Join Our Telegram

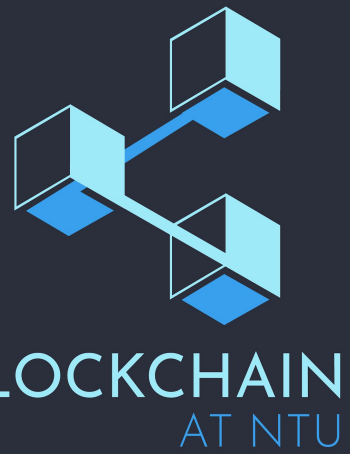
https://t.me/ntublockchain

BLOCKCHAIN AT NTU

Lecture 2:

Nakamoto Consensus & Bitcoin Protocol

Alex Xiong



Who Are We

BLOCKCHAIN
AT NTU

What We Do

Education | R&D | Consulting

BLOCKCHAIN
AT NTU

Agenda

- **Motivation**: Pre-Bitcoin Area
- **Blockchain**: Data Structure for Secure Digital Ledger
- **Pseudonymity**: Identity on Bitcoin
- **Nakamoto Consensus**: Coming to Agreement
- **Bitcoin Protocol**: Putting All Together

Goal:

Secure digital cash with pseudonymity without central authority

data structure & cryptography

identity on Bitcoin

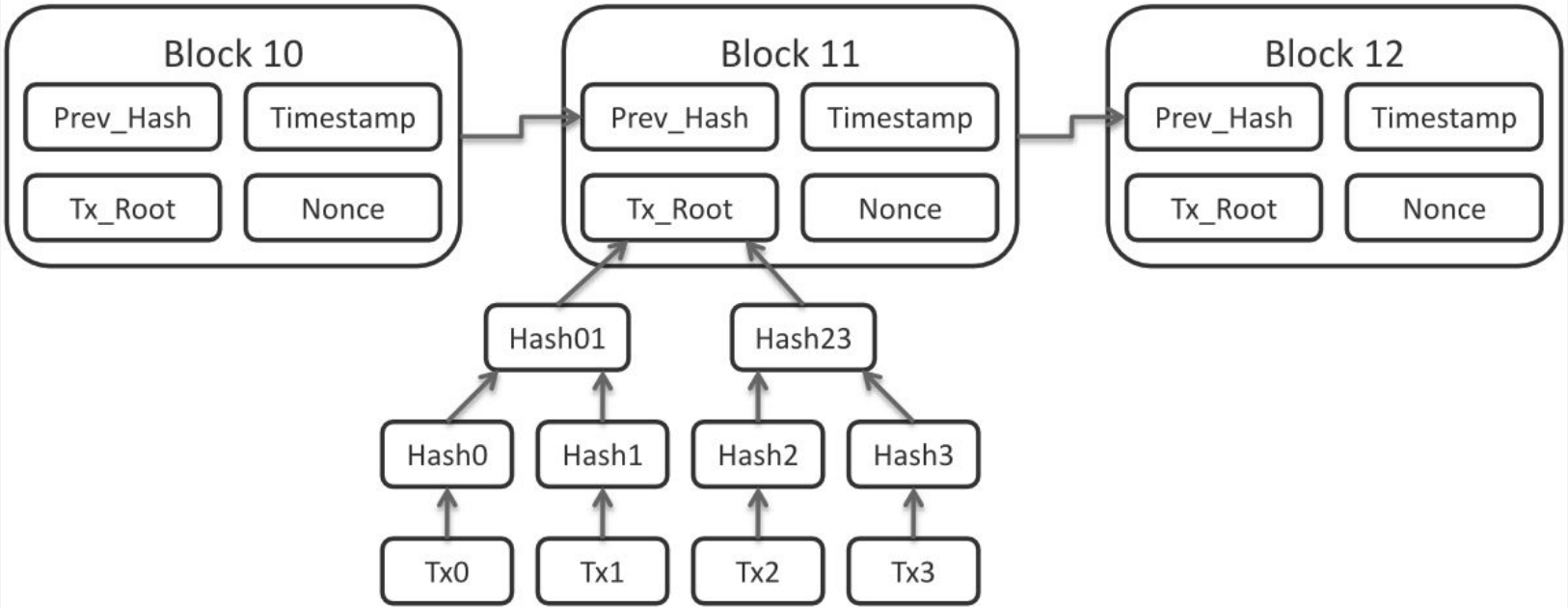
distributed consensus

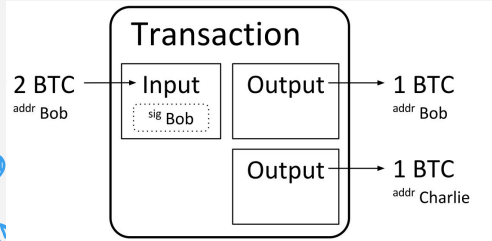
Agenda

- **Motivation**: Pre-Bitcoin Area
- **Blockchain**: Data Structure for Secure Digital Ledger
- **Pseudonymity**: Identity on Bitcoin
- **Nakamoto Consensus**: Coming to Agreement
- **Bitcoin Protocol**: Putting All Together

Revision

Previously on Lecture 1:

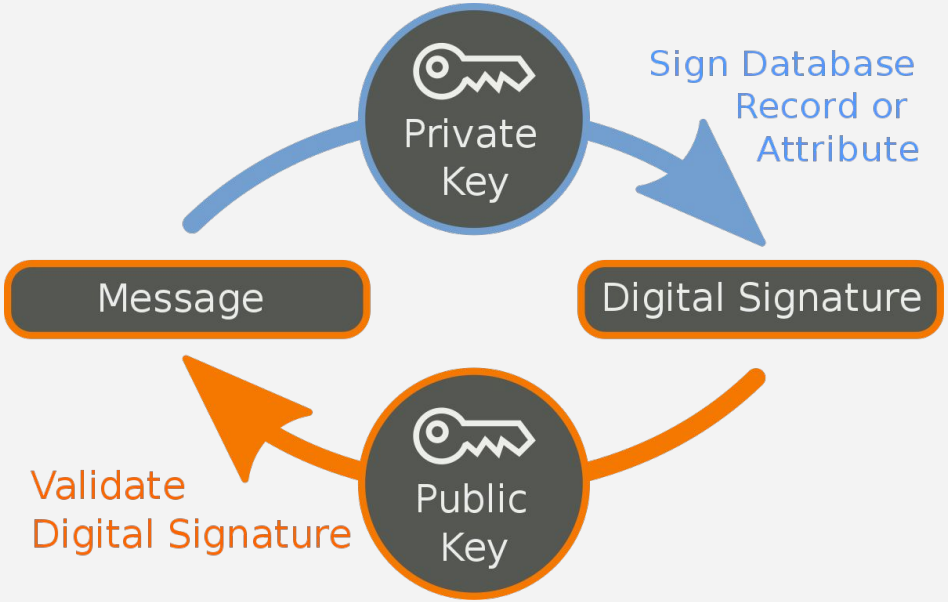




BLOCKCHAIN AT NTU

Revision

- DSA: what & why?



