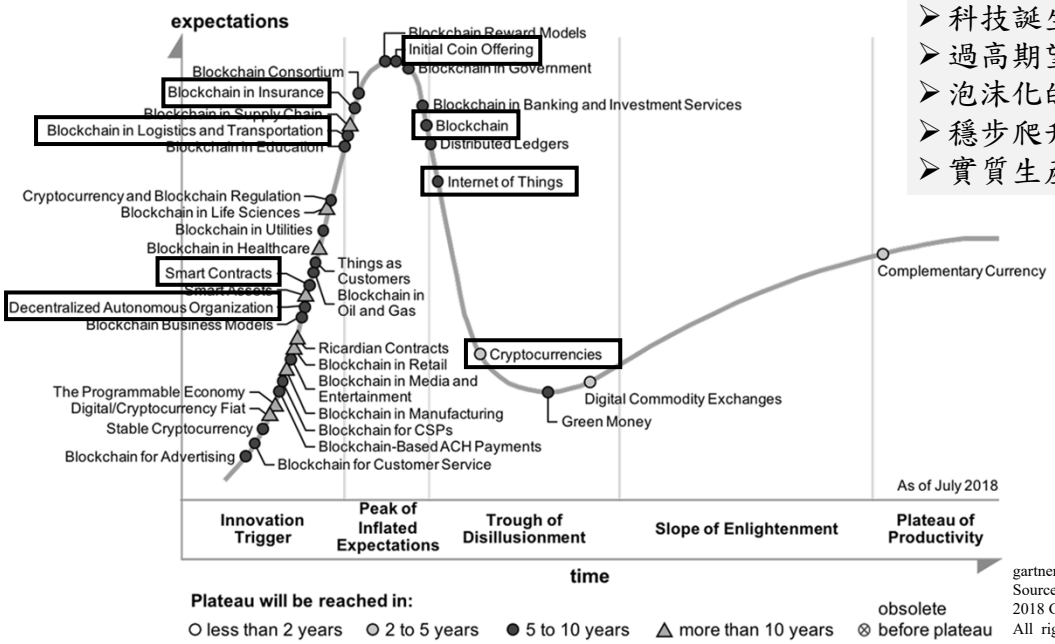
BLOCKCHAIN

Gartner Hype Cycle for Emerging Technologies, 2020



- 科技誕生的促動期
- 過高期望的峰值
- 泡沫化的底谷期
- 穩步爬升的光明期
- 實質生產的高峰期

Gartner Hype Cycle for Blockchain Business, 2018



- 科技誕生的促動期
- 過高期望的峰值
- 泡沫化的底谷期
- 穩步爬升的光明期
- 實質生產的高峰期

gartner.com/SmarterWithGartner
Source: Gartner

Blackchain Security (1/2)

- Is crypto-currency secure?
  - **As a professor, yes.**
    - SHA-256, ECDSA, KECCAK-256, HashCash, Ethash
    - Public blockchain, private key protection, …
  - **As a user, seems not.**
    - Binance security breach results in a loss of $41 million, or 7000 BTC. (May 8, 2019)
    - The DAO, in the first few hours of the attack, 3.6 million ETH were stolen, the equivalent of $70 million at the time. (June 17, 2016)
    - Hackers targeted first-generation exchange Mt. Gox and made off with the equivalent of $460 million dollars in bitcoin. (February, 2014)

https://coiniq.com/cryptocurrency-exchange-hacks/

https://www.crypto51.app/

Blackchain Security (2/2)

智能合約　　證券型代幣

- Is a smart contract or ICO/STO (Initial Coin Offering, Security Token Offering) secure?
  - As a **contract programmer**, absolutely no.
  - As an **investor**, I believe yes.
  - As a **naïve user**, I don't care.
  - As a **government officer**, I don't know, it's not allowed but still working on it.
  - As an **consultant**, probably yes.
  - As a **blockchain-as-service provider**, I want to persuade you yes.
  - As a **database manager**, why don't you use a relational DB?

- An ICO is the cryptocurrency industry's equivalent to an Initial Public Offering (IPO). It acts as a way to raise funds.
- Investors can buy into the offering and receive digital tokens issued by the company. This token may have some utility in using the product or service that the company is offering, or it may just represent a stake in the company or project.

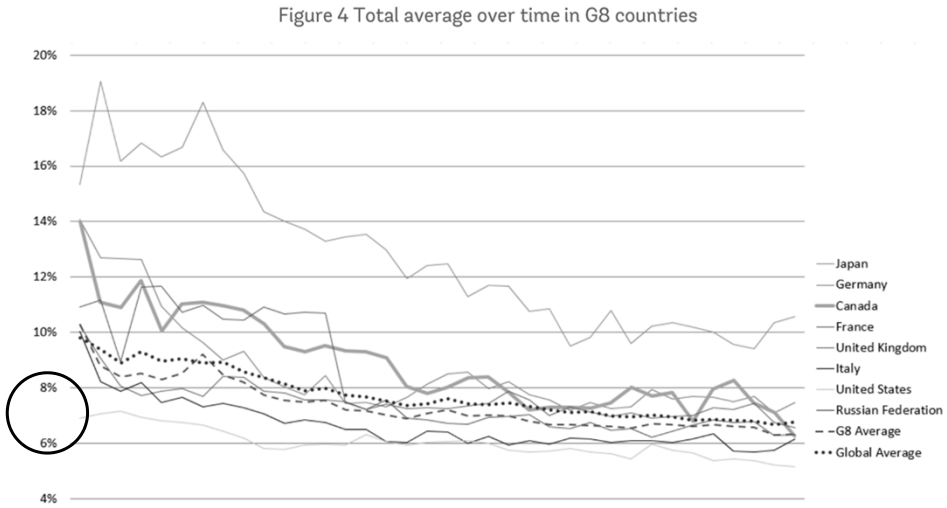
FinTech

- **[Wiki]** Financial technology, also known as FinTech, is an industry composed of companies that use new technology and innovation to leverage available resources in order to compete in the marketplace of traditional financial institutions and intermediaries in the delivery of financial services.
- **[Wharton]** FinTech: an economic industry composed of companies that use technology to make financial systems more efficient.
  - FinTech refers to new applications, processes, products or business models in the financial services industry.

https://en.wikipedia.org/wiki/Financial_technology

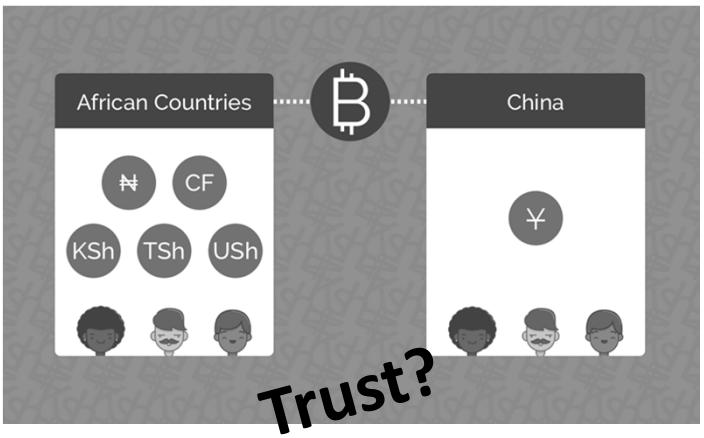
http://www.whartonfintech.org/blog-archive/2016/2/16/what-is-fintech

Why digital currency? Efficiency!



https://remittanceprices.worldbank.org/en September 2020.

bitpesa.co in Kenya



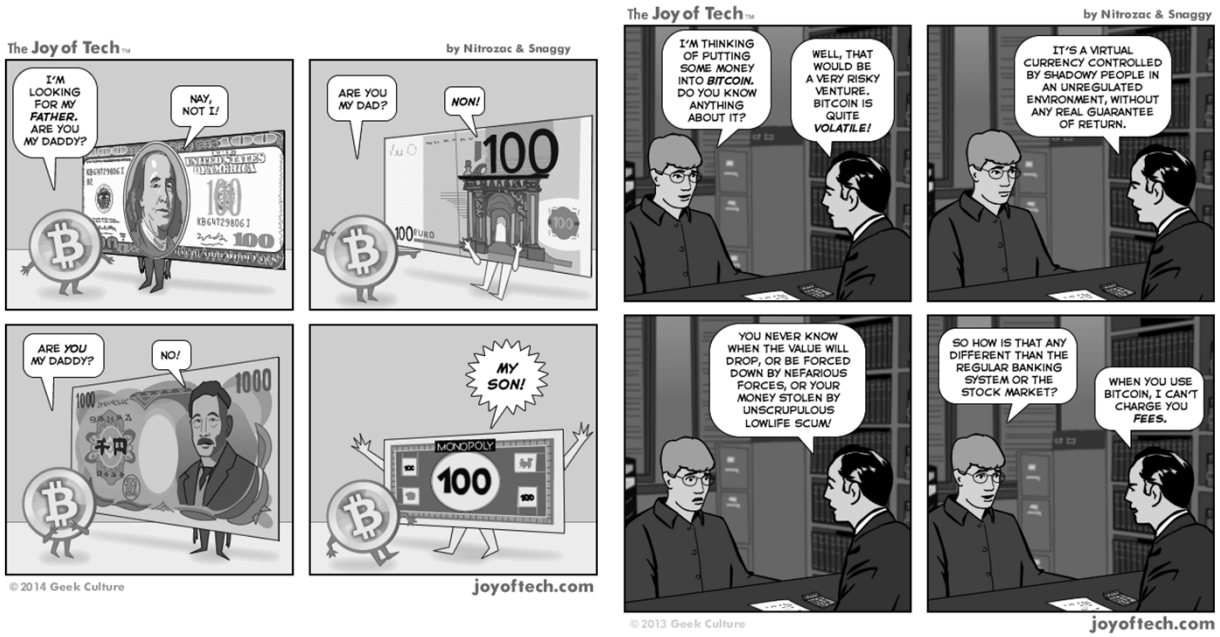
- *"Using BitPesa's digital platform, businesses can now send instant payments in local currency directly from African bank accounts to Chinese bank accounts."*
- *"BitPesa's offers **low-cost, instant payments** from Nigerian Naira and Ugandan Shillings directly into Chinese Yuan."*
- *"Businesses can now make **easy** payments for employees, distributors, or suppliers without using cash or the US dollar as a **middle** currency."*

https://www.bitpesa.co/blog/connecting-payments-with-africa-and-china/

Digital Currency

- **[Wiki] Digital currency** can be defined as an Internet-based form of currency or medium of exchange distinct from physical (such as banknotes and coins) that exhibits properties similar to physical currencies but allows for instantaneous transactions and borderless transfer-of-ownership.

