FISF130020: Introduction to Computer Science

Lecture 11. Blockchain

Hui Xu

xuh@fudan.edu.cn

Outline

❖ 1. Distributed Ledger

❖ 2. Bitcoin and Blockchain

❖ 3. Smart Contract

❖ 4. In-class Practice

1. Distributed Ledger

Distributed Ledger

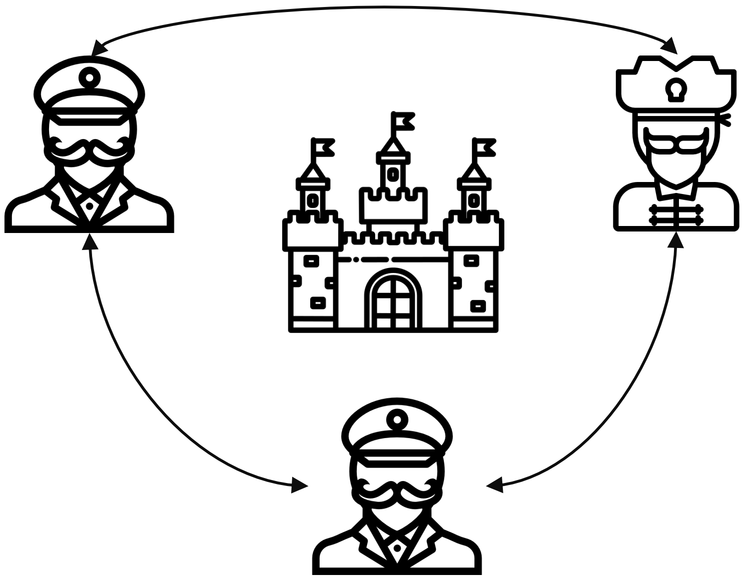
- A decentralized database.
- Maintained across multiple locations or nodes.
- Each participant has a synchronized copy of all records.
- Each transaction is recorded across all nodes.
- Ensure consistency without the need for a central authority.

Challenge

- How to ensure the consistency among all nodes?
  - E.g., multiple nodes could update the ledger simultaneously?
  - We need a consensus algorithm.
- What if there are malicious participants?
  - Is it possible for them to update the ledger for their own benefits?

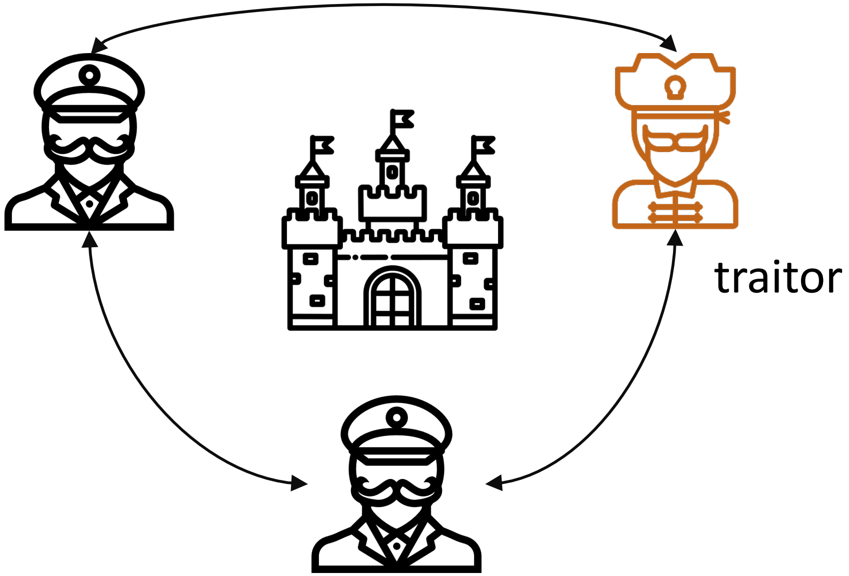
Byzantine Generals Problem

- Several generals of the Byzantine army surround a city.
- They need to agree on a common strategy: either attack or retreat.
- To succeed, all of them should reach a consensus.
- Each general can sending messages to every other generals.
- If all generals are loyal, the challenge is trivial.



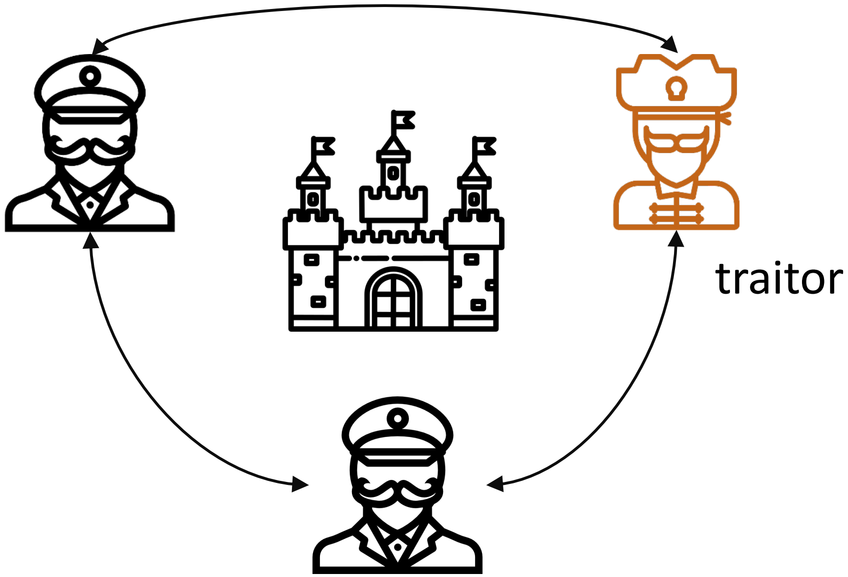
Byzantine Generals Problem

- However, some generals might be traitors, who will try to confuse or mislead the loyal generals into failing to reach consensus.
- To succeed, the loyal generals must ensure that:
    - Agreement: All loyal generals agree on the same plan.
    - Validity: If all loyal generals decide on a plan, it should be the correct one (not influenced by traitors).

