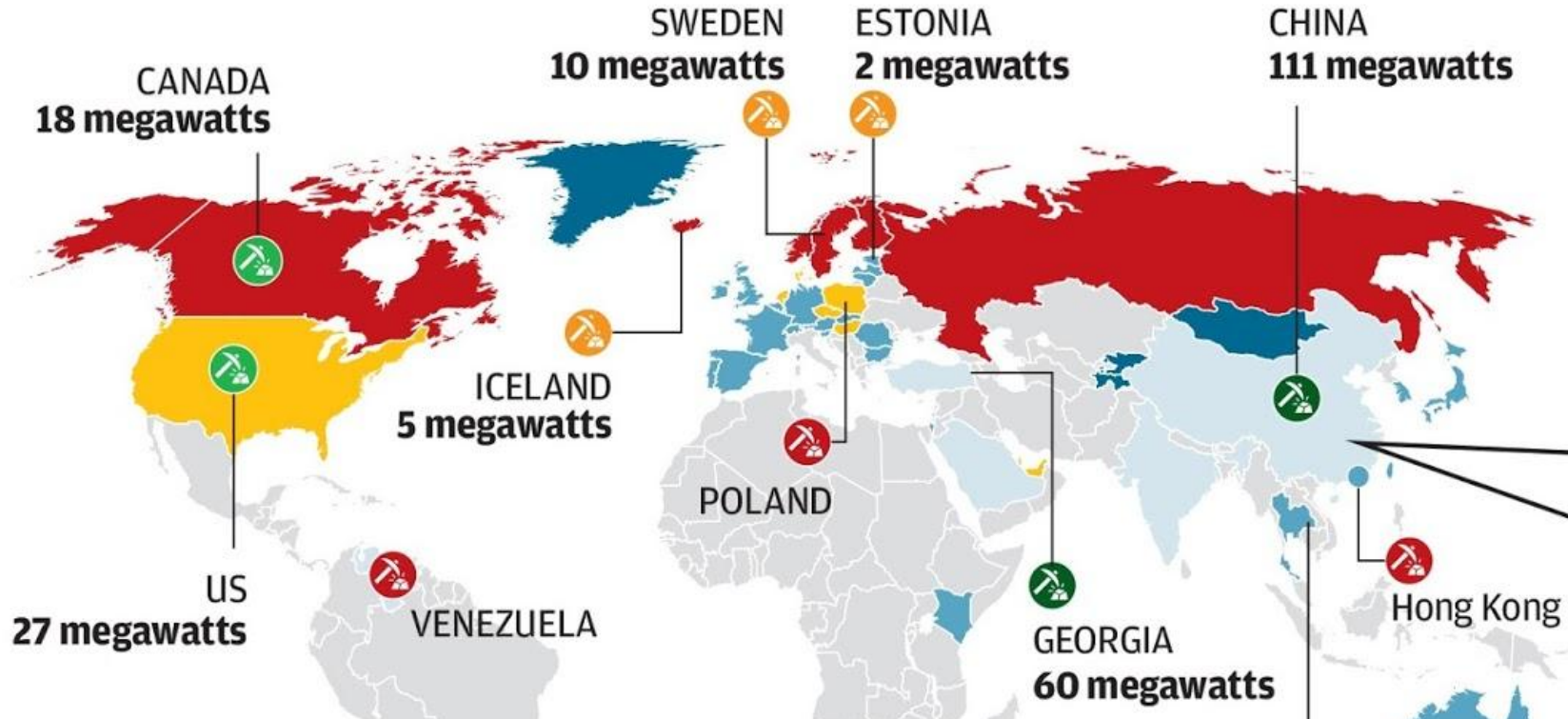


# Global cryptocurrency mining sites



1 Bitcoin equals

**9,760.47 New Zealand Dollar**

6 Sep, 7:44 PM UTC · Disclaimer

1 Bitcoin

9760.47 New Zealand Dollar



- 11-50 megawatts
- >50 megawatts

Source: University of Cambridge

What's behind Bitcoin?



# Outline

1. A centralized financial system

2. A financial Crisis

3. A Decentralized financial system

4. Bitcoin

4.1 Asymmetric Cryptography

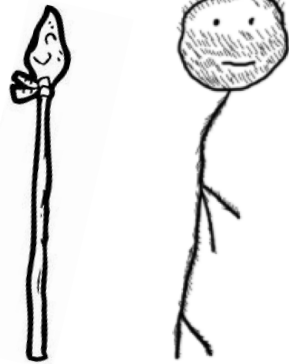
4.2 Decentralized information synchronization protocol

5. Future

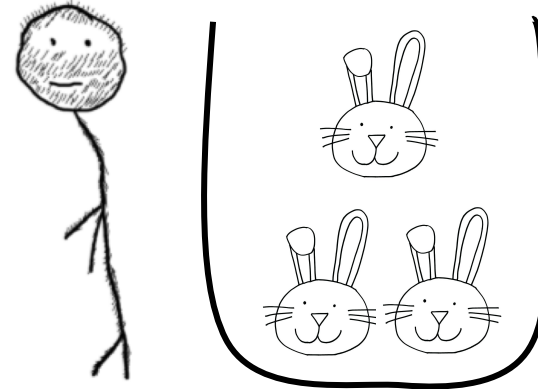
# 1. A centralized financial system

A long time ago in a galaxy far,  
far away....

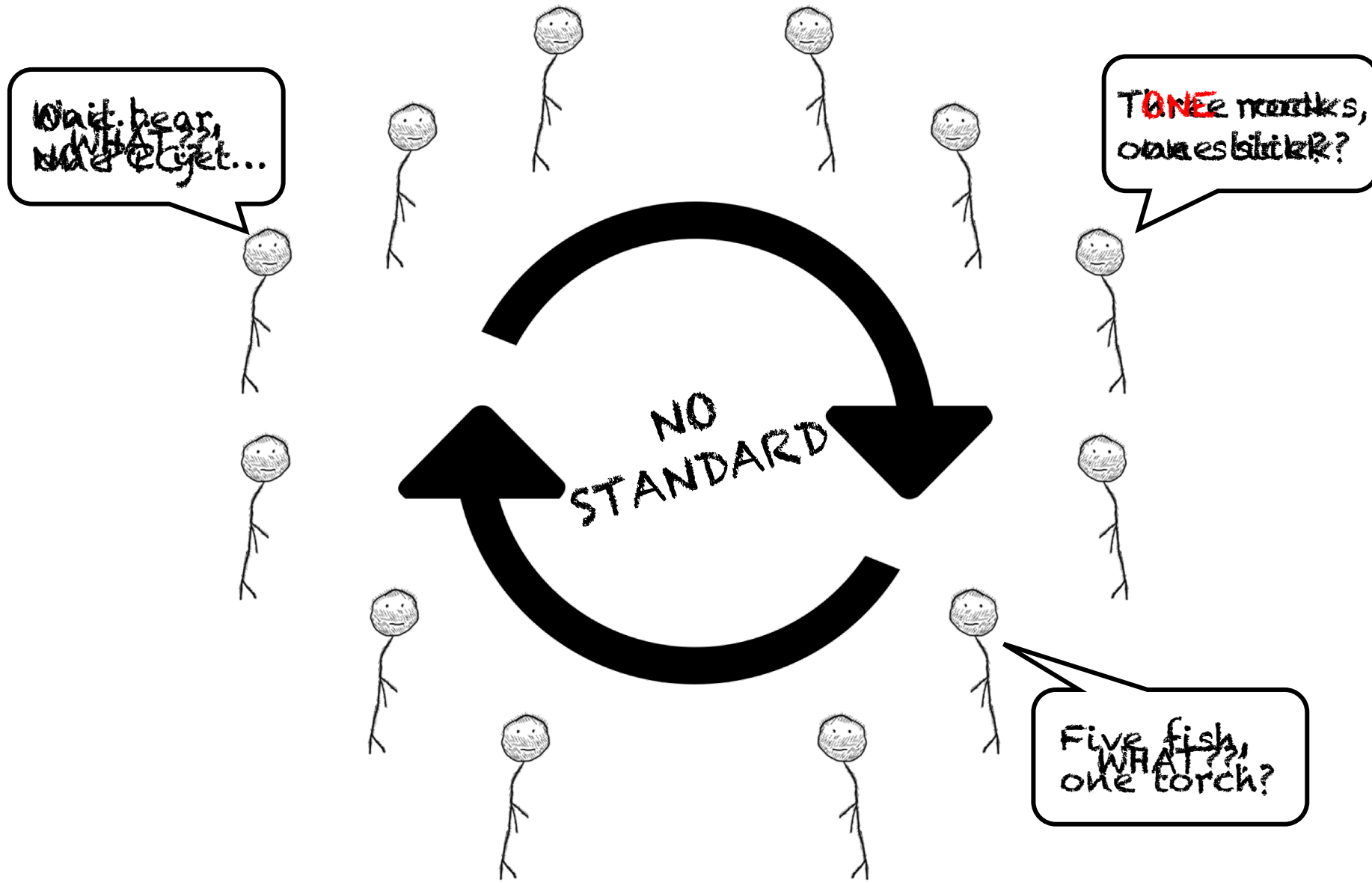
Deal!



Three rabbits,  
one spear?

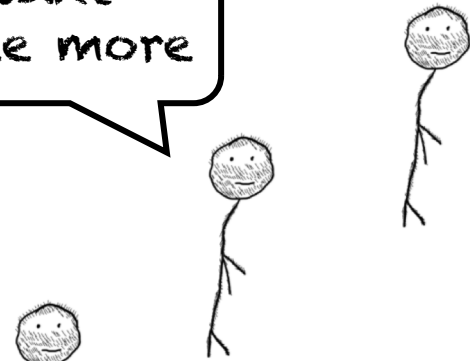


- Each man has his own skill and creates **VALUE**.
- **Exchanging** their **VALUE** can benefit from each other.

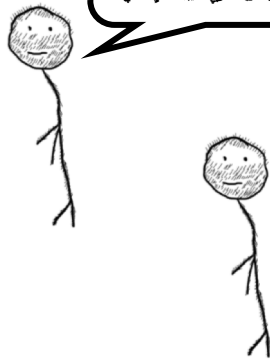


The trade in a tribe

Couldn't agree more



No Problem!



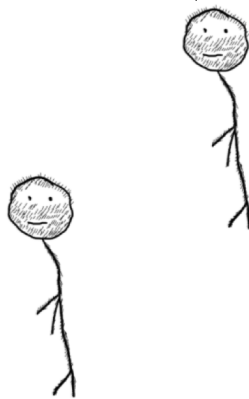
Sounds Good!



Hmmm





Agree!

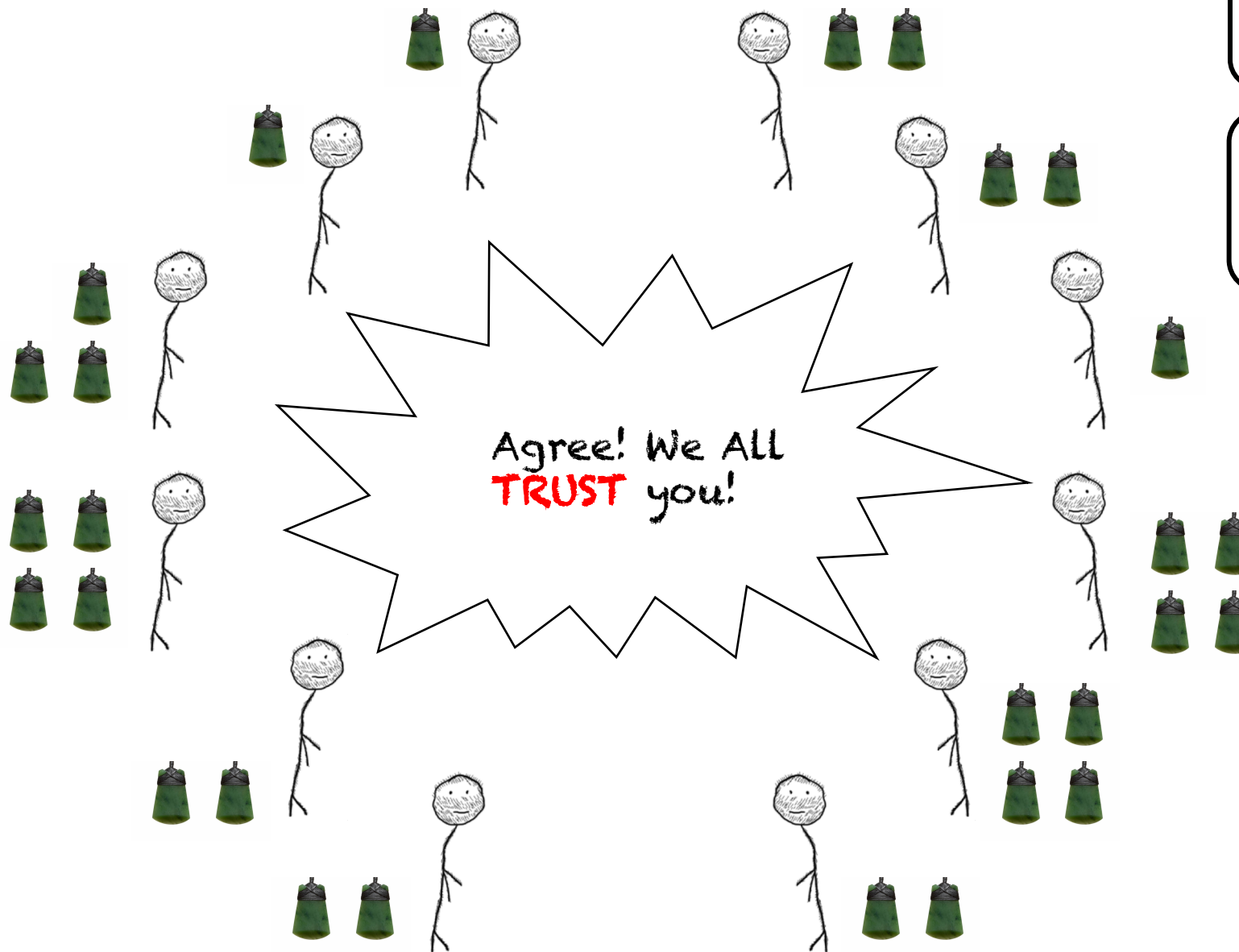


- Set up a Standard

1 fish = 3 Rocks  
1 bear = 10 rabbits  
1 spear = 1 torch  
... = ...

- Issue a currency

1 fish =   
3 Rocks =   
... = ...



Guys, we don't need a physical currency, I can manage your accounts.