https://en.wikipedia.org/wiki/Digital_currency



Crypto-Currency Market Capitalizations

#	Name	Price	24h	7d	Market Cap	Volume	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$11,354.08	0.11%	6.19%	$210,217,931,851	$21,015,482,967 1,850,919 BTC	18,514,750 BTC	
2	Ethereum ETH	$373.38	0.33%	6.08%	$42,181,811,825	$12,318,908,816 32,992,850 ETH	112,972,521 ETH	
3	Tether USDT	$1.00	0.02%	0.09%	$15,735,725,784	$37,548,060,245 37,514,041,132 USDT	15,721,468,977 USDT	
4	XRP XRP	$0.253132	1.05%	2.13%	$11,432,068,451	$1,919,904,140 7,584,584,843 XRP	45,162,407,484 XRP	
5	Bitcoin Cash BCH	$239.38	0.48%	8.47%	$4,438,673,551	$1,757,086,839 7,340,162 BCH	18,542,388 BCH	
6	Binance Coin BNB	$30.22	7.23%	5.17%	$4,364,591,719	$592,692,251 19,609,772 BNB	144,406,561 BNB	
7	Chainlink LINK	$11.14	6.31%	18.42%	$3,898,420,958	$1,562,509,807 140,282,037 LINK	350,000,000 LINK	
8	Polkadot DOT	$4.34	2.4%	3.96%	$3,700,431,965	$410,942,947 94,688,827 DOT	852,647,705 DOT	

https://coinmarketcap.com @ 2020/10/12. The global crypto market cap is $360.74 B.

Digital Currencies Before Bitcoin

- Two fundamental questions for anyone accepting digital money are:
  - Can I trust the money is authentic and not counterfeit?
  - Can I be sure that no one else can claim that this money belongs to them and not me? (aka the "double-spend" problem)
- Paper money
  - Counterfeit: sophisticated papers and printing technology
  - Double-spend: the same paper note cannot be in two places at once
- Digital money
  - Counterfeit: cryptography (digital signature)
  - Double-spend: blockchain (proof-of-work)

Intrinsic Value

- The value of fiat money (法幣) is that the owners believe that the money has certain buying power in the future. Note that the banknote itself is a piece of paper, and it has no value.
- Question: why USD has buying power?

➢ Question: what is valuable in the digital world?

Hashcash

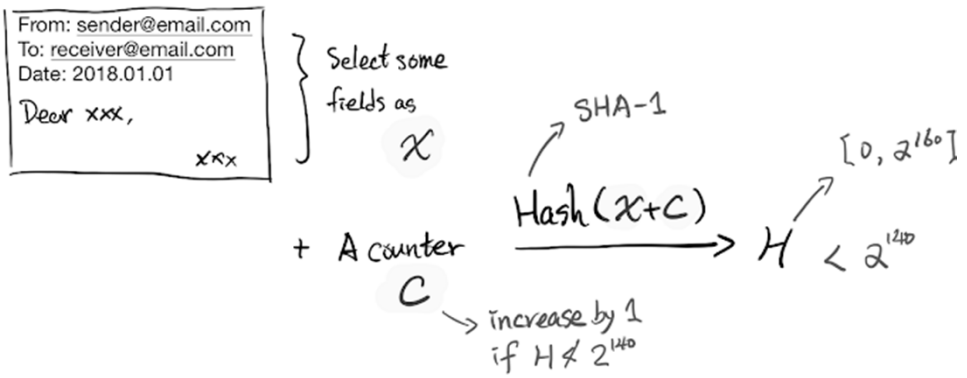
- Computing power is valuable resource, and it should not be wasted.
- If I can prove that I already consume certain amount of my computation power in order to do something next, then you should pay more attention to what I say. But how can I prove that?
- **[Wiki] Hashcash** is a proof-of-work system used to limit email spam and denial-of-service attacks.
  - Email sender performs a small amount of computational work (proof-of-work) and attach the proof in each email.
  - For spammers, the aggregated work is expensive.

http://wp.xin.at/archives/tag/hashcash

Hashcash (cont'd)

- What is hash function? y = Hash(x)
  - x is an any digitized input, such as number, text, sound, image.
  - A hash function has a fixed-length output value.
    - E.g., [0, 2^256-1].
  - A hash function is irreversible.
    - I.e., it is easy to calculate y from x, but it is impossible to calculate y from x.
    - E.g., y = x mod 10
    - The only way to find x from y is brute-force trial.
  - A hash function is deterministic and public-available.

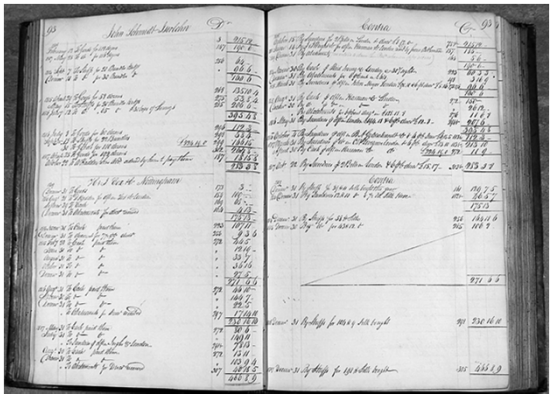
Hashcash (cont'd)



What is blockchain?

Blockchain is not the database that you think about.

- A blockchain — originally, block chain —is a distributed database that maintains a continuously-growing list of data records hardened against tampering and revision.
- Blockchains are "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.



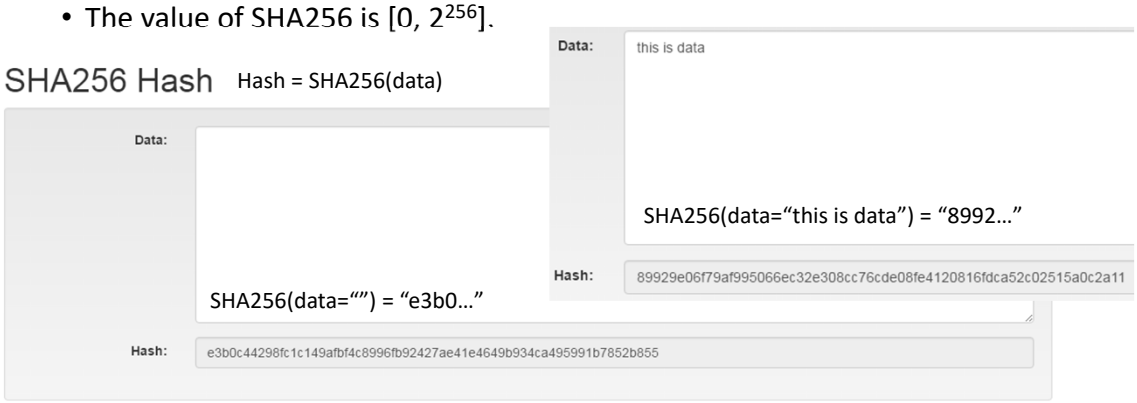
Blockchain Demo

- https://andersbrownworth.com/blockchain/

- Hash
- Block
- Blockchain
- Distributed
- Tokens
- Coinbase

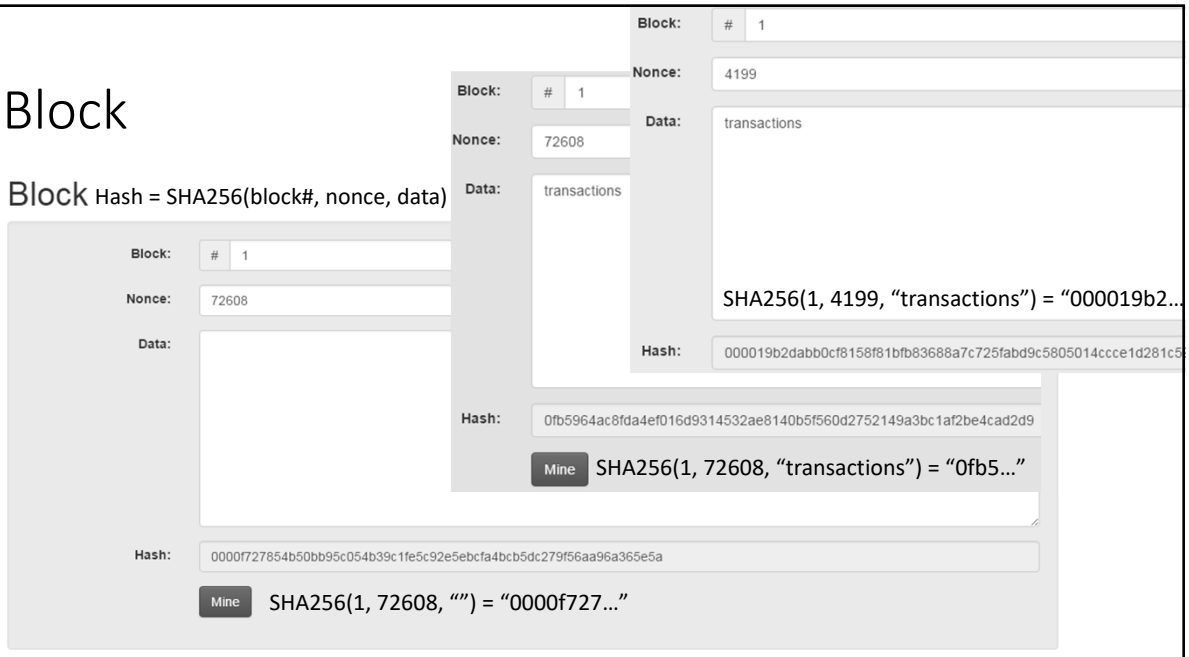
Hash: digital fingerprint

- Properties: determinism, uniformity, defined range, non-invertible.
  - The value of SHA256 is $[0, 2^{256}]$.



