NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

Bitcoin

Analysis of Bitcoin Consensus

Dr Sourav SEN GUPTA
Lecturer, SCSE, NTU

Bitcoin Consensus

Consensus Attacks

Recall : Bitcoin Consensus

Independent operation at each Node in the Bitcoin P2P Network

- **Transaction Validation** : Verification of each transaction by every Full Node
- **Transaction Aggregation** : Recording transactions into blocks by Mining Nodes
- **Proof-of-Work** : Proof of demonstrated computation (mining) by Mining Nodes
- **Block Validation** : Verification of new blocks by every node with the Blockchain
- **Chain Selection** : Selection of "longest" chain with highest total Proof-of-Work

No formal leader election; it is a simple proposer-verifier model for consensus.

No formal round for block validation; voting is implicit through chain extension.

What can go wrong? [1]

Let us consider a few specific attacks on the consensus driven Bitcoin system.

- **Stealing Bitcoins** : Can any player in the network “steal” someone else’s coins?
- **Double Spending** : Can any player “spend” one transaction more than once?
- **Denial of Service** : Can a miner maliciously “exclude” transactions in a block?
- **Invalid Transactions** : Can a miner maliciously “record” invalid transactions?
- **51% Attack** : Can “majority” of miners in bitcoin collude to behave maliciously?

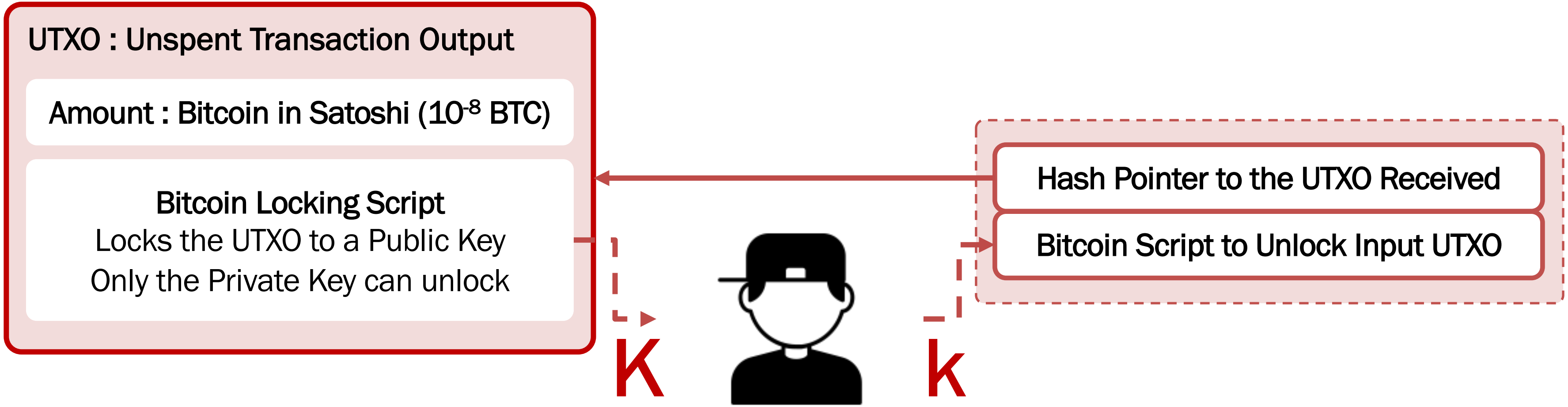
We will see that just the technical mechanism of consensus is not adequate.

[1] reading : Chapter 2 of the book “Bitcoin and Cryptocurrencies”

Stealing Bitcoins

Can any player in the network "steal" someone else's coins?

Not trivially. It's impossible to "steal" someone else's bitcoin (UTXO) unless you own the private key corresponding to their "identity" in the network.



UTXO : Unspent Transaction Output

Amount : Bitcoin in Satoshi (10^{-8} BTC)

Bitcoin Locking Script
Locks the UTXO to a Public Key
Only the Private Key can unlock

Hash Pointer to the UTXO Received

Bitcoin Script to Unlock Input UTXO

Stealing Bitcoins

Can any player in the network "steal" someone else's coins?

