Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System

by Gur Huberman, Jacob D. Leshno, and Ciamac Moallemi

Discussed by Thomas Noe

Bank of Finland/CEPR Conference
Money in the Digital Age

12 June, 2018

Saïd Business School
UNIVERSITY OF OXFORD

OUTLINE

BITCOIN AND DIGITAL CURRENCIES

- Bitcoin–Viable financial asset or tulip?
  - Liquidity demand
  - Speculative demand
  - Money or bubble
- Bitcoin—Viability of the blockchain transaction mechanism?
  - Manipulation by strategic miners: hidden blocks, forks
  - Economic sustainability with "honest" miners.

BITCOIN AND DIGITAL CURRENCIES

- Bitcoin–Viable financial asset or tulip?
  - Liquidity demand
  - Speculative demand
  - Money or bubble
- Bitcoin—Viability of the blockchain transaction mechanism?
  - Manipulation by strategic miners: hidden blocks, forks
  - Economic sustainability with "honest" miners.

BITCOIN AND DIGITAL CURRENCIES

- Bitcoin–Viable financial asset or tulip?
  - Liquidity demand
  - Speculative demand
  - Money or bubble
- Bitcoin—Viability of the blockchain transaction mechanism?
  - Manipulation by strategic miners: hidden blocks, forks
  - Economic sustainability with "honest" miners.

BITCOIN AND DIGITAL CURRENCIES

- Bitcoin–Viable financial asset or tulip?
  - Liquidity demand
  - Speculative demand
  - Money or bubble
- Bitcoin—Viability of the blockchain transaction mechanism?
  - Manipulation by strategic miners: hidden blocks, forks
  - Economic sustainability with "honest" miners.

Saïd Business School
UNIVERSITY OF OXFORD

BITCOIN AND DIGITAL CURRENCIES

- Bitcoin–Viable financial asset or tulip?
  - Liquidity demand
  - Speculative demand
  - Money or bubble
- Bitcoin—Viability of the blockchain transaction mechanism?
  - Manipulation by strategic miners: hidden blocks, forks
  - Economic sustainability with "honest" miners.

BITCOIN AND DIGITAL CURRENCIES

- Bitcoin–Viable financial asset or tulip?
  - Liquidity demand
  - Speculative demand
  - Money or bubble
- Bitcoin—Viability of the blockchain transaction mechanism?
  - Manipulation by strategic miners: hidden blocks, forks
  - Economic sustainability with "honest" miners.

BITCOIN AND DIGITAL CURRENCIES

- Bitcoin–Viable financial asset or tulip?
  - Liquidity demand
  - Speculative demand
  - Money or bubble
- Bitcoin—Viability of the blockchain transaction mechanism?
  - Manipulation by strategic miners: hidden blocks, forks
  - Economic sustainability with "honest" miners.

SUSTAINABILITY

- Two sides of transaction-processing market:
  - Bitcoin users: submit transaction with attached processing fees
  - Miners: Process transactions
- Constraints on system:
  - Inherent to a block chain system: Minimum # of miners to prevent strategic miner behaviour
  - Specific to Bitcoin protocol: Fixed rate of block creation

SUSTAINABILITY

- Two sides of transaction-processing market:
  - Bitcoin users: submit transaction with attached processing fees
  - Miners: Process transactions
- Constraints on system:
  - Inherent to a block chain system: Minimum # of miners to prevent strategic miner behaviour
  - Specific to Bitcoin protocol: Fixed rate of block creation

SUSTAINABILITY

- Two sides of transaction-processing market:
  - Bitcoin users: submit transaction with attached processing fees
  - Miners: Process transactions
- Constraints on system:
  - Inherent to a block chain system: Minimum # of miners to prevent strategic miner behaviour
  - Specific to Bitcoin protocol: Fixed rate of block creation

SUSTAINABILITY

- Two sides of transaction-processing market:
  - Bitcoin users: submit transaction with attached processing fees
  - Miners: Process transactions
- Constraints on system:
  - Inherent to a block chain system: Minimum # of miners to prevent strategic miner behaviour
  - Specific to Bitcoin protocol: Fixed rate of block creation

SUSTAINABILITY

- Two sides of transaction-processing market:
  - Bitcoin users: submit transaction with attached processing fees
  - Miners: Process transactions
- Constraints on system:
  - Inherent to a block chain system: Minimum # of miners to prevent strategic miner behaviour
  - Specific to Bitcoin protocol: Fixed rate of block creation