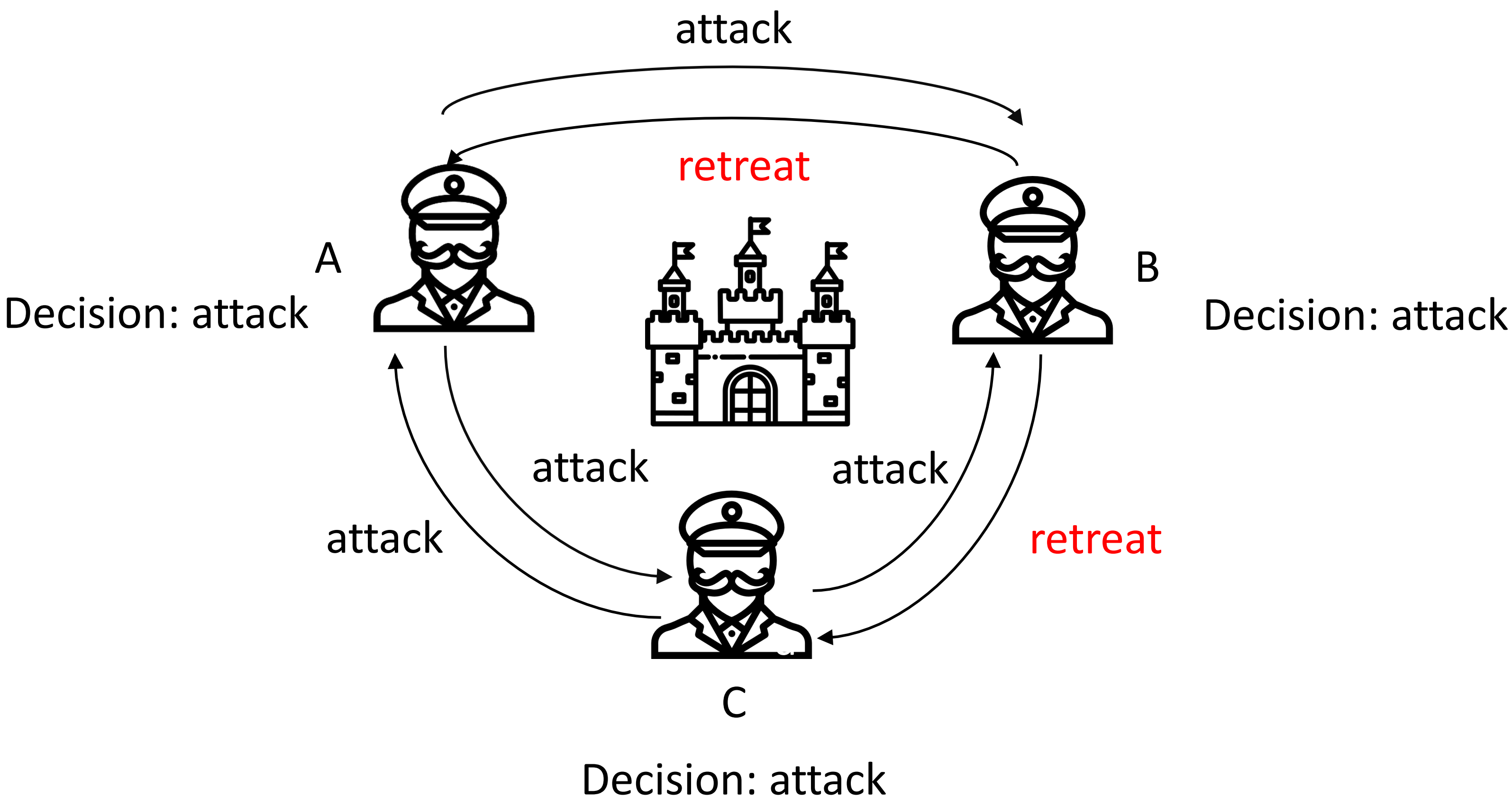


Assumption

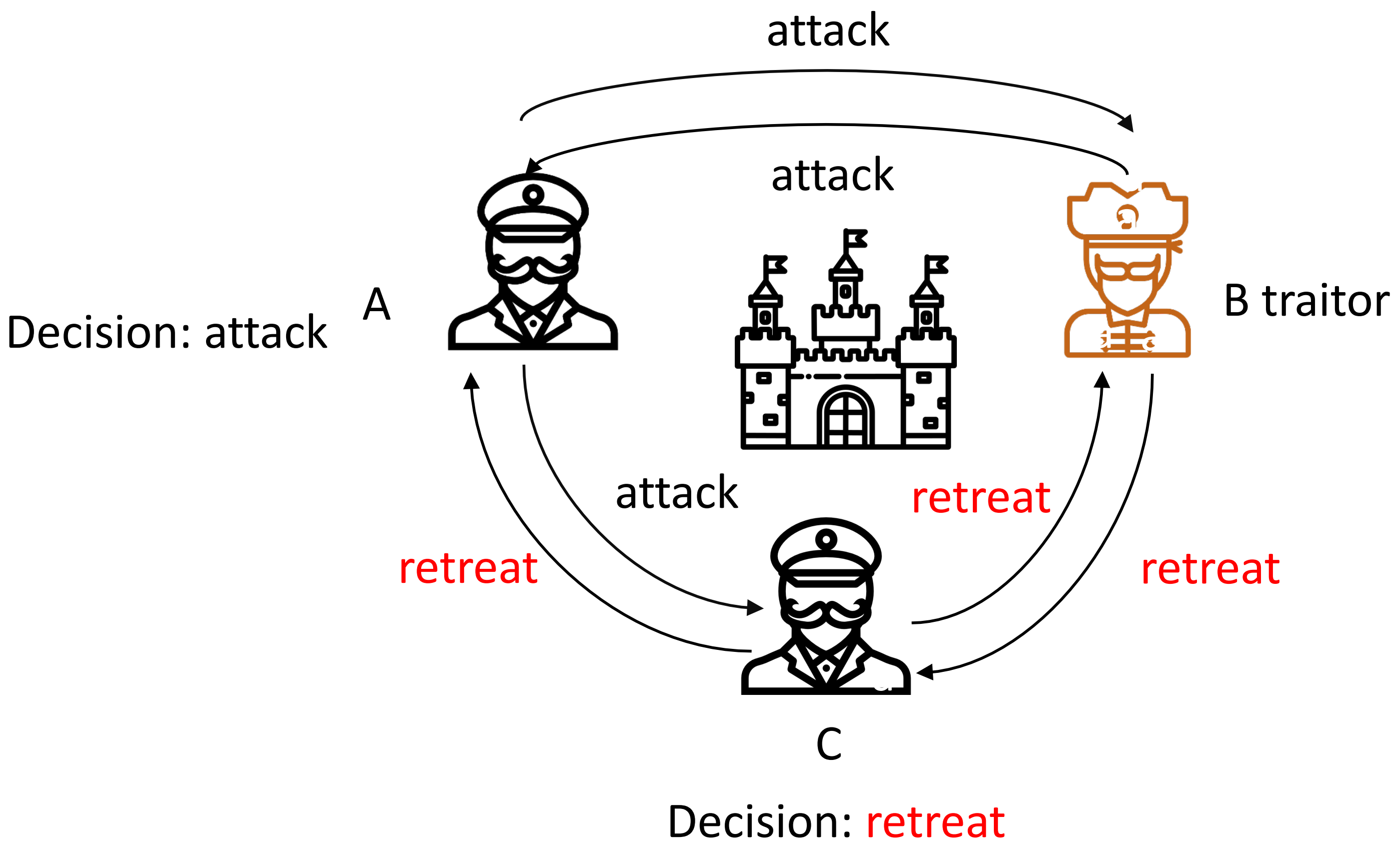
- Communication is synchronous.
- How many generals at least are needed to ensure consensus?



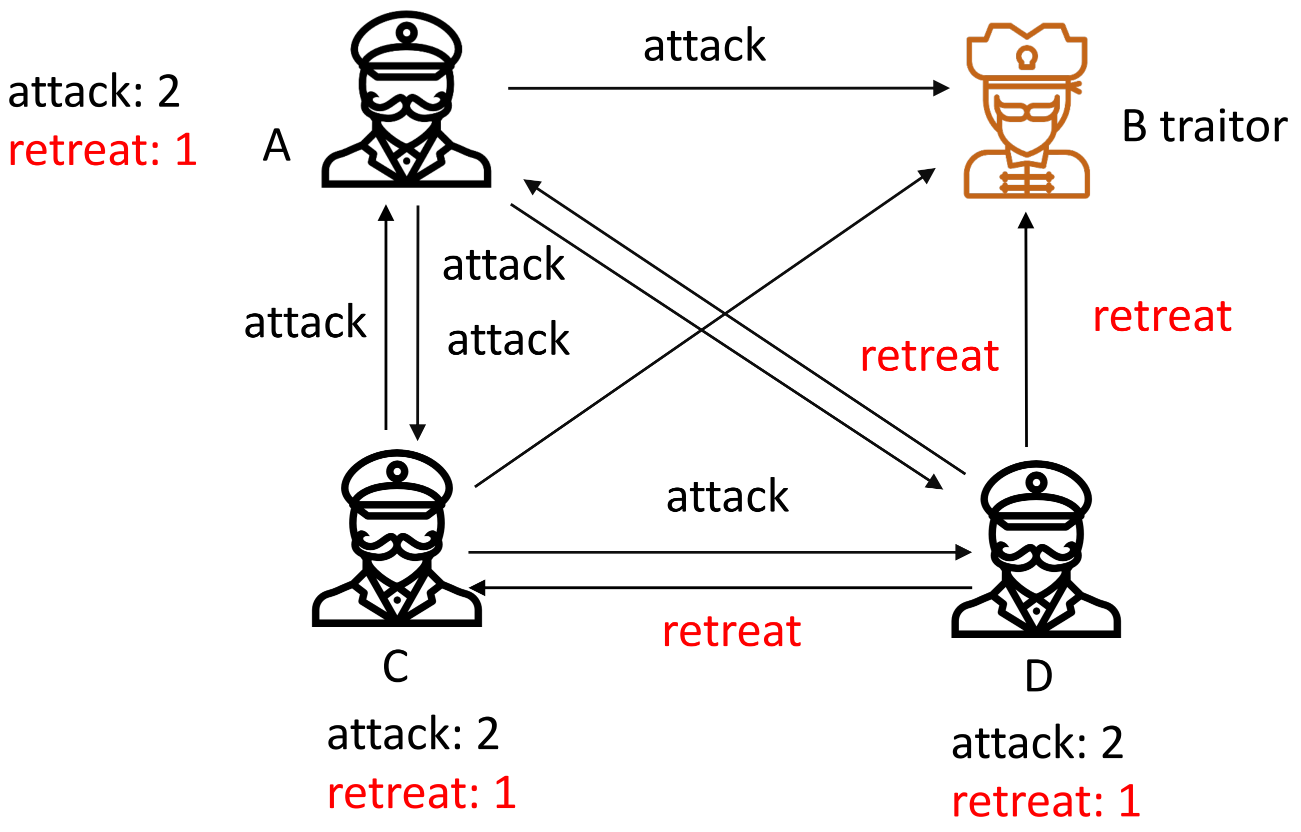
Example: 3 Generals with no Traitor



Example: 3 Generals with 1 Traitor



Example: 4 or More Generals with 1 Traitor



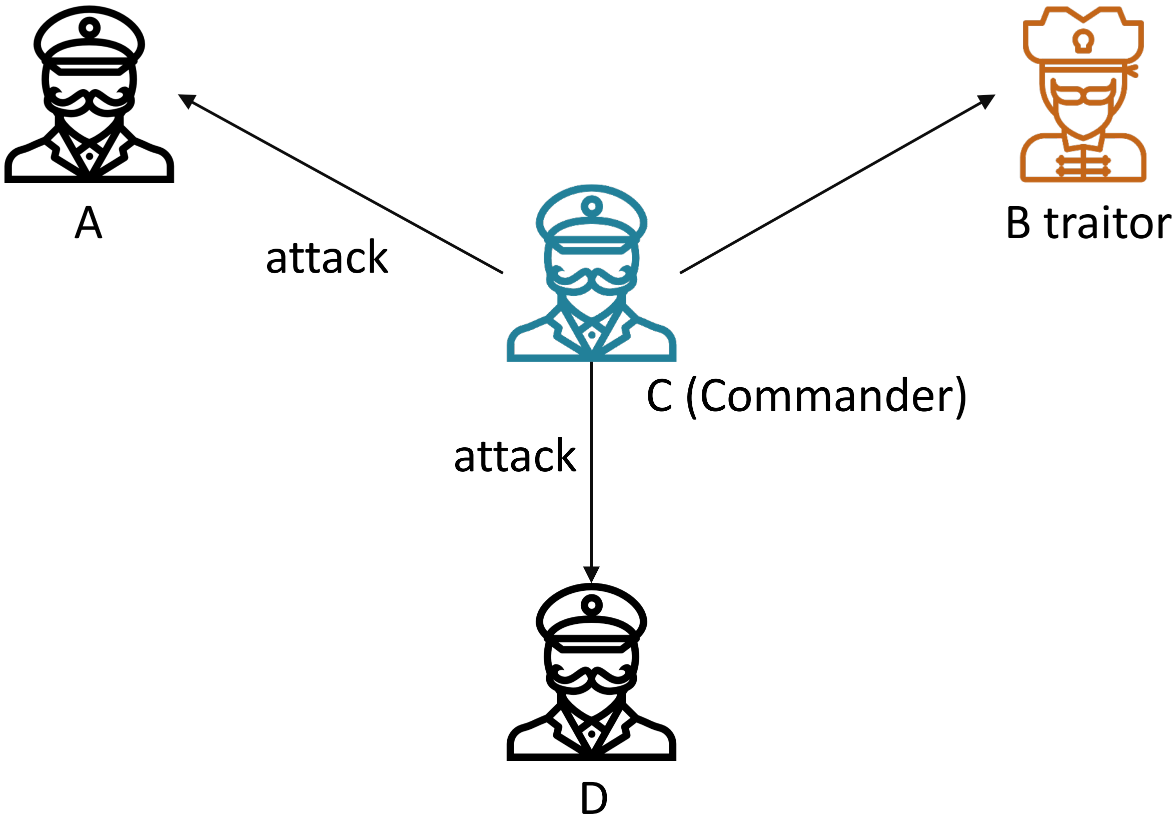
The traitor may fool A and C to attack and fool D to retreat.