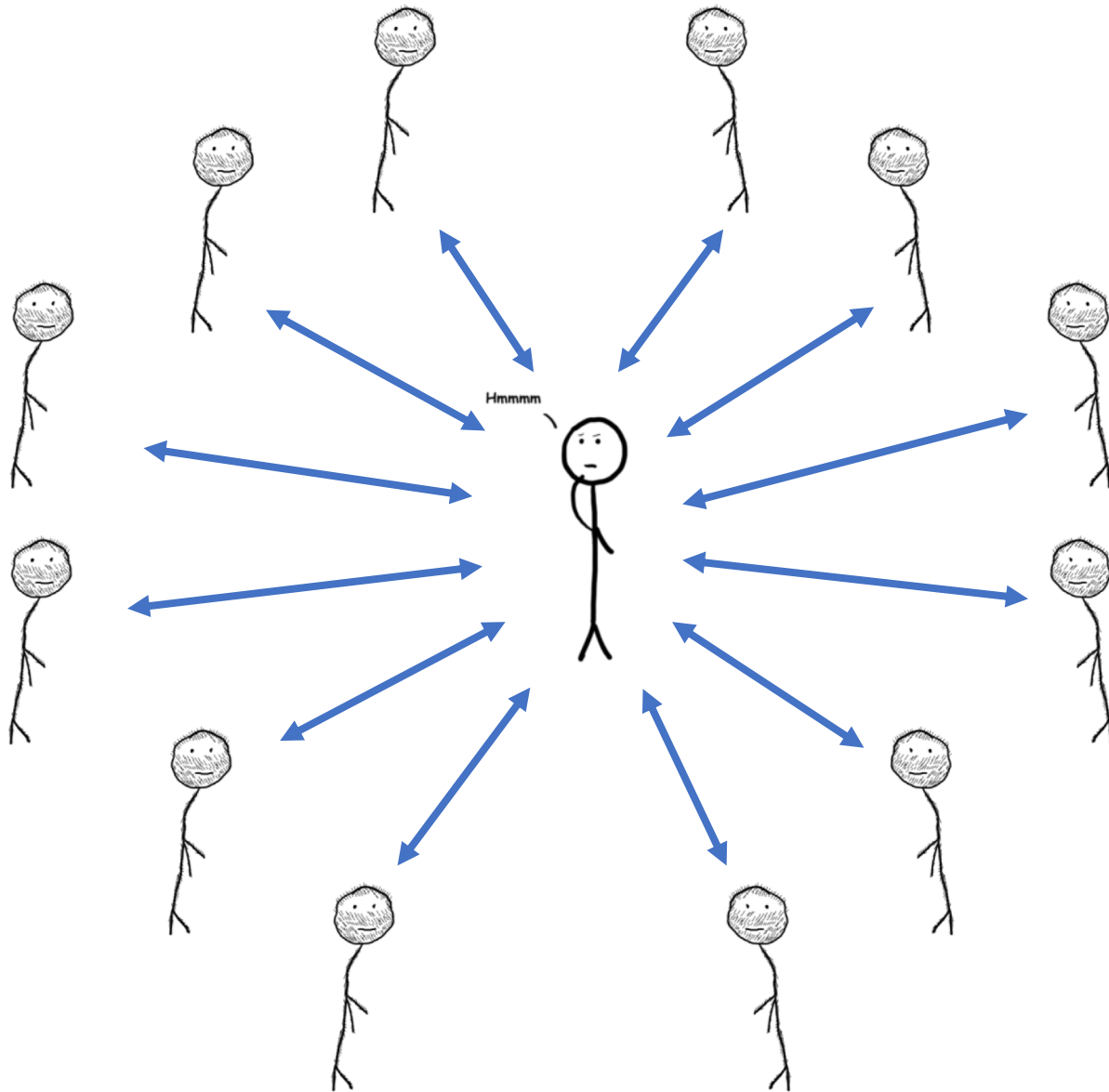
Since I know all of you, I can verify your trades and update your accounts.

- Manage accounts

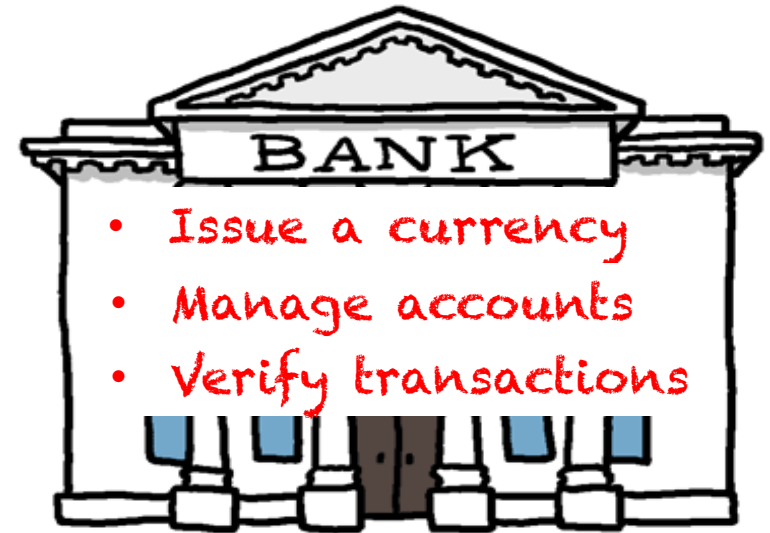
Tom	Bob	Amy
30 -2	13 +2 ...	24

"Tom buys two fish from Bob."

- Verify transactions



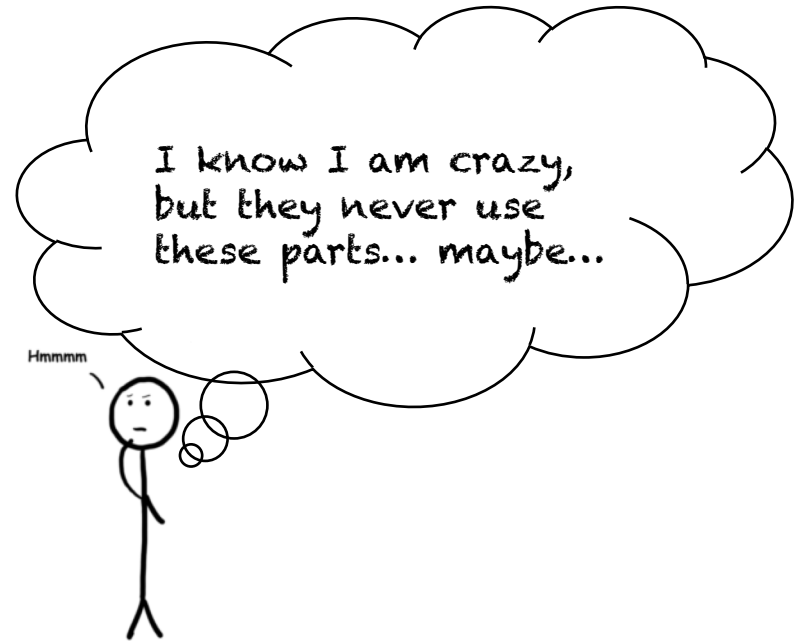
A **centralized** financial system



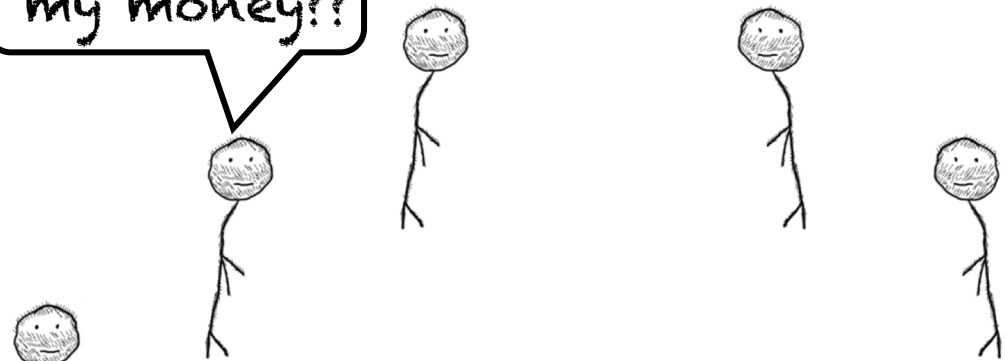


## 2. A financial Crisis

Tom	Bob	...	Frank
10	8	...	13



WHERE is my money??



WHERE is my money??



Hmmm

Does Anyone want a loan? Really Low interest...



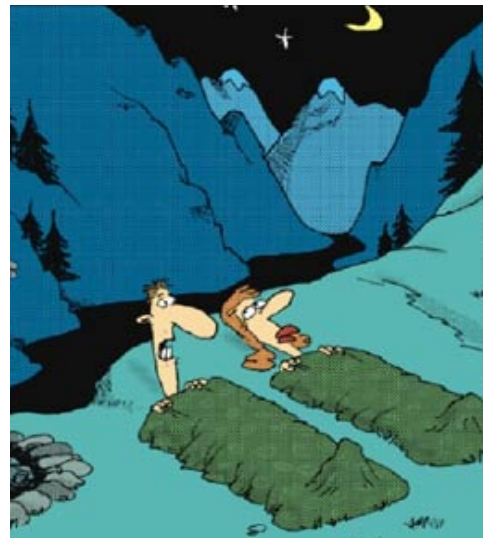
OMG



WHERE is my money??



David





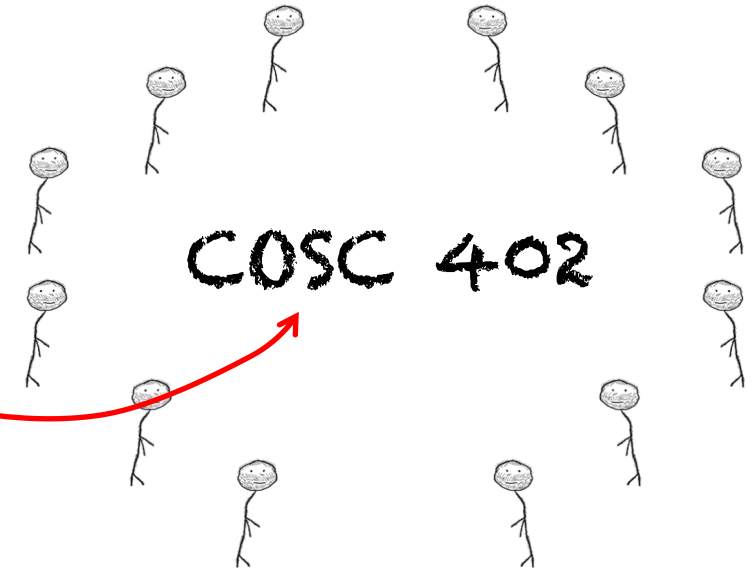
# 3. A Decentralized financial system

The collapse of the centralized system



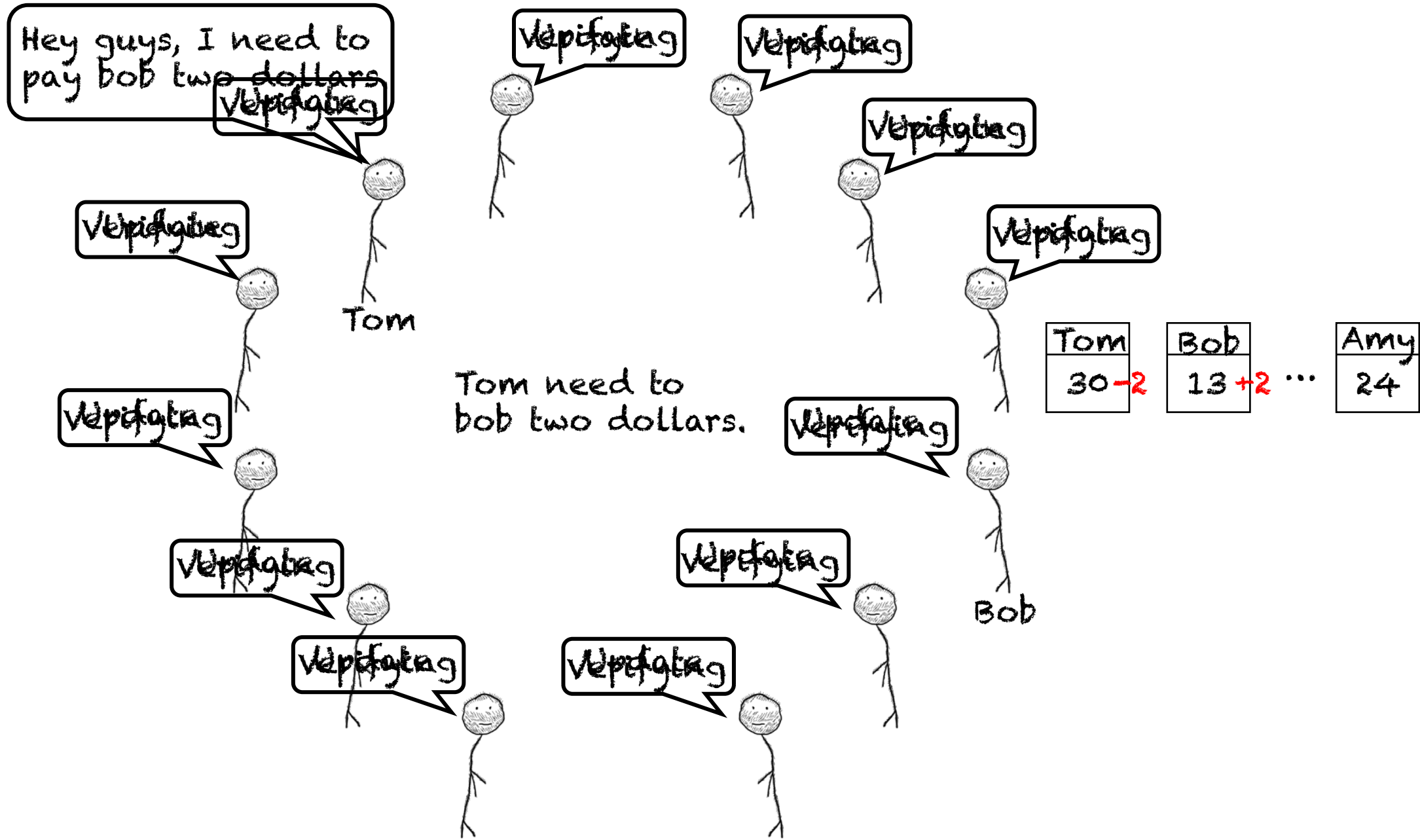
A Decentralized financial system

- There is **no central node**
- Everyone is **equal**
- Issue and **trust** a new currency



General Idea:

- No central guy helps them to maintain the system
- **Everyone** needs to do the central guy's job
- **Everyone** needs to manage **all** the accounts!
- **Everyone** needs to verify **all** the transactions!
- **Everyone** keeps the **SAME** ledger!



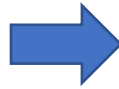
An example of the Decentralized system

## 4. Bitcoin: A Peer-to-Peer Electronic Cash System

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

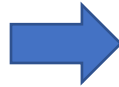


- A **new** currency?