Block

Block Hash = SHA256(block#, nonce, data)



A valid (signed) block must has a hash value below a target value.

Uniformity

Hash = SHA256(block#, nonce, data)

Nonce	Hash
0	baa53f13fd719bd4783df3f5a701307fe07f58f0429b7cf354df675574155700
1	ed1aa5ac024adacc4c24dc36e5cd80686e98182cd243ca2c88da045879c73c0a
2	78b9a7ce2aa42804d0467928ced9379c1d46e0be90c682cc964239ec6ea4376a
3	c2a14d5560965309561694b612cd20eba80680512aae807a450f6a81ba51a6f5
4	1c36ff1639ea413d1f0dfffab93ee30ac150c86f95c6d3b838691f0655c3e8e6
5	226dbc8b98fc30c11b54396eee60706ff00114b20eade097c83bd43fe19b9dc1
6	40f27b239f0e2318c38cc0e658d58b318e318723656e4a6e1236c830725e6367
7	562574f76f44baa039b0146ac1ddfea791ad4197d31c78bb5f30132bf4bc9216
8	df143a97d757d582060362247c92f11cec1063a213059d01cbed4b2eedc8c49d
9	585971d555cafcd1746f1d22b2dc35c6409f7b3d6cec3f0d929bc0552c1c2ff4
⋮	

Nonce	Hash
4194	fe090988c2a7222829c0a43e35e4a4c324529dd3a55bdaf21f4664313da5420c
4195	52c385a291350a2a7972869a8363438900ee592980d30994de5373486ada6201
4196	9a2509ec716a31b40d931834fe26dc6eaec1feb433930f91630b1990abf08a35
4197	54d573689aa78f34cf0bfe3f1298c6b6217aefc3284b3e79fe536a8924a0e2b5
4198	34b2dcffea74ecb4778db49ccba4235a7be8b06d6af6a5e642de82950f685c3a
4199	**000019b2dabb0cf8158f81bfb83688a7c725fabd9c5805014ccce1d281c59333**
4200	06eddd5bf4748ac7205ec6acd16a4dd75dc34a9657e2246d71c9b37fe3d9d93d
4201	5042fb839757a7f6fd11f82b263978185e0280607dd6fa01823c32ea45baa4ab
4202	e31220f70538a429a939da8aede308452f8d32b7d2b3671e5b708c062107cc22
4203	5e7d84f9b7220cf064670141112297edf4f1a97ee7ed7fcb904079caf21260ee
⋮	

Block (cont'd) Hash = SHA256(block#, nonce, data)

- A valid (signed) block
  - A valid block must has a hash value below a target value, e.g., leading 32 bits are zero.
  - Since you cannot change block index and data, you can create a valid block by only selecting a nonce value in [0, 2^{32}]. The process is called "mining".
  - Because of "uniformity", mining is a mathematic lottery.
  - Easy to verify; difficult to mine.

https://en.bitcoin.it/wiki/Difficulty

Sudoku

- Sudoku can be viewed as a mathematical problem that is difficult to find its solution.
- It is easy to verify the correctness of a solution independently.
- The difficulty of a sudoku problem can be adjusted easily.
- Proof of Work (PoW): if a solution is found, he/she must perform some computational works.

		3	9			7	6	
	4				6			9
6		7		1				4
2			6	7			9	
		4	3		5	6		
	1			4	9			7
7				9		2		1
3			2				4	
	2	9			8	5		

Genesis Block

- A genesis block is the first block of a block chain.
  - Modern versions of Bitcoin assign it block number 0, though older versions gave it to number 1.
- The genesis block is almost always hardcoded into the software.
- It is a special case in that it does not reference a previous block.
- This block contains the dated title of a Times article.


THE TIMES

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salman Rushdie I won't marry again

Giant killing? Guide to the FA Cup third round

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

https://en.bitcoin.it/wiki/Genesis_block

Block #0

Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799 (0x1d00ffff)
Size	0.285 KB
Version	1
Nonce	2083236893
Block Reward	50 BTC

Hashes	
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	0000000000000000000000000000000000000000000000000000000000000000
Next Block(s)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Network Propagation

g.co/staticmaperror/key

https://www.blockchain.com/btc/block/0

Transactions

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b			2009-01-03 18:15:05
No Inputs (Newly Generated Coins)	→	1A1zP1eP5QGefi2... (Genesis of Bitcoin)	50 BTC

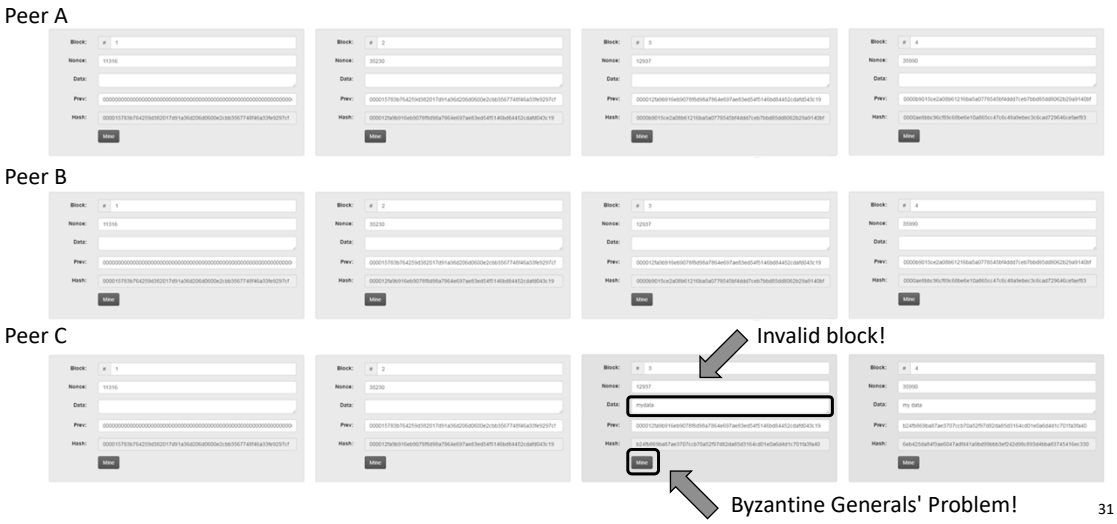
Blockchain

Hash = SHA256(block#, nonce, data, prev)

Chain Reaction

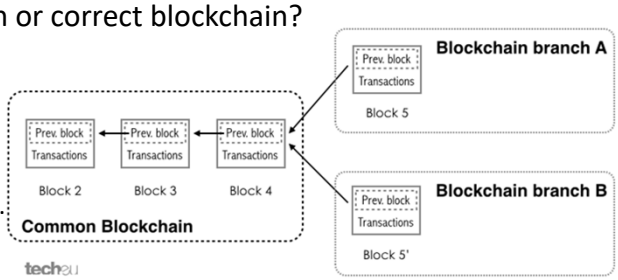
- If you change/mutate the data in a block, you have to re-mine all the following blocks to keep all blocks valid.
- The more blocks that go by, the harder and harder it is to make a change to the past data. That is how a blockchain resists mutation and change.
- Question: How do you know your blockchain is re-mined?

Distributed Blockchain



Distributed Blockchain

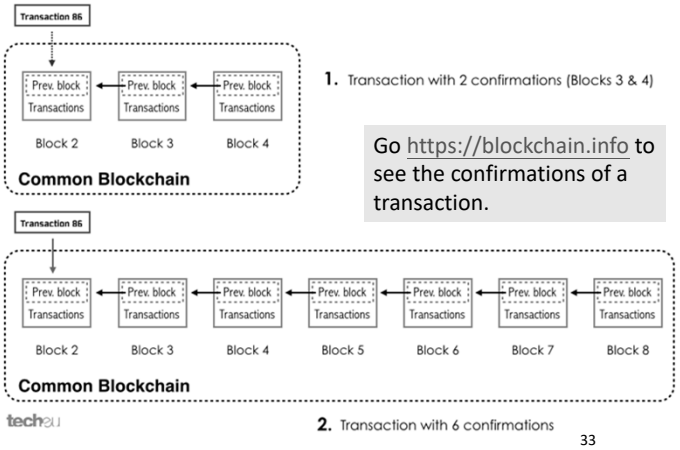
- Two consensus problems caused by the distributed blockchain
  - Who has the right to append next (his/her) block to the current blockchain?
    - The one who finds next valid block (i.e., nonce) and sends it to the P2P network.
    - Remember that mining is a mathematic lottery. Anyone can win the lottery.
  - Who's blockchain is the current, main or correct blockchain?
    - Block-level: every peer can quickly examine the validation of a block. Invalid block will be ignored by peer.
    - Chain-level: What if we have two block winners? Peers keep working on the next block(s), and the longer chain wins.
    - Miners working on the shorter one will get prompted to cease any work and switch to the longer branch.



http://tech.eu/features/926/bitcoin-ecosystem/

Confirmations

- Each time a new block is added to the blockchain after this one, the confirmation count grows.
- Since the blockchain might have a fork. If we accept a transaction before waiting for at least six confirmations, it might happen the network drops that branch.
  - It expose us to a fraud situation or double spending.
- Why six confirmations?
  - Because generating an alternate Blockchain branch bigger and faster than the rest of the network would require vast amounts of computational power.

