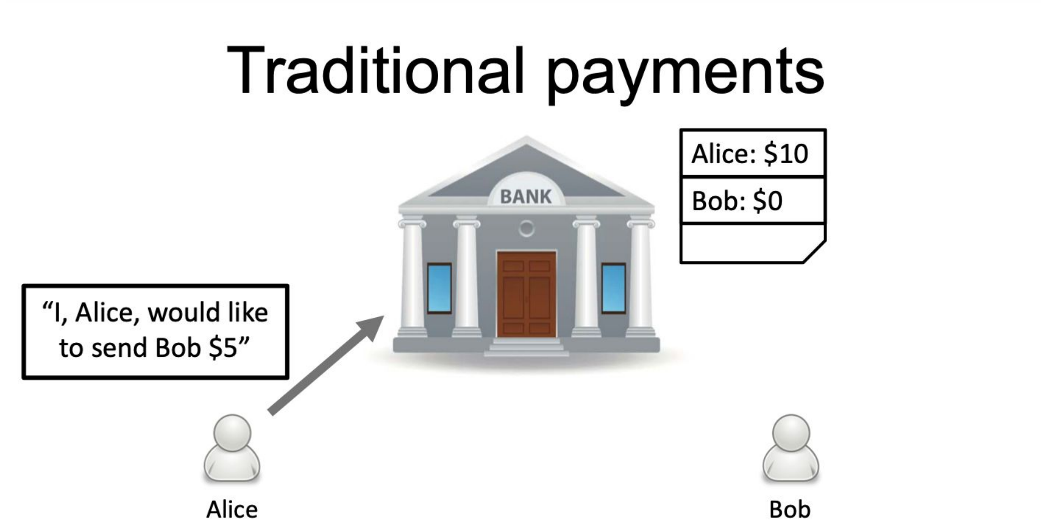
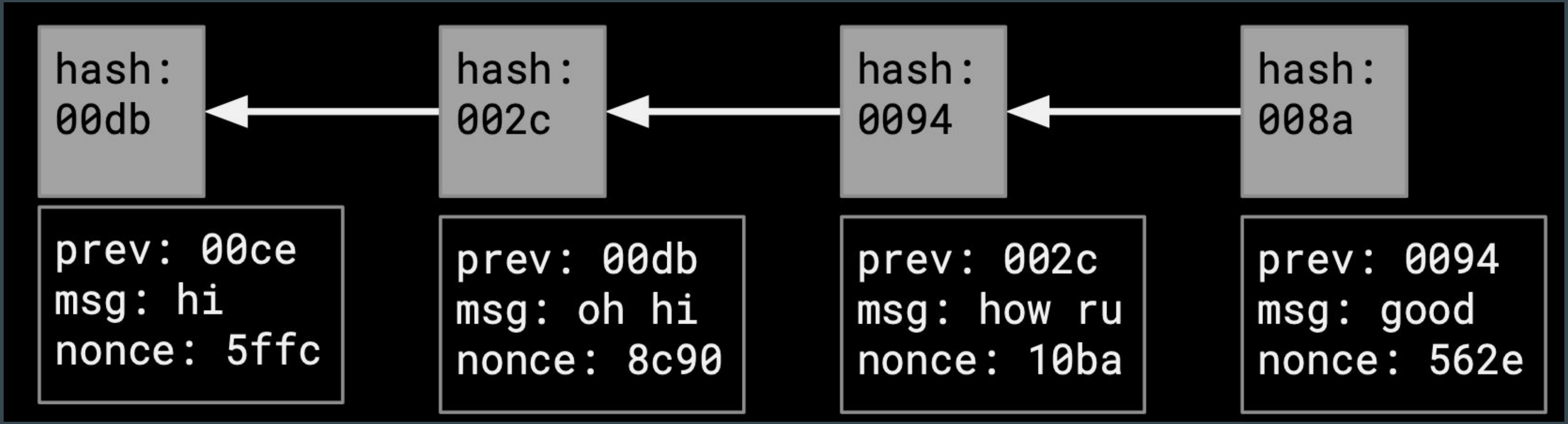
BitcoinF: Achieving Fairness for Bitcoin in Transaction-Fee-Only Model

Bitcoin?