Conclusion under the Assumption

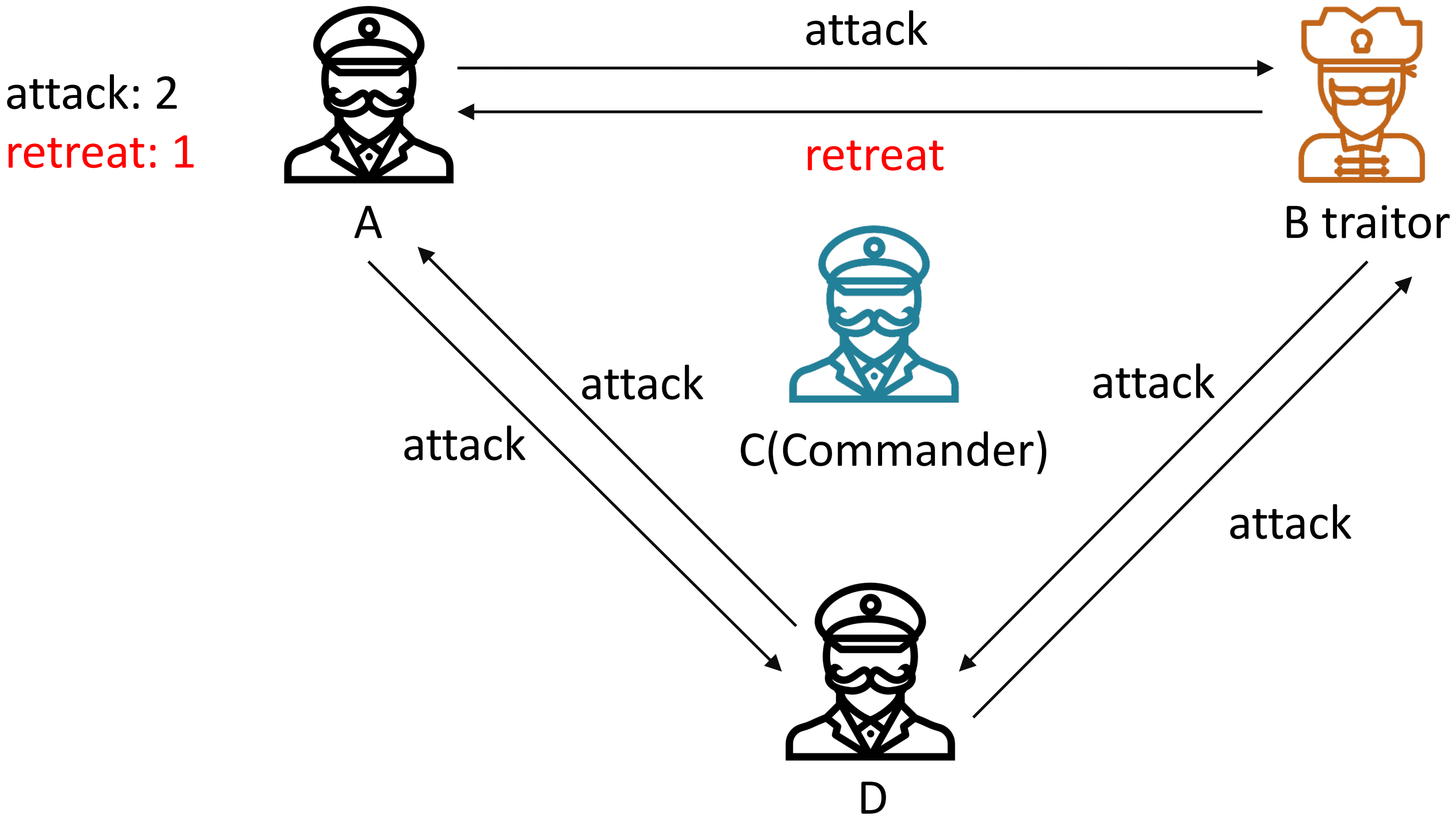
- Assumption: The communication is synchronous.
- It is possible to fail with only one traitor.
  - When half of the loyal generals vote for attack, and half for retreat.

Further Assumption: One Commander

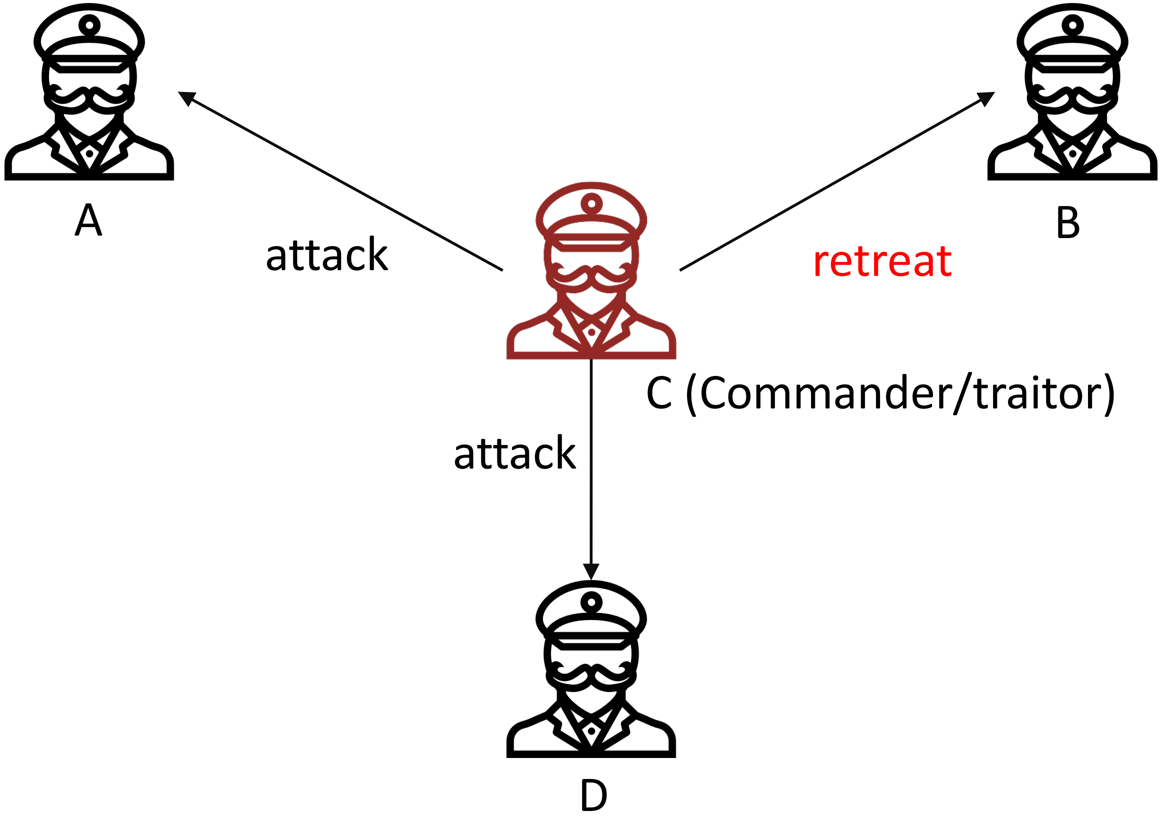
- All generals receive commands from the commander before voting.