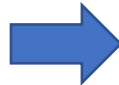
- Bitcoin

- How to **Verify** Transactions?



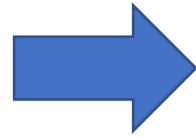
- Private and public Keys

- How to make sure **everyone** keeps the **SAME** ledger?



- Blockchain

# 4.1 A New Currency?

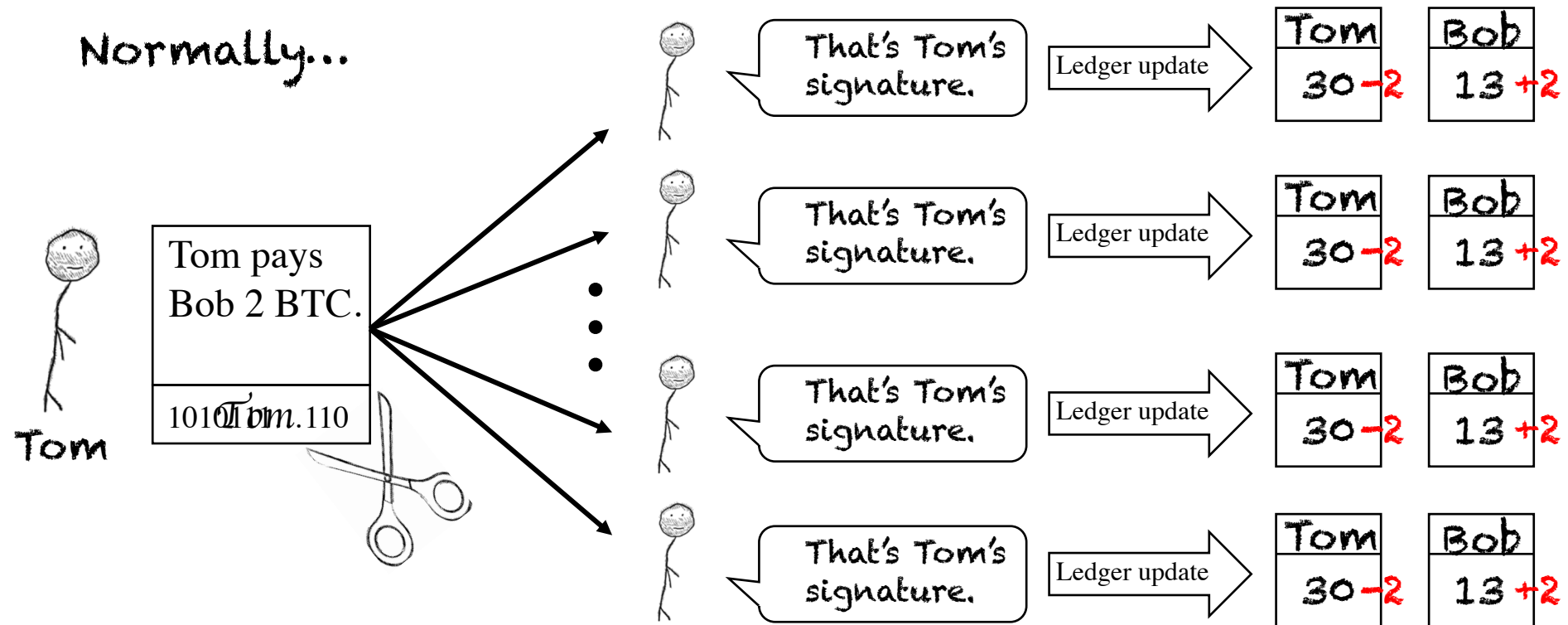


BTC

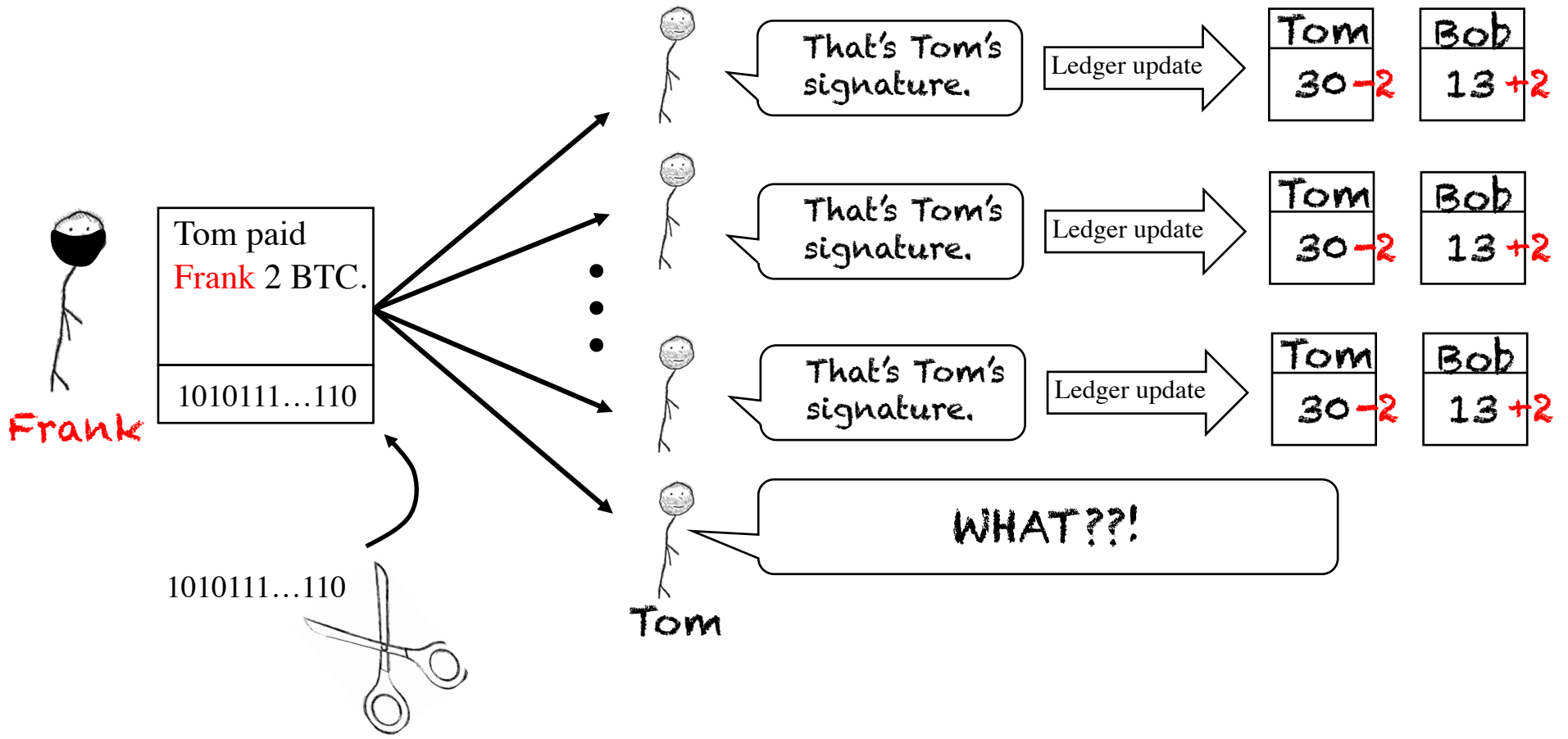
Numbers with TRUST

# 4.2 How to **Verify Transactions** in Bitcoin System?

## 4.2.1 Digital Signature





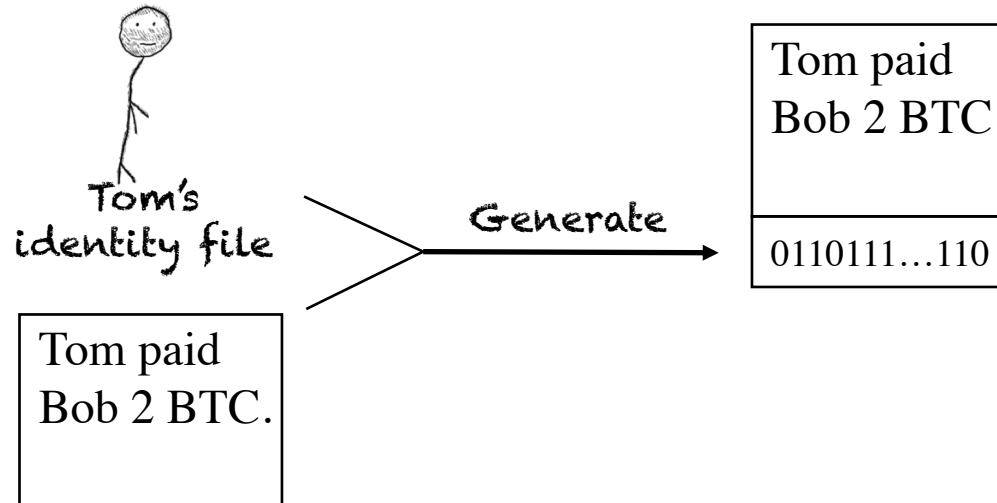


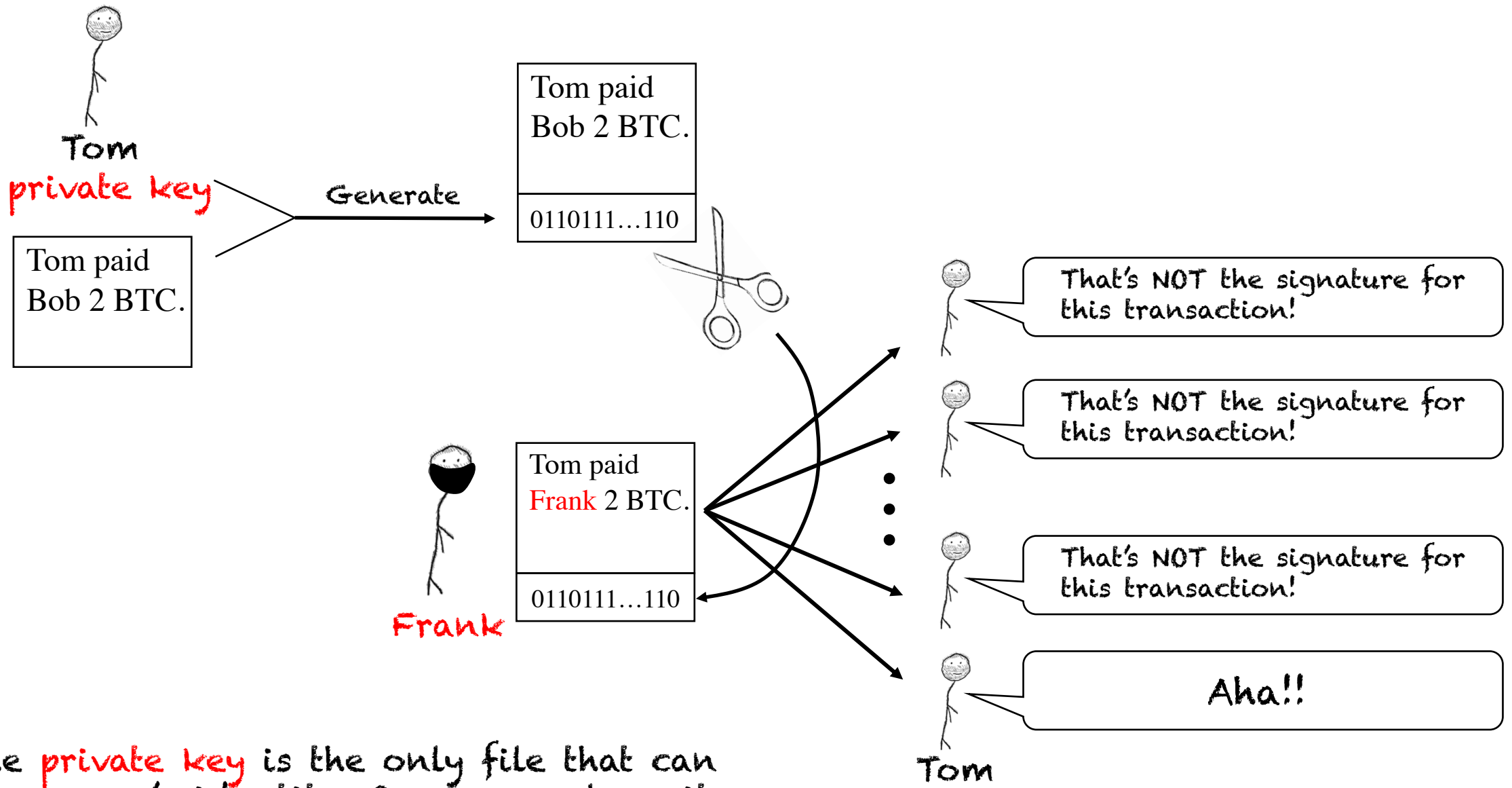
## 4.2.2 Digital Signature Requirement

- A signature that can **represent** Tom's identity.
- Copy a signature from one transaction and paste it on another is **invalid**.



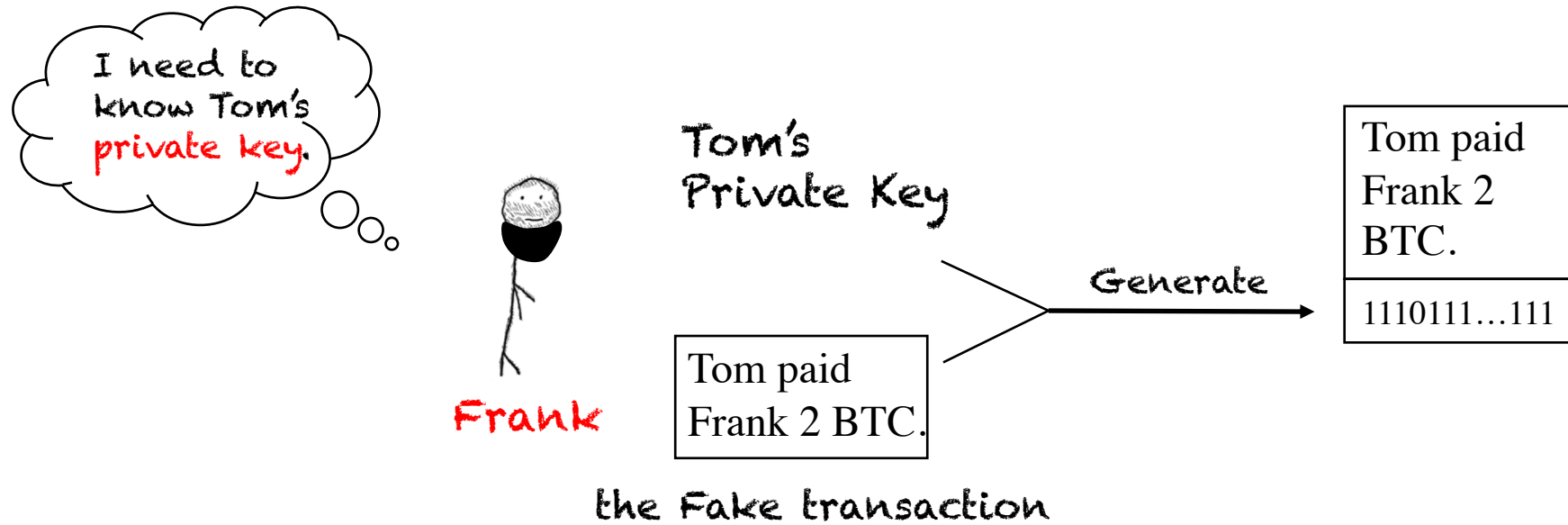
- **Each** transaction has its **unique** signature.





