# FINE 434: FinTech

## Lecture 15

Professor Fahad Saleh

McGill University - Desautels

# An Economic Analysis

The blockchain folk theorem*

Bruno Biais† Christophe Bisière‡ Matthieu Bouvard§
Catherine Casamatta¶

"As argued by Nakamoto (2008) ... it is commonly assumed that a single blockchain will prevail... [We] examine the validity of that 'folk theorem'"

# An Economic Analysis

The blockchain folk theorem*

Bruno Biais† Christophe Bisière‡ Matthieu Bouvard§
Catherine Casamatta¶

"As argued by Nakamoto (2008) ... it is commonly assumed that a single blockchain will prevail... [We] examine the validity of that 'folk theorem'"

... was Nakamoto correct?

# Yes!

"[Miners] are paid in the cryptocurrency associated with the chain on which they are solving blocks... the value of that cryptocurrency depends on the credibility of the corresponding chain"

"Hence, miners benefit from coordinating on a single chain, which they can achieve by playing the longest chain rule (hereafter LCR), as suggested by Nakamoto (2008)."

# ... nevermind

"a miner who has accumulated rewards by solving several blocks on a given chain has a vested interest in this chain remaining active"

"Vested interests may counteract coordination motives for a group of miners, inducing them to keep mining a minority chain, and sustaining persistent forks in equilibrium"

**Why would honest nodes control the majority CPU power?**

They wouldn't necessarily...

**Why would honest nodes control the majority CPU power?**

They wouldn't necessarily...

... but they might and perhaps they do

More formally: There are multiple equilibria, and BTC may have obtained a good equilibrium

# Uh Oh

## Majority is not Enough: Bitcoin Mining is Vulnerable

Ittay Eyal and Emin Gün Sirer

Department of Computer Science, Cornell University
ittay.eyal@cornell.edu, egs@systems.cs.cornell.edu

# Selfish Mining

"we show that the conventional wisdom is wrong: the Bitcoin protocol, as prescribed and implemented, is not incentive-compatible. We describe a strategy [called Selfish Mining] that can be used by a minority pool to obtain more revenue than the pool's fair share, that is, more than its ratio of the total mining power."

# The Strategy

“a pool... keep[s] its discovered blocks private... The honest nodes continue to mine on the public chain, while the pool mines on its own private branch. If the pool discovers more blocks, it develops a longer lead on the public chain, and continues to keep these new blocks private. When the public branch approaches the pool’s private branch in length, the selfish miners reveal blocks from their private chain to the public.”

# Why it Works

"This strategy leads honest miners that follow the Bitcoin protocol to waste resources on mining cryptopuzzles that end up serving no purpose. Our analysis demonstrates that, while both honest and selfish parties waste some resources, the honest miners waste proportionally more, and the selfish pool's rewards exceed its share of the network's mining power, conferring it a competitive advantage and incentivizing rational miners to join the selfish mining pool."

**Are there some hidden assumptions in Nakamoto's argument?**

Yes: Nakamoto's argument precludes selfish mining

**Are there some hidden assumptions in Nakamoto's argument?**

Yes: Nakamoto's argument precludes selfish mining

Is there a reason to believe that miners might behave "honestly" irrespective?

# Blockchain Without Waste: Proof-of-Stake*

Fahad Saleh†

*McGill University, Desautels*

January 15, 2019

**Abstract**

A blockchain constitutes a distributed ledger that records transactions across a network of agents. Blockchain's value proposition requires that agents eventually agree on the ledger's contents since payments possess risk otherwise. Restricted blockchains ensure this consensus by appointing a central authority to dictate payment validity. Permissionless blockchains (e.g. Bitcoin, Ethereum), however, admit no central authority and therefore face a non-trivial issue of inducing consensus endogenously. Nakamoto (2008) provided a temporary solution to the problem by invoking an economic mechanism known as Proof-of-Work (PoW). PoW, however, lacks sustainability, so, in recent years, a variety of alternatives have been proposed. This paper studies the most famous such alternative, Proof-of-Stake (PoS). I provide the first formal economic model of PoS and demonstrate that PoS induces consensus in equilibrium. My result arises because I endogenize blockchain coin prices. Propagating disagreement introduces illiquidity and thereby reduces blockchain coin value which implies that stake-holders face an implicit cost from delaying consensus. PoS pseudo-randomly selects a stake-holder to update the blockchain and provides her an explicit monetary incentive, a "block reward," for her service. In the event of disagreement, block rewards constitute a perverse incentive, but I demonstrate that restricting updating ability to large stake-holders induces an equilibrium in which consensus obtains as soon as possible. I also demonstrate that consensus obtains eventually almost surely in any equilibrium so long as the blockchain employs a modest block reward schedule. My work reveals the economic viability of permissionless blockchains.