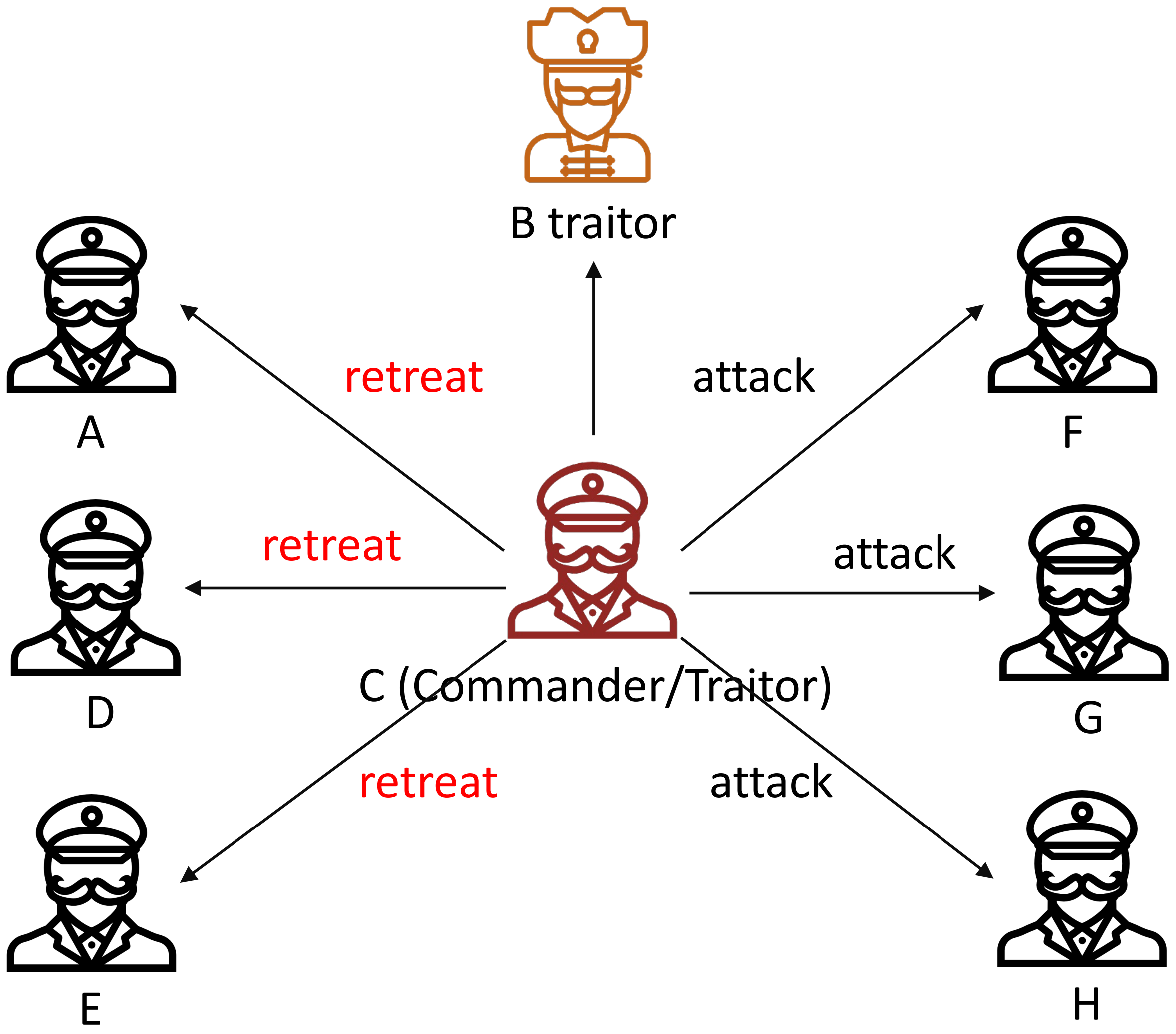
Further Assumption: One Commander



What If The Commander Is a Traitor?



What If The Commander Is a Traitor?



Problem: How to Select the Commander?

- Proof of Work
- Proof of Space
- Proof of Stake

Proof-of-Work

- To find a hash value starting with N zeros (bits), it requires O(2N) time.
- Practical test: Start from 0, increment gradually, and calculate the hash.

Time (seconds)	**Nonce**	**Hash Value**
3e-05	0	4c8f1205f49e70248939df9c7b704ace62…
0.000138	12	05017256be77ad2985b36e75e486af325…
0.000482	112	00ae7e0956382f55567d0ed9311cfd41dd…
0.014505	3728	000b5a6cfc0f076cd81ed3a60682063887c…
0.595024	181747	0000af058b74703b55e27437b89b1ebcc4…
3.491151	1037701	00000e55bd0d2027f3024c378e0cc51154…
32.006105	9913520	00000077a77854ee39dc0dc996dea72dad…
90.89462	186867248	0000000225060b16117b23dbea9ce6be86…
4686.171007	1424462909	000000002dd743724609a9f57260e24929…

Proof-of-Space (Capacity)

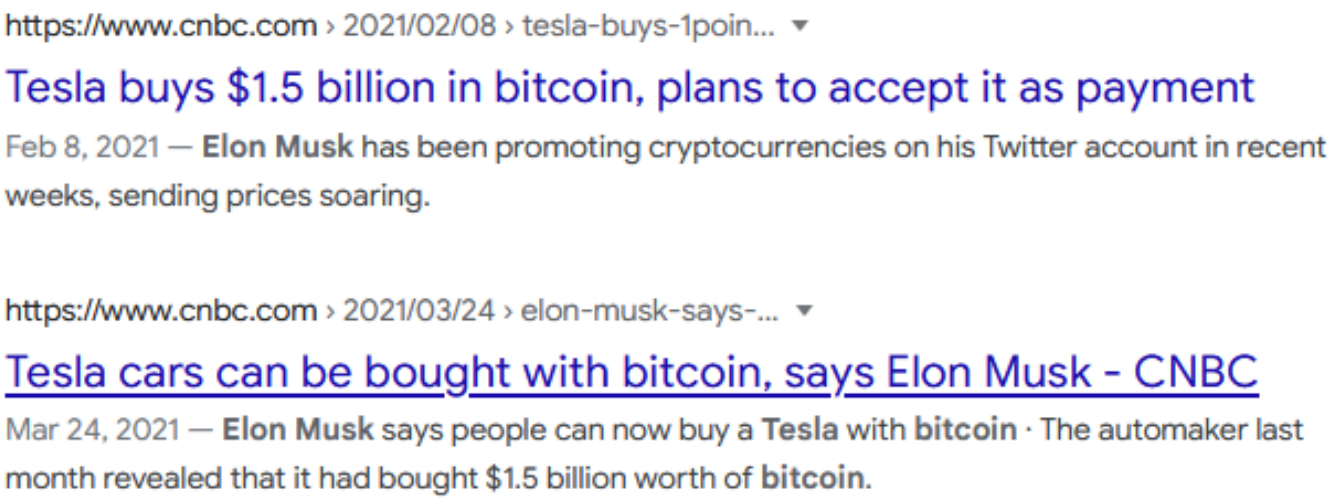
- **Plotting Phase:**
  - Miners precompute and store cryptographic hash values (plots) on their storage devices.
  - These plots are generated using algorithms such as SHA-256.
- **Mining Phase:**
  - The network issues a challenge, and miners use their precomputed plots to find a solution.
  - The probability of finding a solution is proportional to the amount of storage allocated.
- **Block Generation:**
  - The miner with the best response (e.g., closest to the challenge target) wins the right to create the next block and receive rewards.

Proof-of-Stake

- Validator Selection:
  - The network uses an algorithm to choose a validator to propose the next block.
  - Probability of selection is proportional to the amount of cryptocurrency staked.
- Block Proposal and Validation:
  - The chosen validator creates a new block and broadcasts it to the network.
  - Other validators verify the block's validity.
- Consensus Achievement:
  - Once a block gains sufficient approvals, it is added to the blockchain, and the proposer receives a reward.

Comparison of Different Consensus Mechanism

	Proof-of-Work (PoW)	**Proof-of-Capacity (PoC)**	**Proof-of-Stake (PoS)**
Resource Used	Computational Power	Storage Space	Stake
Energy Efficiency	Low	High	High
Scalability	Moderate	Moderate	High
Decentralization	Moderate	High	Risk of Centralization



https://www.cnbc.com › 2021/02/08 › tesla-buys-1poin... ▾

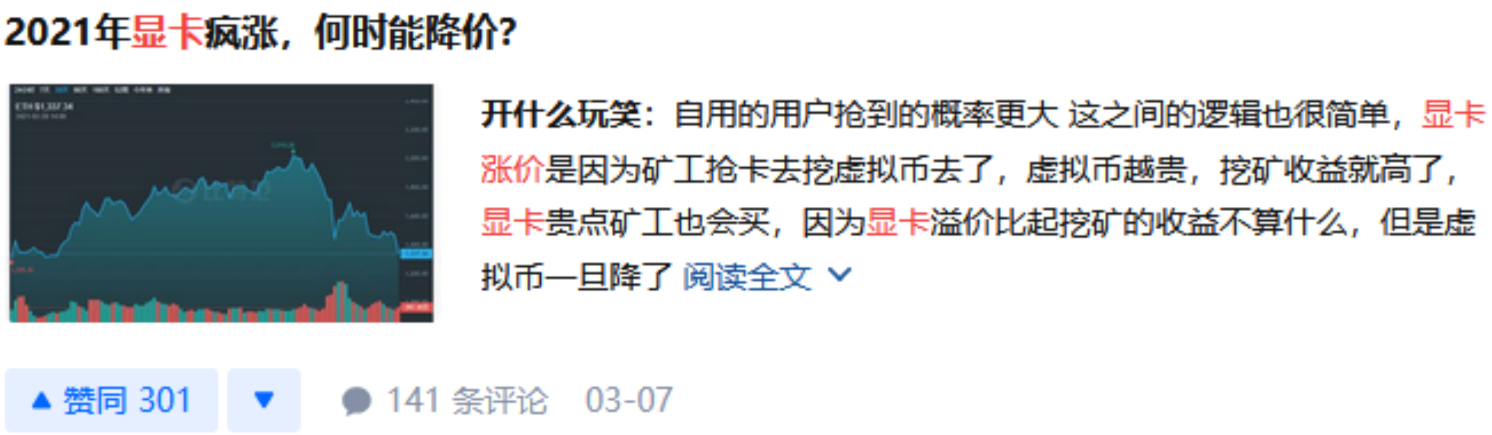
Tesla buys $1.5 billion in bitcoin, plans to accept it as payment

Feb 8, 2021 — **Elon Musk** has been promoting cryptocurrencies on his Twitter account in recent weeks, sending prices soaring.

https://www.cnbc.com › 2021/03/24 › elon-musk-says-... ▾

Tesla cars can be bought with bitcoin, says Elon Musk - CNBC

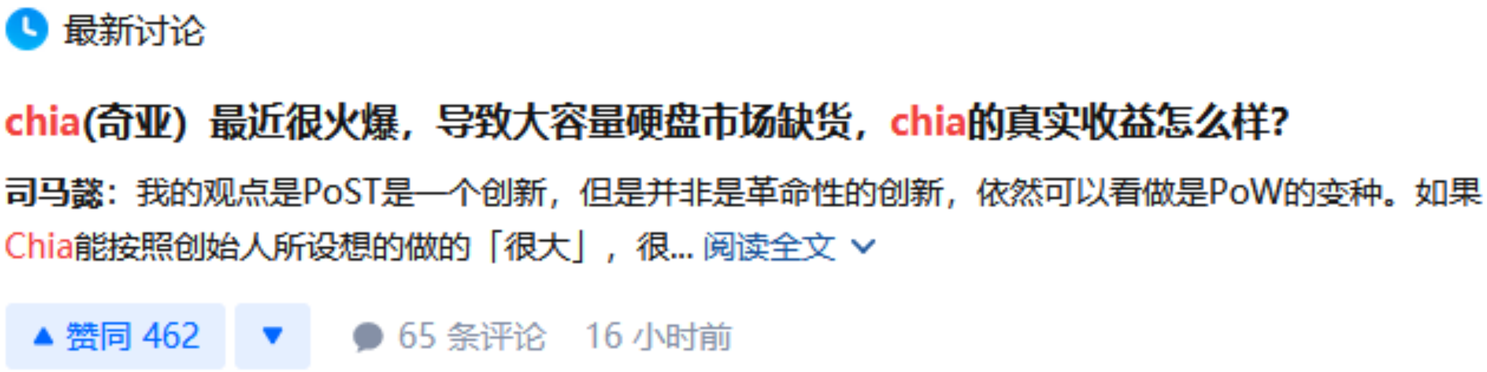
Mar 24, 2021 — **Elon Musk** says people can now buy a **Tesla** with **bitcoin** · The automaker last month revealed that it had bought $1.5 billion worth of **bitcoin**.