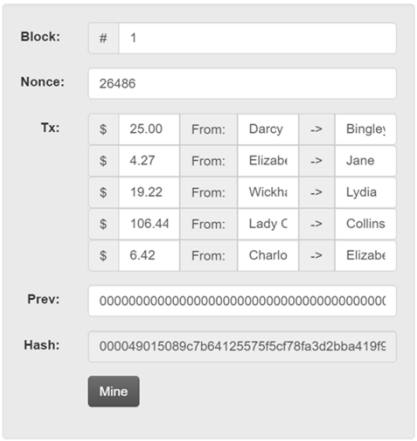


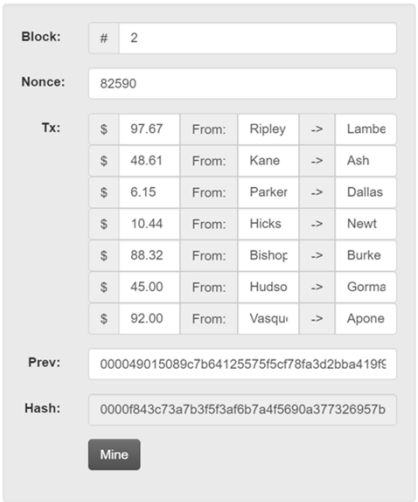
Go https://blockchain.info to see the confirmations of a transaction.

Transactions (over-simplified)

Hash = SHA256(block#, nonce, tx, prev)

- [**Wiki**] A Bitcoin transaction is a transfer of Bitcoin value that is broadcast to the network and it is collected into blocks by miners.
- For Bitcoin, it lists transactions in the block; not account balances.

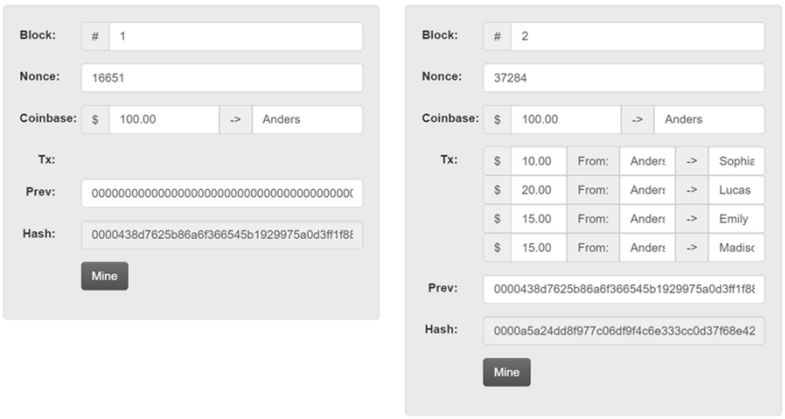




Coinbase

Hash = SHA256(block#, nonce, coinbase, tx, prev)

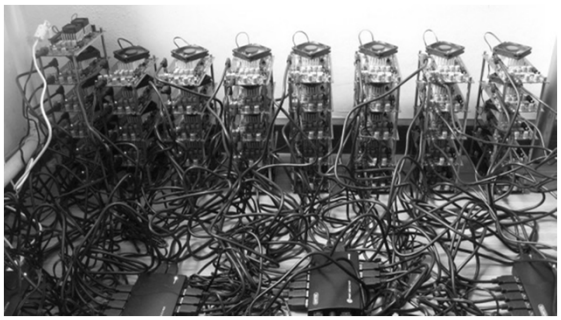
- A special tx.
- No 'from*'.
- Usually 'to' the account of the miner.
- Create new coins from nothing to the miner.
- Now it looks like a ledger.
- Note: still no balance!



The coinbase can contain any arbitrary data. See Genesis Block.

Miners

- Need computational infrastructure to obtain high hash per second.
- CPU -> GPU -> FPGA (Field-Programmable Gate Array) ->ASIC (Application-Specific Integrated Circuit)
- Mining efficiency
  - Mhash/s = millions hashes per second
  - Mhash/J = millions hashes per joule (J)
  - W (watt) = 1 J/s
- Google "bitcoin mining profit".



https://en.bitcoin.it/wiki/List_of_Bitcoin_mining_ASICs

Global Bitcoin Nodes Distribution

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Mon Oct 19 2020 23:52:50 GMT+0800 (台北標準時間).

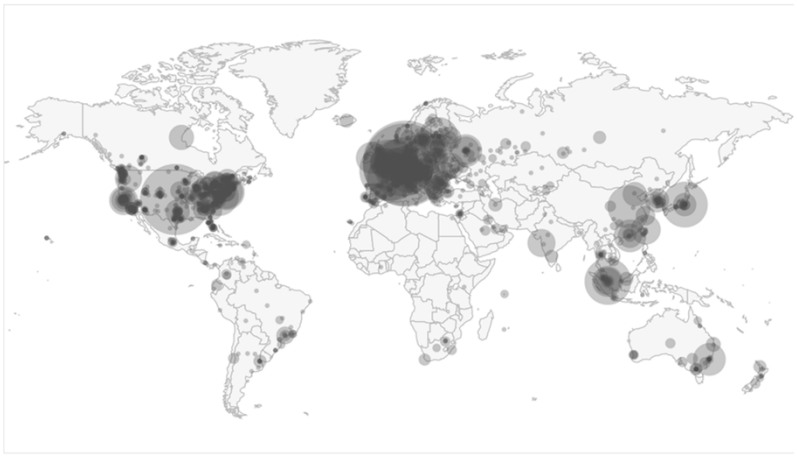
10756 NODES

24-hour charts »

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

RANK	COUNTRY	NODES
1	n/a	2726 (25.34%)
2	Germany	1842 (17.13%)
3	United States	1818 (16.90%)
4	France	566 (5.26%)
5	Netherlands	428 (3.98%)
6	Canada	294 (2.73%)
7	United Kingdom	284 (2.64%)
8	Singapore	261 (2.43%)
9	Russian Federation	221 (2.05%)
10	Japan	215 (2.00%)

More (99) »



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

LIVE MAP

https://bitnodes.io/@ 2020/10/20

Blockchain Charts

- https://www.blockchain.com/charts

The total number of mined bitcoin that are currently circulating on the network.

The average USD market price across major bitcoin exchanges.

The total USD value of bitcoin in circulation.

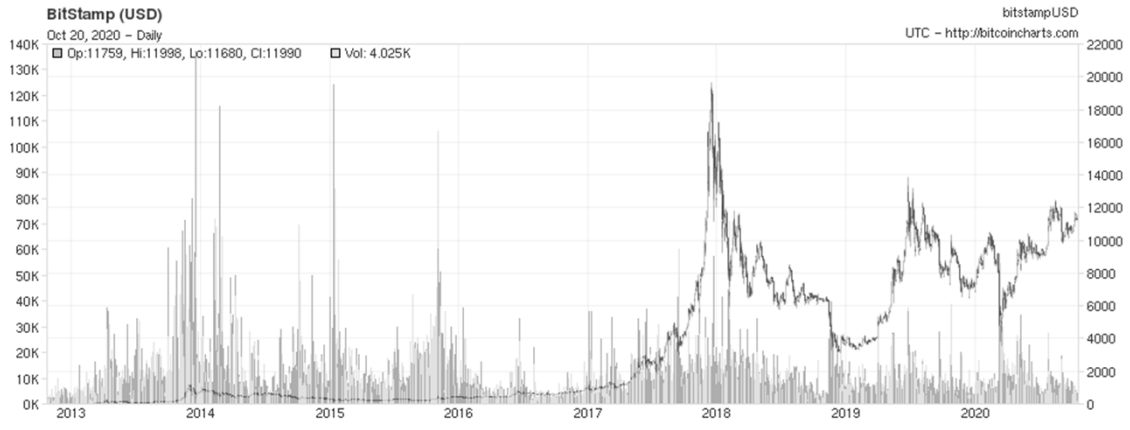
The total USD value of trading volume on major bitcoin exchanges.

Bitcoin's protocol halves the rate at which new bitcoin are created every 4 years, and limits the total number of bitcoin that will be created to a fixed total just below 21 million coins (approximately by the year 2140).

Bitcoin

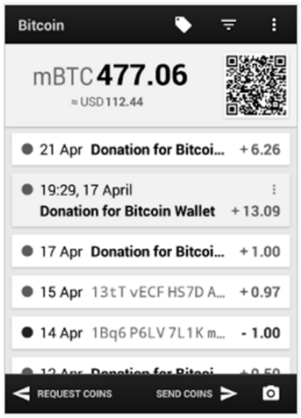
- Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network.
- Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part.
- Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
  - The key innovation was to use a distributed computation system (called a "Proof-of-Work" algorithm) to conduct a global "election" every 10 minutes, allowing the de-centralized network to arrive at consensus about the state of transactions.
  - This elegantly solves the issue of double-spend.

Bitcoin Market



https://bitcoincharts.com

Bitcoin Client (Wallet): Android

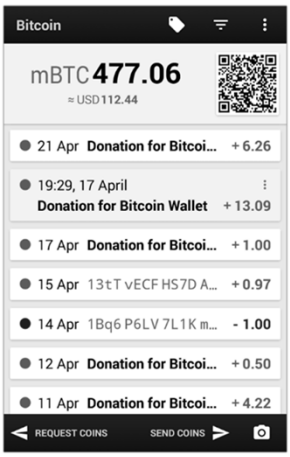


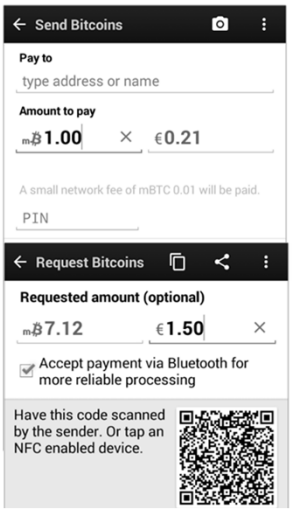
- No registration, web service or cloud needed!
- This wallet is de-centralized and peer to peer.
- Sending and receiving of Bitcoin via NFC, QR-codes or Bitcoin URLs.
- Address book for regularly used Bitcoin addresses.
- When you're offline, you can still pay via Bluetooth.
- Sweeping of paper wallets (e.g., those used for cold storage).
- App widget for Bitcoin balance.