The private key is the only file that can prove one's identity. Once you lose it, everything is gone.

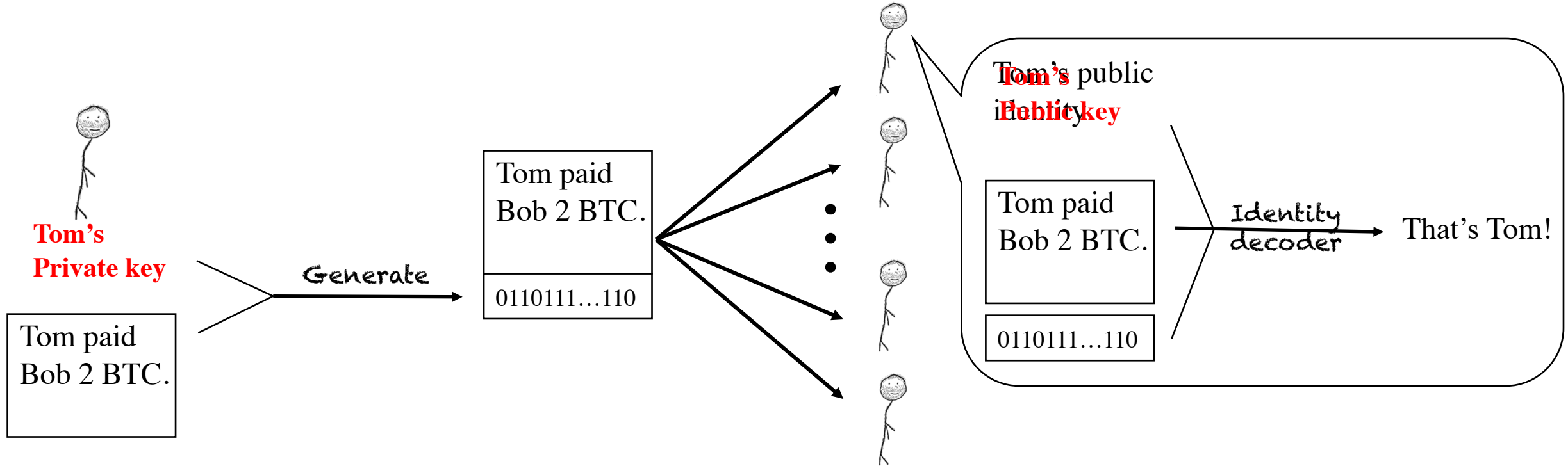
## 4.2.3 Private Key



- BUT, only Tom himself know his private key! There is no chance to forge one!

So, How to **Verify** the digital signatures?

## 4.2.4 Public Key



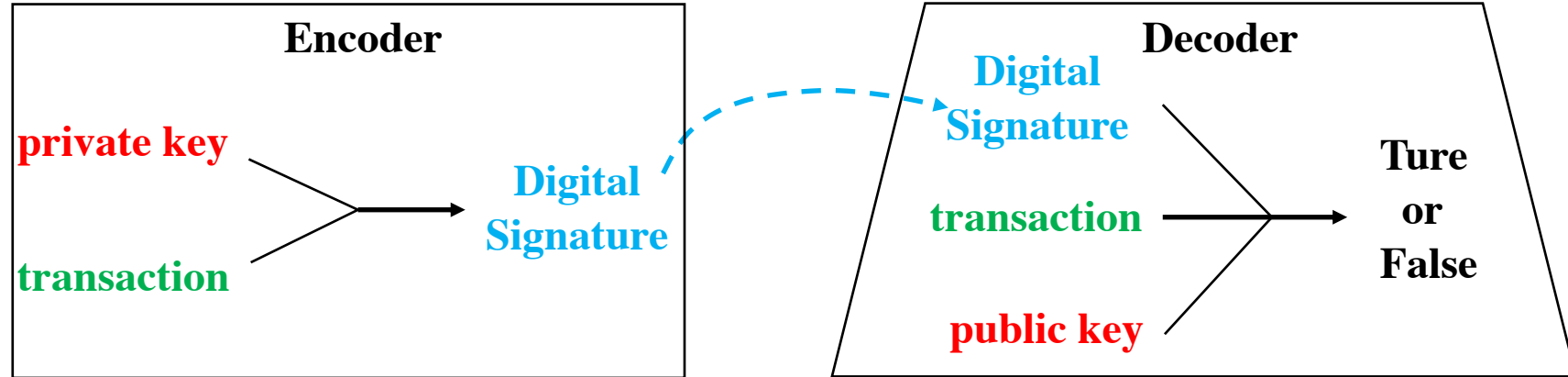
- Tom's private key is the unique file to prove his identity.
- The digital signature contains the information of the private key.
- People can use Tom's public key to find out whether the signature contains the private information.
- The private and public keys are in pairs.

```
workstation$ ssh-keygen -b 2048 -t rsa
Generating public/private rsa key pair.
Just press enter for this next one to accept the default.
Enter file in which to save the key (/Users/theauthor/.ssh/id_rsa):
Use a strong passphrase! These won't be echoed.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/theauthor/.ssh/id_rsa.
Your public key has been saved in /Users/theauthor/.ssh/id_rsa.pub.
The key fingerprint is: Yours will be different...
1a:91:52:bf:41:78:7b:bc:19:a7:c1:ea:1a:cd:1f:2d Comment
```

## 4.2.5 Asymmetric Cryptography

Transaction Verification  
in Bitcoin System

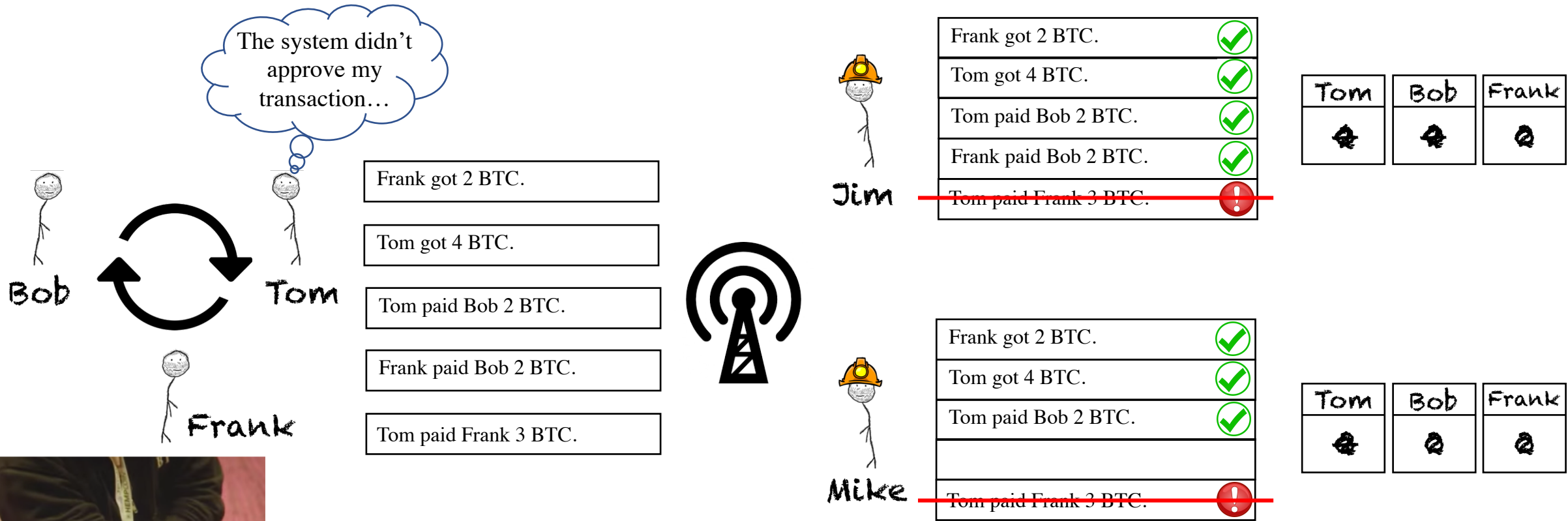
1. **Digital Signature** = *Signature\_Generator* (**private key**, **transaction**)
2. **Ture or False** = *Identity\_Decoder* (**Digital Signature**, **transaction**, **public key**)



How to make sure everyone  
keeps the **SAME** ledger?

Imagine...We are in a complex Internet environment...

## 4.3 How to make sure everyone keeps the **SAME** Ledger?



- Different miners may have different ledgers.
- However, the **Decentralized** system need a standard ledger.
- The different ledgers are all possible options for the standard.
- Which one?
- We need a method to select a system ledger at this time point.



# 4.3.1 Proof of Work



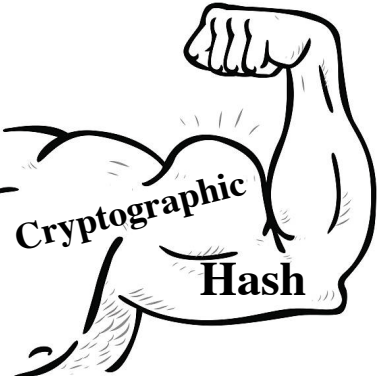
Hi Jim! If you want your ledger to be a part of the system one, please tell me **a number**, which meets the requirement below.

I think I may need thousands of thousands of guesses and calculations to find the number!



Oh No... This is **Cryptographic Hash**, I have **no chance** to do reverse engineering... **Easy!**

Frank got 2 BTC.	✓
Tom got 4 BTC.	✓
Tom paid Bob 2 BTC.	✓
Frank paid Bob 2 BTC.	✓



**SHA\_256**

Verified Ledger

Frank got 2 BTC.	✓
Tom got 4 BTC.	✓
Tom paid Bob 2 BTC.	✓
Frank paid Bob 2 BTC.	✓

, Jim's random guess number

**72 bits Zero**

0000000000	0000000000
0000000000	0000000000
0000000000	0000000000
0000000000	0011010111
1000100000	0011000110
.....	

- Normally, it takes several years for one computer to find an answer.
- But, generally, a lucky miner in the system can guess a right number in ten minutes.
- The more computing power a miner has, the luckier he would be.



OK. Your verified ledger will be **a block** of the system ledger and I will give you 12.5 BTC as a reward.

I guessed and calculated many many times and finally got this number. I am the **first** one to find the solution.



*SHA\_256*

Jim's Verified Ledger

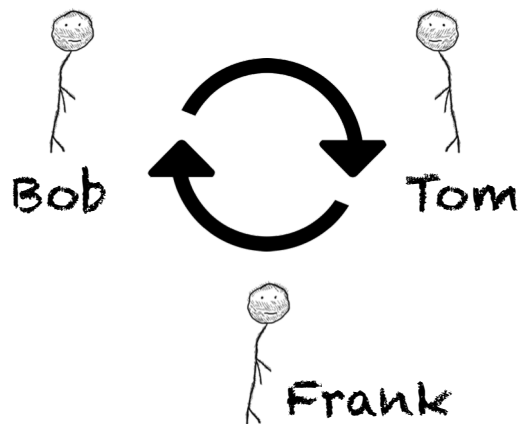
**10110001110**

=

**72 bits Zero**  
 0000000000 0000000000  
 0000000000 0000000000  
 0000000000 0000000000  
 0000000000 0011010111  
 1000100000 0011000110  
 .....

Frank got 2 BTC.	✓
Tom got 4 BTC.	✓
Tom paid Bob 2 BTC.	✓
Frank paid Bob 2 BTC.	✓
<b>Jim got 12.5 BTC.</b>	✓
<b>10110001110</b>	

The System Ledger all the users need to follow



Bob paid Frank 1 BTC.

Bob paid Tom 1 BTC.

Tom paid Frank 3 BTC.



Bob paid Frank 1 BTC.	✓
Bob paid Tom 1 BTC.	✓
Tom paid Frank 3 BTC.	✓

Tom	Bob	Frank
<del>2</del>	<del>4</del>	<del>4</del>

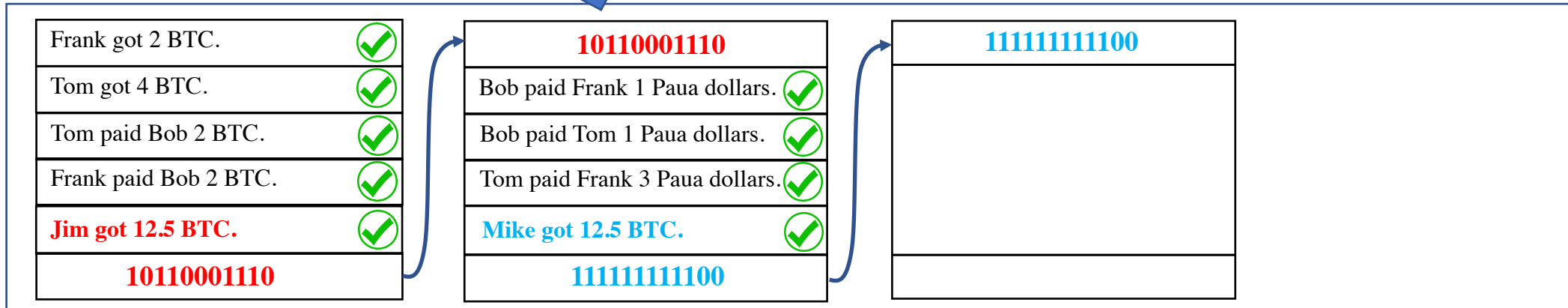
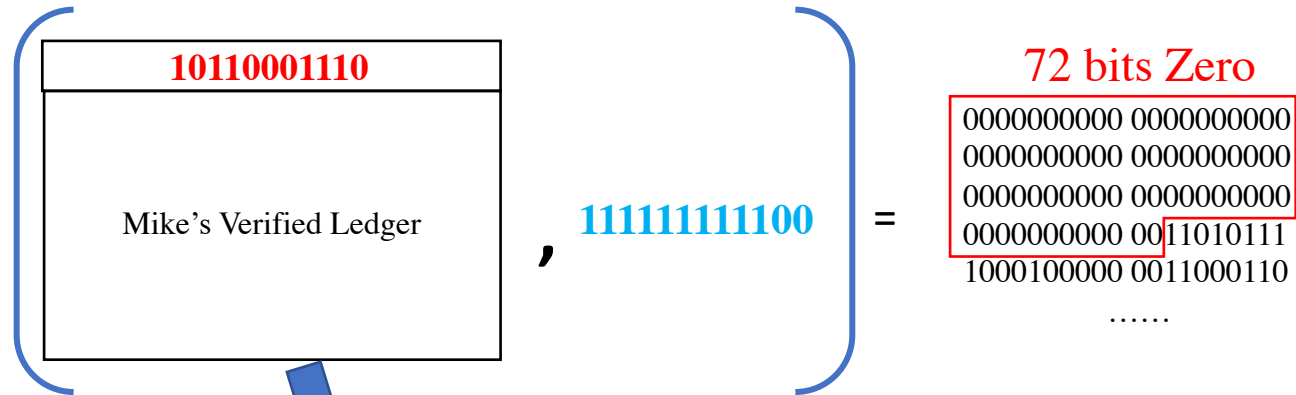