SUSTAINABILITY

- Two sides of transaction-processing market:
  - Bitcoin users: submit transaction with attached processing fees
  - Miners: Process transactions
- Constraints on system:
  - Inherent to a block chain system: Minimum # of miners to prevent strategic miner behaviour
  - Specific to Bitcoin protocol: Fixed rate of block creation

OUTLINE

USER SIDE

- Auction in which users bid fees in order to win processing
- Paper shows that fee-bidding mechanism is equivalent to an efficient VGA
- So fees assign priority efficiently to users based on the externality the users impose on the system

USER SIDE

- Auction in which users bid fees in order to win processing
- Paper shows that fee-bidding mechanism is equivalent to an efficient VGA
- So fees assign priority efficiently to users based on the externality the users impose on the system

USER SIDE

- Auction in which users bid fees in order to win processing
- Paper shows that fee-bidding mechanism is equivalent to an efficient VGA
- So fees assign priority efficiently to users based on the externality the users impose on the system

MINER SIDE

- Binary-effort all-pay auction:
  - Miners compete to attach blocks to the chain through solving a "puzzle"
  - Miners cannot vary the intensity of their efforts (hence binary): (a) mine and pay a fixed effort cost, c_m or (b) not mine.
  - First to solve wins, efforts of others wasted (hence all-pay)
  - Free entry into mining
  - So competition dissipates miner rents, and effort costs and mining revenue determine the number of miners.

MINER SIDE

- Binary-effort all-pay auction:
  - Miners compete to attach blocks to the chain through solving a "puzzle"
  - Miners cannot vary the intensity of their efforts (hence binary): (a) mine and pay a fixed effort cost, c_m or (b) not mine.
  - First to solve wins, efforts of others wasted (hence all-pay)
  - Free entry into mining
  - So competition dissipates miner rents, and effort costs and mining revenue determine the number of miners.

MINER SIDE

- Binary-effort all-pay auction:
  - Miners compete to attach blocks to the chain through solving a "puzzle"
  - Miners cannot vary the intensity of their efforts (hence binary): (a) mine and pay a fixed effort cost, c_m or (b) not mine.
  - First to solve wins, efforts of others wasted (hence all-pay)
  - Free entry into mining
  - So competition dissipates miner rents, and effort costs and mining revenue determine the number of miners.

MINER SIDE

- Binary-effort all-pay auction:
  - Miners compete to attach blocks to the chain through solving a "puzzle"
  - Miners cannot vary the intensity of their efforts (hence binary): (a) mine and pay a fixed effort cost, c_m or (b) not mine.
  - First to solve wins, efforts of others wasted (hence all-pay)
  - Free entry into mining
  - So competition dissipates miner rents, and effort costs and mining revenue determine the number of miners.

MINER SIDE

- Binary-effort all-pay auction:
  - Miners compete to attach blocks to the chain through solving a "puzzle"
  - Miners cannot vary the intensity of their efforts (hence binary): (a) mine and pay a fixed effort cost, c_m or (b) not mine.
  - First to solve wins, efforts of others wasted (hence all-pay)
  - Free entry into mining
  - So competition dissipates miner rents, and effort costs and mining revenue determine the number of miners.

MINER SIDE

- Binary-effort all-pay auction:
  - Miners compete to attach blocks to the chain through solving a "puzzle"
  - Miners cannot vary the intensity of their efforts (hence binary): (a) mine and pay a fixed effort cost, c_m or (b) not mine.
  - First to solve wins, efforts of others wasted (hence all-pay)
  - Free entry into mining
  - So competition dissipates miner rents, and effort costs and mining revenue determine the number of miners.

CONTRIBUTION

- Developing a framework of analysis for fundamentally new form of economic organization
  - Framework applicable beyond the cryptocurrency setting:
    - Many ICOs, e.g. Filecoin, involve the same user fee/miner economic model
- Applying the framework to Bitcoin:
  - Congestion required to generate sufficient miner profits to induce a stability-assuring number of miners
  - To much congestion will lead to user exit.
  - With stochastic demand, and the Bitcoin protocol restriction, hard to assure optimal congestion
- Use the analysis of Bitcoin to provide concrete policy suggestions