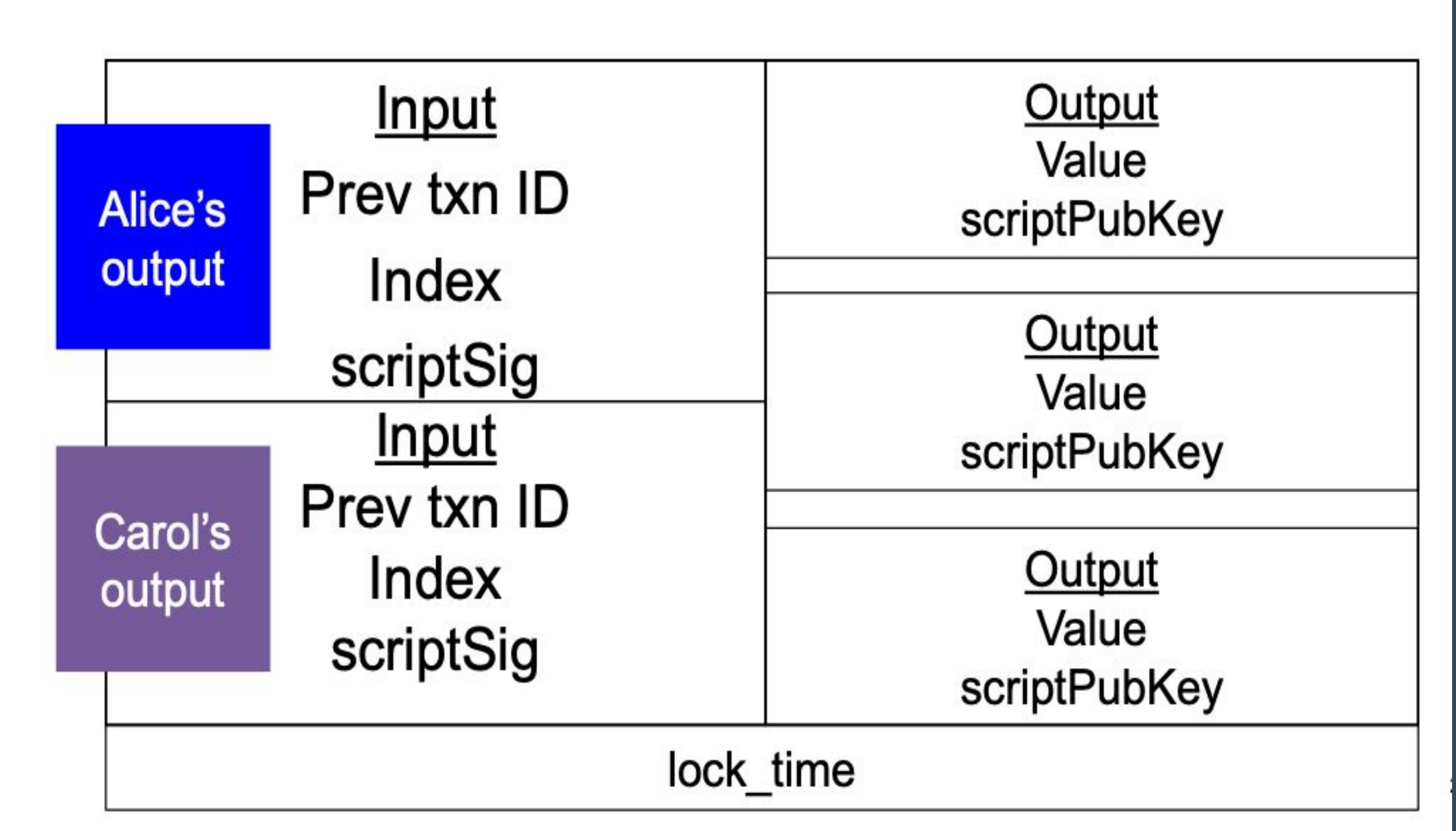
- A lot of things can go wrong
- Yes Bank?
- 2007-08 crisis?