Bob paid Frank 1 BTC.	✓
Bob paid Tom 1 BTC.	✓
Tom paid Frank 3 BTC.	✓

Tom	Bob	Frank
0	2	4

## 4.3.2 Block Chain

*SHA\_256*



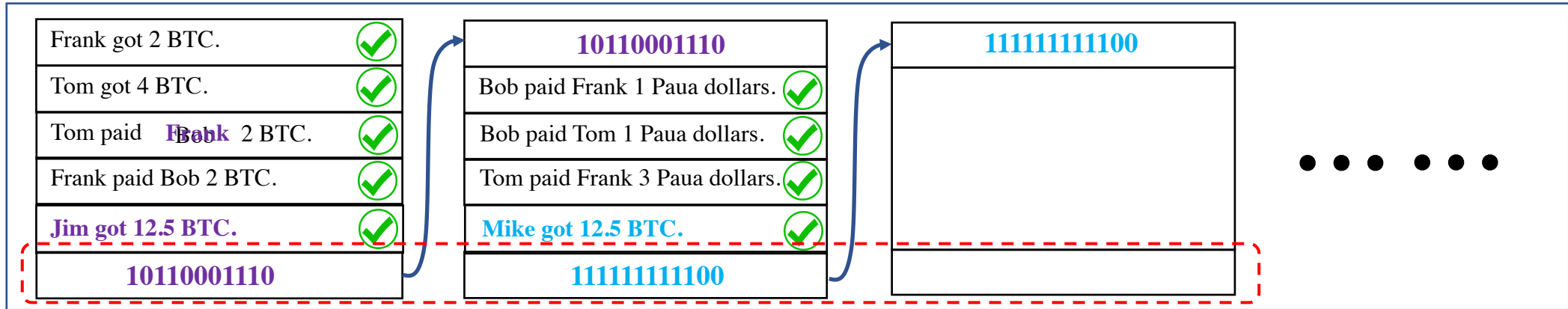
The System Ledger all the users need to follow

**Decentralized information synchronization protocol**

Frank



# Change the previous transactions in Block Chain?

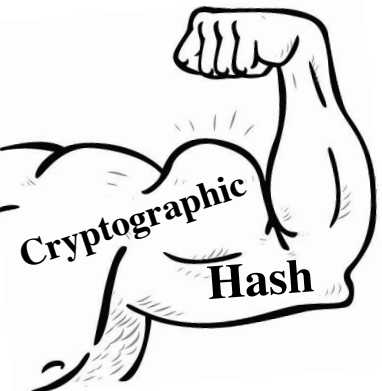


Recalculate

“Normally, it takes several years for one computer to find an answer.”

Theoretically, yes. But the hacker needs to have at least 51% computational power of the whole network.

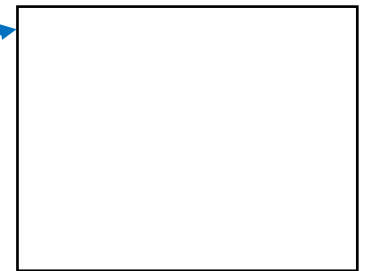
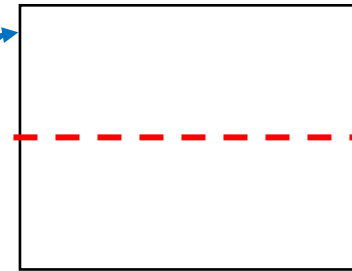
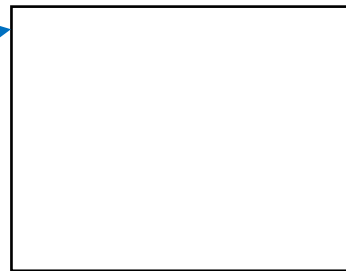
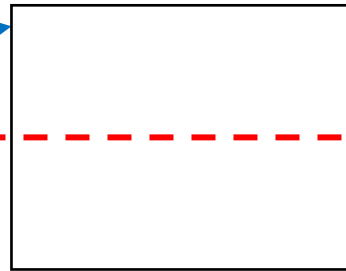
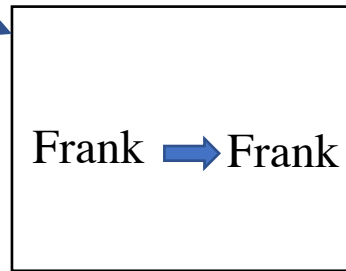
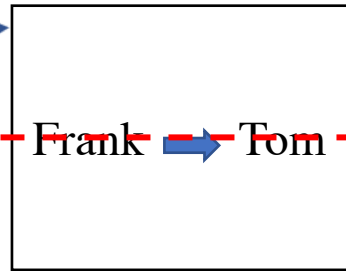
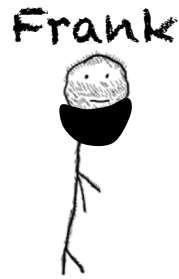
So, practically, it is impossible to forge a transaction in a stable Blockchain. Because once a hacker does this, he needs to recalculate all the blocks after the fake one, which would spend an incredibly long time.



- Double Spend Attack in Blockchain?

Frank got 2 BTC.	✓
Tom got 4 BTC.	✓
Tom paid Bob 2 BTC.	✓
Frank paid Bob 2 BTC.	✓
Jim got 12.5 BTC.	✓
<b>10110001110</b>	

<b>10110001110</b>
Bob paid Frank 1 Paua dollars. ✓
Bob paid Tom 1 Paua dollars. ✓
Tom paid Frank 3 Paua dollars. ✓
Mike got 12.5 BTC. ✓
<b>111111111100</b>



Shipping the product



<https://www.youtube.com/watch?v=Lx9zgZCMqXE&t=767s>

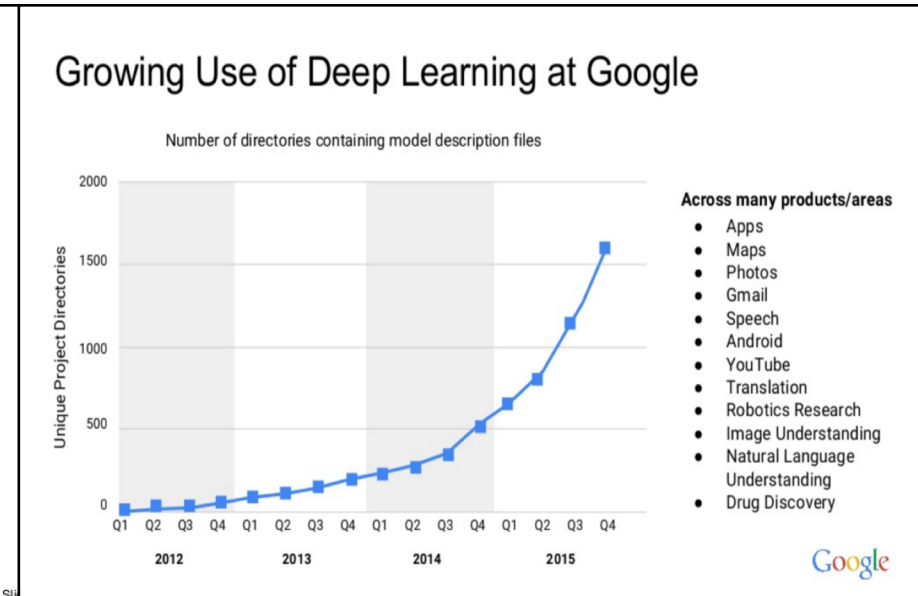
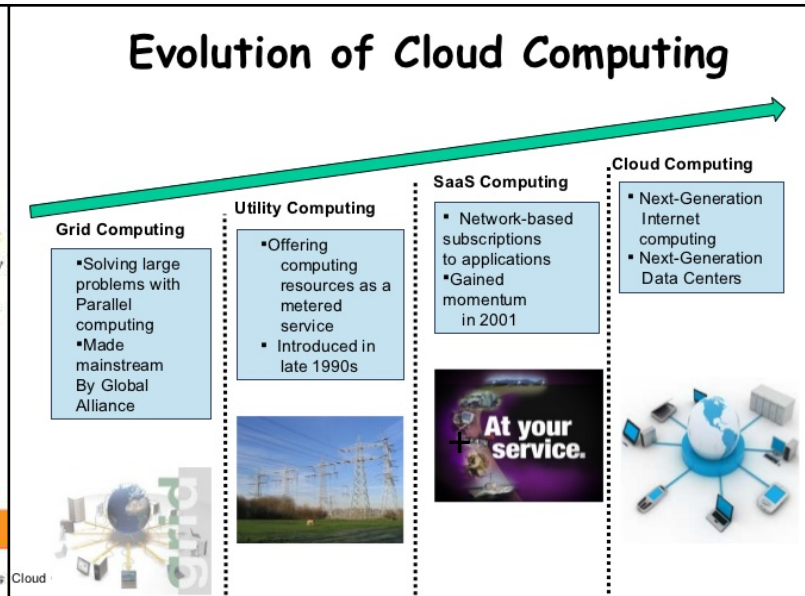
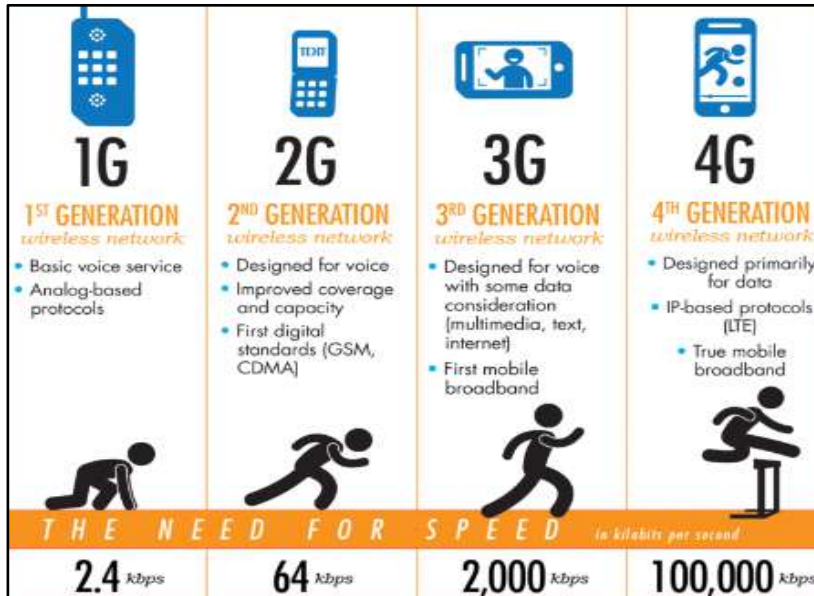
<https://www.youtube.com/watch?v=Lx9zgZCMqXE&t=666s>

<https://www.youtube.com/watch?v=S00MWI3YeP4>

<https://www.youtube.com/watch?v=K8kua5B5K3I>


<https://www.youtube.com/watch?v=s4g1XFU8Gto>

# 5. Future?



Accumulation + timing





# A Brief Introduction to Decentralized Consensus

Speaker: Luming Wan

Email: [lwan@cs.otago.ac.nz](mailto:lwan@cs.otago.ac.nz)



# Outlines

- Blockchain structure
- Decentralized consensus
- Blockchain forking
- Other consensus protocols
- Applications & Future trend


















## Bitcoin price (BTC)

\$12,654.08 - \$334.17 (2.58%)

\$13,159.46

September 29 6:44 AM

11:36 AM 3:32 PM 7:28 PM 11:24 PM 3:20 AM 7:16 AM 11:24 AM

1	 Bitcoin BTC	NZ\$12,649.79	-0.20%	NZ\$227.2B
2	 Ethereum ETH	NZ\$266.42	-1.43%	NZ\$28.8B
3	 XRP XRP	NZ\$0.37	-0.23%	NZ\$16.1B
4	 Bitcoin Cash BCH	NZ\$347.73	+2.24%	NZ\$6.3B
5	 Litecoin LTC	NZ\$85.12	-1.20%	NZ\$5.4B
6	 EOS EOS	NZ\$4.37	-0.63%	NZ\$4.1B
7	 Stellar Lumens XLM	NZ\$0.0901	-1.02%	NZ\$1.8B
8	 Dash DASH	NZ\$109.71	-0.77%	NZ\$994.1M
9	 Chainlink LINK	NZ\$2.68	+4.18%	NZ\$936.7M
10	 Tezos XTZ	NZ\$1.35	-0.21%	NZ\$894.4M
11	 Ethereum Classic ETC	NZ\$7.23	-0.55%	NZ\$822.9M
12	 USD Coin USDC	NZ\$1.55		NZ\$664.0M
13	 Zcash ZEC	NZ\$59.76	+1.82%	NZ\$449.1M
14	 Basic Attention Token BAT	NZ\$0.25	-0.62%	NZ\$338.9M
15	 Ox ZRX	NZ\$0.32	-4.54%	NZ\$192.5M
16	 Augur REP	NZ\$12.86	-2.07%	NZ\$141.5M
17	 Dai DAI	NZ\$1.56	-0.11%	NZ\$124.2M