2021年显卡疯涨，何时能降价?

开什么玩笑: 自用的用户抢到的概率更大 这之间的逻辑也很简单，显卡涨价是因为矿工抢卡去挖虚拟币去了，虚拟币越贵，挖矿收益就高了，显卡贵点矿工也会买，因为显卡溢价比起挖矿的收益不算什么，但是虚拟币一旦降了 阅读全文 ⌄

▲ 赞同 301 ▼ 141 条评论 03-07



最新讨论

chia(奇亚) 最近很火爆，导致大容量硬盘市场缺货，chia的真实收益怎么样?

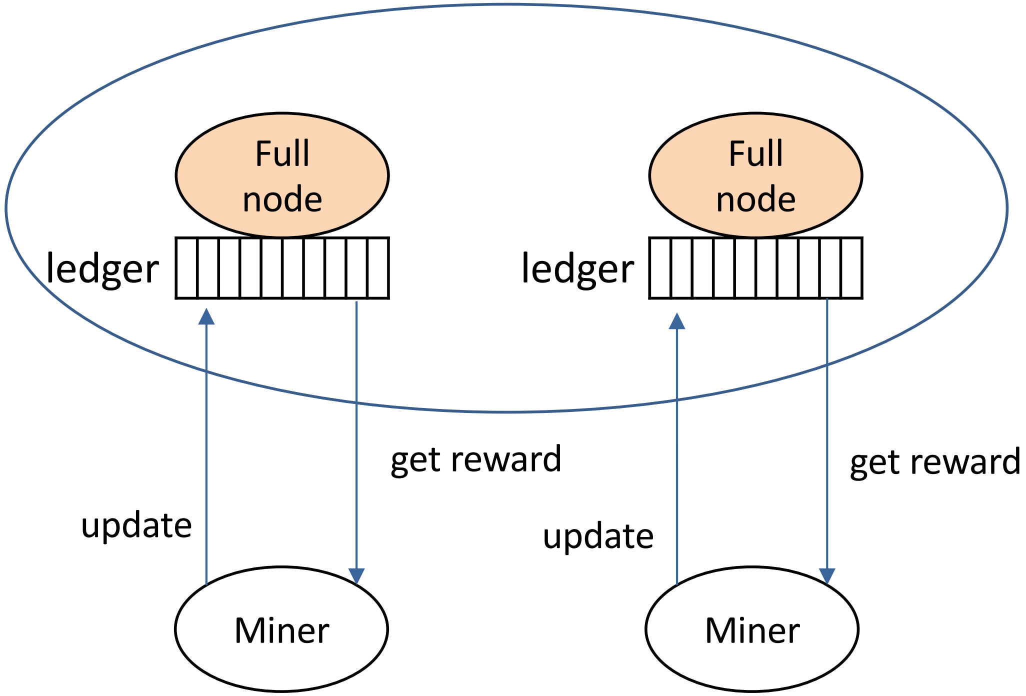
司马懿: 我的观点是PoST是一个创新，但是并非是革命性的创新，依然可以看做是PoW的变种。如果Chia能按照创始人所设想的做的「很大」，很... 阅读全文 ⌄

▲ 赞同 462 ▼ 65 条评论 16 小时前

2. Bitcoin and Blockchain

Bitcoin

- **Full Nodes:** Store the ledger locally.
- **Miner:** Incrementally update the ledger by writing data.

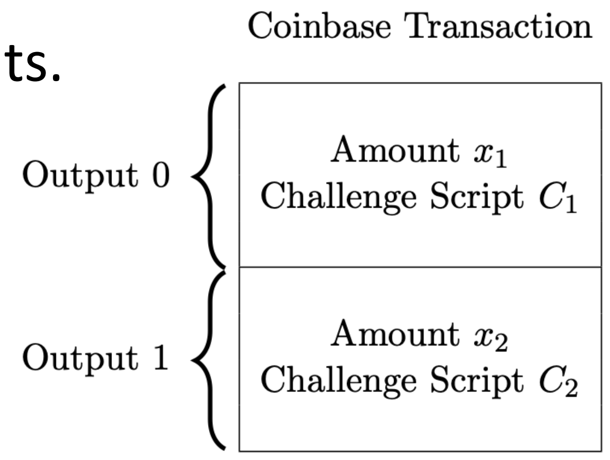


Bitcoin

- 21 million BTC in total.
- Initial reward: 50 BTC per block, halving every 210,000 blocks (approximately every 4 years).
- 1 BTC = 100 million satoshis.
- When the reward is less than 1 satoshi, no reward will be issued (around the year 2140).
- Earn transaction fees.
- Difficulty adjusts dynamically to maintain a block computation time of approximately 10 minutes.

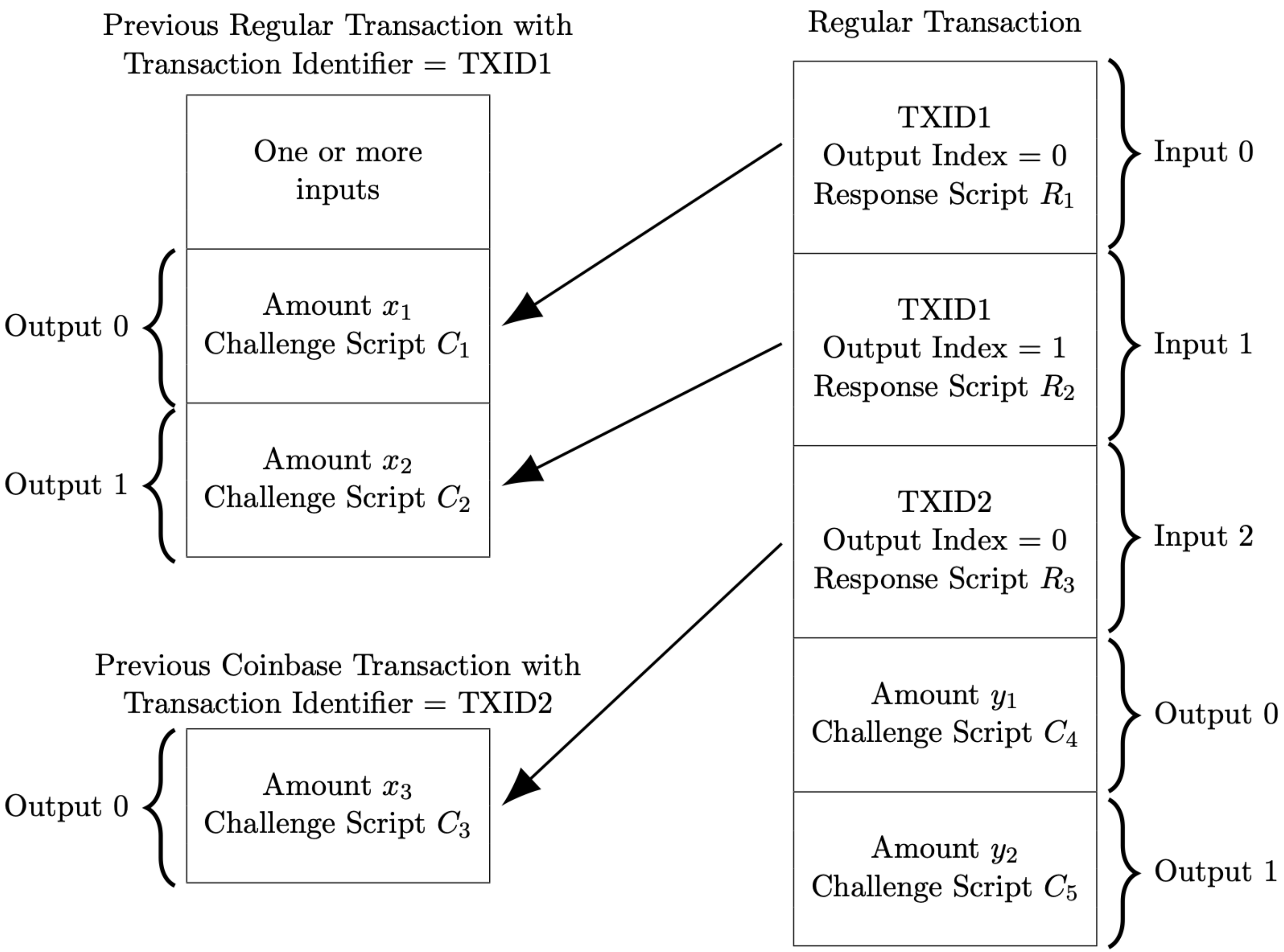
Transaction

- **Input:** The source of the Bitcoin.
- **Output:** The target of a Bitcoin transfer.
- **Transaction:** set the challenge (Pay-to-Public-Key-Hash):
  - The recipient must provide their public key.
  - The sender verifies that the public key matches the hash (the P2PKH address).
  - The recipient must also provide a digital signature created with their private key to prove ownership of the private key.
- **Coinbase Transaction:** A transaction with no inputs.