Not trivially. It's impossible to "steal" someone else's bitcoin (UTXO) unless you own the private key corresponding to their "identity" in the network.

If you own the private key, you may generate the signing script to spend the UTXO belonging to that identity and move it to your own address.

Prevention : Ensuring security of Private Keys and Bitcoin Wallets

(physical "paper wallets", offline "cold storage", hardware wallets, vaults, etc.)

Double Spending

Can any player “spend” one transaction more than once?

Not trivially. It’s impossible to “spend” the same UTXO more than once and get validated by a miner, unless you are a miner yourself, or you collude with one.

If you are not a miner (or not colluding with one)

- First use of the UTXO will move it from the UTXO pool to denote “spent”
- Second use of the same UTXO will not be validated by an honest miner

The second use of the same UTXO will not be recorded in the blockchain.

Double Spending

Can any player "spend" one transaction more than once?

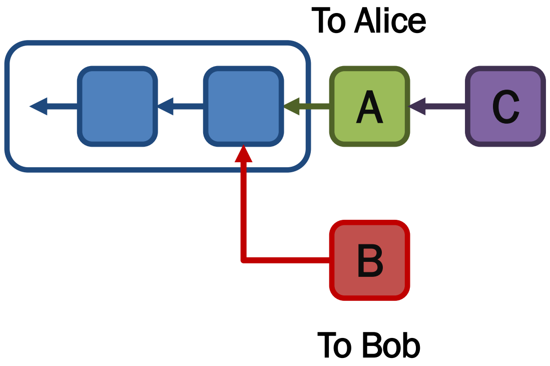
Not trivially. It's impossible to "spend" the same UTXO more than once and get validated by a miner, unless you are a miner yourself, or you collude with one.

If you are a miner yourself

- ○ First use of the UTXO in block A
- ○ Second use in "forked" block B

First, you need to mine block B yourself.

Finally, the next honest block C decides!



Double Spending

Can any player “spend” one transaction more than once?

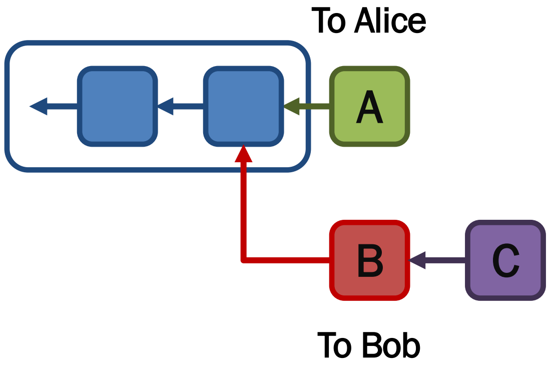
Not trivially. It’s impossible to “spend” the same UTXO more than once and get validated by a miner, unless you are a miner yourself, or you collude with one.

If you are colluding with a miner

- ○ First use of the UTXO in block A
- ○ Second use in “forked” block B

First, the colluding miner mines block B.

Finally, the next honest block C decides!



Recall : Attacks on Bitcoin

Attacks posed by individual nodes

- **Stealing Bitcoins** : Can any player in the network “steal” someone else’s coins?
- **Double Spending** : Can any player “spend” one transaction more than once?

Attacks posed by the mining nodes

- **Denial of Service** : Can a miner maliciously “exclude” transactions in a block?
- **Invalid Transactions** : Can a miner maliciously “record” invalid transactions?
- **51% Attack** : Can “majority” of miners in bitcoin collude to behave maliciously?

Attacks posed by miners are prevented through a clever design of incentives.

Bitcoin Consensus

Incentive Design

Denial of Service

Can a miner maliciously "exclude" transactions in a block?

Yes, of course. However, it's not a big issue for any end-user, as some "honest" miner will pick up the "excluded" transaction in one of the future blocks.

If you have a high-value old UTXO being spent in the transaction, it is more likely for honest miners to pick it up in their block, as it demands priority.