---

# Blockchain

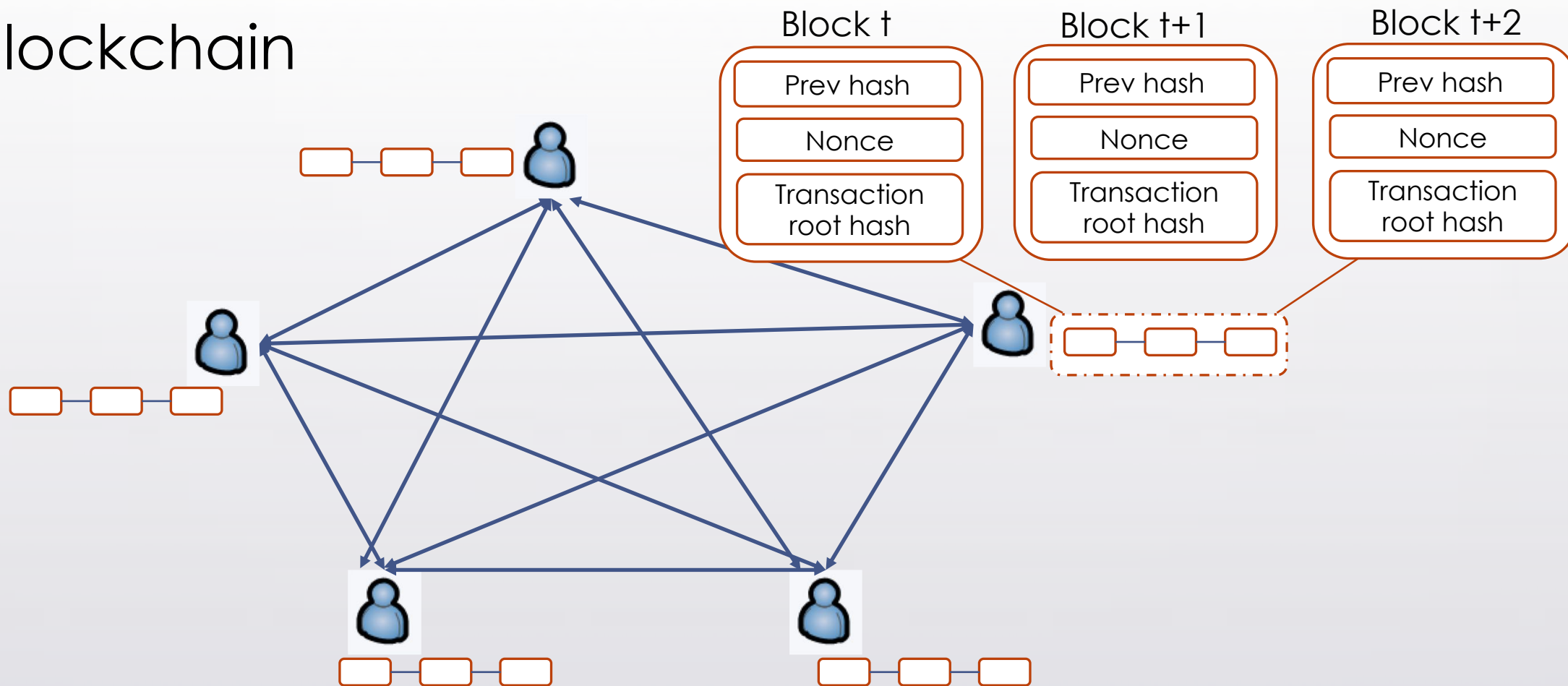
- Firstly introduced by Satoshi Nakamoto in 2009.
- Blockchain is the fundamental protection mechanism and digital ledger for Bitcoin transactions.
- **Provide a trustful environment to untrusted users.**



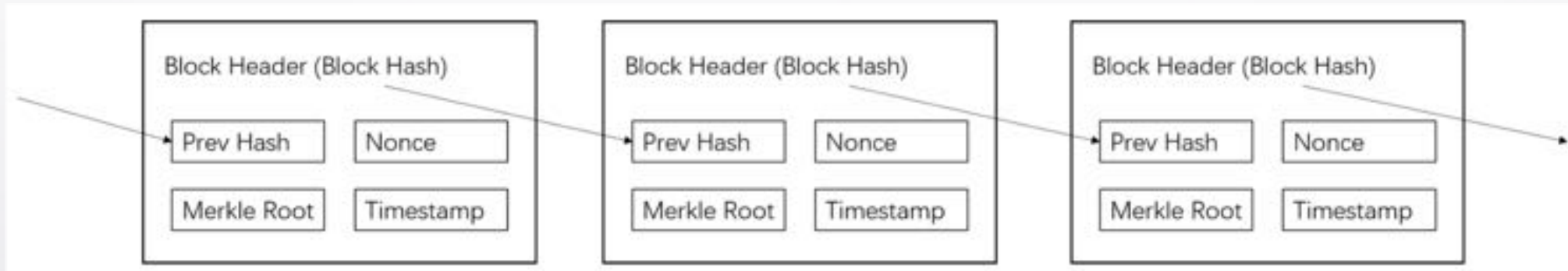
# Technologies used by blockchain

- Public-private key (COSC244): for transaction validation
- Hash (COSC242): block identification, transaction Merkle Tree
- Linked list (COSC241)

# Blockchain

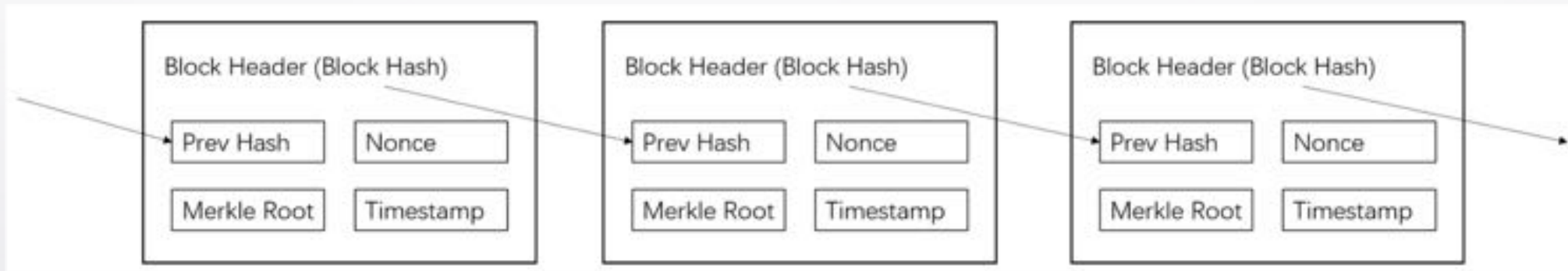


# Block structure



- Blockchains are linked lists that contain data and a hash pointer that points to the previous block, creating a chain of connected blocks, hence the name “blockchain”.
- **Proof-of-work (PoW) mining:** solving a certain level difficulty hash puzzle (SHA256), by slightly adjusting the nonce value.
- A PoW mining winner could create a new block, and gain reward (bitcoin) from this newly mined block.

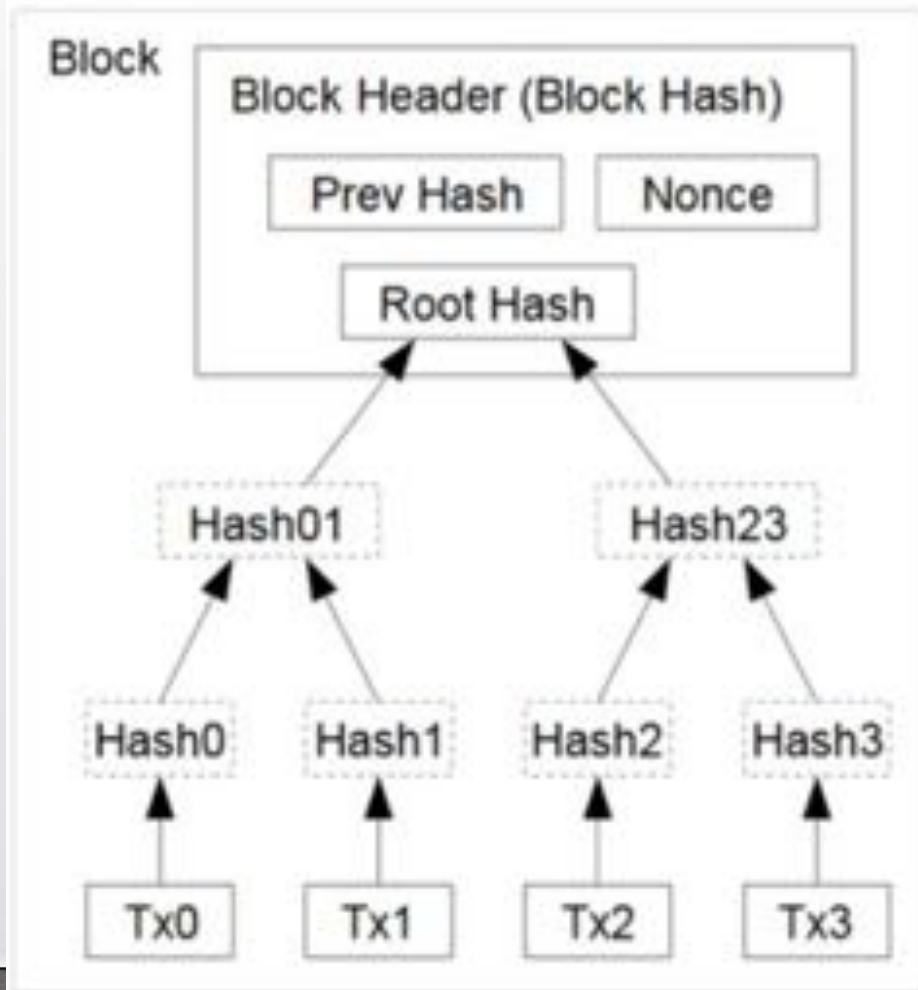
# Block structure



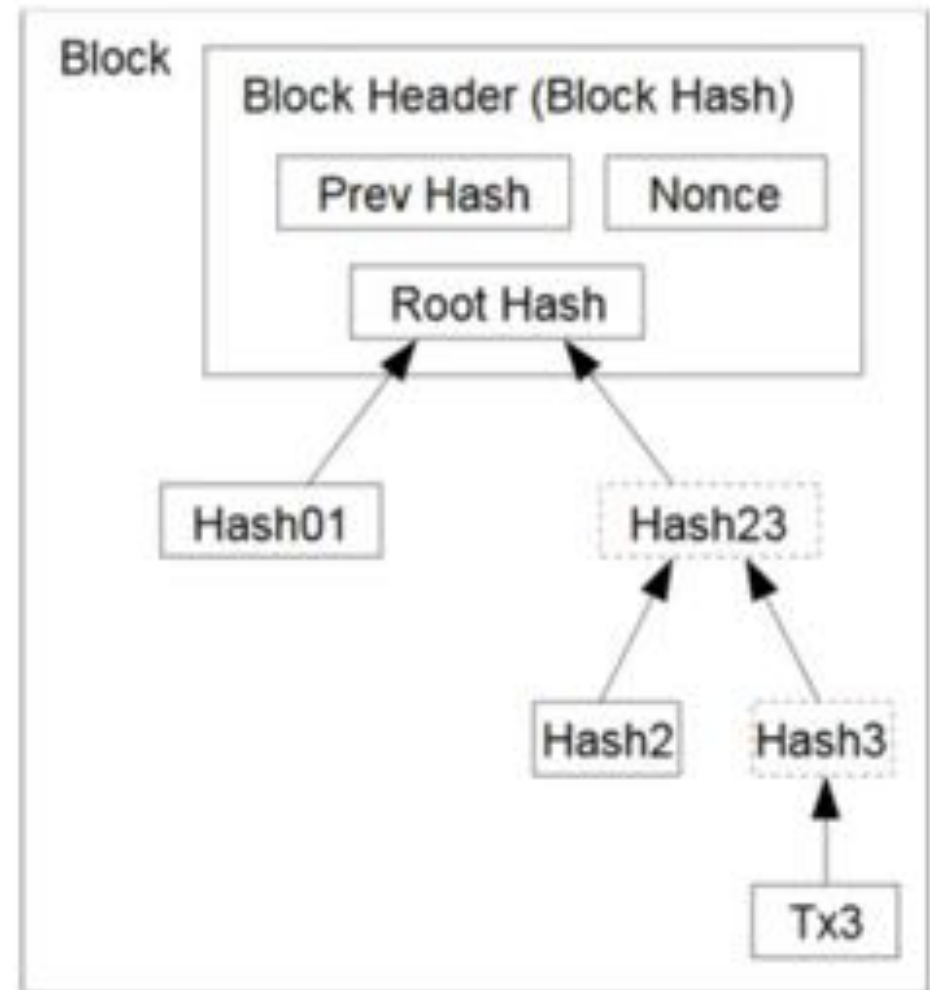
- **Hash consecutiveness:** a block always contains the overall hash value of its previous block.
- Block validation: check the correctness of each block based on its 256 bits overall hash value.



# Merkle Tree

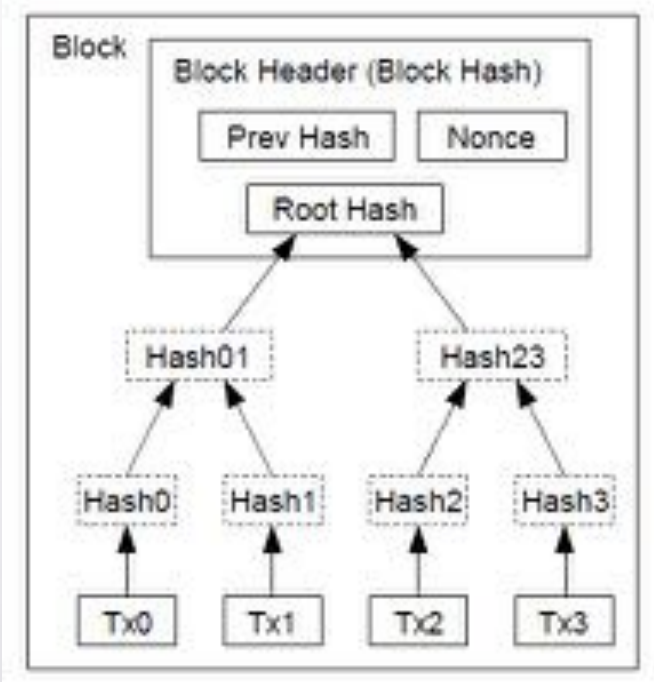


Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

# Why Merkle Tree?



- Transactions are hashed in pairs (still SHA256).
- Most notably, as outlined in the whitepaper, this allows for existence of Simple Payment Verification (SPV) nodes, also known as “lightweight clients”. These nodes do not have to download the entire Bitcoin blockchain, only the block headers of the longest chain.
- The most important benefit of Merkle Tree structure is the ability to authenticate arbitrarily large sets of data through a similar hashing mechanism that is used to verify much smaller amounts of data. The tree is advantageous for distributing large sets of data into manageable smaller parts where the barrier for the verification of integrity is substantially reduced despite the overall larger data size.