- Also Privacy!



- **Users** broadcast their transactions
- **Miners** pick transactions from the network into a block and then start mining
  - Mining literally means to find a nonce that solves a cryptographic problem
- For example miners try to find nonce such that
  - hash(content of the block + nonce) has k leading zeros

Transactions: How to spend a Bitcoin?



Alice's output

Input
Prev txn ID
Index
scriptSig

Carol's output

Input
Prev txn ID
Index
scriptSig

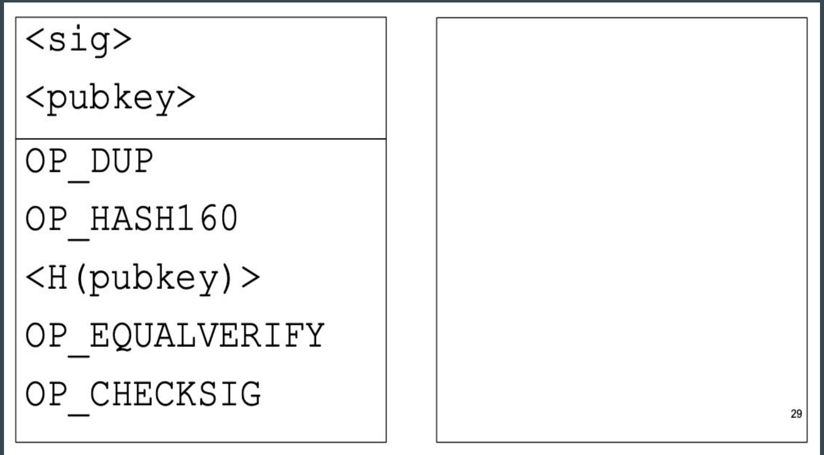
Output
Value
scriptPubKey

Output
Value
scriptPubKey

Output
Value