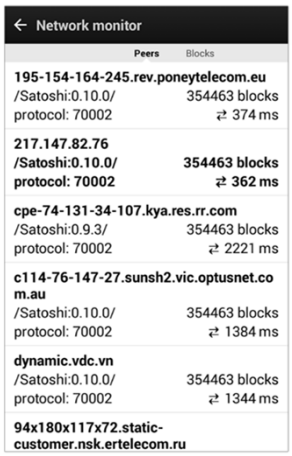
- Bitcoin Wallet is **open source** and **free software**.

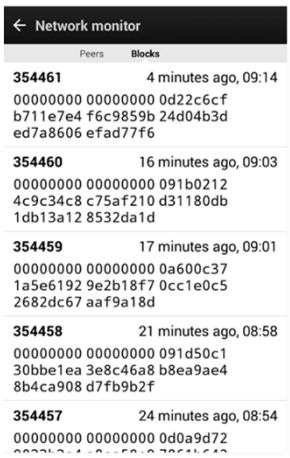
https://play.google.com/store/apps/details?id=de.schildbach.wallet

Bitcoin Client (cont'd)

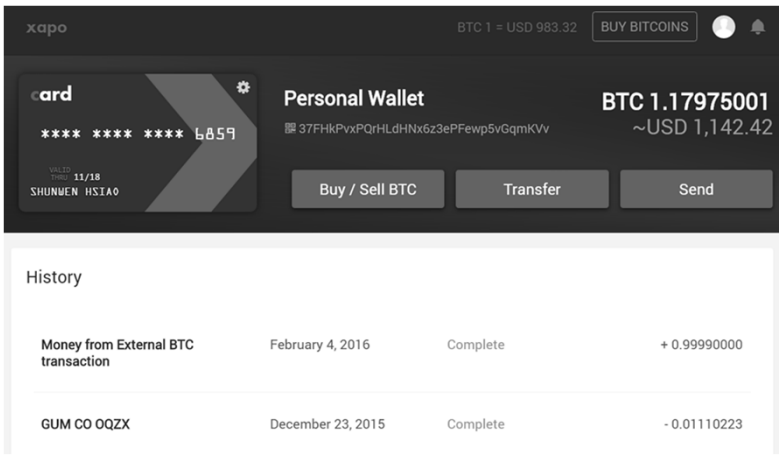








Bitcoin Client: web-based



Note: It is very high-risk choice to use web-based wallet,
since you have no idea how the Cryptocurrency Exchange protect your cryptography parameters.

Bitcoin Transaction

- Transactions are like lines in a double-entry bookkeeping ledger.
- Each transaction contains one or more "inputs", which are debits against a bitcoin account.
- On the other side of the transaction, there are one or more "outputs", which are credits added to a bitcoin account.
- The inputs and outputs (debits and credits) do **not** necessarily add up to the same amount.
  - Instead, outputs add up to slightly less than inputs and the difference represents an implied "transaction fee", a small payment collected by the miner who includes the transaction in the ledger.

Transaction as Double-Entry Bookkeeping

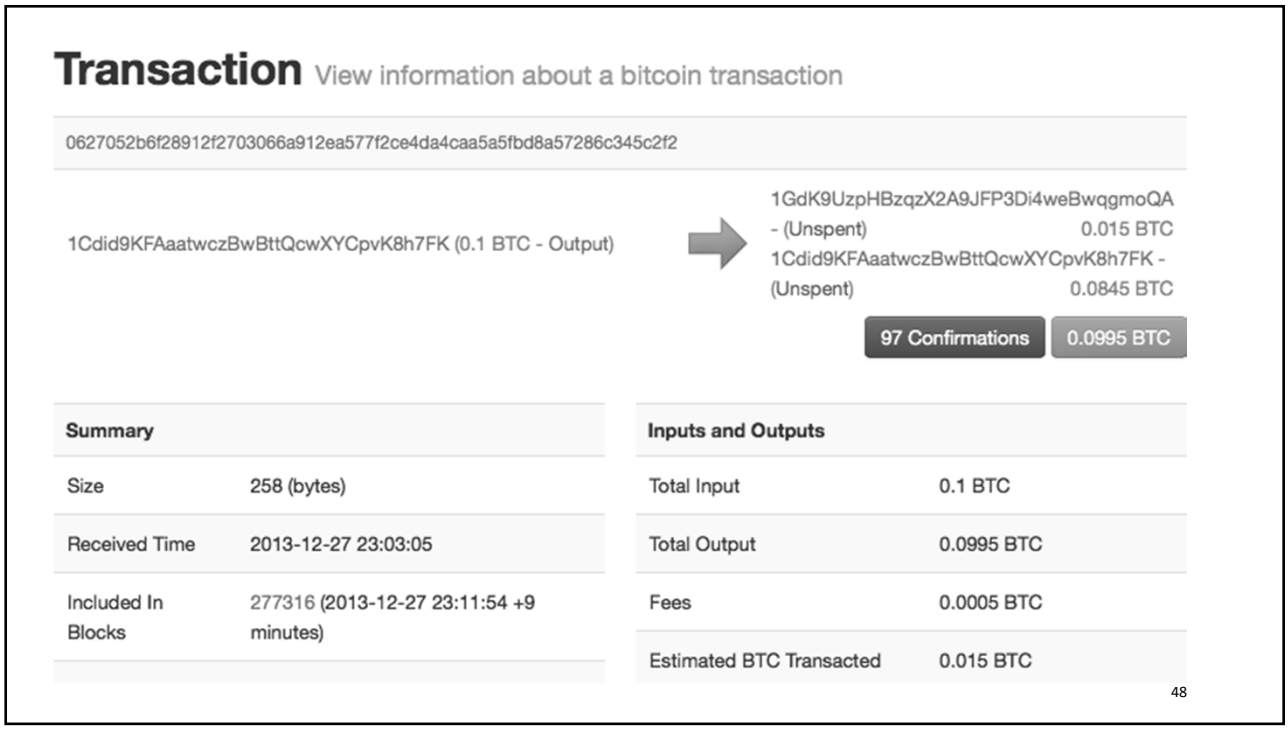
Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

Transaction!
Not block!


Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18
INPUTS From
From (previous transactions Joe has received):
Joe 0.1005 BTC
OUTPUTS To
Output #0 Alice's Address 0.1000 BTC (spent)
Transaction Fees: 0.0005 BTC
Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
INPUTS From
7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0
Alice 0.1000 BTC
OUTPUTS To
Output #0 Bob's Address 0.0150 BTC (spent)
Output #1 Alice's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC
Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4
INPUTS From
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0
Bob 0.0150 BTC
OUTPUTS To
Output #0 Gopesh's Address 0.0100 BTC (unspent)
Output #1 Bob"s Address (change) 0.0045 BTC (unspent)
Transaction Fees: 0.0005 BTC

47

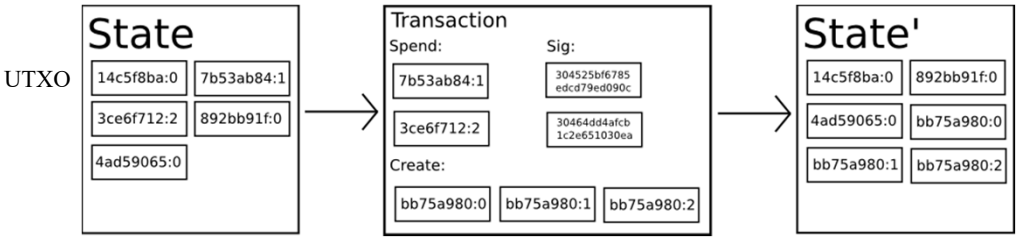

Transaction View information about a bitcoin transaction
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)
1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (Unspent) 0.015 BTC
1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (Unspent) 0.0845 BTC
97 Confirmations
0.0995 BTC
Summary
Size 258 (bytes)
Received Time 2013-12-27 23:03:05
Included In Blocks 277316 (2013-12-27 23:11:54 +9 minutes)
Inputs and Outputs
Total Input 0.1 BTC
Total Output 0.0995 BTC
Fees 0.0005 BTC
Estimated BTC Transacted 0.015 BTC

48

Bitcoin as a State Transition System

The "state" in Bitcoin is the collection of all coins that have been mined and not yet spent (technically, "unspent transaction outputs" or UTXO).

- The ledger of Bitcoin can be thought of as a state transition system, where there is a "state" consisting of the ownership status of bitcoins and a "state transition function" that takes a state and a transaction and outputs a new state which is the result.



https://github.com/ethereum/wiki/wiki/White-Paper

Bitcoin Transaction Structure

- The real message syntax stored in the "Data" field in a Bitcoin block.

- Bitcoin Developer Reference Working Paper
  - Last changes: 30th July 2016
  - Krzysztof Okupski
  - Technische Universiteit Eindhoven, The Netherlands
  - k.s.okupski@student.tue.nl

Field name		Type (Size)	Description
nVersion		int (4 bytes)	Transaction format version (currently 1).
#vin		VarInt (1-9 bytes)	Number of transaction input entries in *vin*.
vin[]	hash	uint256 (32 bytes)	Double-SHA256 hash of a past transaction.
	n	uint (4 bytes)	Index of a transaction output within the transaction specified by *hash*.
	scriptSigLen	VarInt (1-9 bytes)	Length of *scriptSig* field in bytes.
	scriptSig	CScript (Variable)	Script to satisfy spending condition of the transaction output (*hash*,*n*).
	nSequence	uint (4 bytes)	Transaction input sequence number.
#vout		VarInt (1-9 bytes)	Number of transaction output entries in *vout*.
vout[]	nValue	int64_t (8 bytes)	Amount of 10^{-8} BTC.
	scriptPubkeyLen	VarInt (1-9 bytes)	Length of *scriptPubkey* field in bytes.
	scriptPubkey	CScript (Variable)	Script specifying conditions under which the transaction output can be claimed.
nLockTime		unsigned int (4 bytes)	Timestamp past which transactions can be replaced before inclusion in block.