Revision

- DSA: what & why?
- Hash: what & what properties & example?

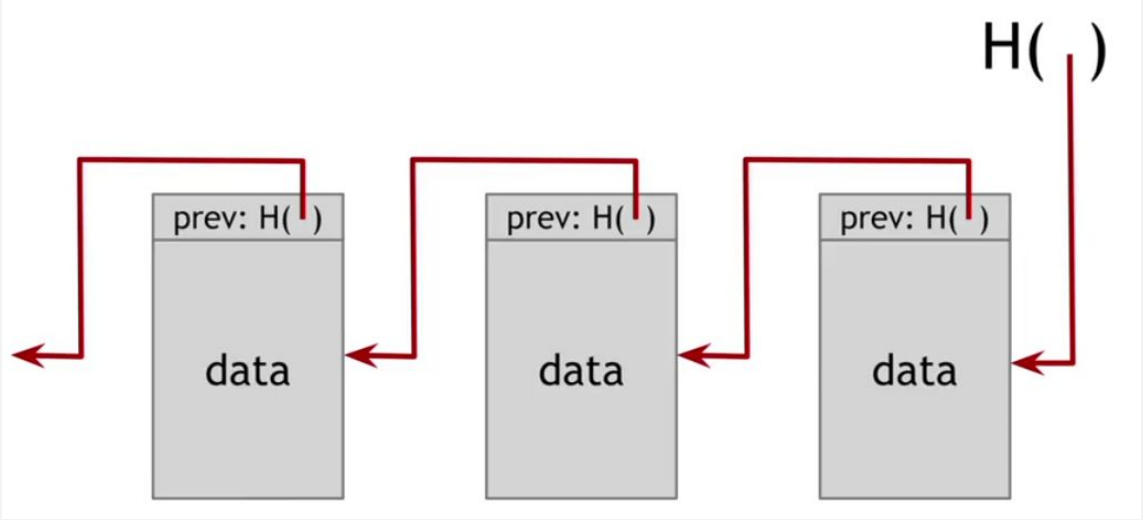
```
alex@alex:~$ cat test
NTU is No.11 on QS ranking, higher than Yale, Princeton, Cornell, John
 Hopkins, Duke, Tsinghua...

The list goes on and on... bragging, showing off, being pround without
 knowing why, trashtalking, trashtaking, trashtalking.

Come bite me!
alex@alex:~$ sha1sum test
59cfd628ef278db56cf2ed635912d6bfb16cae63  test
```

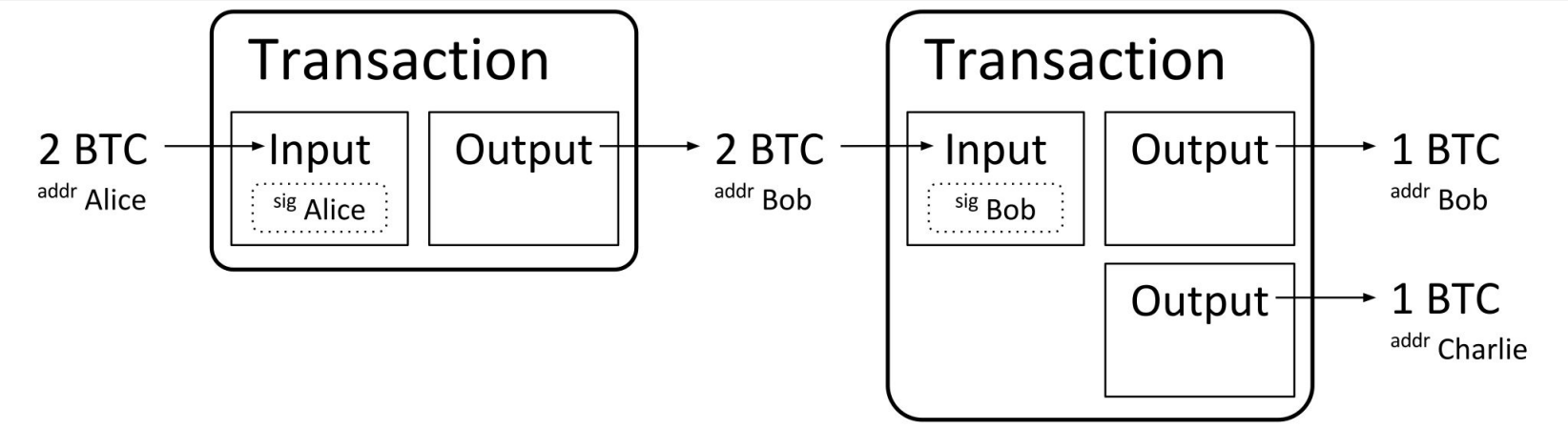
Revision

- DSA: what & why?
- Hash: what & what properties & example?
- Hash Pointer: what & why?



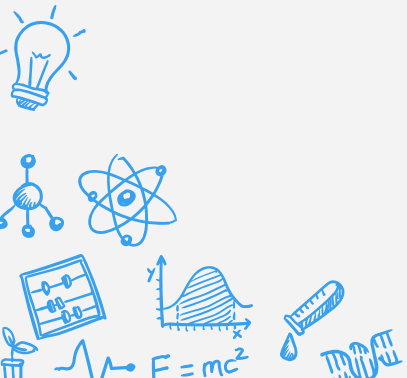
Revision

- ❑ DSA: what & why?
- ❑ Hash: what & what properties & example?
- ❑ Hash Pointer: what & why?
- ❑ UTXO: what & internal fields?