scriptPubKey

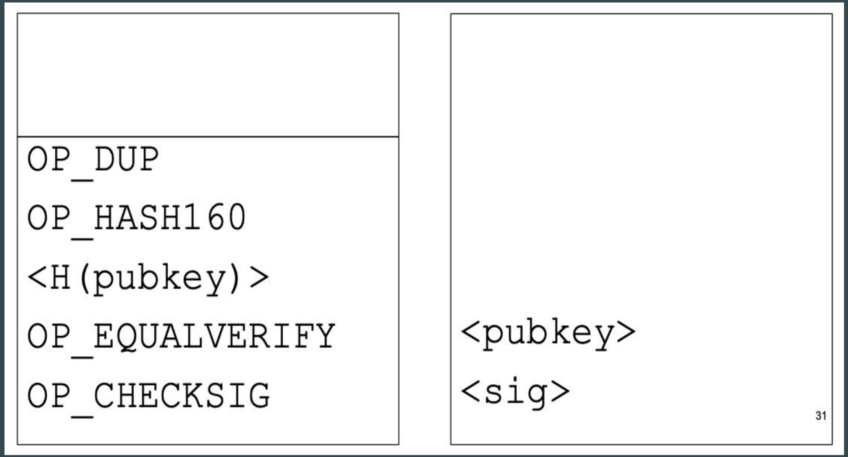
lock_time

Verifying a transaction



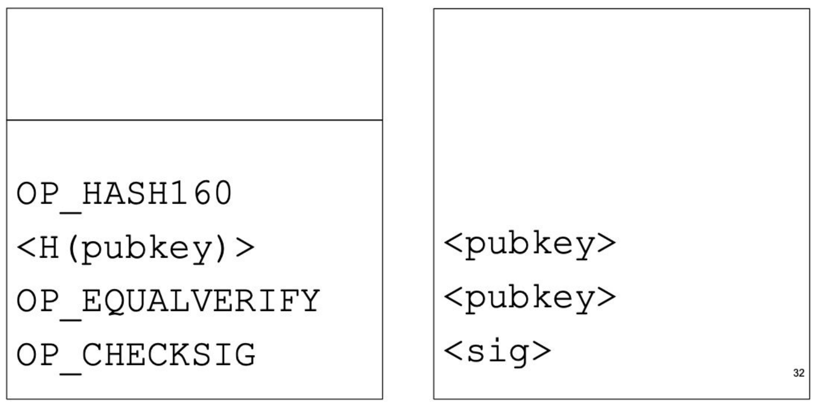
```
<sig>
<pubkey>
```

```
OP_DUP
OP_HASH160
<H(pubkey)>
OP_EQUALVERIFY
OP_CHECKSIG
```



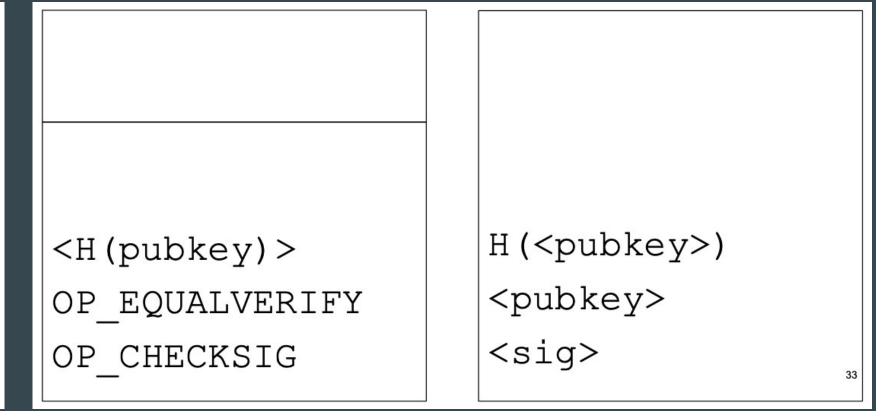
```
OP_DUP
OP_HASH160
<H(pubkey)>
OP_EQUALVERIFY
OP_CHECKSIG
```

```
<pubkey>
<sig>
```



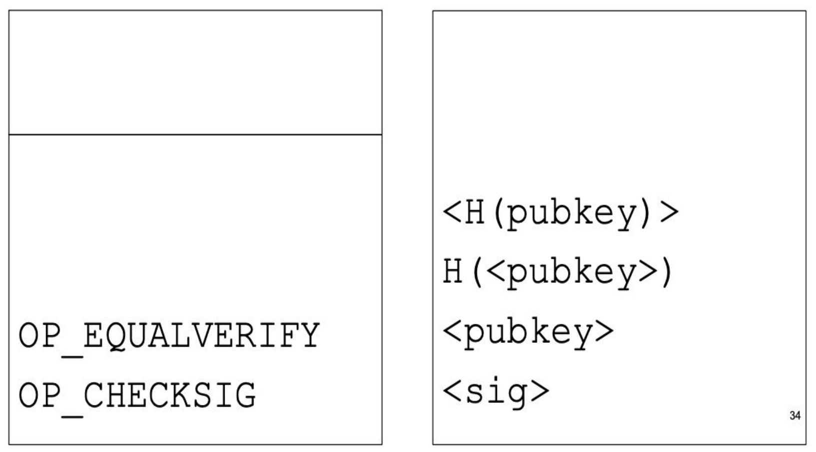
```
OP_HASH160
<H(pubkey)>
OP_EQUALVERIFY
OP_CHECKSIG
```

```
<pubkey>
<pubkey>
<sig>
```



```
<H(pubkey)>
OP_EQUALVERIFY
OP_CHECKSIG
```

```
H(<pubkey>)
<pubkey>
<sig>
```