Table 3.2. Regular Transaction Structure

Blockchain Network Structure

Real-world Problem/Adoption

Security and Security Management

Security 《周易》〈繫辭上〉：「形而上者謂之道，形而下者謂之器。」

- Safety
  - Metaphysical (形而上的) goals/objectives
  - CIA: Confidentiality, Integrity, Availability
- Security
  - (形而下的) Tangible security control/action
  - AAA: Authentication, Authorization, Accounting
- Assurance
  - A guaranteed safeguard
  - MAT: Monitoring, Auditing, Testing

Risk Assessment

- Risk
  - Probability
  - Impact
- (Reasonable) Cost
- Value of Security
  - Security management validates that appropriates policy/procedure/standard are implemented to ensure business are conducted within an accepted level of risk.

Risk Matrix

Hazard Severity	Likelihood of Occurrence: Very Unlikely (Little or no chance of occurrence)	Unlikely (A rare combination of factors would be required for an incident to result)	Possible (Not certain to happen but an additional factor may result in an accident)	Probable (More likely to occur than not)
Minor (No or minor injury (first aid))	CARE	CARE	CARE	CAUTION
Moderate (Off-site medical treatment or DAFW*)	CARE	CARE	CAUTION	ALERT
Serious (More than one DAFW, long-term absence)	CARE	CAUTION	ALERT	STOP!
Major (Permanent disability or harm, fatality)	CAUTION	ALERT	STOP!	STOP!

*DAFW – Day Away From Work

CARE	Minor harm possible, serious harm very unlikely to occur; implement controls and ensure care is taken when performing activity.
CAUTION	Minor harm probable, major harm unlikely to occur; follow all control measures, increased level of competence required and ongoing self-assessment of risks identified.
ALERT	Moderate degree of harm probable but major harm unlikely; critically assess the risks and appropriate controls. Specific competence required and ongoing assessment of risks by individual and/or supervisor.
STOP!	Serious or major harm will probably occur; stop the activity and critically assess the risks, review safety aspects of activity and implement further, appropriate controls. Consider referencing HSE or other Best Practice, consider involving HSS.

https://www.dur.ac.uk/computer.science/current/healthandsafety/riskassess/raform/genriskassess/

Questions

- Can blockchain help to improve the security level of my application or service?
  - Immutable database, transparency, distributed system, …
  - However?
- Does blockchain introduce any additional security holes to my application or service?
  - 51% attack, programming flaws, cyber-physical system, …
  - Because …

Blockchainized Application and Decentralized App (DApp)

Smart Contract

- A **smart contract** is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions, minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. (Nick Szabo)
  - Satoshi Nakamoto did not mention anything about smart contract in his bitcoin paper.
- Blockchain makes it possible to be implemented.

一個智能合約就是能夠執行合約條款的電腦化交易協定。
設計智能合約的目的是：滿足合約條款、不出現意外的情形，無論是惡意的還是意外的；不需要信任的中間方。

Ethereum

Ethereum pronunciation
https://www.youtube.com/watch?v=n7c6DHnV_8U

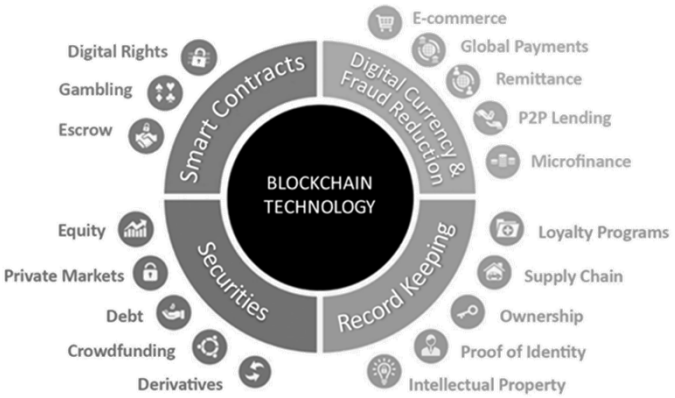
- Ethereum is a programmable blockchain.
  - It can store codes, variables and executions on the blockchain.
- It is a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts (i.e., codes) where they can create their own arbitrary rules for ownership, transaction formats and state transition functions.
- It serves as a platform for many different types of decentralized blockchain applications, including but not limited to cryptocurrencies.
- Decentralized consensus gives Ethereum extreme levels of fault tolerance, ensures zero downtime, and makes data stored on the blockchain forever unchangeable and censorship-resistant.

Contract

- Note that "contracts" in Ethereum should **not** be seen as something that should be "fulfilled" or "complied with".
- Rather, they are more like "autonomous agents" that live inside of the Ethereum execution environment.
- It always executing a specific piece of code when "poked" by a transaction sent by the user wallet.
- Contracts have direct control over their own wallet and their own key/value store to keep track of persistent variables.

Blockchain Applications

- Data
  - Document, game records, digital rights management
- Finance
  - Payment, clearance, security, insurance
- Supply Chain
  - IoT, traceable agricultural products, logistics, anti-counterfeiting
- Government
  - Certificate, registration, IP

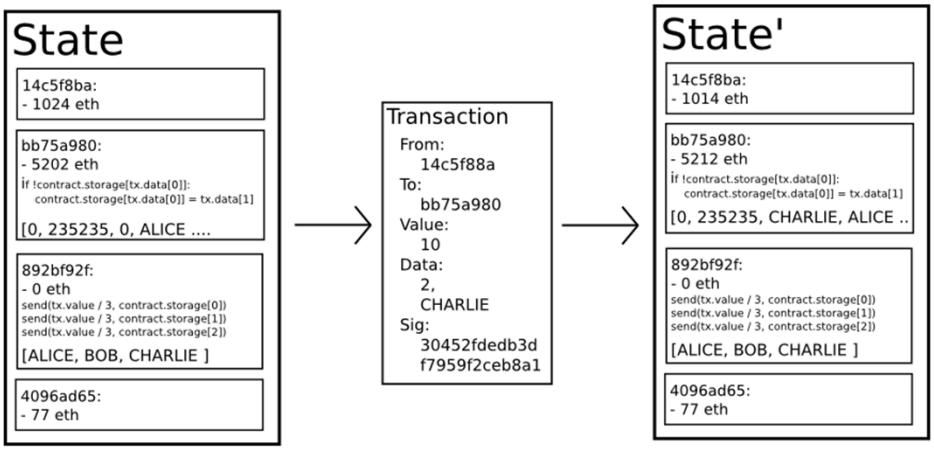


https://www.aciworldwide.com/insights/expert-view/2017/march/blockchain-for-retailers-producing-real-business-benefits

Benefit of Blockchain-Driven FinTech

- Simplified process
- Regulation
- Lower risk
- Improved transaction transparency
- Reduced intermediation costs
- Low transaction time
- Improve efficiency (Liquidity)
- Minimize fraud

Smart Contract as a State Transition System



Ethereum Accounts

- The Ethereum blockchain tracks the state of every account, and all state transitions on the Ethereum blockchain are transfers of value and information between accounts.
- An Ethereum account contains four fields
  - The **nonce**, a counter used to make sure each transaction can only be processed once
  - The account's current **ether balance**
  - The account's **contract code**, if present
  - The account's **storage** (empty by default)
- "Ether" is the main internal crypto-fuel of Ethereum, and is used to pay transaction fees.

Two types of accounts

- **Externally Owned Accounts** (EOAs) -> “account”
  - controlled by private keys
  - Has no code
  - one can send messages from an externally owned account by creating and signing a transaction
- **Contract Accounts** -> “contract”
  - controlled by their internal code
  - every time the contract account receives a message its code activates, allowing it to read and write to internal storage and send other messages or create contracts in turn

The popular term “smart contracts” refers to code in a Contract Account – programs that execute when a transaction is sent to that account.

Code Execution

- The code in Ethereum contracts is written in a low-level, stack-based bytecode language, referred to as "Ethereum virtual machine code" or "EVM code".
- The code consists of a series of bytes, where each byte represents an operation.
- In general, code execution is an infinite loop that consists of repeatedly carrying out the operation at the current program counter (which begins at zero) and then incrementing the program counter by one, until the end of the code is reached or an error or STOP or RETURN instruction is detected.

Code Execution -- Storage (cont'd)

- The operations have access to three types of space in which to store data:
  - The **stack**, a last-in-first-out container to which values can be pushed and popped
  - **Memory**, an infinitely expandable byte array
  - The **contract's long-term storage**, a key/value store. Unlike stack and memory, which reset after computation ends, storage persists for the long term.
- The code can also access the **`value`**, **`sender`** and **`data`** of the incoming message, as well as block header data, and the code can also return a byte array of data as an output.

Proof of Stake

- **Proof of stake** is a consensus algorithm (i.e., voting) for public blockchains which is intended to serve as an alternative to proof of work.
- **Proof of work** is the mechanism that underpins the security behind Bitcoin, the current version of Ethereum and many other blockchains, however it has been criticized for environmental damage and electricity cost associated with the "mining" process because of the environmentally unfriendly energy sources that some mining operations use.
  - Bitcoin's proof of work has been calculated to consume electricity comparable to Ireland's electricity consumption.
- **Proof of stake** attempts to resolve these issues by removing the concept of "mining" entirely, and replacing it with a different mechanism.