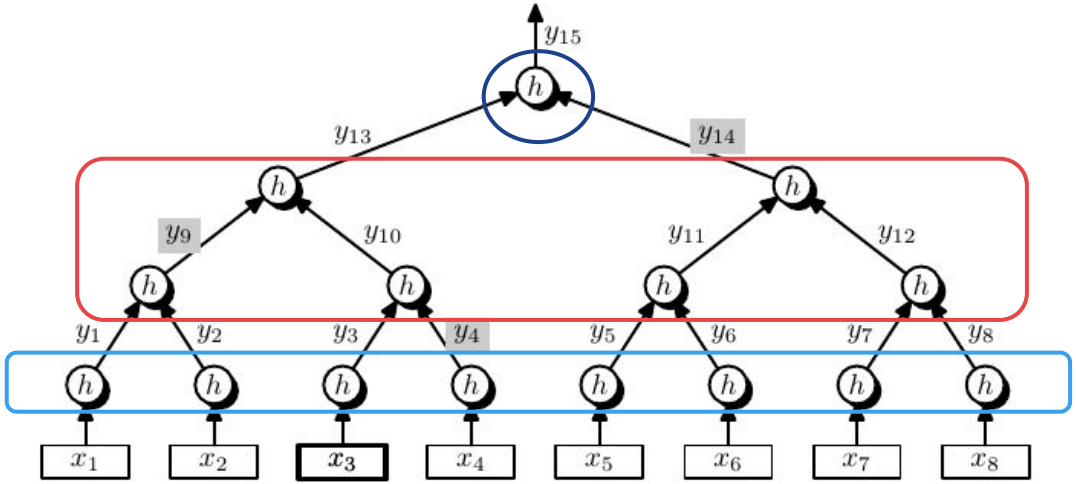
Revision

- ❑ DSA: what & why?
- ❑ Hash: what & what properties & example?
- ❑ Hash Pointer: what & why?
- ❑ UTXO: what & internal fields?
- ❑ Merkle Tree: why & what & why useful?

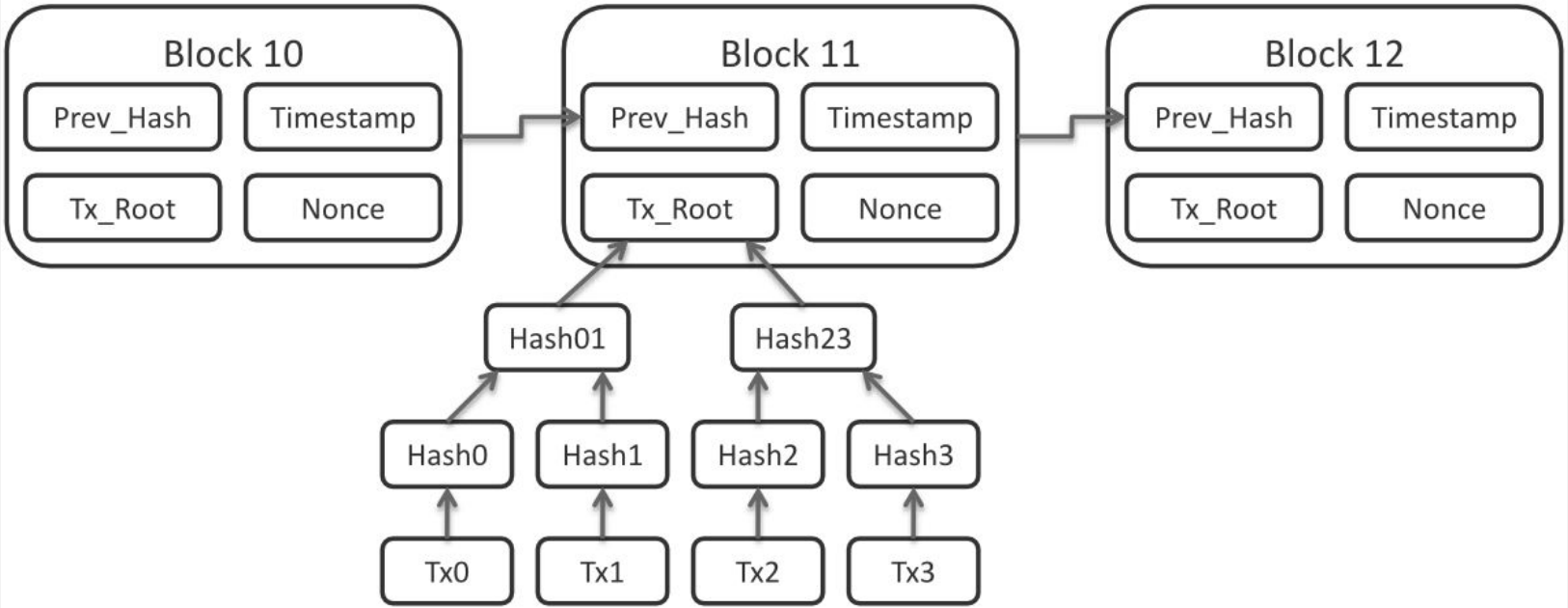


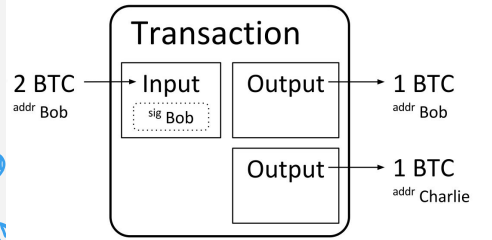
Revision: Merkle Tree

- Leaf node value = H (tx content)
- Intermediate node value = H (left_child || right_child)
- Only ***root hash*** is included in block header
- Proof of membership: ***Merkle Path***
  - $\log_2(n) * 256$ proof size
  - v.s. n*256 proof size



Revision: Picture Description





BLOCKCHAIN AT NTU

Revision: properties

- ❑ Non-repudiation
- ❑ Tamper-evident → double spending evident
- ❑ Efficient proof of membership (historical look-up)
- ❑ Permissionless network

Goal:

Secure digital cash
with pseudonymity
without central authority

What does “authority” entail ?

		
Who maintain the ledger?	Bank	
Who decides which tx to include?	Bank	
Who gets to proposed next block?	Bank	
Who creates new coin/prints cash?	Government	

With Central Authority

Without Central Authority?

BLOCKCHAIN AT NTU

Bitcoin Consensus

		
Who maintain the ledger?	Bank	Full node
Who decides which tx to include?	Bank	Individual miner*
Who gets to proposed next block?	Bank	“hardworking” miner
Who creates new coin/prints cash?	Government	“hardworking” miner

Roles in Bitcoin

- Miners
  - Ledger **maintainer** & tx validity **verifier**
  - New **block producer**
- Full nodes
  - Miner or not to miner
  - Ledger maintainer (keep a copy)
- Light nodes*
  - Only store the block header, not entire block
- Users
  - Send transactions to miners
  - Query history & balance from full nodes

Consensus in Bitcoin

1. New TX broadcasted to all nodes (gradually)
2. Miners collect all new TXs, verifies them and put them into the next block he is building.
3. Each round, one “**random**” lucky miner gets to proposed *his* block.
4. Other miners verify the proposed block
5. Other miners (implicitly) express their acceptance by building their next block *on top* of the proposed block

Consensus in Bitcoin

1. New TX broadcasted to all nodes (gradually)
2. Miners collect all new TXs, verifies them and put them into the next block he is building.
3. Each round, one "**random**" lucky miner gets to proposed *his* block.
4. Other miners verify the proposed block
5. Other miners (implicitly) express their acceptance by building their next block *on top* of the proposed block

TX:

Input: UTXO #20 [4]

Output: $\text{Address}_{\text{Bob}}$

Amount: 10 BTC

Signature: 0x23abf464...