Strategy : Providing adequate Transaction Fee to incentivize miners
(even if the priority of your transaction is low, miners will pick up for the fee)

Invalid Transactions

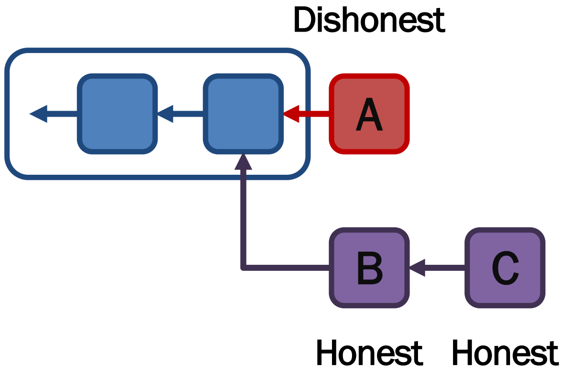
Can a miner maliciously "record" invalid transactions (or blocks)?

Technically, possible. Whichever miner solves the mining puzzle and provides proof-of-work, can "record" any set of transactions or any block in that round.

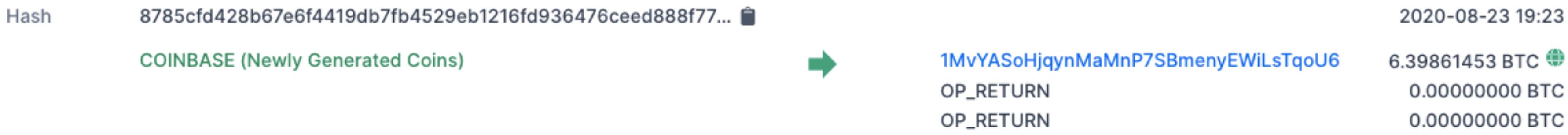
If you just solved the mining puzzle,
you may "record" an invalid block A.

Honest miners will fork out blocks B, C etc.

Consequently, your block will be voted out.



Incentive through Coinbase

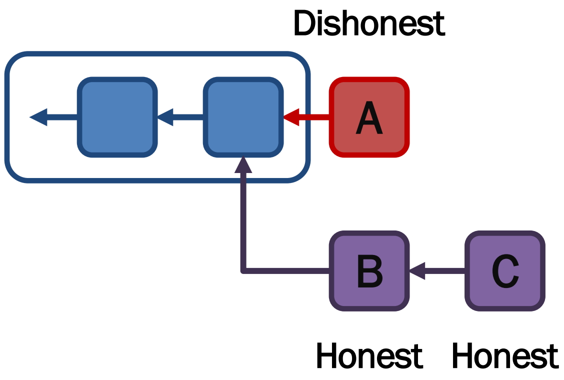


Hash	8785cfd428b67e6f4419db7fb4529eb1216fd936476ceed888f77...		2020-08-23 19:23
	COINBASE (Newly Generated Coins)	1MvYASoHjqynMaMnP7SBmenyEWiLsTqoU6	6.39861453 BTC
		OP_RETURN	0.00000000 BTC
		OP_RETURN	0.00000000 BTC

Incentive for Mining and Proof-of-Work

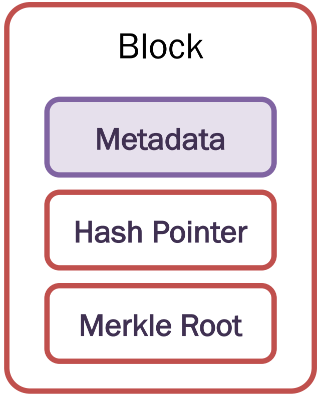
- Mining Reward included in block A.
- Transaction Fee included in block A.

Coinbase transaction can't be "spent" before 100 confirmations of the block.



ref : https://www.blockchain.com/btc/tx/8785cfd428b67e6f4419db7fb4529eb1216fd936476ceed888f77daaec63fd64

Recall : Difficulty in Proof-of-Work



Block 644984

Hash	0000000000000000000906cc2122074a dc6c7a5dda178e050626c4102e2ef685
Nonce	654,975,388
Difficulty	16,947,802,333,946.61

- ○ Requires a compute power of few tera-hash/sec (often through a “pool”)
- ○ Requires a system with expensive maintenance (electricity and cooling)

Dishonest behavior is economically unsustainable if Incentive < Mining Cost

ref : https://www.blockchain.com/btc/block/644984

Motivation for Incentives

Goal of the System

- Creating a verifiable tamper-resilient distributed ledger of transactions
- Active peer-to-peer network for end-users to reliably record transactions

Demand of End-Users

- Prompt and correct recording of transactions in the distributed ledger
- Value of transactions significantly higher than the cost of verification

Bitcoin satisfies both by incentives designed for Consensus and Verification

Design of Incentives

Incentive for Consensus

Built within the system to ensure rewards for honest behavior from the nodes.