Saïd Business School
UNIVERSITY OF OXFORD

CONTRIBUTION

- Developing a framework of analysis for fundamentally new form of economic organization
  - Framework applicable beyond the cryptocurrency setting:
    - ⋆ Many ICOs, e.g. Filecoin, involve the same user fee/miner economic model
- Applying the framework to Bitcoin:
  - Congestion required to generate sufficient miner profits to induce a stability-assuring number of miners
  - To much congestion will lead to user exit.
  - With stochastic demand, and the Bitcoin protocol restriction, hard to assure optimal congestion
- Use the analysis of Bitcoin to provide concrete policy suggestions

CONTRIBUTION

- Developing a framework of analysis for fundamentally new form of economic organization
  - Framework applicable beyond the cryptocurrency setting:
    - ★ Many ICOs, e.g. Filecoin, involve the same user fee/miner economic model
- Applying the framework to Bitcoin:
  - Congestion required to generate sufficient miner profits to induce a stability-assuring number of miners
  - To much congestion will lead to user exit.
  - With stochastic demand, and the Bitcoin protocol restriction, hard to assure optimal congestion
- Use the analysis of Bitcoin to provide concrete policy suggestions

CONTRIBUTION

- Developing a framework of analysis for fundamentally new form of economic organization
  - Framework applicable beyond the cryptocurrency setting:
    - ★ Many ICOs, e.g. Filecoin, involve the same user fee/miner economic model
- Applying the framework to Bitcoin:
  - Congestion required to generate sufficient miner profits to induce a stability-assuring number of miners
  - To much congestion will lead to user exit.
  - With stochastic demand, and the Bitcoin protocol restriction, hard to assure optimal congestion
- Use the analysis of Bitcoin to provide concrete policy suggestions

CONTRIBUTION

- Developing a framework of analysis for fundamentally new form of economic organization
  - Framework applicable beyond the cryptocurrency setting:
    - ★ Many ICOs, e.g. Filecoin, involve the same user fee/miner economic model
- Applying the framework to Bitcoin:
  - Congestion required to generate sufficient miner profits to induce a stability-assuring number of miners
  - To much congestion will lead to user exit.
  - With stochastic demand, and the Bitcoin protocol restriction, hard to assure optimal congestion
- Use the analysis of Bitcoin to provide concrete policy suggestions

CONTRIBUTION

- Developing a framework of analysis for fundamentally new form of economic organization
  - Framework applicable beyond the cryptocurrency setting:
    - ★ Many ICOs, e.g. Filecoin, involve the same user fee/miner economic model
- Applying the framework to Bitcoin:
  - Congestion required to generate sufficient miner profits to induce a stability-assuring number of miners
  - To much congestion will lead to user exit.
  - With stochastic demand, and the Bitcoin protocol restriction, hard to assure optimal congestion
- Use the analysis of Bitcoin to provide concrete policy suggestions

CONTRIBUTION

- Developing a framework of analysis for fundamentally new form of economic organization
  - Framework applicable beyond the cryptocurrency setting:
    - ★ Many ICOs, e.g. Filecoin, involve the same user fee/miner economic model
- Applying the framework to Bitcoin:
  - Congestion required to generate sufficient miner profits to induce a stability-assuring number of miners
  - To much congestion will lead to user exit.
  - With stochastic demand, and the Bitcoin protocol restriction, hard to assure optimal congestion
- Use the analysis of Bitcoin to provide concrete policy suggestions

CONTRIBUTION

- Developing a framework of analysis for fundamentally new form of economic organization
  - Framework applicable beyond the cryptocurrency setting:
    - ★ Many ICOs, e.g. Filecoin, involve the same user fee/miner economic model
- Applying the framework to Bitcoin:
  - Congestion required to generate sufficient miner profits to induce a stability-assuring number of miners
  - To much congestion will lead to user exit.
  - With stochastic demand, and the Bitcoin protocol restriction, hard to assure optimal congestion
- Use the analysis of Bitcoin to provide concrete policy suggestions

OUTLINE

CONTRIBUTION

- Analysis of user side of the transaction processing excellent and a major advance relative to the literature (e.g., Easley,OHara, and Basu, 2017).
- The analysis of the miner side is a bit less satisfying: hard to understand what is going on a micro level.
- Effect of the fluctuation of bit coin prices in dollar terms on stability might be worth considering

CONTRIBUTION

- Analysis of user side of the transaction processing excellent and a major advance relative to the literature (e.g., Easley,OHara, and Basu, 2017).
- The analysis of the miner side is a bit less satisfying: hard to understand what is going on a micro level.
- Effect of the fluctuation of bit coin prices in dollar terms on stability might be worth considering

CONTRIBUTION

- Analysis of user side of the transaction processing excellent and a major advance relative to the literature (e.g., Easley,OHara, and Basu, 2017).
- The analysis of the miner side is a bit less satisfying: hard to understand what is going on a micro level.
- Effect of the fluctuation of bit coin prices in dollar terms on stability might be worth considering

IS THE BLOCK-SIZE UPPER BOUND A BINDING CONSTRAINT?