TX:

Input: UTXO #20 [4]

Output: $\text{Address}_{\text{Bob}}$

Amount: 10 BTC

Signature: 0x23abf464...

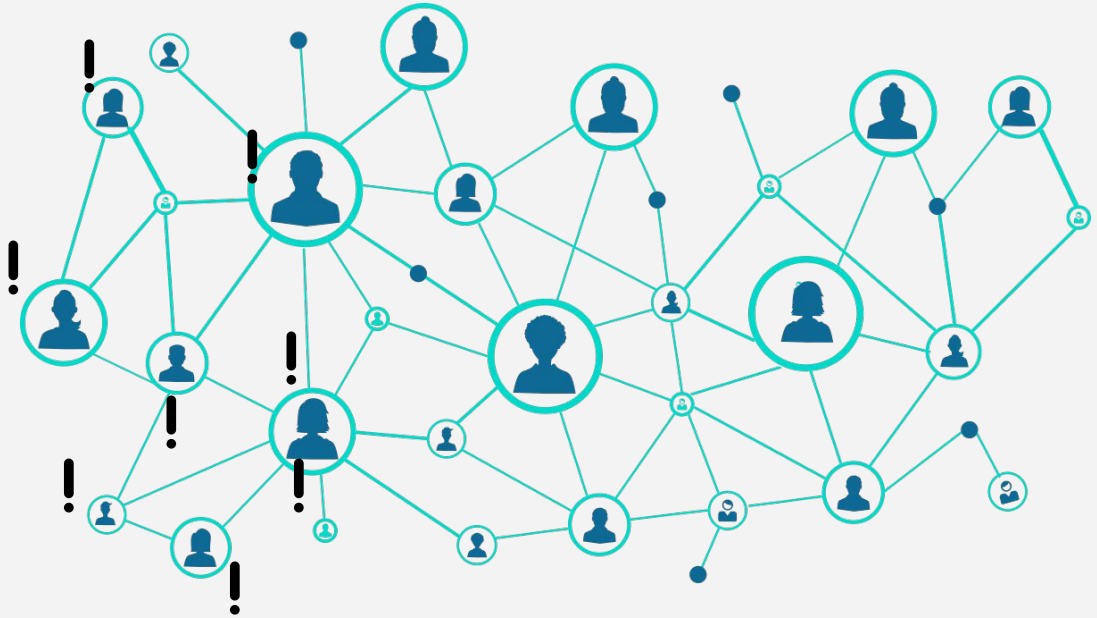
TX:

Input: UTXO #20 [4]

Output: $\text{Address}_{\text{Bob}}$

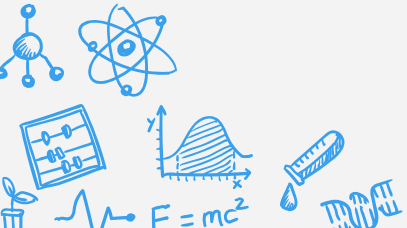
Amount: 10 BTC

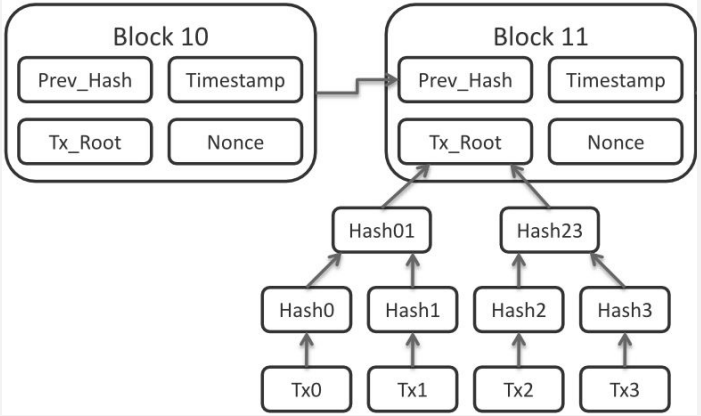
Signature: 0x23abf464...



Consensus in Bitcoin

1. New TX broadcasted to all nodes (gradually)
2. Miners collect all new TXs, verifies them and put them into the next block he is building.
3. Each round, one "**random**" lucky miner gets to proposed *his* block.
4. Other miners verify the proposed block
5. Other miners (implicitly) express their acceptance by building their next block *on top* of the proposed block





TX:

Input: UTXO #20 [4]
Output: $Address_{Bob}$
Amount: 10 BTC
Signature: 0x23abf464...

Consensus in Bitcoin

1. New TX broadcasted to all nodes (gradually)
2. Miners collect all new TXs, verifies them and put them into the next block he is building.
3. Each round, one "**random**" lucky miner gets to proposed *his* block.
4. Other miners verify the proposed block
5. Other miners (implicitly) express their acceptance by building their next block *on top* of the proposed block

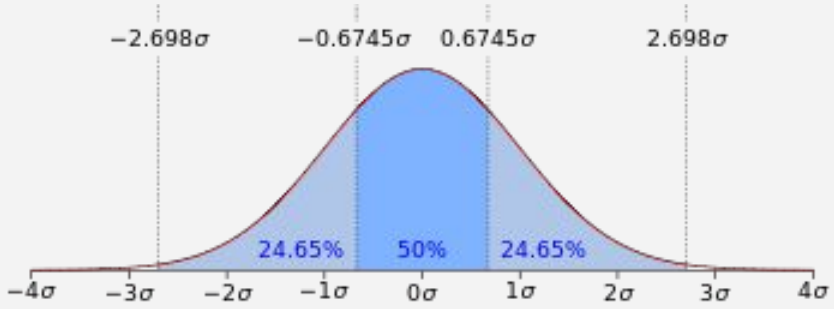
Proof of Work

- "Non-monopolizable" resource : Computation Power
- **Computation Puzzle**:
  - H (nonce || pre_hash || timestamp || tx merkle root) < **difficulty level**