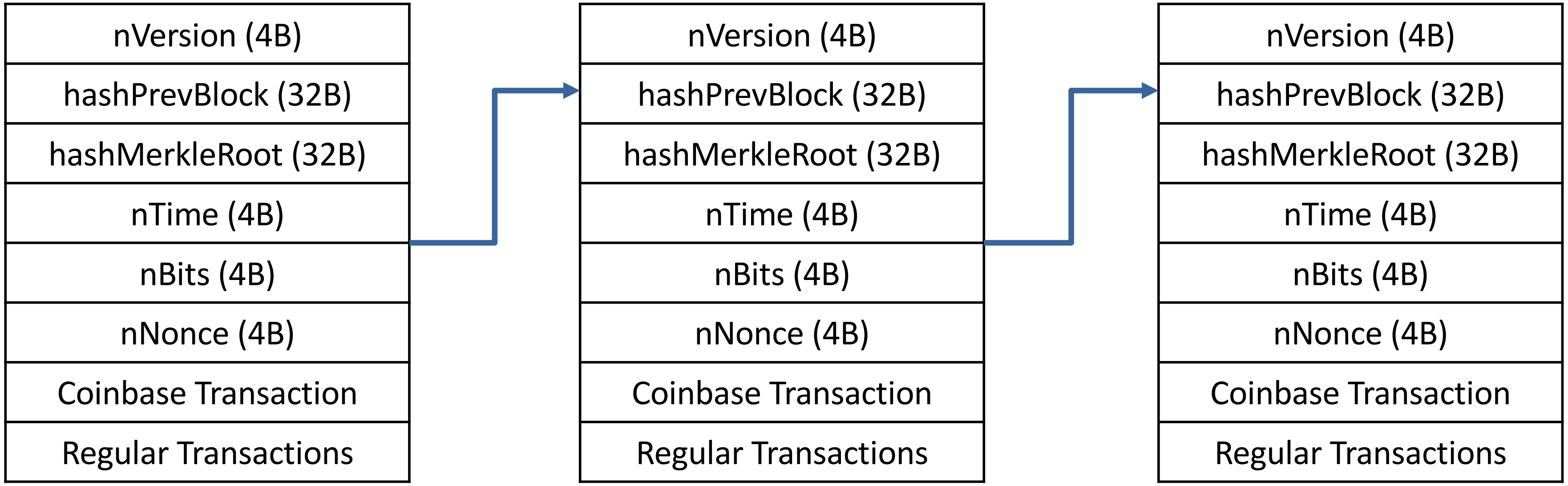


Regular Transaction (Spend money)

- Response script: Use the private key to sign (encrypt) as the response to the challenge of the previous output.



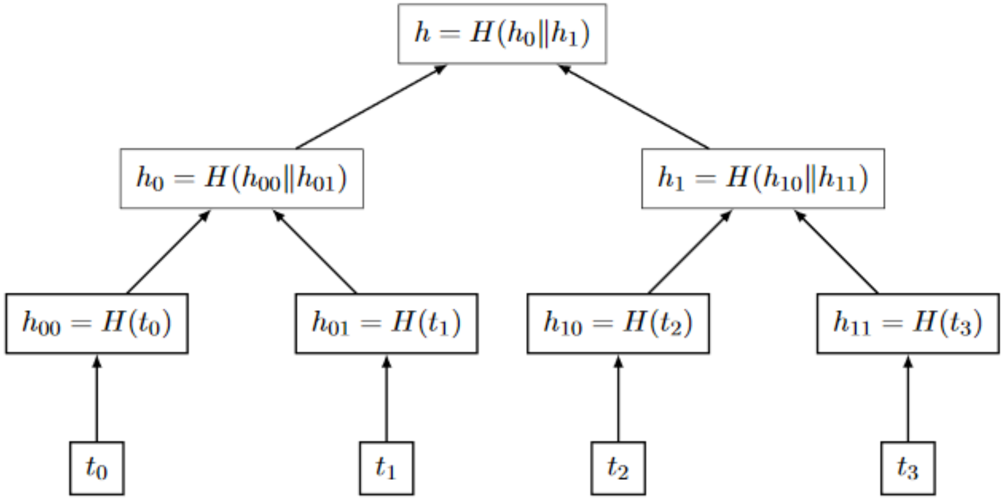
Ledger



nVersion (4B)
hashPrevBlock (32B)
hashMerkleRoot (32B)
nTime (4B)
nBits (4B)
nNonce (4B)
Coinbase Transaction
Regular Transactions

nVersion (4B)
hashPrevBlock (32B)
hashMerkleRoot (32B)
nTime (4B)
nBits (4B)
nNonce (4B)
Coinbase Transaction
Regular Transactions

nVersion (4B)
hashPrevBlock (32B)
hashMerkleRoot (32B)
nTime (4B)
nBits (4B)
nNonce (4B)
Coinbase Transaction
Regular Transactions



Merkle Root保存了交易哈希值

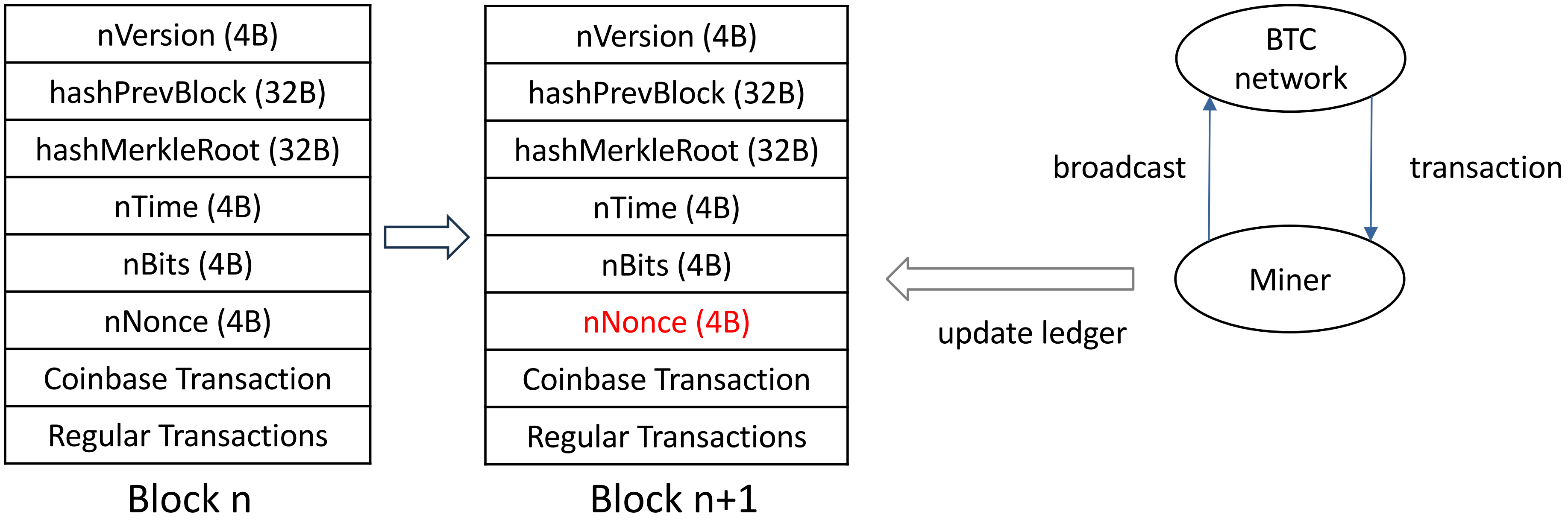
- 二叉树
- t_0, t_1 , t_2 , t_3都是交易记录

为什么采用Merkle Tree

- 相比H(t_0, t_1 , t_2 , t_3)交易有效性证明效率（数据存取）更高
  - O($\log_2$n) vs O(n)

Mining (PoW)

- Find a valid nNonce such that the hash value does not exceed the threshold (n-bits).



nVersion (4B)
hashPrevBlock (32B)
hashMerkleRoot (32B)
nTime (4B)
nBits (4B)
nNonce (4B)
Coinbase Transaction
Regular Transactions

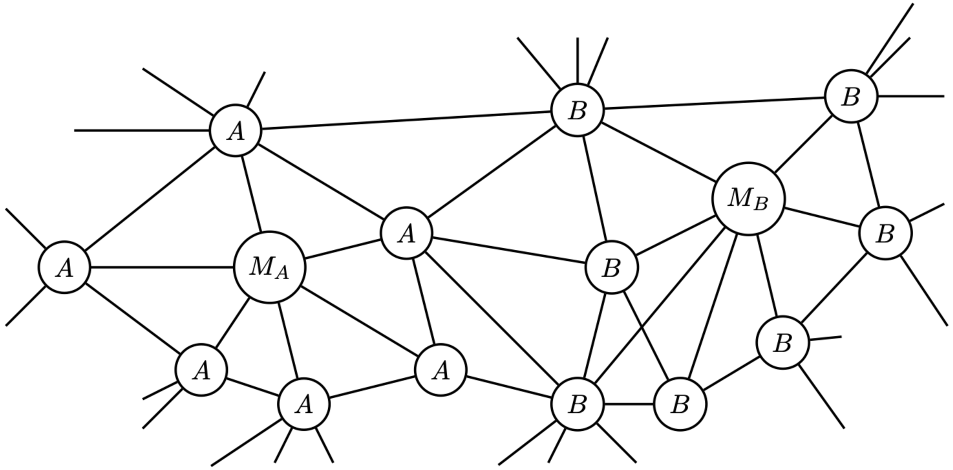
Block n

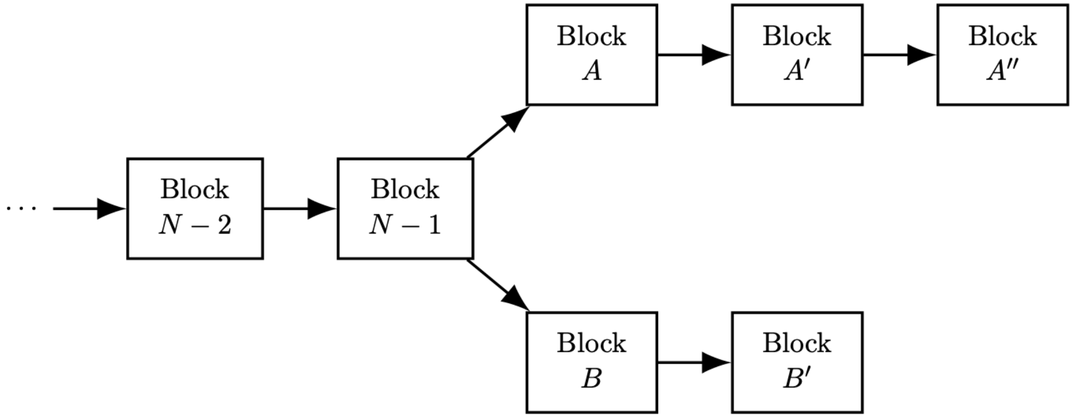
nVersion (4B)
hashPrevBlock (32B)
hashMerkleRoot (32B)
nTime (4B)
nBits (4B)
nNonce (4B)
Coinbase Transaction
Regular Transactions

