FINE 434: FinTech

Lecture 14

Professor Fahad Saleh

McGill University - Desautels

Liveness

"New blocks will continue to be added and valid transactions with appropriate fees will be included in the blockchain within a reasonable amount of time"

i.e., We need somebody to update the ledger!

Liveness

"New blocks will continue to be added and valid transactions with appropriate fees will be included in the blockchain within a reasonable amount of time"

i.e., We need somebody to update the ledger!

... how do we induce agents/ nodes to update the ledger?

Liveness

"New blocks will continue to be added and valid transactions with appropriate fees will be included in the blockchain within a reasonable amount of time"

i.e., We need somebody to update the ledger!

... how do we induce agents/ nodes to update the ledger?

Nakamoto: Block Rewards and Transaction Fees

Two Forms of Compensation

- **Block Rewards**
  "a new coin owned [given to] the creator of the block"
- **Transaction Fees**
  Transaction Sender pays the creator of the block

"Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free."

Coinbase Transaction

"By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block."

"This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them."

Coinbase Transaction

"By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block."

"This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them."

Who funds the new coins?

Seigniorage

What is seigniorage?

If the private sector is willing to hold paper money that the government supplies, the government can buy real goods and services that the private sector produces with money that is (virtually) costless for the government to print.[1]

Welfare Implications

Proposition 3.6. *(PoW) Blockchain With Waste*

$\forall T : W_T^{Trad} \geqslant W_T^{PoW}$

- Block Rewards transfer welfare from cryptocurrency holders to miners
- Mining is competitive, so miner welfare gains are minimal
- On net, this system decreases welfare

Welfare Loss?

MENU

nature climate change

Comment | Published: 29 October 2018

Bitcoin emissions alone could push global warming above 2°C

Camilo Mora, Randi L. Rollins, Katie Taladay, Michael B. Kantar, Mason K. Chock, Mio Shimada & Erik C. Franklin

Nature Climate Change **8**, 931–933 (2018) | Download Citation

Nakamoto's Take

"If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction."

Nakamoto's Take

"If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction."

"Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free."

Economists' Take

- Fees impose no loss on cryptocurrency holders
- Fees are paid by a user if she gains from the payment
- On net, this system increases welfare

Economists' Take

- Fees impose no loss on cryptocurrency holders
- Fees are paid by a user if she gains from the payment
- On net, this system increases welfare

Is there any downside?

Instability

On the Instability of Bitcoin Without the Block Reward

Miles Carlsten
carlsten@cs.princeton.edu

Harry Kalodner
kalodner@cs.princeton.edu

S. Matthew Weinberg
smweinberg@princeton.edu

Arvind Narayanan
arvindn@cs.princeton.edu

"There has been an implicit belief that whether miners are paid by block rewards or transaction fees does not affect the security of the block chain. We show that this is not the case."

Undesirable Mining Incentives

"Our key insight is that with only transaction fees, the variance of the block reward is very high due to [possibly lengthy block times], and it becomes attractive to fork a 'wealthy' block to 'steal' the rewards therein."

BLOCKS TRANSACTIONS

Height	Age	Transactions	Miner	Size (bytes)
564397	5 minutes	2996	Unknown	1,305,983
564396	37 minutes	173	Unknown	52,076
564395	38 minutes	445	SlushPool	428,665

Block “Wealth” Inequality

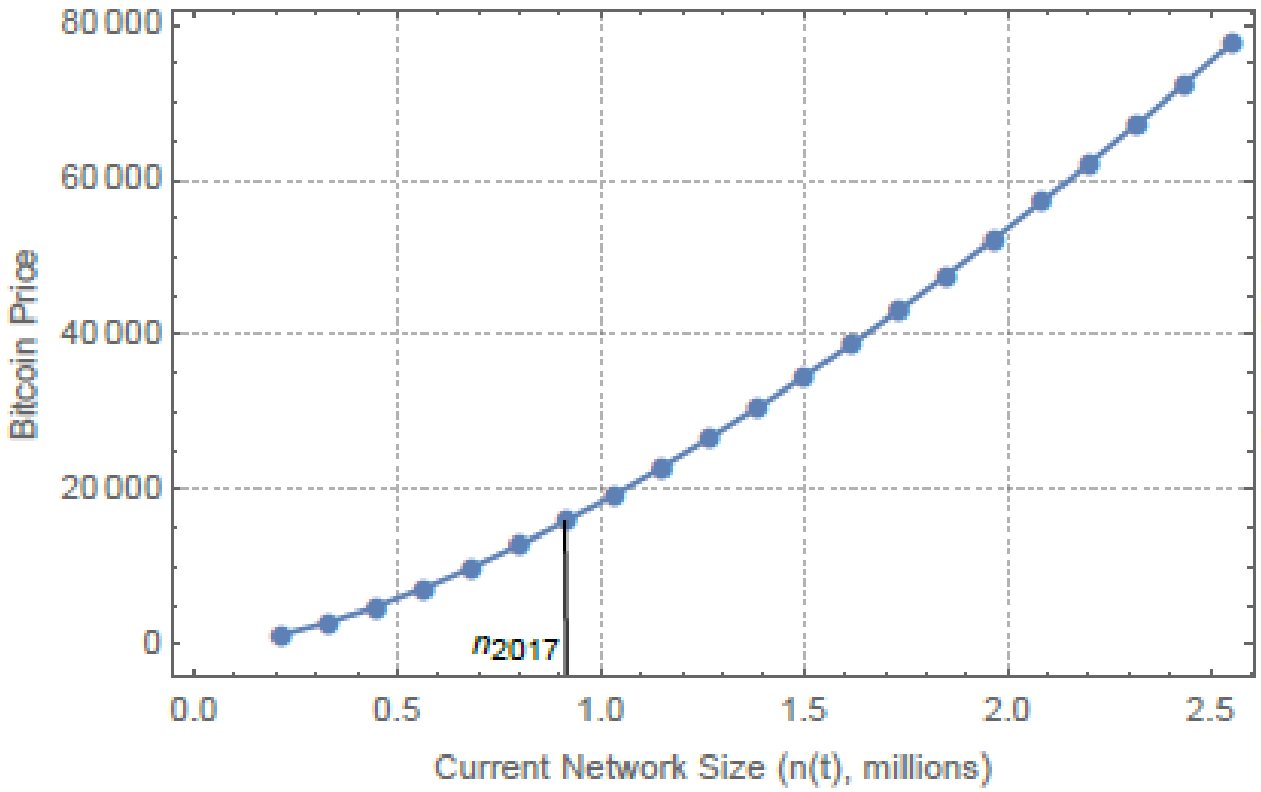
Block #564397

Summary	
Number Of Transactions	2996
Output Total	11,728.69593741 BTC
Estimated Transaction Volume	1,554.75943381 BTC
Transaction Fees	0.41330543 BTC
Height	564397 (Main Chain)
Timestamp	2019-02-24 04:17:48

Block #564396

Summary	
Number Of Transactions	173
Output Total	170.23526997 BTC
Estimated Transaction Volume	7.03022903 BTC
Transaction Fees	0.00537711 BTC
Height	564396 (Main Chain)
Timestamp	2019-02-24 03:45:19

What about liveness - why would any node even work to solve the PoW puzzle?



Source: Pagnotta and Buraschi (2018)