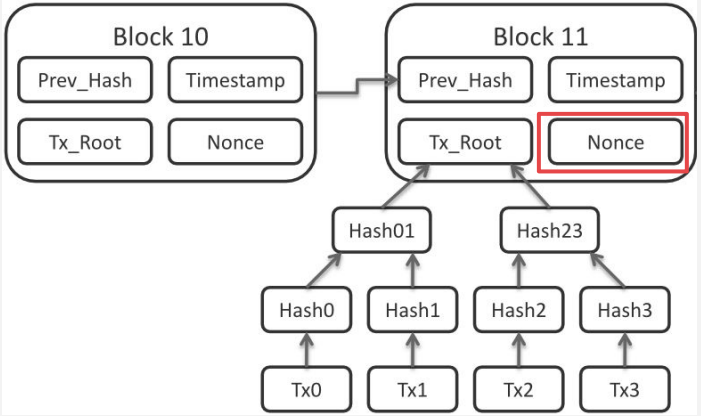
```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Proof of Work

- “Non-monopolizable” resource : Computation Power
- **Computation Puzzle**:
  - H (nonce || pre_hash || timestamp || tx merkle root) < **difficulty level**
  - Hard to find (brutal force), trivial to verify
  - How long does it take to solve? → ~ 10 min, but adjustable

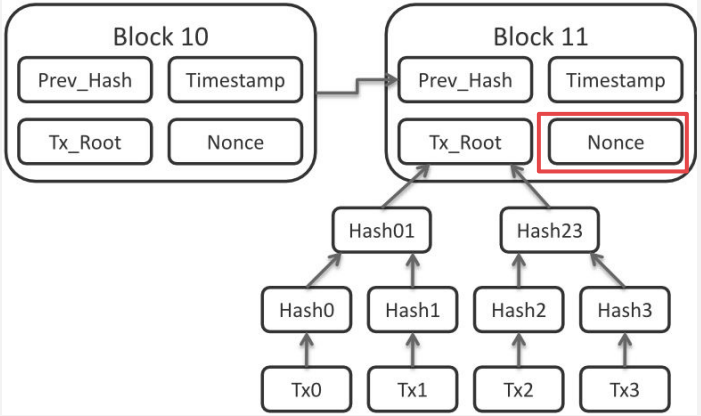


BLOCKCHAIN AT NTU



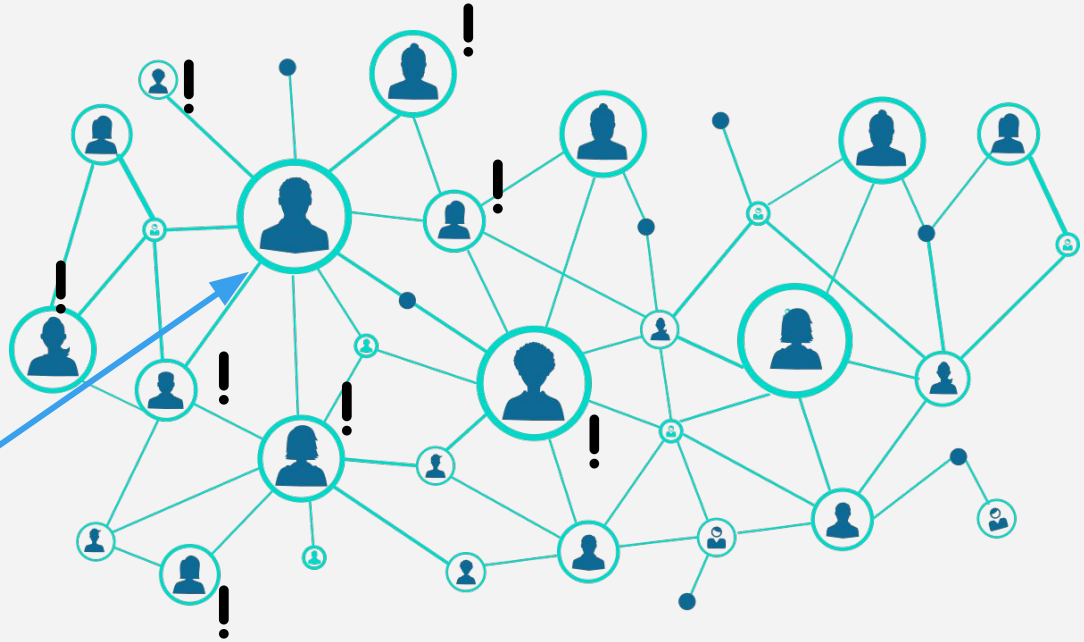
TX:

Input: UTXO #20 [4]
Output: $Address_{Bob}$
Amount: 10 BTC
Signature: 0x23abf464...



TX:

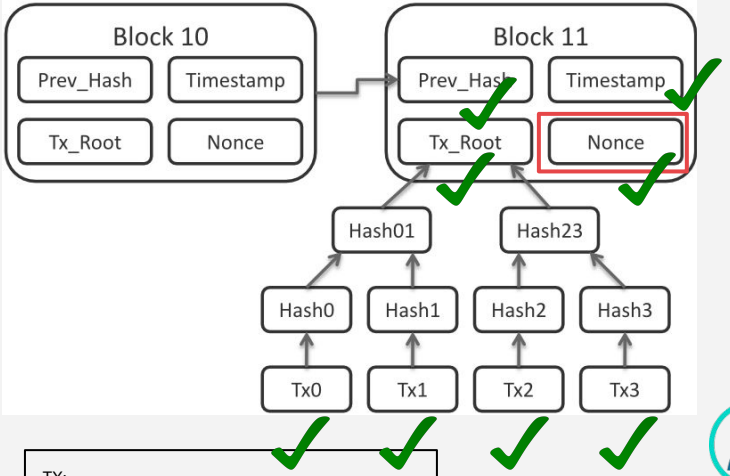
Input: UTXO #20 [4]
Output: $Address_{Bob}$
Amount: 10 BTC
Signature: 0x23abf464...



BLOCKCHAIN AT NTU

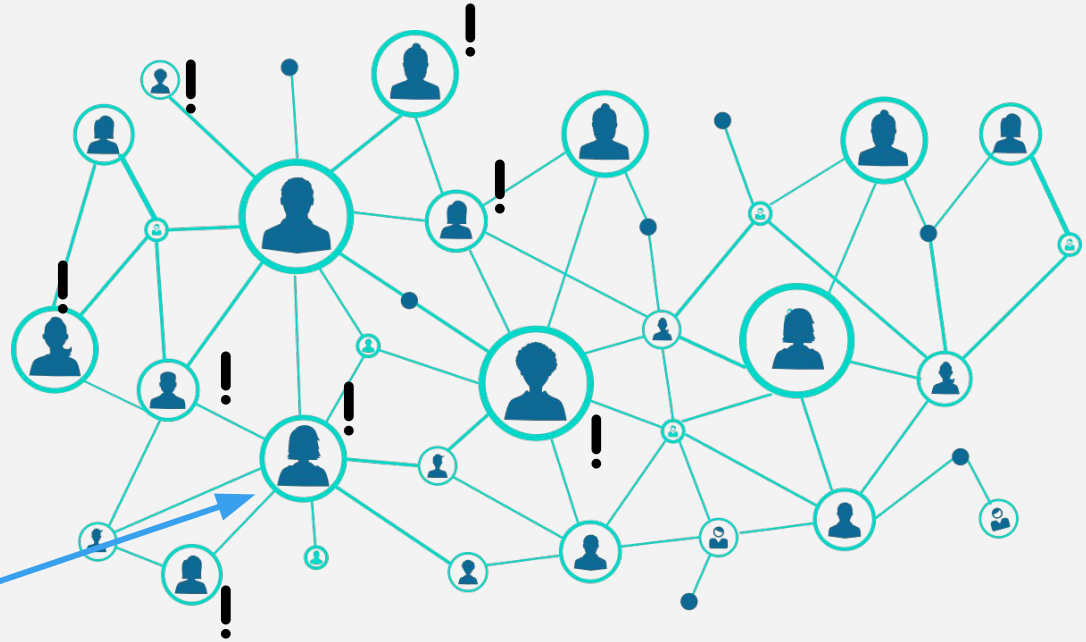
Consensus in Bitcoin

1. New TX broadcasted to all nodes (gradually)
2. Miners collect all new TXs, verifies them and put them into the next block he is building.
3. Each round, one "**random**" lucky miner gets to proposed *his* block.
4. Other miners verify the proposed block
5. Other miners (implicitly) express their acceptance by building their next block *on top* of the proposed block



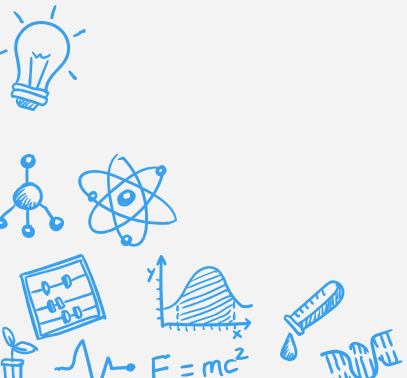
TX:

Input: UTXO #20 [4]
Output: $\text{Address}_{\text{Bob}}$
Amount: 10 BTC
Signature: 0x23abf464...



Other Miners Checking

- ❑ Validity of all TX included, their signatures on spending UTXO
- ❑ Correctness of Merkle root
- ❑ Correctness of pre_hash & strictly larger timestamp
- ❑ Correctness of nonce, s.t. *H (block header) < difficulty level*
- ❑ And...

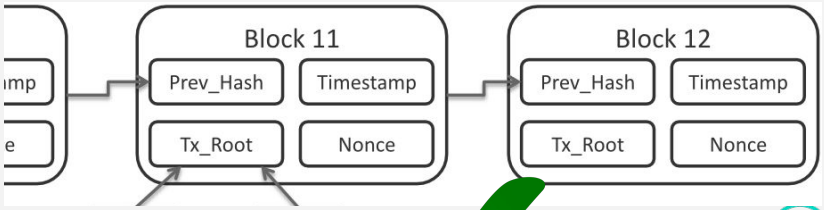


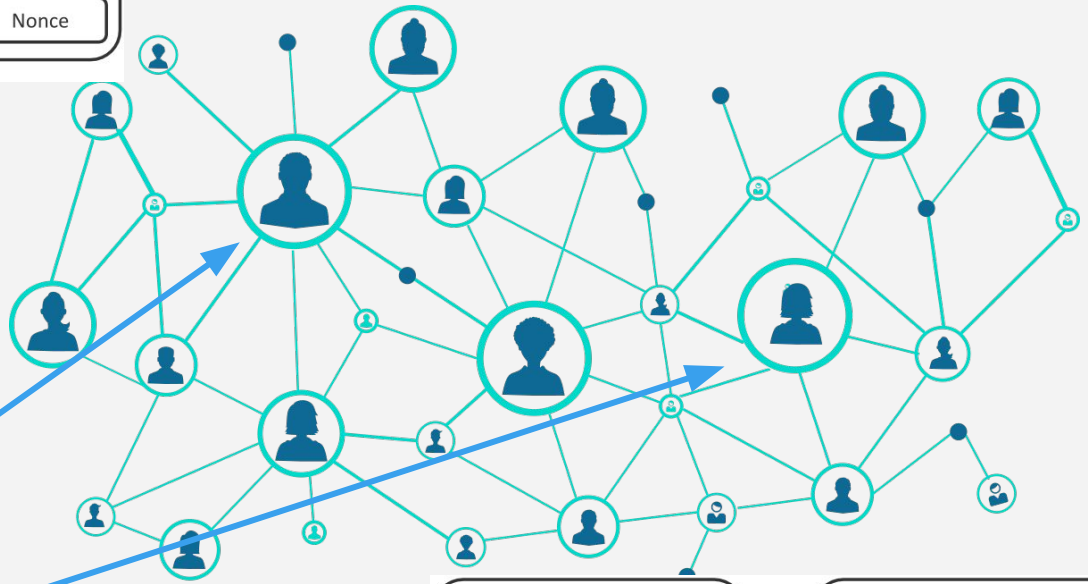