Block n+1

Temporary Fork

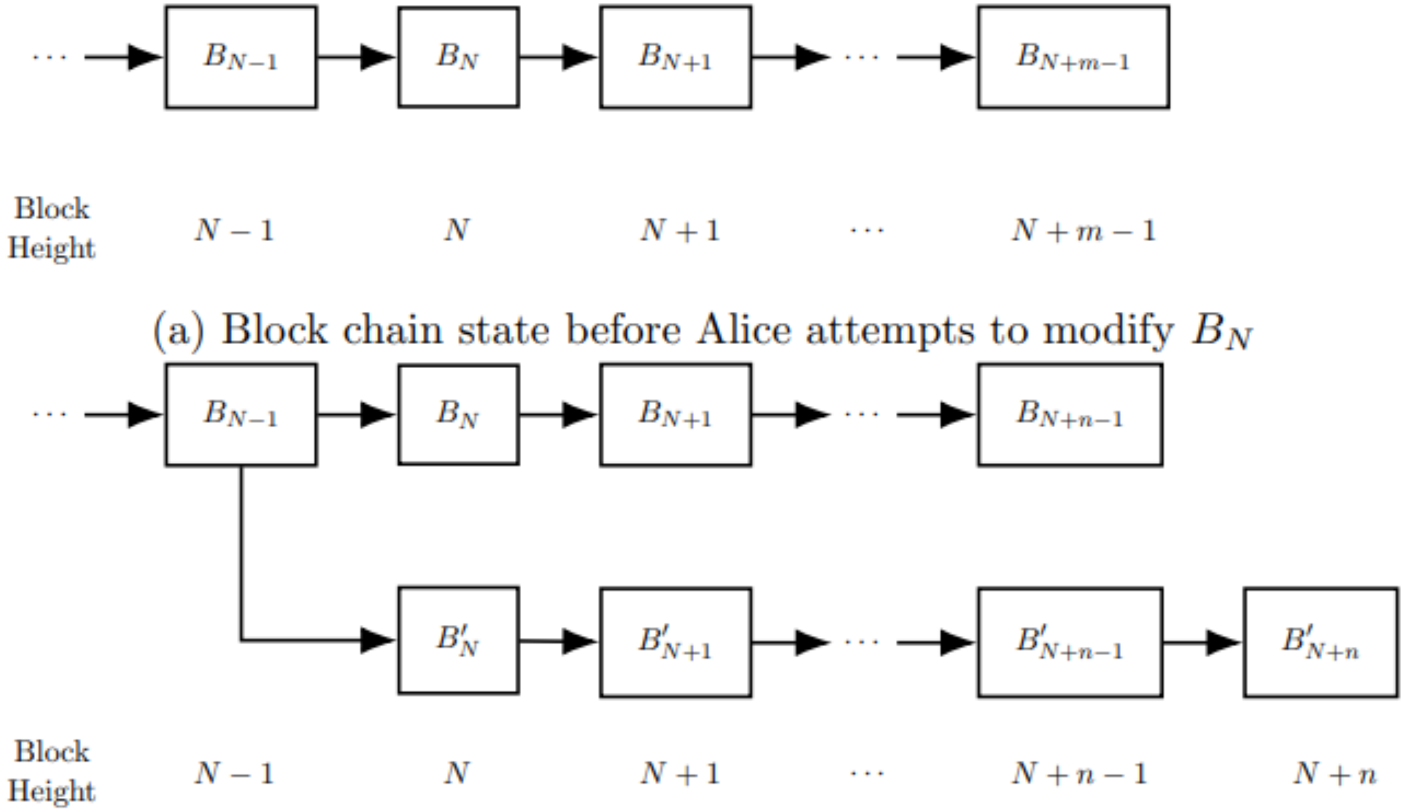
- When two miners find a solution to a block simultaneously, a temporary fork in the blockchain can occur.
- This situation is resolved by the blockchain network following the longest chain rule.





51% Attack

- If an attacker wants to tamper with an already agreed-upon block BN, they would need to make their chain longer than the original chain.



(a) Block chain state before Alice attempts to modify B_N

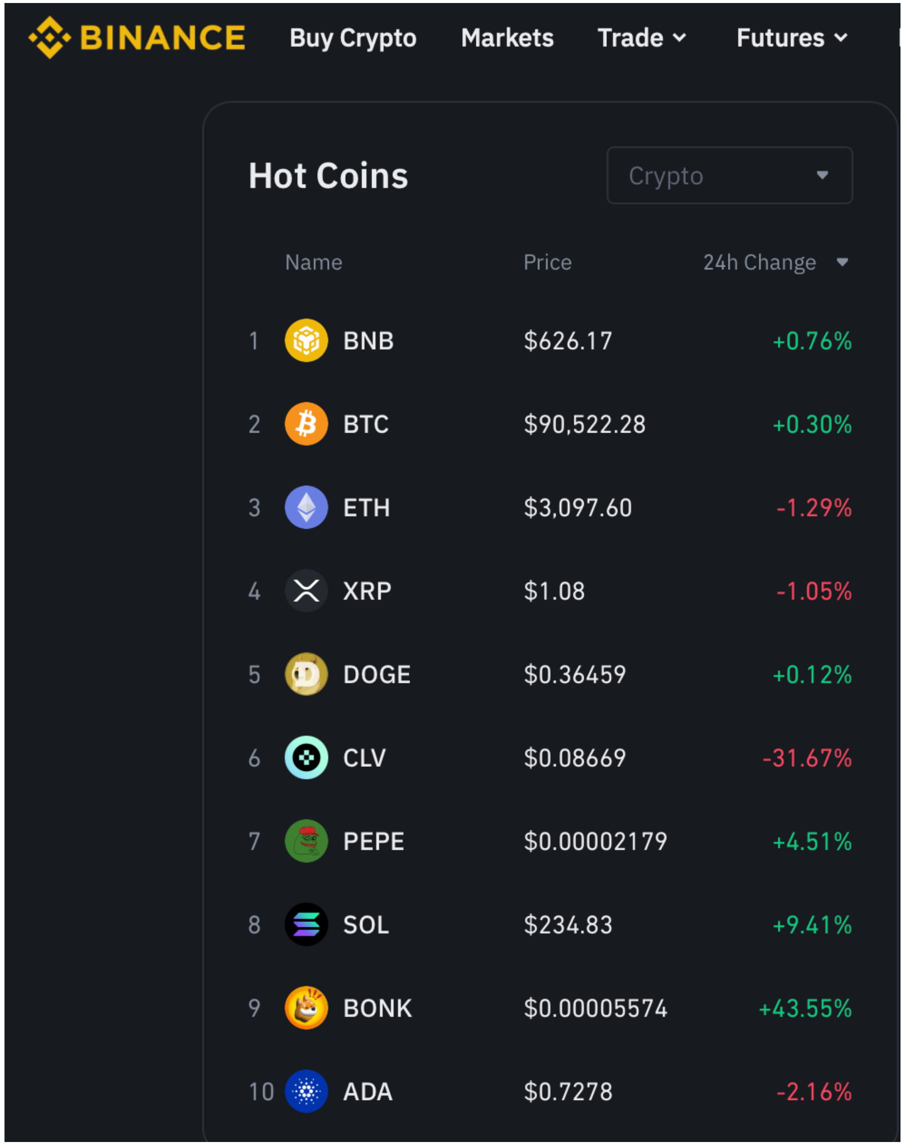
(b) Block chain state when the branch containing B'_N overtakes the branch containing B_N. Here $n \geq m$.

Question

- Does the recipient deliver the product once receiving the bitcoin?
- Are bitcoins transaction anonymous?

Binance

- One of the largest cryptocurrency exchange platforms in the world.
- Cryptocurrency:



Hot Coins

	Name	Price	24h Change
1	BNB	$626.17	+0.76%
2	BTC	$90,522.28	+0.30%
3	ETH	$3,097.60	-1.29%
4	XRP	$1.08	-1.05%
5	DOGE	$0.36459	+0.12%
6	CLV	$0.08669	-31.67%
7	PEPE	$0.00002179	+4.51%
8	SOL	$234.83	+9.41%
9	BONK	$0.00005574	+43.55%
10	ADA	$0.7278	-2.16%

3. Smart Contract

Proposed by Szabo in 1994

“ A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.”