OP_EQUALVERIFY

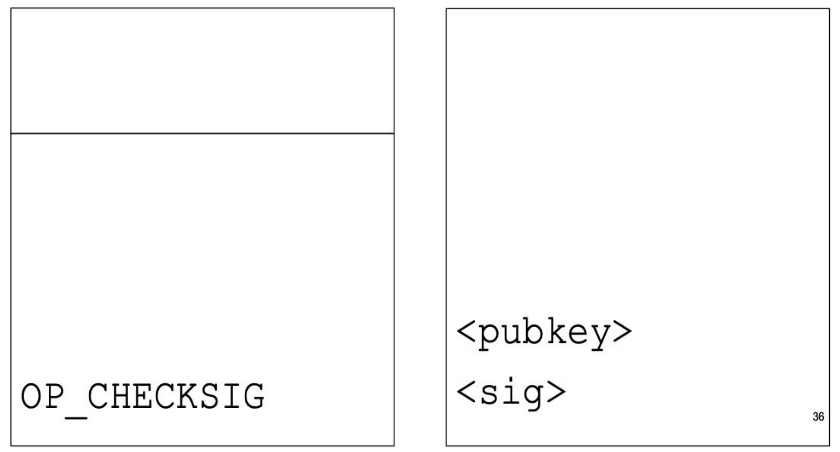
OP_CHECKSIG

<H(pubkey)>

H(<pubkey>)

<pubkey>

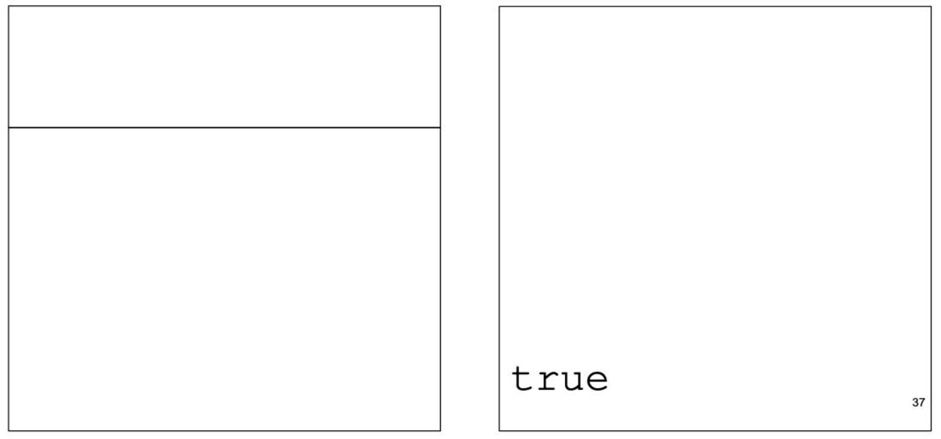
<sig>



OP_CHECKSIG

<pubkey>

<sig>



true

Block Reward and Transaction Fee

- Miners are rewarded a fixed amount of bitcoins for every block mined called Block Reward
- This acts as an incentive for the miners to mine in the first place
- In order to counter inflation bitcoin is designed to halve Block Reward for every 210,000th blocks
- So essentially there can exist at most 21 Million Bitcoins
- Miners can also earn by charging the transactions a certain fee to include them in their minted block
    - But the miner can’t enforce certain amount of fee onto a transaction instead user will generate a transaction such that *(value of input) > (value of output)*
    - And fee earned by the miner is *(value of input) - (value of output)*