If majority of miners do not “agree” on a block, its incentive implicitly forfeits.

Incentive for Verification

Option for end-users to incentivize the miners for verification and recording.

Minimum set to a threshold to ensure less spamming and an active network.

Coinbase Transaction and Reusable Proof-of-Work are crucial for the design.

Recall : What can go wrong?

Let us consider a few specific attacks on the consensus driven Bitcoin system.

- **Stealing Bitcoins** : Can any player in the network "steal" someone else's coins?
- **Double Spending** : Can any player "spend" one transaction more than once?
- **Denial of Service** : Can a miner maliciously "exclude" transactions in a block?
- **Invalid Transactions** : Can a miner maliciously "record" invalid transactions?
- **51% Attack** : Can "majority" of miners in bitcoin collude to behave maliciously?

Incentives do not seem to prevent attacks by majority of the miners colluding.

Bitcoin Consensus

51% Attack

51% Attack [1]

Can “majority” of miners in bitcoin collude to behave maliciously?

Technically, possible. Even if the hashing power for proof-of-work of the group of malicious miners is less than 50%, there is some chance of such attacks.

What can the majority accomplish?

- Can they “steal” bitcoin from other identities in the bitcoin network?
- Can they “deny service” to other nodes by not recording transactions?
- Can they help “double spending” of transactions by dishonest nodes?
- Can they change the “mining reward” and gain more bitcoin per block?

[1] reading : Chapter 2 of the book “Bitcoin and Cryptocurrencies”

51% Attack : Stealing Bitcoin

Can "majority" of miners steal bitcoin from other identities in the network?

Not trivially. There is no easy way to gain access to the private key of another identity in the network. The only option is to create an "invalid" transaction.

If the majority of miners collude to create an "invalid" transaction and record it in a block, the honest miners will fork a branch of the chain.

Moreover, any honest node will believe only in the "honest" branch.
(even if the branch propagated by the malicious miners is the longest one)

51% Attack : Denial of Service

Can "majority" of miners suppress transaction to deny service to any node?

Technically, possible. The majority control the "longest chain" in the system, and unless they include invalid transactions, their blocks will be respected.

Every transaction is broadcast to the entire network through neighborhood propagation. Thus, even if the transaction is not recorded in any block of the longest chain, it will be observed by every "full node" in the network.

Thus, even though the attack is possible, it will be apparent to everyone.

51% Attack : Double Spending

Can “majority” of miners help in double spending without forking a branch?

Not trivially. There is no easy way to include two transactions with the same input UTXO in one branch. Only option is to create an “invalid” transaction.

If the majority of miners collude to create an “invalid” transaction and record it in a block, the honest miners will fork a branch of the chain.

Moreover, any honest node will believe only in the “honest” branch.

(even if the branch propagated by the malicious miners is the longest one)

51% Attack : Double Spending

Can "majority" of miners help in double spending by extending wrong branch?

Technically, possible. The majority control the "longest chain" in the system, and unless they include invalid transactions, their blocks will be respected.

Every transaction is broadcast to the entire network. Thus, the order of communication for the transactions is also a common knowledge.

Thus, even though the attack is possible, it will be apparent to everyone.

(this will reduce confidence in the system and adversely affect the market)

Bitcoin Consensus

Backbone Protocol

Recall : Bitcoin Consensus

Independent operation at each Node in the Bitcoin P2P Network

- **Transaction Validation** : Verification of each transaction by every Full Node
- **Transaction Aggregation** : Recording transactions into blocks by Mining Nodes
- **Proof-of-Work** : Proof of demonstrated computation (mining) by Mining Nodes
- **Block Validation** : Verification of new blocks by every node with the Blockchain
- **Chain Selection** : Selection of “longest” chain with highest total Proof-of-Work

No formal leader election; it is a simple proposer-verifier model for consensus.