- Miners can choose to submit smaller block than the upper bound on block size.
- is the assumption that they will always submit blocks equal to the minimum of the number of transactions in the mempool and the upper bound rationalizable by equilibrium behaviour?
- The fixed-cost of puzzle solving militates for maximum block size
- But could a few transactions with sufficiently large processing fee in a mempool with sufficiently low arrival intensity make pre-emptively processing a smaller block optimal?

IS THE BLOCK-SIZE UPPER BOUND A BINDING CONSTRAINT?

- Miners can choose to submit smaller block than the upper bound on block size.
- is the assumption that they will always submit blocks equal to the minimum of the number of transactions in the mempool and the upper bound rationalizable by equilibrium behaviour?
- The fixed-cost of puzzle solving militates for maximum block size
- But could a few transactions with sufficiently large processing fee in a mempool with sufficiently low arrival intensity make pre-emptively processing a smaller block optimal?

IS THE BLOCK-SIZE UPPER BOUND A BINDING CONSTRAINT?

- Miners can choose to submit smaller block than the upper bound on block size.
- is the assumption that they will always submit blocks equal to the minimum of the number of transactions in the mempool and the upper bound rationalizable by equilibrium behaviour?
- The fixed-cost of puzzle solving militates for maximum block size
- But could a few transactions with sufficiently large processing fee in a mempool with sufficiently low arrival intensity make pre-emptively processing a smaller block optimal?

IS THE BLOCK-SIZE UPPER BOUND A BINDING CONSTRAINT?

- Miners can choose to submit smaller block than the upper bound on block size.
- is the assumption that they will always submit blocks equal to the minimum of the number of transactions in the mempool and the upper bound rationalizable by equilibrium behaviour?
- The fixed-cost of puzzle solving militates for maximum block size
- But could a few transactions with sufficiently large processing fee in a mempool with sufficiently low arrival intensity make pre-emptively processing a smaller block optimal?

OPTIMAL TO PROCESS THE TRANSACTIONS IN ORDER OF FEES?

- Suppose the block limit is 100,
- 100 miners are mining
- 200 transactions are in the mempool,
  - 100 with high fees and
  - 100 with low fees
- 99 of the 100 miners are competing to process the 100 high fee transactions, each having a 1/99 chance of attaching this block to the chain
- could the remaining miner increase revenue by processing the 100 low fee transactions rather than joining in the competition to process the high fee transactions?

Saïd Business School
UNIVERSITY OF OXFORD

OPTIMAL TO PROCESS THE TRANSACTIONS IN ORDER OF FEES?

- Suppose the block limit is 100,
- 100 miners are mining
- 200 transactions are in the mempool,
  - 100 with high fees and
  - 100 with low fees
- 99 of the 100 miners are competing to process the 100 high fee transactions, each having a 1/99 chance of attaching this block to the chain
- could the remaining miner increase revenue by processing the 100 low fee transactions rather than joining in the competition to process the high fee transactions?

OPTIMAL TO PROCESS THE TRANSACTIONS IN ORDER OF FEES?

- Suppose the block limit is 100,
- 100 miners are mining
- 200 transactions are in the mempool,
  - 100 with high fees and
  - 100 with low fees
- 99 of the 100 miners are competing to process the 100 high fee transactions, each having a 1/99 chance of attaching this block to the chain
- could the remaining miner increase revenue by processing the 100 low fee transactions rather than joining in the competition to process the high fee transactions?

OPTIMAL TO PROCESS THE TRANSACTIONS IN ORDER OF FEES?

- Suppose the block limit is 100,
- 100 miners are mining
- 200 transactions are in the mempool,
  - 100 with high fees and
  - 100 with low fees
- 99 of the 100 miners are competing to process the 100 high fee transactions, each having a 1/99 chance of attaching this block to the chain
- could the remaining miner increase revenue by processing the 100 low fee transactions rather than joining in the competition to process the high fee transactions?