Smart Contract Example – Digital Token

- (Please see next page)
- User can use his/her wallet to issue a transaction to another account.
  - Note: a contract itself has an account as well.
- The programmer deployed the contract myToken, and set _totalSupply.
- There is a global variable “balanceOf” stored in the contract, which is an array indexed by account id.
  - Note: all tokens are set to the programmer initially.
  - balanceOf[msg.sender] = _totalSupply.
- Any user can invoke the transer() function to transfer token store in the balanceOf array.

https://ethereum.org/en/developers/


```
pragma solidity ^0.4.2;
contract MyToken {
    string public name;
    uint256 public totalSupply;

    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        string _tokenName,
        uint256 _totalSupply
        ) {
        name = _tokenName;
        totalSupply = _totalSupply;
        balanceOf[msg.sender] = totalSupply;
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        if (balanceOf[msg.sender] < _value) throw;           // Check if the sender has enough balance
        if (balanceOf[_to] + _value < balanceOf[_to]) throw; // Check for overflows
        balanceOf[msg.sender] -= _value;                     // Subtract from the sender
        balanceOf[_to] += _value;                            // Add the same to the recipient
    }

    /* This unnamed function is called whenever someone tries to send ether to it */
    function () {
        throw;     // Prevents accidental sending of ether
    }
}
```

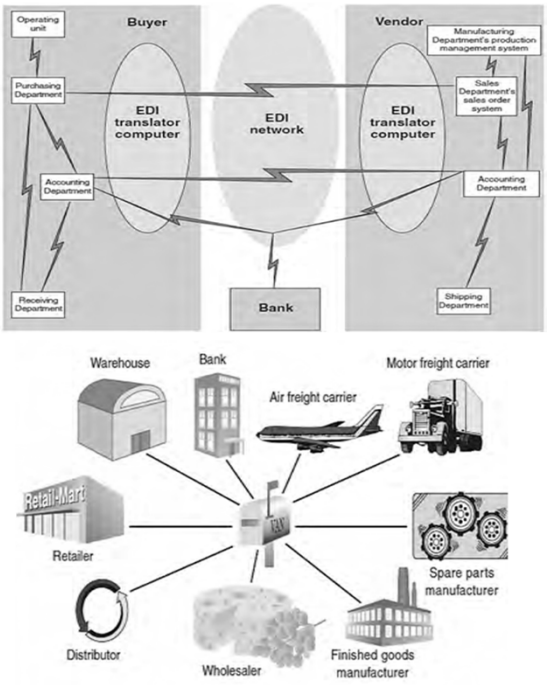
Smart Contract Example – Digital Token

- Although the digital token example seems quite simple; however, it is now a de facto standard in Ethereum.
  - ERC 20: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/
  - https://blockchair.com/ethereum/erc-20
  - Tether USD (USDT), Wrapped Ether (WETH), USD//C (USDC) are implemented by ERC20.
- Tether (USDT) is a cryptocurrency that is USD-pegged, otherwise known as a stablecoin. USDT is backed 100% by actual assets in the Tether platform's reserve account.
  - Therefore, each unit of USDT has a monetary value of one US dollar. USDT provides protection from the volatility of cryptocurrencies.

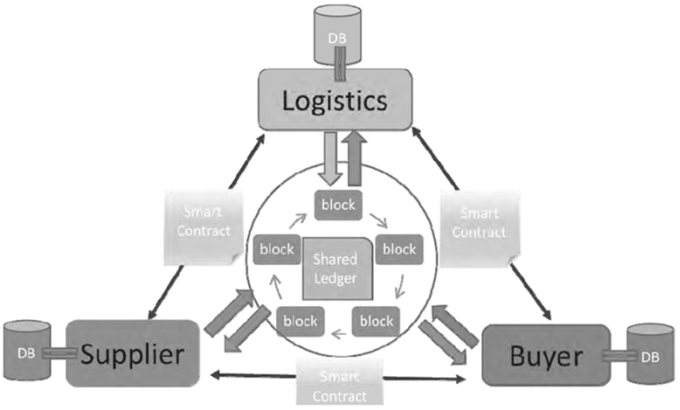
Smart Contract – Supply Chain

- For supply chain purposes, an operational smart contract between a retailer and a manufacturer could state:
  - The cost of manufacturing items as part of a specific order
  - Timescales for manufacturing items between receiving that order and shipping
  - Penalty and bonus clauses
  - Payment terms for settling invoices
- Is a Supply Chain Smart Contract the Same as a Legal Contract?
  - No. A legal contract sets up the high-level agreements and contractual relationships between two supply chain organizations. The smart contract is an operational tool that ensures lower-level, specific agreements and arrangements are being met.

https://www.blumeglobal.com/learning/smart-contracts-blockchain/

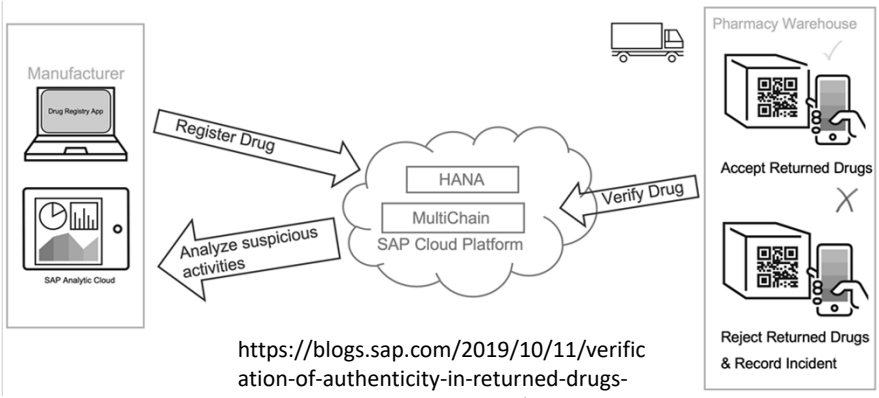


Chang, S. E., Chen, Y. C., & Lu, M. F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technological Forecasting and Social Change*, *144*, 1-11.



Smart Contract – Supply Chain Example

- Example Verification of Authenticity in Returned Drugs Using SAP Blockchain Service



https://blogs.sap.com/2019/10/11/verification-of-authenticity-in-returned-drugs-using-sap-blockchain-service/

Smart Contract – Supply Chain Example

- Governments are enacting legislation to fight the falsification of drugs, requiring the serialization of drugs and reporting to governmental or institutional databases and/or supply chain partners.
- Drug Supply Chain Security Act (DSCSA) requires each individual unit of a pharmaceutical product to have a unique product identifier. It will be linked to vital information about the origin of the product, the pharmaceutical product batch number when it was manufactured and the expiration date.
- SAP use blockchain and advanced data analytics to eliminate fake medicines from the supply chain and bring about greater efficiencies. Integrating the manufacturers, warehouse, shipping and logistics companies, all the way to the hospital or pharmacy, we track each item and package on the blockchain.

ICO - Initial Coin Offering

- An initial coin offering (ICO) is a means of crowdfunding the release of a new cryptocurrency (or a new digital token recorded in the blockchain).
- Generally, tokens for the new cryptocurrency are sold to raise money for technical development before the cryptocurrency is released.
  - Unlike an initial public offering (IPO), acquisition of the tokens does not grant ownership in the company developing the new cryptocurrency.
  - Unlike an IPO, there is little or no government regulation of an ICO.
- The first ICO was for Mastercoin in 2013. Ethereum raised money with an ICO in 2014.
  - https://www.icoalert.com/

ICO example: DAO

- Decentralized autonomous organizations are entities that operate through smart contracts.
  - Its financial transactions and rules are encoded on a blockchain, effectively removing the need for a central governing authority — hence the descriptors “decentralized” and “autonomous.”
- The DAO had a creation period during which anyone was allowed to send some digital currency (ETH) to a unique wallet address in exchange for DAO tokens.
- The platform would allow anyone with a project to pitch their idea to the community and potentially receive funding from The DAO. Anyone with DAO tokens could vote on plans, and would then receive rewards if the projects turned a profit.

https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee 77

THE DAO

- The DAO was a digital decentralized autonomous organization and a form of investor-directed venture capital fund.
  - It was instantiated on the Ethereum blockchain, and had **no** conventional management structure or board of directors.
  - The DAO is a corporation built in code, not law.
  - The code of the DAO is open-source.
    https://github.com/slockit/DAO
  - The DAO was crowdfunded via a token sale in May 2016.
    - It set the record for the largest crowdfunding campaign in history.
- The Hack
  - In June 2016, users exploited a vulnerability in the DAO code to enable them to siphon off one third of The DAO's funds to a subsidiary account.

https://en.wikipedia.org/wiki/The_DAO_(organization) 78

THE DAO (cont'd)

- The DAO was stateless, and not tied to any particular nation state.
- The original theory underlying the DAO was that by removing delegated power from directors and placing it directly in the hands of owners, the DAO removed the ability of directors and fund managers to misdirect and waste investor funds.
  - Everything was done by the code, which anyone could see and audit.
- The DAO was intended to operate as "a hub that disperses funds to projects".
  - Investors received voting rights by means of a digital share token; they vote on proposals that are submitted by "contractors" and a group of volunteers called "curators" check the identity of people submitting proposals and make sure the projects are legal before "whitelisting" them.
  - The profits from the investments will then flow back to its stakeholders.

Why DAO?

- Corporate entities are governed by rules that describe permitted and proscribed conduct.
  - These rules may exist as private contracts or law.
- Corporations have only been able to act through people, and this presents two simple and fundamental problems.
  1. people do not always follow the rules
  2. people do not always agree what the rules actually require
- Its goal is to codify the rules and decision making apparatus of an organization.
  - Eliminating the need for documents and people in governing, creating a structure with decentralized control.

How it works?

1. A group of people writes the smart contracts that will run the organization.
2. There is an initial funding period, in which people add funds to the DAO by purchasing tokens that represent ownership – this is called a crowdsale, or an initial coin offering (ICO) – to give it the resources it needs.
3. When the funding period is over, the DAO begins to operate.
4. People then can make proposals to the DAO on how to spend the money, and the members who have bought in can vote to approve these proposals.

How it works? (cont'd)

- Once a proposal was white-listed by one of the curators, the DAO token holders would need to vote on the proposal.
- If the proposal got a 20% quorum the requested funds would be released into the white-listed contractor's wallet address.