Summary	
Number Of Transactions	3251
Output Total	13,034.68792267 BTC
Estimated Transaction Volume	<a href="#">738.25446397</a> BTC
Transaction Fees	<a href="#">0.29329686</a> BTC
Height	<a href="#">589537 (Main Chain)</a>
Timestamp	2019-08-10 21:32:09
Received Time	2019-08-10 21:32:09
Relayed By	<a href="#">F2Pool</a>
Difficulty	9,985,348,008,059.55
Bits	387723321
Size	1214.169 kB
Weight	3998.226 kWU
Version	0x20000000
Nonce	3384837851
Block Reward	12.5 BTC

Hashes	
Hash	<a href="#">000000000000000000000075e3eb7791fafd790f869c9faa4e32467a46ed43ec37b</a>
Previous Block	<a href="#">000000000000000000000017e5cfa2d73a0231b56be77e006a7086f676b3f910ffab</a>
Next Block(s)	<a href="#">00000000000000000000001ab424beddf698f6bb863bb9d4efa911b614c594e578f4</a>
Merkle Root	<a href="#">976d4774b58ffaca5b5c48415c952a49f09899794c2900e4770042bec780810b</a>

Overall hash value of current block  
Overall hash value of previous block  
Transaction root hash

Proof-of-Work mining

---

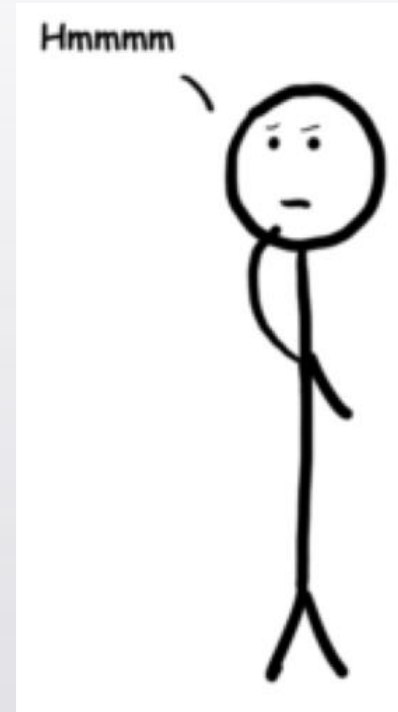
# Blockchain

- Everyone maintain a copy of blockchain.
- Blocks and transactions are almost immutable when they are included in the blockchain.
- Ancient blocks are extremely well protected!

---

# Questions

- Why hash?
- Why Proof-of-Work mining?
- Why blockchain is a chain structure?





# Decentralized/Distributed Consensus

- Many parties safely store and share information, without having to rely on a central authority or trust any other participants in the network.
- Decentralized consensus of blockchain:
  - **Block convergence:** users maintain the same blockchain
- The decentralized consensus of blockchain is supported by:
  - **Proof-of-Work**
  - **Blockchain forking**

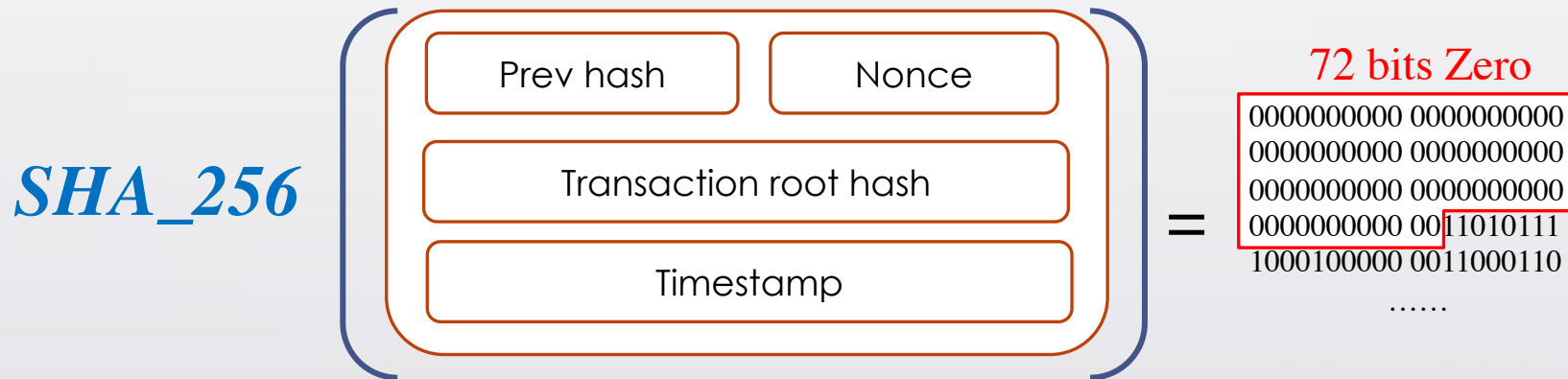


# Decentralized consensus

- Single point failure: a single device failure will not affect the system, because data can be recovered from anyone in the network.
- Easy detection for manipulated information.
- **What's the purpose of having hash and Proof-of-Work (PoW)?**

# Why hash and Proof-of-Work?

- **PoW:** Solving a certain level difficulty of hash puzzle, with a fixed number of leading 0s at the front of overall hash.



- Any tiny modification to the block result in huge change on block hash.
- **A block is easy to be inspected by looking at its hash.**
- **Because of PoW, a block is hard to be re-solved by attackers, if they want to change something inside.**





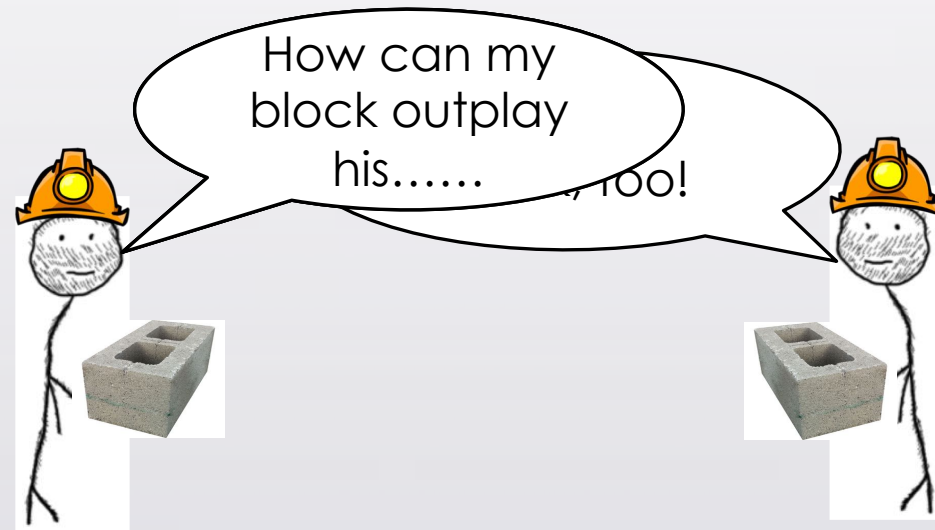
# Why chain structure?

- Satoshi intended to design a new digital currency payment system.
- Transaction history is definitely not allowed to be modified.
- Target on solving the hash puzzle of a single block is still possible.
- But chaining blocks together, the solving workload is linearly increased if the target block is buried deeper.

---

# Blockchain forking

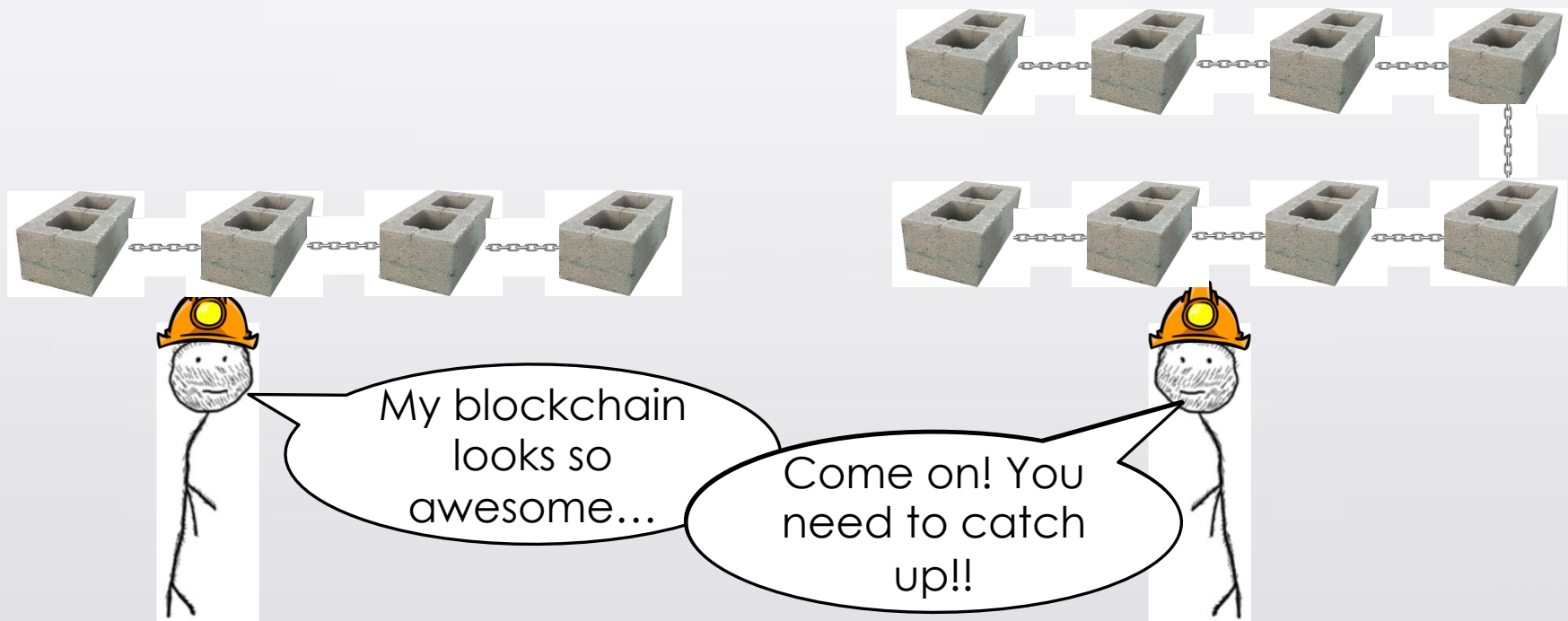
- Internet is a complex environment.





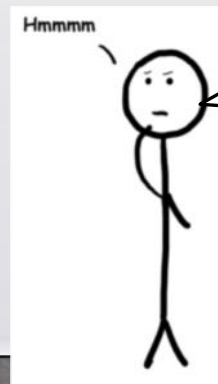
# Blockchain forking

- Or...



# Blockchain forking

- For two simultaneous blocks: other users randomly choose one, and append it to their own blockchain.
- Blockchain users always follow ~~the longest chain~~ if found.

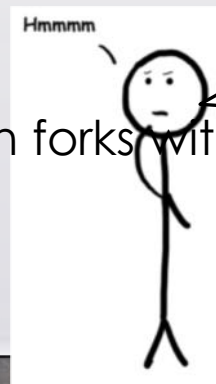


I can produce some easy blocks to gain some easy money!

# Blockchain forking

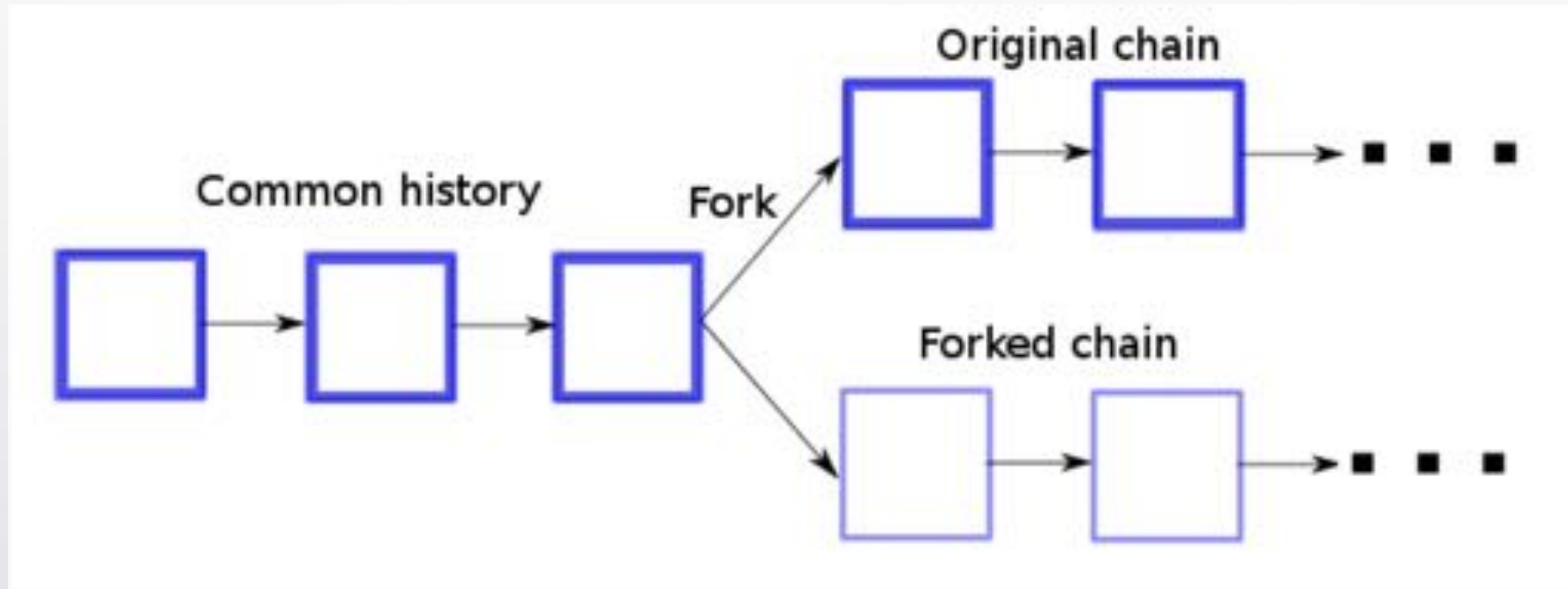
- For two simultaneous blocks: other users randomly choose one, and append it to their own blockchain.
- Blockchain users always follow the hardest-solving and the longest chain, if found.

What if two blockchain forks with the same difficulty and same length?



I can produce some easy blocks to gain some easy money!