Smart Contract Implementation: Blockchain 2.0

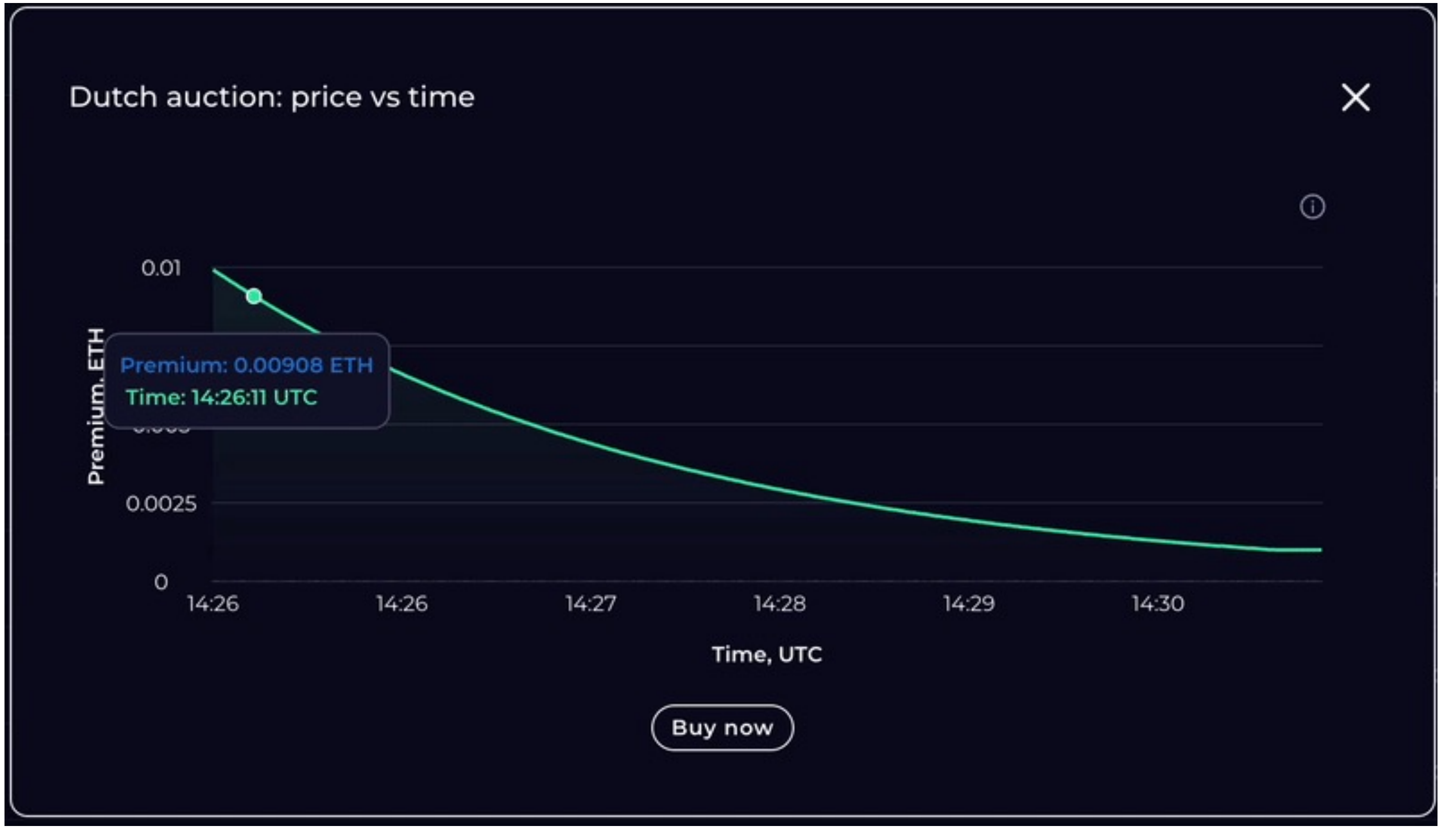
- Self-executing program stored on a blockchain that automatically enforces rules and agreements when predefined conditions are met.
- Designed for decentralized applications (dApps), NFTs, DeFi, etc.
  - Fully programmable with Turing-complete languages (e.g., Solidity).
- Bitcoin is a special smart contract focused on financial transactions.
  - Only support basic programmable transactions using its Script language.
  - Blockchain 1.0

How Do Smart Contracts Work?

- Define the Agreement: Write the terms in code (e.g., using Solidity for Ethereum).
- Deploy to Blockchain: Upload the code to a blockchain like Ethereum.
- Trigger Execution: When conditions are met, the contract executes automatically.

Example: Dutch Auction

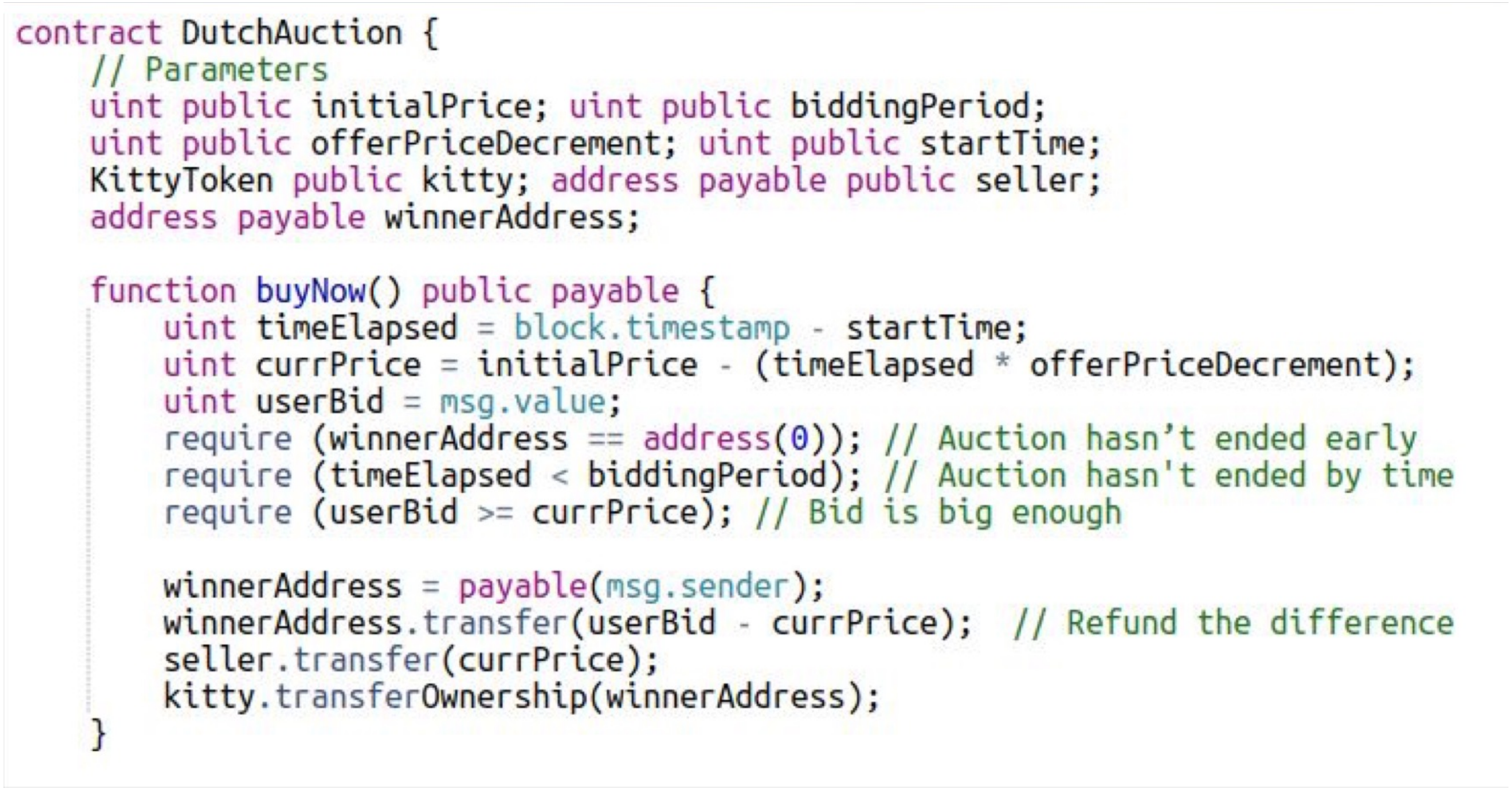
- The auction starts with a high initial price for the item or asset.
- The price is lowered incrementally over time at a set interval or rate.
- The first participant to accept the current price wins the item.



Dutch Auction: NFT (Non-Fungible Token)

- An NFT is a unique digital asset that represents ownership or proof of authenticity of a specific item, stored on a blockchain.
- Tokenization: An item (e.g., digital art, video, music, game item) is tokenized, creating a unique NFT tied to that asset.
- NFTs rely on smart contracts to define ownership, transferability, and royalties for creators.

Example: Dutch Auction in Ethereum/Solidity



```
contract DutchAuction {
    // Parameters
    uint public initialPrice; uint public biddingPeriod;
    uint public offerPriceDecrement; uint public startTime;
    KittyToken public kitty; address payable public seller;
    address payable winnerAddress;

    function buyNow() public payable {
        uint timeElapsed = block.timestamp - startTime;
        uint currPrice = initialPrice - (timeElapsed * offerPriceDecrement);
        uint userBid = msg.value;
        require (winnerAddress == address(0)); // Auction hasn’t ended early
        require (timeElapsed < biddingPeriod); // Auction hasn't ended by time
        require (userBid >= currPrice); // Bid is big enough

        winnerAddress = payable(msg.sender);
        winnerAddress.transfer(userBid - currPrice);  // Refund the difference
        seller.transfer(currPrice);
        kitty.transferOwnership(winnerAddress);
    }
```

https://rdi.berkeley.edu/berkeley-defi/assets/material/Lecture%203%20Slides.pdf

4. In-class Practice

In-class Practice

- Design an experiment to measure the time cost of a PoW consensus algorithm under different difficulty settings.
  - Implement a program and execute it multiple times for each setting.
  - Finally, plot the results as a box plot.

Time (seconds)	Nonce	Setting (Hash Value)
?	?	0XXX…
?	?	00XXX…
?	?	000XXX…
?	?	0000XXX…
?	?	00000XXX…