Consensus in Bitcoin

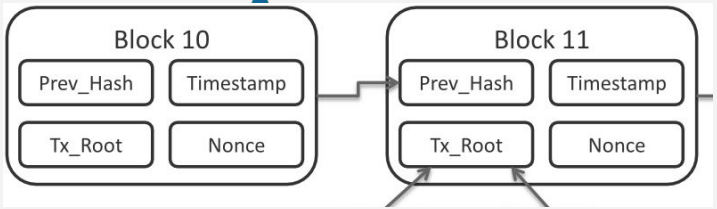
1. New TX broadcasted to all nodes (gradually)
2. Miners collect all new TXs, verifies them and put them into the next block he is building.
3. Each round, one "**random**" lucky miner gets to proposed *his* block.
4. Other miners verify the proposed block
5. Other miners (implicitly) express their acceptance by building their next block *on top* of the proposed block

What’s the consensus?

Longest Chain Wins !







BLOCKCHAIN AT NTU

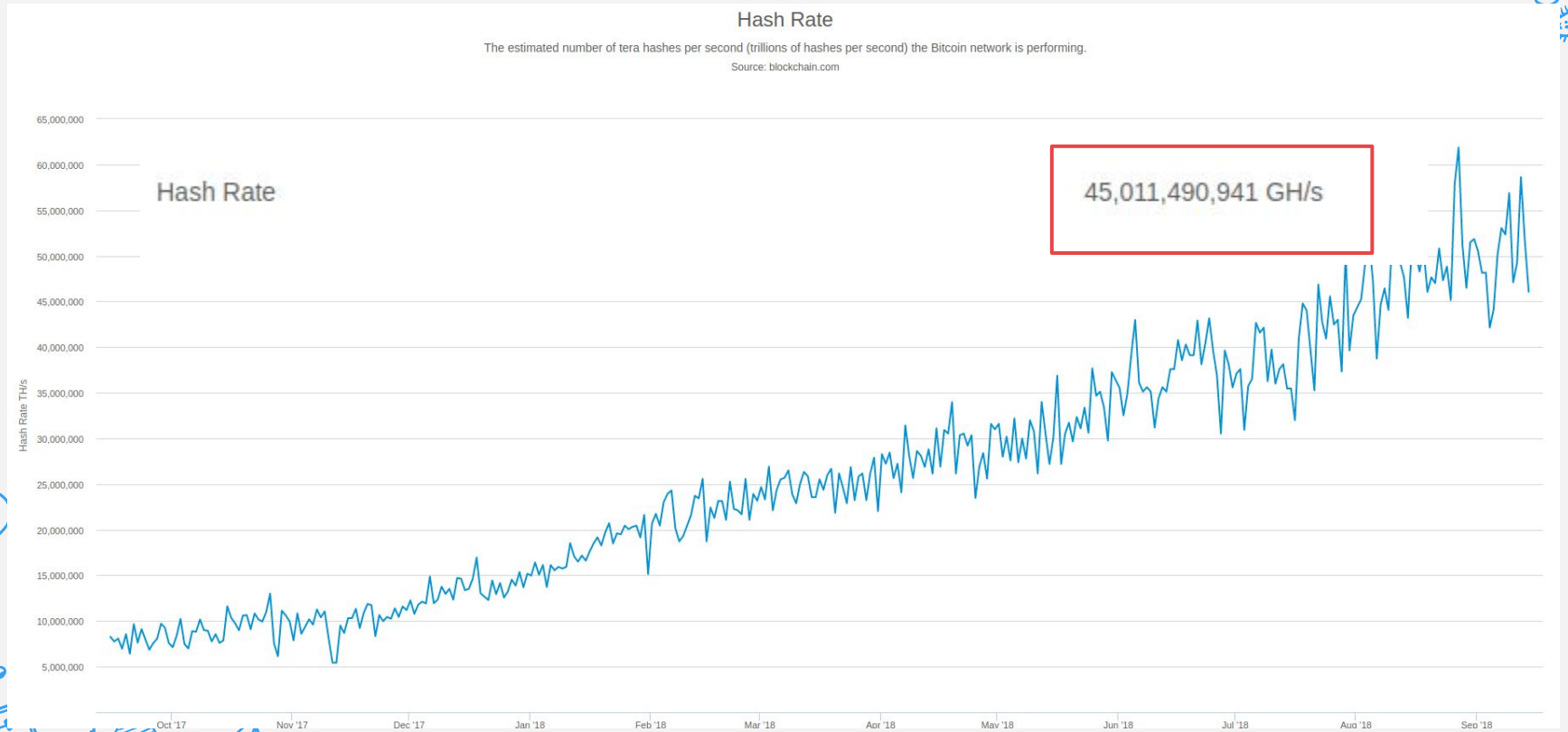
Nakamoto Consensus

- Proof of Work
- Longest chain wins
  - Canonical chain

Nakamoto Consensus :: Analysis

- Why decentralized?
  - Every miner could compete, **probabilistically become the first** to solve the puzzle
  - Anyone dominates the PoW race?

Nakamoto Consensus :: Analysis



BLOCKCHAIN AT NTU

Incentive in Bitcoin

- Block Reward
  - ↳ Allowed to include one “**coin creation**” transaction in the new block

Consensus in Bitcoin

1. New TX broadcasted to all nodes (gradually)
2. Miners collect all new TXs, verifies them and put them into the next block he is building.
3. Each round, one "**random**" lucky miner gets to proposed *his* block.
4. Other miners verify the proposed block*
5. Other miners (implicitly) express their acceptance by building their next block *on top* of the proposed block

Incentive in Bitcoin

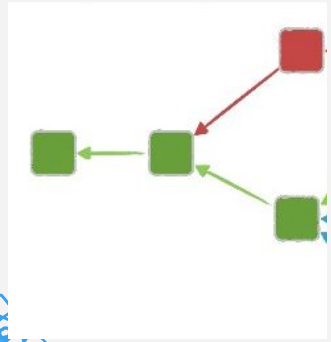
- Block Reward
  - Allowed to include one "**coin creation**" transaction in the new block
  - 12.5 BTC/block, halves every 210,000 block
  - Total supply: **21 million BTC** (Year 2040)
- Transaction Fee