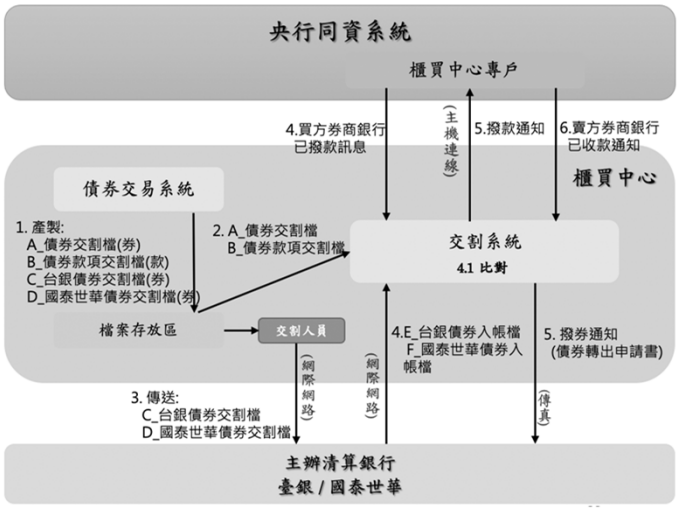
- The DAO was created with an "exit door" known as the "split function".
  - This function allowed users to revert the process and to get back the Ether they sent to the DAO.
  - If somebody decided to split from The DAO, they would create their own "Child DAOs" and approve their proposal to send Ether to an address after 28 days.

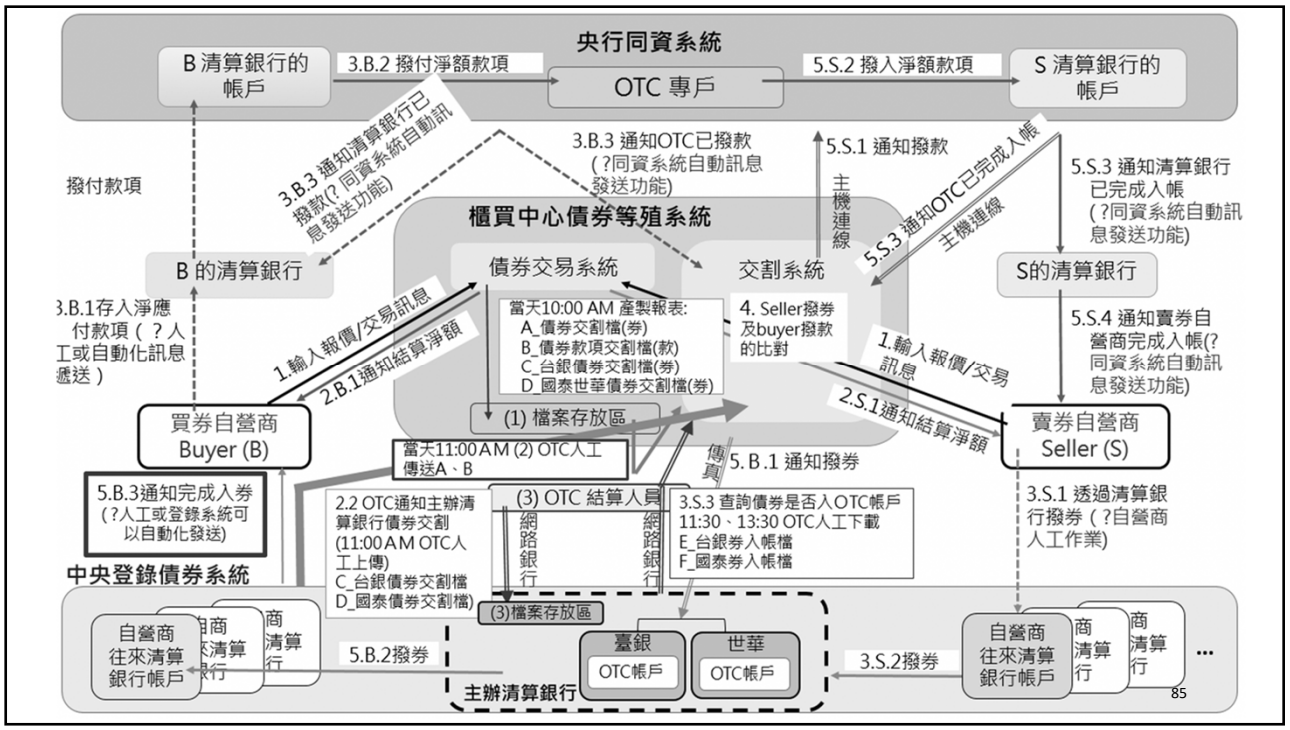
Case:
Blockchainized Financial System

Bond Trading System

債券等殖清算

- 央行同資系統
  - 各清算銀行與櫃買中心設有專戶
- 櫃買中心等殖交易系統
  - 債券交易系統（平台）
  - 交割系統：負責比對作業
- 中央登錄債券系統
  - 共16家清算銀行(保管銀行)
    - 櫃買中心不具保管銀行的角色
    - 同資系統“櫃買中心專戶”及於主辦清算銀行開立之帳戶每日需歸零
  - 櫃買中心設有專戶，由指定之主辦清算銀行進行撥券動作
    - 下載債券入帳檔查詢債券狀況
    - 以人工傳真方式通知主辦清算銀行將債券撥入買方帳戶





Trading Problems

- Transaction time is too long
  - T+2, T+3
- Counterparty risk
  - What if the counterparty defaults on delivery?
- Operational risk
  - Technology or human errors
- Settlement ambiguity
  - Settled or not?
- Safekeeping account complexity
  - Every peers need to have an account in banks.
- Expensive intermediation cost
  - Fee

Problems? It is not a vending machine!

Trading Market

- High efficiency
- Complex process
- Privacy

- Manual Process
  - File generation, human validation, manual data transmission
- Heterogeneous system
- Synchronized Transaction
  - Data flow and cash flow

Blockchain (Distributed Ledger Technology)

- Ownership registry

- Public or private chain?
- Oracle (decentralized external information provider)
- PoW (proof of work) and beyond
- No encryption
  - Privacy?

87

Blockchainized Solutions for Bond Trading?

✓ Trade = Settlement

- Linkage with Existing Settlement Infrastructure by Smart Contract
- Digital Fiat Currency (Central Bank Digital Currency, CBDC)
- Money Token for Settlement

➢ Which one of above is better?

88

Blockchainized Application

- Blockchainization is a process of "Code Refactoring" and "Process Reengineering".

- Think
  - How do we introduce e-banking and i-banking many years ago?
  - How does the government regulate e-banking and i-banking?

Core Value of Blockchain

- Trust among peers
  - Trust creates value.
  - Verifiable (process, data, transaction)
  - Decentralized (encourage, but not limited to)
- Transparent, Accountability
- Efficiency
  - Autonomous System, DAO
  - Time, Cost

Legal Code & Computer Code

- **Legal code**
  - Extrinsic law
  - Can break.
  - Penalty.
- **Computer code**
  - Technical code covers software and protocol.
  - Intrinsic i.e., machine should follow the codes, if any violation, system should report errors. No exception.
  - Bitcoin/Ethereum is an implementation of technical code.

Case: Blockchainized Financial System

Insurance and insurance company

Decentralized Autonomous Organization

Insurance

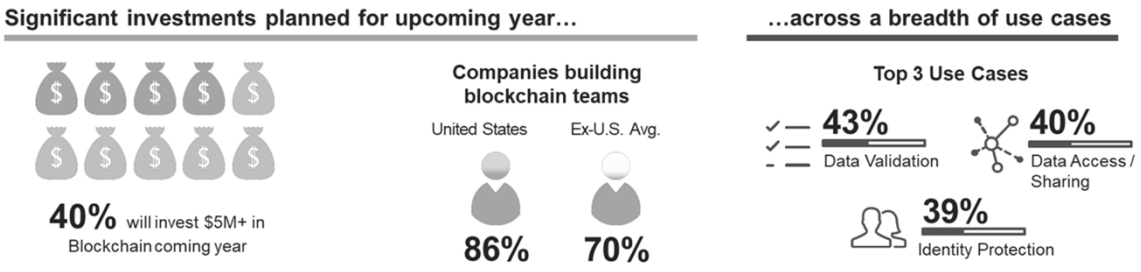
- Investment target
- Life annuity
- Online insurance
- Auto insurance claim
- Car insurance
- …

Other DAO

- Financial clearance
- Flight time limitation
- Registration
- Logistics
- …
- ➢ What if a smart contract has a bug and needs to be modified?

Adoption or not?

- The corporate blockchain hype cycle is slowing in 2019.



https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Consulting/Blockchain-Trends-2020-report.pdf

Adoption or not?

- Industries seeing rapid adoption and potential for 2020.
  - Life Sciences and Healthcare
    - an industry in which data transparency, speed of access, immutability, traceability, and trustworthiness can provide the information necessary for life-altering decisions.
    - The possibility of utilizing blockchain technology in clinical trials and pharmaceutical supply chains have been at the center.
  - Farming and Supply Chain
    - The supply chain is at the heart of every manufacturing organization; it is the channel through which information, materials, services, and financial resources flow from idea to end-use delivery in a life cycle of value-added transactions.
  - Financial Services
    - Central Bank Digital Currencies (CDBCs)
    - ICO, digital assets

Adoption or not?

- What scenario truly need blockchain?
  - Transactions
    - However, do you need the decentralized trust to replace centralized trust?
  - Records
    - Immutable, transparent, credibility, traceable, no-human-involvement.
    - E.g., donation
  - Identity
    - Wallet has crypto-keys. It makes it easy to deploy identity-related application, such as smart lock, digital signature.
- Final word
  - Private blockchain is not necessary indicate the chain is immutable, transparent, credibility, traceable, …

Blockchain Security and Its Business Application Cases

國立政治大學 資訊管理學系
Dept. of Management Information Systems
National Chengchi University

蕭舜文 助理教授
Dr. Shun-Wen Hsiao
hsiaom@nccu.edu.tw

2020.10.23