Transaction Fee Only Model

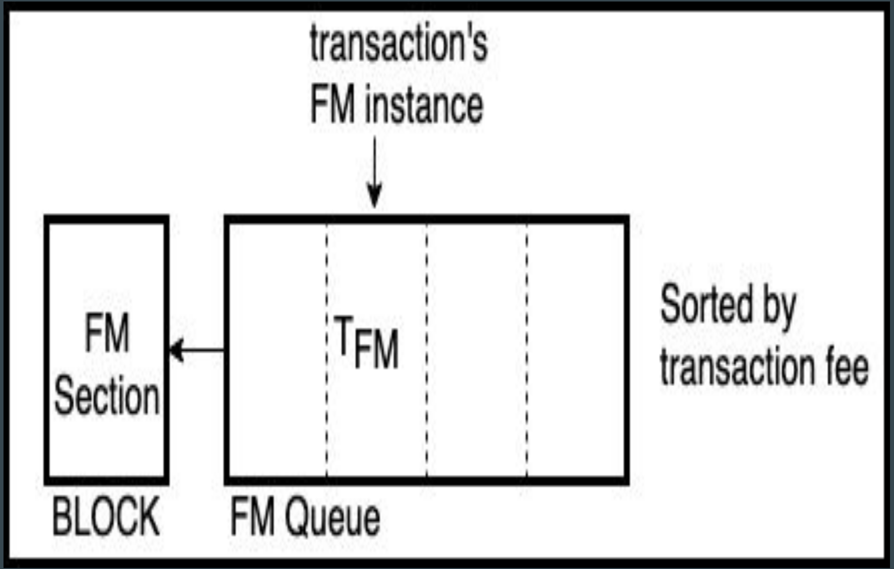
- What happens when Block Reward becomes negligible?
  - Transaction fees become the main source of revenue for miners
  - Depending on the popularity of Bitcoin transaction fees may vary

- Miners may only accept transactions with high fees into their blocks, leaving out transactions that pay low fees to suffer high waiting times (confirmation)

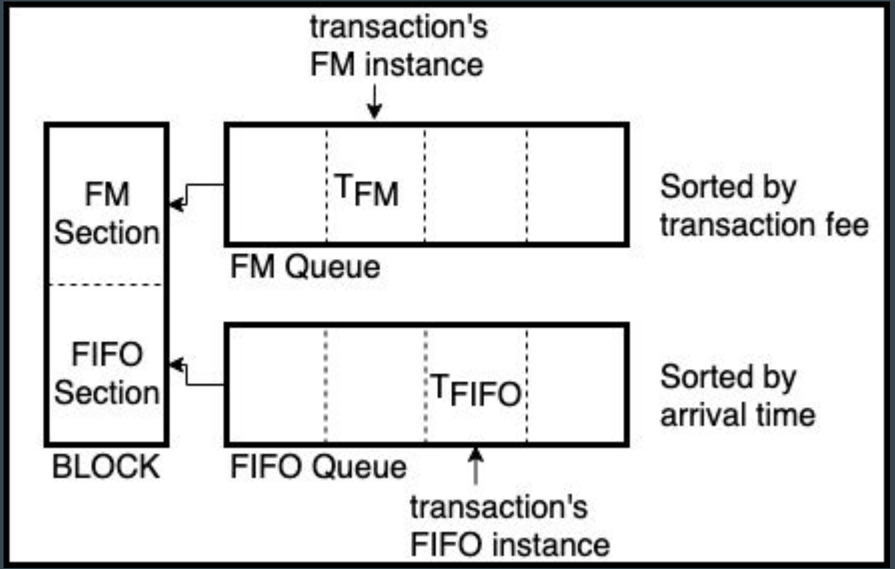
- Users may stop using Bitcoin altogether (since the fees have increased dramatically or there may be a better alternative) in which case the miners will suffer due to low revenue that makes it hard to sustain Bitcoin as a whole.