OPTIMAL TO PROCESS THE TRANSACTIONS IN ORDER OF FEES?

- Suppose the block limit is 100,
- 100 miners are mining
- 200 transactions are in the mempool,
  - 100 with high fees and
  - 100 with low fees
- 99 of the 100 miners are competing to process the 100 high fee transactions, each having a 1/99 chance of attaching this block to the chain
- could the remaining miner increase revenue by processing the 100 low fee transactions rather than joining in the competition to process the high fee transactions?

OPTIMAL TO PROCESS THE TRANSACTIONS IN ORDER OF FEES?

- Suppose the block limit is 100,
- 100 miners are mining
- 200 transactions are in the mempool,
  - 100 with high fees and
  - 100 with low fees
- 99 of the 100 miners are competing to process the 100 high fee transactions, each having a 1/99 chance of attaching this block to the chain
- could the remaining miner increase revenue by processing the 100 low fee transactions rather than joining in the competition to process the high fee transactions?

OPTIMAL TO PROCESS THE TRANSACTIONS IN ORDER OF FEES?

- Suppose the block limit is 100,
- 100 miners are mining
- 200 transactions are in the mempool,
  - 100 with high fees and
  - 100 with low fees
- 99 of the 100 miners are competing to process the 100 high fee transactions, each having a 1/99 chance of attaching this block to the chain
- could the remaining miner increase revenue by processing the 100 low fee transactions rather than joining in the competition to process the high fee transactions?

INTENSITY OF MINING AND ALL PAY AUCTIONS

- Can miners vary the intensity of mining effort?
- $\mathbb{E}[\text{time to solution}] = t$ and cost equals $c(t)$ where c is decreasing and convex?
- If so, problem maps into models of R&D all-pay competitions
- Rents are dissipated but total revenue will not fix number of miners
- Equilibria both with many lazy miners or a few aggressive minors exist
- Equilibria with a few miners are much more efficient (Che & Gale, 2003)

INTENSITY OF MINING AND ALL PAY AUCTIONS

- Can miners vary the intensity of mining effort?
- $\mathbb{E}[\text{time to solution}] = t$ and cost equals $c(t)$ where c is decreasing and convex?
- If so, problem maps into models of R&D all-pay competitions
- Rents are dissipated but total revenue will not fix number of miners
- Equilibria both with many lazy miners or a few aggressive minors exist
- Equilibria with a few miners are much more efficient (Che & Gale, 2003)

INTENSITY OF MINING AND ALL PAY AUCTIONS

- Can miners vary the intensity of mining effort?
- $\mathbb{E}[\text{time to solution}] = t$ and cost equals $c(t)$ where c is decreasing and convex?
- If so, problem maps into models of R&D all-pay competitions
- Rents are dissipated but total revenue will not fix number of miners
- Equilibria both with many lazy miners or a few aggressive minors exist
- Equilibria with a few miners are much more efficient (Che & Gale, 2003)

INTENSITY OF MINING AND ALL PAY AUCTIONS

- Can miners vary the intensity of mining effort?
- $\mathbb{E}[\text{time to solution}] = t$ and cost equals $c(t)$ where c is decreasing and convex?
- If so, problem maps into models of R&D all-pay competitions
- Rents are dissipated but total revenue will not fix number of miners
- Equilibria both with many lazy miners or a few aggressive minors exist
- Equilibria with a few miners are much more efficient (Che & Gale, 2003)

INTENSITY OF MINING AND ALL PAY AUCTIONS

- Can miners vary the intensity of mining effort?
- $\mathbb{E}[\text{time to solution}] = t$ and cost equals $c(t)$ where c is decreasing and convex?
- If so, problem maps into models of R&D all-pay competitions
- Rents are dissipated but total revenue will not fix number of miners
- Equilibria both with many lazy miners or a few aggressive minors exist
- Equilibria with a few miners are much more efficient (Che & Gale, 2003)

INTENSITY OF MINING AND ALL PAY AUCTIONS

- Can miners vary the intensity of mining effort?
- $\mathbb{E}[\text{time to solution}] = t$ and cost equals $c(t)$ where c is decreasing and convex?
- If so, problem maps into models of R&D all-pay competitions
- Rents are dissipated but total revenue will not fix number of miners
- Equilibria both with many lazy miners or a few aggressive minors exist
- Equilibria with a few miners are much more efficient (Che & Gale, 2003)

BITCOIN VOLATILITY AND DENOMINATION RISK

- Bitcoin's volatility in currency terms is huge: approx 40x the S&P500
- Effort cost (CPU time ?) cost will be denominated in dollars but miners will be paid in Bitcoins
- User waiting costs could be dollar costs or Bitcoin costs
  - speculative vs.
  - transactional demand
- Could a shock to the value of bit coins reduce the number of miners below the stability-assuring minimum?