  - Tx fee = **Σ**(output amount) - **Σ**(input UTXO)
  - "*Ledger maintenance as a service*"

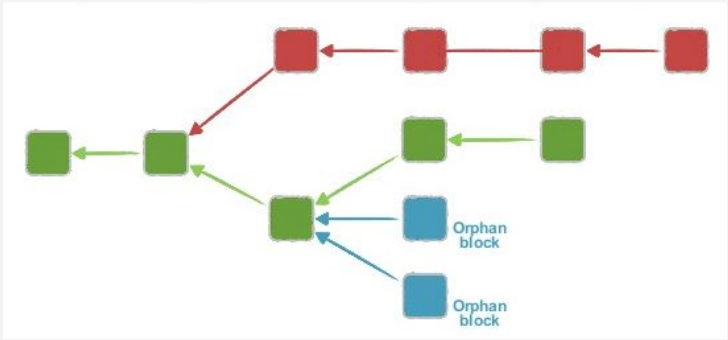
Nakamoto Consensus :: Analysis

- Why decentralized?
  - Every miner could compete, **probabilistically become the first** to solve the puzzle
  - Anyone dominates the PoW race?
- Will ever agree?
  - TX that block didn't include? TX that I didn't hear about before?
  - Invalid block get accepted?
  - Ignore valid block mined by others?
  - Hearing **multiple valid solutions** at around the same time?

Nakamoto :: Attack !!

- Revert the chain !
  - Pay for commodity, wait for TX included in green block
  - Secretly build another red block excluding the payment tx
  - Once commodity is delivered, broadcast a longer red chain
  - History Reverted !!

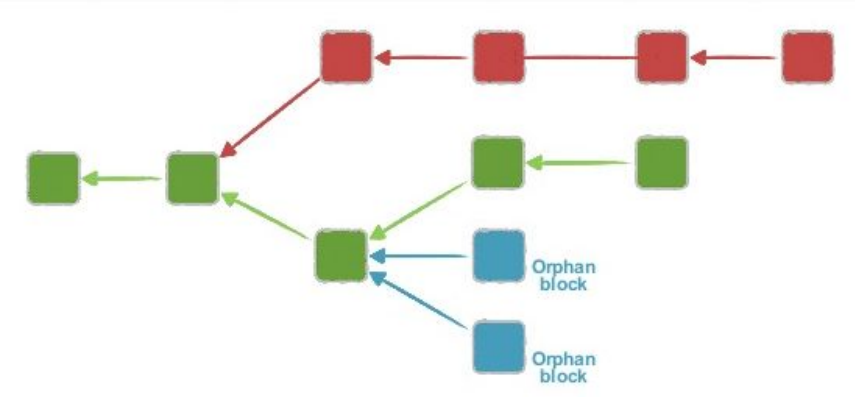




BLOCKCHAIN AT NTU

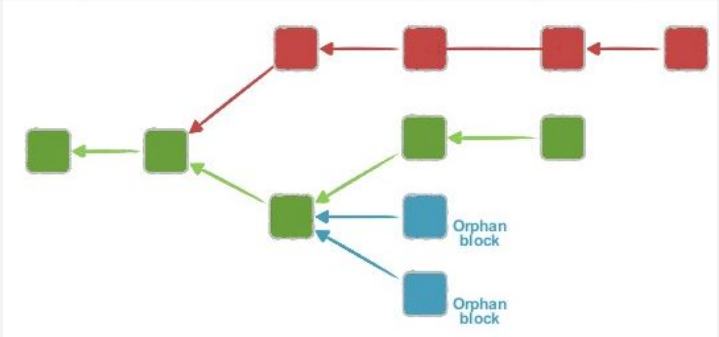
Nakamoto :: Attack Analysis

- How likely would the attack succeed?
  - *Will you be able to find a valid block faster than the rest of the network*?
  - **51% attack**



Nakamoto :: Chain Fork Rule

- **Fork**s: two versions of history
  - Temporary fork (i.e. divergence on current view of blockchain state)
  - Wait longer for confirmations
- **Confirmation**s: depth from the latest mined block
  - Likelihood of attack with X confirmations.
  - Recommended: **6 block** / 1 hour



BLOCKCHAIN AT NTU

Nakamoto Consensus :: Analysis

- Why decentralized?
  - Every miner could compete, **probabilistically become the first** to solve the puzzle
  - Anyone dominates the PoW race?
- Will ever agree?
  - TX that block didn't include? TX that I didn't hear about before?