# Blockchain forking



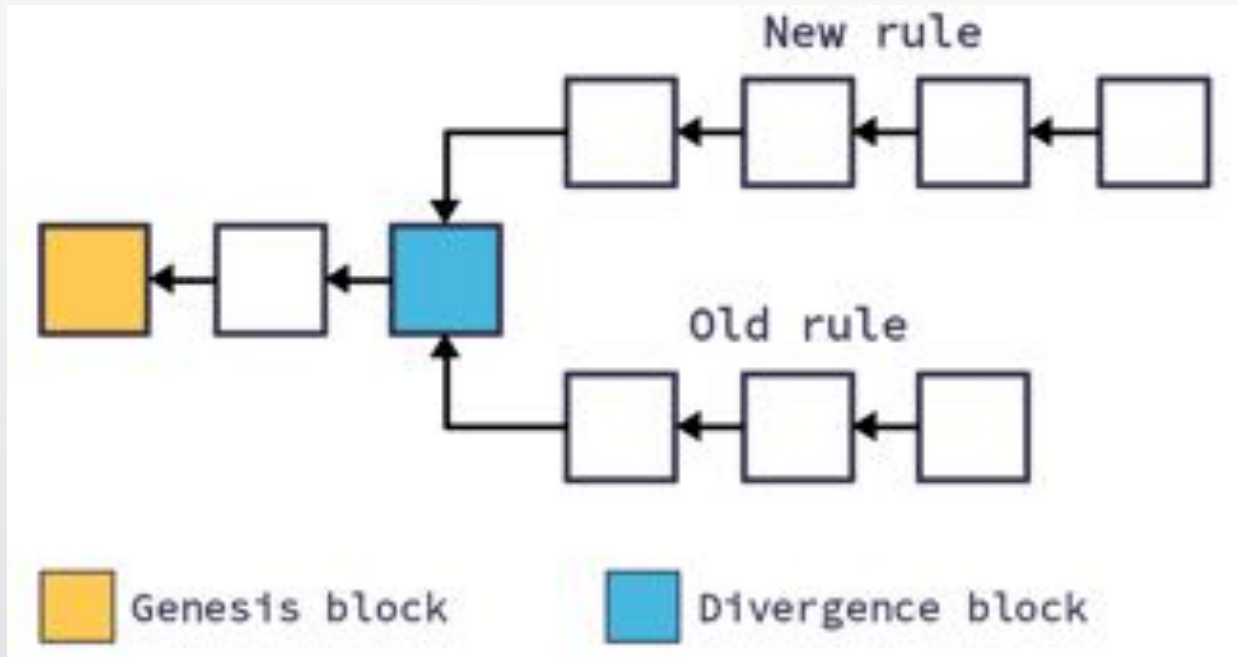
Wait for one of the forks grow longer, and overwrite another.



# More seriously

- What if there is a big change on the protocol?
- E.g. blockchain structure, consensus rule, transaction validating rule, software version upgrading etc.
- Soft fork: new version block is accepted by old version users, but old version block is not valid for new version users.
- Hard fork: old version is invalid. If the old version is still running, they will end up with a different protocol and with different data than the new version.















# Soft fork



- Old version blocks are keep rejected by new version users, thus force them to upgrade.
- More than 15 soft fork events happened since blockchain started, and they are all recorded in **Blockchain Improvement Protocols(BIP)**



# Hard fork

1	 Bitcoin BTC	NZ\$12,649.79	-0.20%	NZ\$227.2B
2	 Ethereum ETH	NZ\$266.42	-1.43%	NZ\$28.8B
3	 XRP XRP	NZ\$0.37	-0.23%	NZ\$16.1B
4	 Bitcoin Cash BCH	NZ\$347.73	+2.24%	NZ\$6.3B
5	 Litecoin LTC	NZ\$85.12	-1.20%	NZ\$5.4B
6	 EOS EOS	NZ\$4.37	-0.63%	NZ\$4.1B
7	 Stellar Lumens XLM	NZ\$0.0901	-1.02%	NZ\$1.8B
8	 Dash DASH	NZ\$109.71	-0.77%	NZ\$994.1M
9	 Chainlink LINK	NZ\$2.68	+4.18%	NZ\$936.7M
10	 Tezos XTZ	NZ\$1.35	-0.21%	NZ\$894.4M
11	 Ethereum Classic ETC	NZ\$7.23	-0.55%	NZ\$822.9M
12	 USD Coin USDC	NZ\$1.55		NZ\$664.0M
13	 Zcash ZEC	NZ\$59.76	+1.82%	NZ\$449.1M
14	 Basic Attention Token BAT	NZ\$0.25	-0.62%	NZ\$338.9M



# Summary of blockchain

- Blockchain technology is surprisingly good in practice.
- All the mechanisms are designed with the purpose of maintaining the consistency of the block convergence state for all users, thus to satisfy decentralized consensus.
- Proof-of-Work with SHA256
- Chain structure
- Blockchain forking
- Other consensus protocols are also designed with the purpose of maintaining agreements between users. Some of them only achieve partially decentralized consensus to reduce the workload and complexity of protocol itself.



Q: What can we buy with bitcoin?

Or with other cryptocurrencies...



# Bitcoin price (BTC)

\$12,654.08 - \$334.17 (2.58%) **\$13,159.46** ALL  
September 29 6:44 AM



1	Bitcoin BTC	NZ\$12,649.79	-0.20%	NZ\$227.2B
2	Ethereum ETH	NZ\$266.42	-1.43%	NZ\$28.8B
3	XRP XRP	NZ\$0.37	-0.23%	NZ\$16.1B
4	Bitcoin Cash BCH	NZ\$347.73	+2.24%	NZ\$6.3B
5	Litecoin LTC	NZ\$85.12	-1.20%	NZ\$5.4B
6	EOS EOS	NZ\$4.37	-0.63%	NZ\$4.1B
7	Stellar Lumens XLM	NZ\$0.0901	-1.02%	NZ\$1.8B
8	Dash DASH	NZ\$109.71	-0.77%	NZ\$994.1M
9	Chainlink LINK	NZ\$2.68	+4.18%	NZ\$936.7M
10	Tezos XTZ	NZ\$1.35	-0.21%	NZ\$894.4M
11	Ethereum Classic ETC	NZ\$7.23	-0.55%	NZ\$822.9M
12	USD Coin USDC	NZ\$1.55		NZ\$664.0M
13	Zcash ZEC	NZ\$59.76	+1.82%	NZ\$449.1M
14	Basic Attention Token BAT	NZ\$0.25	-0.62%	NZ\$338.9M
15	Ox ZRX	NZ\$0.32	-4.54%	NZ\$192.5M
16	Augur REP	NZ\$12.86	-2.07%	NZ\$141.5M
17	Dai DAI	NZ\$1.56	-0.11%	NZ\$124.2M



# Some interesting features of Bitcoin

- Transaction throughput: 7 transactions per second, GLOBALLY!
- Block generation rate: 10 minutes per block, GLOBALLY!
- **Six confirmations:** a transaction can only be committed and transacting parties can finally get paid after 6 blocks are mined.
- You have to wait for **an hour** to receive your payment.
- Hmmmmm.... Why 6?

q	1	2	3	4	5	6	7	8	9	10
2%	4%	0.237%	0.016%	0.001%	$\approx 0$	$\approx 0$	$\approx 0$	$\approx 0$	$\approx 0$	$\approx 0$
4%	8%	0.934%	0.120%	0.016%	0.002%	$\approx 0$	$\approx 0$	$\approx 0$	$\approx 0$	$\approx 0$
6%	12%	2.074%	0.394%	0.078%	0.016%	0.003%	0.001%	$\approx 0$	$\approx 0$	$\approx 0$
8%	16%	3.635%	0.905%	0.235%	0.063%	0.017%	0.005%	0.001%	$\approx 0$	$\approx 0$
10%	20%	5.600%	1.712%	0.546%	0.178%	0.059%	0.020%	0.007%	0.002%	0.001%
12%	24%	7.949%	2.864%	1.074%	0.412%	0.161%	0.063%	0.025%	0.010%	0.004%
14%	28%	10.662%	4.400%	1.887%	0.828%	0.369%	0.166%	0.075%	0.034%	0.016%
16%	32%	13.722%	6.352%	3.050%	1.497%	0.745%	0.375%	0.190%	0.097%	0.050%
18%	36%	17.107%	8.741%	4.626%	2.499%	1.369%	0.758%	0.423%	0.237%	0.134%
20%	40%	20.800%	11.584%	6.669%	3.916%	2.331%	1.401%	0.848%	0.516%	0.316%
22%	44%	24.781%	14.887%	9.227%	5.828%	3.729%	2.407%	1.565%	1.023%	0.672%
24%	48%	29.030%	18.650%	12.339%	8.310%	5.664%	3.895%	2.696%	1.876%	1.311%
26%	52%	33.530%	22.868%	16.031%	11.427%	8.238%	5.988%	4.380%	3.220%	2.377%
28%	56%	38.259%	27.530%	20.319%	15.232%	11.539%	8.810%	6.766%	5.221%	4.044%
30%	60%	43.200%	32.616%	25.207%	19.762%	15.645%	12.475%	10.003%	8.055%	6.511%
32%	64%	48.333%	38.105%	30.687%	25.037%	20.611%	17.080%	14.226%	11.897%	9.983%
34%	68%	53.638%	43.970%	36.738%	31.058%	26.470%	22.695%	19.548%	16.900%	14.655%
36%	72%	59.098%	50.179%	43.330%	37.807%	33.226%	29.356%	26.044%	23.182%	20.692%
38%	76%	64.691%	56.698%	50.421%	45.245%	40.854%	37.062%	33.743%	30.811%	28.201%
40%	80%	70.400%	63.488%	57.958%	53.314%	49.300%	45.769%	42.621%	39.787%	37.218%
42%	84%	76.205%	70.508%	65.882%	61.938%	58.480%	55.390%	52.595%	50.042%	47.692%
44%	88%	82.086%	77.715%	74.125%	71.028%	68.282%	65.801%	63.530%	61.431%	59.478%
46%	92%	88.026%	85.064%	82.612%	80.480%	78.573%	76.836%	75.234%	73.742%	72.342%
48%	96%	94.003%	92.508%	91.264%	90.177%	89.201%	88.307%	87.478%	86.703%	85.972%
50%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Table 1: The probability of a successful double spend, as a function of the attacker’s hashrate  $q$  and the number of confirmations  $n$ .



# Some interesting features of Bitcoin

- Not good enough to work for our daily financial activity.
- As a currency, bitcoin is able to be exchanged to real-world money, but:
  - Extreme dynamic exchange rate
  - Lack of government control



# Other decentralized consensus

- To solve the privacy, complexity, scalability, transaction throughput, and my other issues...
- Proof-of-Stake (PoS), Delegated Proof-of-Stake(DPoS)
- Proof-of-activity (PoA)
- Hyperledger: hybrid blockchain
- Avalanche
- Many others...






















# Blockchain 2.0

- Decentralized application platform
- Smart contract, rather than transfer of currency:
  - a programming script
  - One or a serious conditions that must be satisfied.
  - Expand the functionality of blockchain
- Ethereum: 15 transactions/second, 3 seconds/block

# Blockchain 3.0

- Ethereum still has a low transaction throughput (15tx/second)
- More efficient, higher scalability than Blockchain 2.0
- Apply blockchain in more domains
- EOS: 500ms/block, 1 million transactions (they announced)

1	 Bitcoin BTC	NZ\$12,649.79	-0.20%	NZ\$227.2B
2	 Ethereum ETH	NZ\$266.42	-1.43%	NZ\$28.8B
3	 XRP XRP	NZ\$0.37	-0.23%	NZ\$16.1B
4	 Bitcoin Cash BCH	NZ\$347.73	+2.24%	NZ\$6.3B
5	 Litecoin LTC	NZ\$85.12	-1.20%	NZ\$5.4B
6	 EOS EOS	NZ\$4.37	-0.63%	NZ\$4.1B
7	 Stellar Lumens XLM	NZ\$0.0901	-1.02%	NZ\$1.8B
8	 Dash DASH	NZ\$109.71	-0.77%	NZ\$994.1M
9	 Chainlink LINK	NZ\$2.68	+4.18%	NZ\$936.7M
10	 Tezos XTZ	NZ\$1.35	-0.21%	NZ\$894.4M
11	 Ethereum Classic ETC	NZ\$7.23	-0.55%	NZ\$822.9M
12	 USD Coin USDC	NZ\$1.55		NZ\$664.0M
13	 Zcash ZEC	NZ\$59.76	+1.82%	NZ\$449.1M
14	 Basic Attention Token BAT	NZ\$0.25	-0.62%	NZ\$338.9M
15	 Ox ZRX	NZ\$0.32	-4.54%	NZ\$192.5M
16	 Augur REP	NZ\$12.86	-2.07%	NZ\$141.5M
17	 Dai DAI	NZ\$1.56	-0.11%	NZ\$124.2M



# Blockchain 4.0

- Not yet...

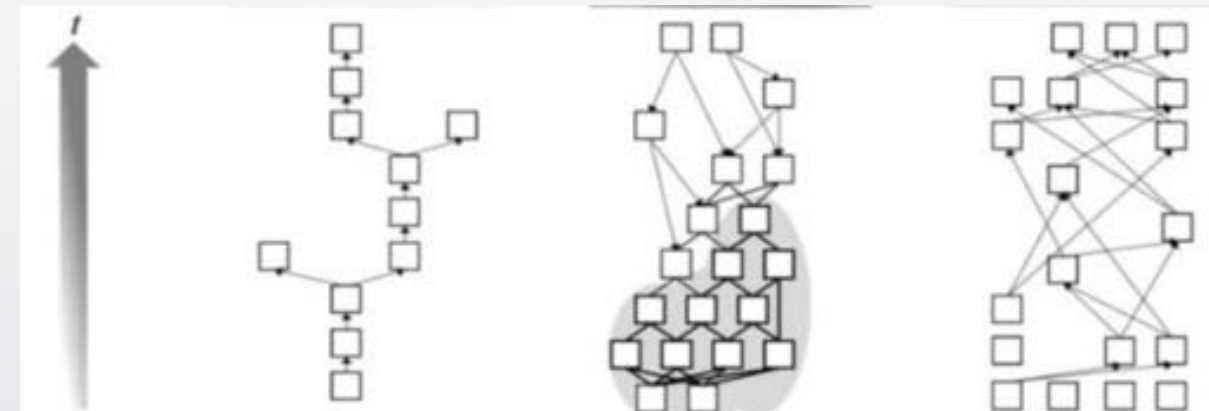


# Applications Beyond Cybercurrency

- Internet-of-Things
- Government
- Medical and Charity
- Market
- ...

# Future Trends

- Industry:
  - Applications, scalability
  - Higher transaction throughput, block generation speed
- Academic:
  - More efficient consensus, achieved by:
    - Less computation and communication
    - Low storage consumption
  - Against various types of attack



<b>Technology</b>	Block chain	Directed acyclic graph	Directed acyclic graph
<b>Copyright</b>	Open source	Open source	Patented
<b>Consensus</b>	Proof of Work: SHA256-Hash	Proof of Work: check of Tangle tip	Virtual voting
<b>Openness</b>	Public ledger	Public ledger	Private ledger
<b>Applications</b>	Bitcoin	Iota	Swirls
<b>Efficiency (tps)</b>	3-4	500-800	> 250,000



Thanks!