BITCOIN VOLATILITY AND DENOMINATION RISK

- Bitcoin's volatility in currency terms is huge: approx 40x the S&P500
- Effort cost (CPU time ?) cost will be denominated in dollars but miners will be paid in Bitcoins
- User waiting costs could be dollar costs or Bitcoin costs
  - speculative vs.
  - transactional demand
- Could a shock to the value of bit coins reduce the number of miners below the stability-assuring minimum?

Said Business School
UNIVERSITY OF OXFORD

BITCOIN VOLATILITY AND DENOMINATION RISK

- Bitcoin's volatility in currency terms is huge: approx 40x the S&P500
- Effort cost (CPU time ?) cost will be denominated in dollars but miners will be paid in Bitcoins
- User waiting costs could be dollar costs or Bitcoin costs
  - speculative vs.
  - transactional demand
- Could a shock to the value of bit coins reduce the number of miners below the stability-assuring minimum?

BITCOIN VOLATILITY AND DENOMINATION RISK

- Bitcoin's volatility in currency terms is huge: approx 40x the S&P500
- Effort cost (CPU time ?) cost will be denominated in dollars but miners will be paid in Bitcoins
- User waiting costs could be dollar costs or Bitcoin costs
  - speculative vs.
  - transactional demand
- Could a shock to the value of bit coins reduce the number of miners below the stability-assuring minimum?

BITCOIN VOLATILITY AND DENOMINATION RISK

- Bitcoin's volatility in currency terms is huge: approx 40x the S&P500
- Effort cost (CPU time ?) cost will be denominated in dollars but miners will be paid in Bitcoins
- User waiting costs could be dollar costs or Bitcoin costs
  - speculative vs.
  - transactional demand
- Could a shock to the value of bit coins reduce the number of miners below the stability-assuring minimum?

BITCOIN VOLATILITY AND DENOMINATION RISK

- Bitcoin's volatility in currency terms is huge: approx 40x the S&P500
- Effort cost (CPU time ?) cost will be denominated in dollars but miners will be paid in Bitcoins
- User waiting costs could be dollar costs or Bitcoin costs
  - speculative vs.
  - transactional demand
- Could a shock to the value of bit coins reduce the number of miners below the stability-assuring minimum?

CONCLUSION

- Paper is well worth reading
- Both for the specific insights it provides into Bitcoin and for its "translation" of the Bitcoin mechanism into the language of economics
- Paper needs a resolve the degree to which the specified mining strategies are "hardwired," and and thus perhaps suboptimal, vs. being weakly dominant strategies vs. being strategies that can be supported by a Nash equilibrium
- More analysis of miner block-forming strategies required but perhaps not in this paper or by these authors.

CONCLUSION

- Paper is well worth reading
- Both for the specific insights it provides into Bitcoin and for its "translation" of the Bitcoin mechanism into the language of economics
- Paper needs a resolve the degree to which the specified mining strategies are "hardwired," and and thus perhaps suboptimal, vs. being weakly dominant strategies vs. being strategies that can be supported by a Nash equilibrium
- More analysis of miner block-forming strategies required but perhaps not in this paper or by these authors.

CONCLUSION

- Paper is well worth reading
- Both for the specific insights it provides into Bitcoin and for its "translation" of the Bitcoin mechanism into the language of economics
- Paper needs a resolve the degree to which the specified mining strategies are "hardwired," and and thus perhaps suboptimal, vs. being weakly dominant strategies vs. being strategies that can be supported by a Nash equilibrium
- More analysis of miner block-forming strategies required but perhaps not in this paper or by these authors.

CONCLUSION

- Paper is well worth reading
- Both for the specific insights it provides into Bitcoin and for its "translation" of the Bitcoin mechanism into the language of economics
- Paper needs a resolve the degree to which the specified mining strategies are "hardwired," and and thus perhaps suboptimal, vs. being weakly dominant strategies vs. being strategies that can be supported by a Nash equilibrium
- More analysis of miner block-forming strategies required but perhaps not in this paper or by these authors.