  - Invalid block get accepted?
  - Ignore valid block mined by others?
  - Hearing **multiple valid solutions** at around the same time?
- Why censorship resistance?

Bitcoin Consensus

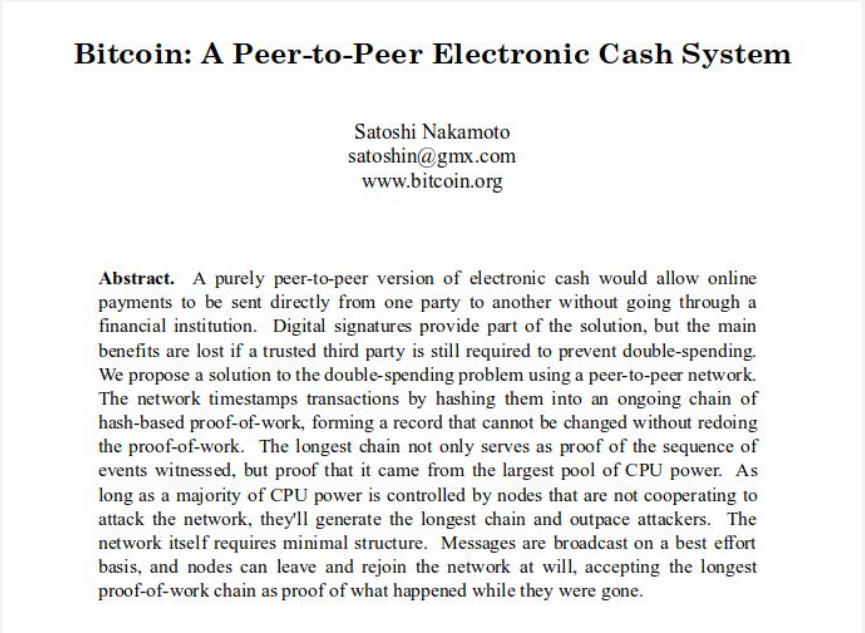
		
Who maintain the ledger?	Bank	Full node
Who decides which tx to include?	Bank	Individual miner*
Who gets to proposed next block?	Bank	“hardworking” miner
Who creates new coin/prints cash?	Government	“hardworking” miner

Goal:

Secure digital cash
with pseudonymity
without central authority

Bitcoin Whitepaper

Satoshi Nakamoto



Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

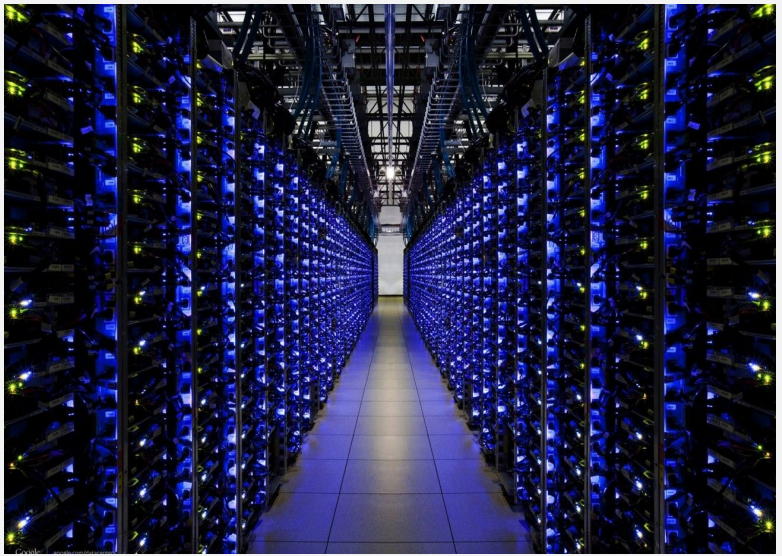
BLOCKCHAIN AT NTU

Always Ask For More!

- Is fork necessarily bad?
  - **Hard fork**: backward **incompatible** changes
    - e.g. block size, hash function choice, block rewards
  - **Soft fork**: backward **compatible** changes
    - Some new functionalities (cover next time: bitcoin script)

Always Ask For More!

- Mining Pool
  - Coordinated puzzle solving
  - Reduce ROI variance
  - Centralization risk?
  - 51% attack?



Conclusion

- **Motivation**: Pre-Bitcoin Area
- **Blockchain**: Data Structure for Secure Digital Ledger
- **Pseudonymity**: Identity on Bitcoin
- **Nakamoto Consensus**: Coming to Agreement
- **Bitcoin Protocol**: Putting All Together

Assignment

- Reviewing:
  - Visualize Bitcoin consensus flow
- Reading:
  - <How does blockchain works> second half
  - Bitcoin Whitepaper
- Thinking:
  - What are some problems with Proof of Work?
  - Continue on “proof of non-membership” solution

Thank you!

🔨 with 💙 by

👷 Alex Xiong

💬 https://t.me/ntublockchain