- Hence in both scenarios Bitcoin is unfair to either the users or the miners

Transaction processing in Bitcoin

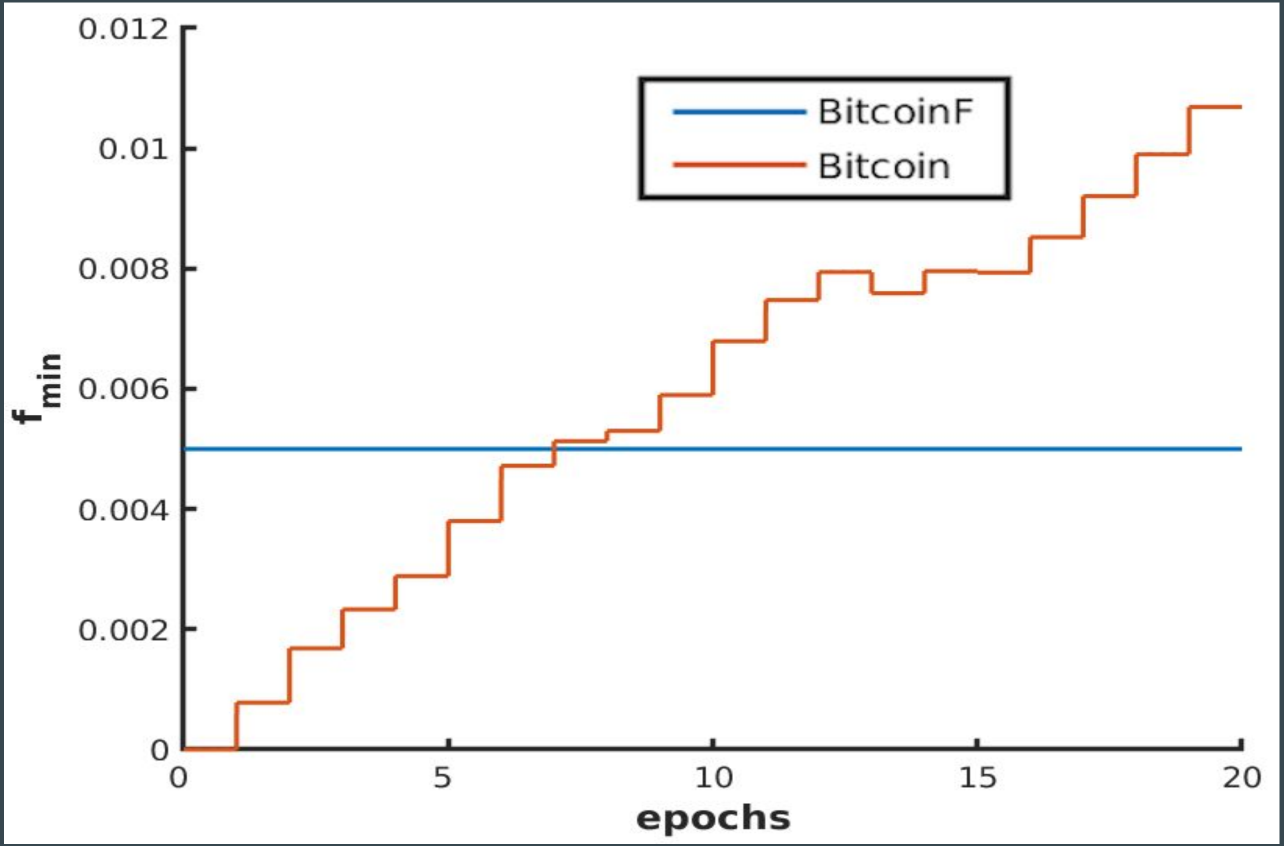


Transaction processing in BitcoinF

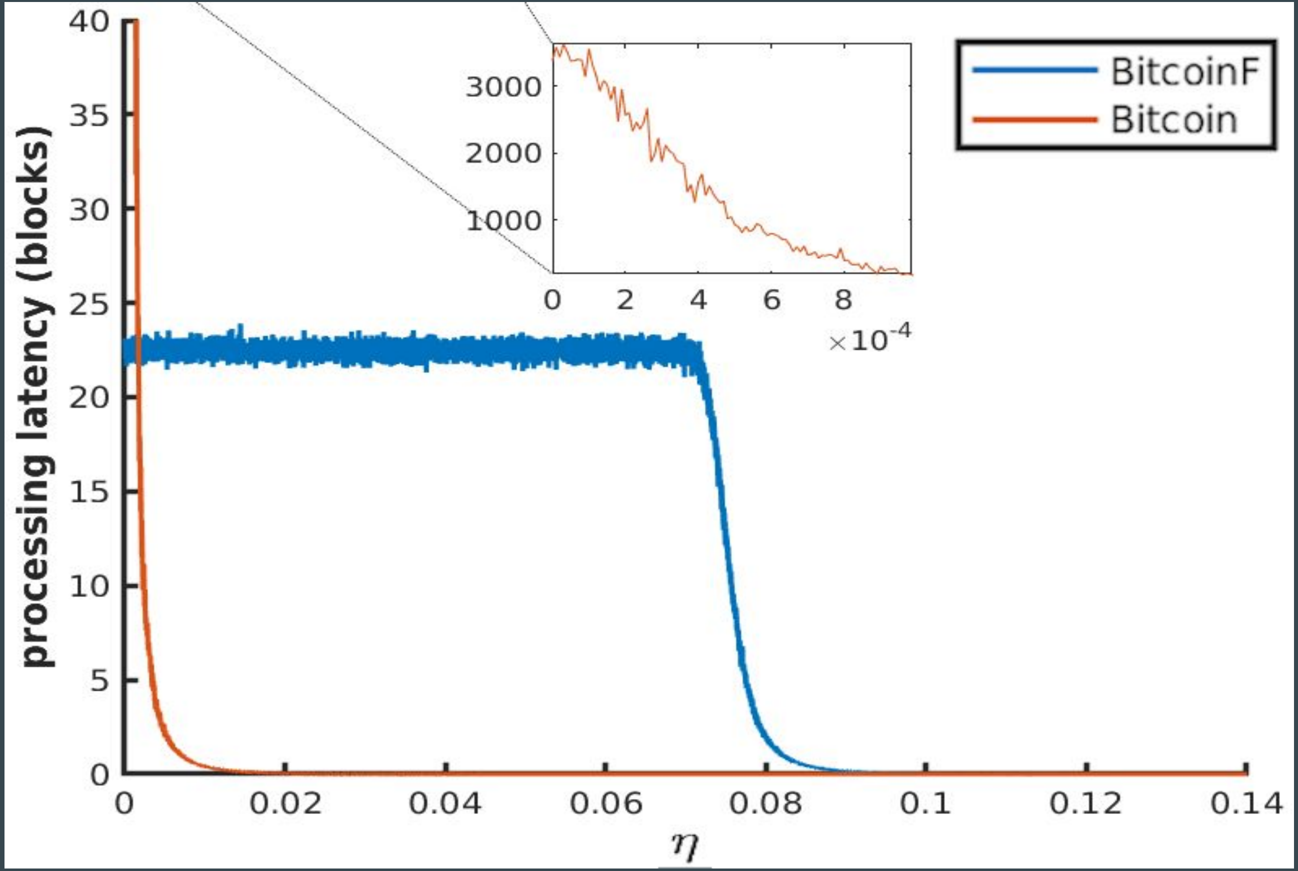


‘µ’ represents the FIFO section of the Block

f_{min} Vs steps



Processing Latency Vs Aggression level in f_{extra}



Discussion

We suggest

- μ = 0.2
- *f*_{min} = (average cost of mining a block)/(blocksize_{max})
    - Blocksize_{max} is maximum allowed number of transactions in a block assuming all transactions are optimized to a constant size

Payment Channel Network?

Thank You !
GoBuyBTC