No formal round for block validation; voting is implicit through chain extension.

Bitcoin Backbone Protocol [2]

Desired properties from the Bitcoin protocol are as follows.

- **Common Prefix** : Ensures “Agreement” in Byzantine setting
  Any pair of honest nodes have a common prefix of blocks in their chains.

- **Chain Quality** : Ensures “Validity” in Byzantine setting
  Honest nodes have bounded number of dishonest blocks in their chains.

- **Chain Growth** : Ensures “Liveness” in Partial Synchrony
  The blockchain grows at a certain rate given a number of rounds of mining.

[2] ref : https://eprint.iacr.org/2014/765.pdf

Bitcoin Backbone Protocol

Operational transaction ledger under three assumptions

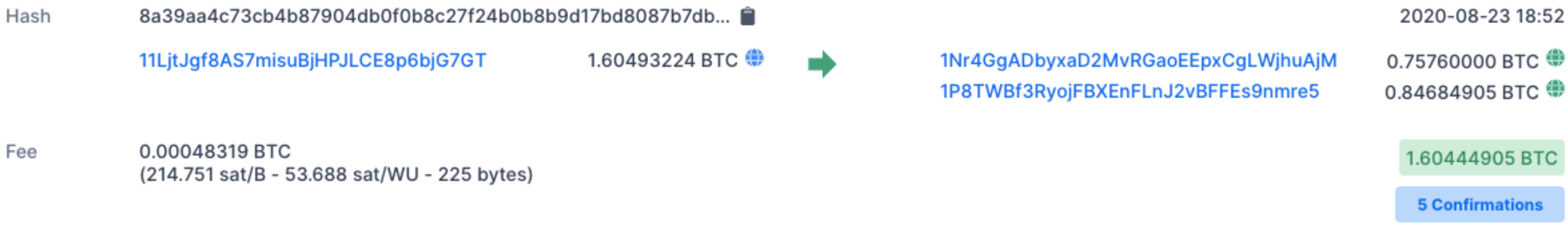
- the adversary controls less than half (50%) of the total hashing power,
- the network synchronizes much faster relative to the PoW solution rate,
- the digital signatures used in transactions and blocks cannot be forged.

Works under “synchrony”, as well as “partial synchrony” bounded by PoW.

Honest majority is not sufficient to maintain the ledger in “asynchrony”.

Communication delay across the network is much smaller than PoW epoch.

Bitcoin Confirmations



Hash 8a39aa4c73cb4b87904db0f0b8c27f24b0b8b9d17bd8087b7db... 2020-08-23 18:52

11LjtJgf8AS7misuBjHPJLCE8p6bjG7GT 1.60493224 BTC → 1Nr4GgADbyxaD2MvRGaoEEpxCgLWjhuAjM 0.75760000 BTC

1P8TWBf3RyojFBXEnFLnJ2vBFFEs9nmre5 0.84684905 BTC

Fee 0.00048319 BTC
(214.751 sat/B - 53.688 sat/WU - 225 bytes)

1.60444905 BTC

5 Confirmations

Given the “common prefix” property of bitcoin, it is sufficient to get just a few blocks to extend the chain in which a certain transaction is recorded.

Each block extending the block with your transaction is a “confirmation”, and the recipient may decide on the minimum number of confirmations.

ref : https://www.blockchain.com/btc/tx/8a39aa4c73cb4b87904db0f0b8c27f24b0b8b9d17bd8087b7dba7342ab8a0be8

The Consensus Game

Hashrate is not distributed uniformly amongst Bitcoin Miners.

Thus, it is more of a plutocratic mining game (not democratic).

- There is no fixed strategy or game plan for miners.
- It is assumed that each miner is incentive driven.
- Naturally, each miner is independent and rational.
- Miners may form pools to invest in hashing power.

Overall, Bitcoin runs on an incentive driven consensus.