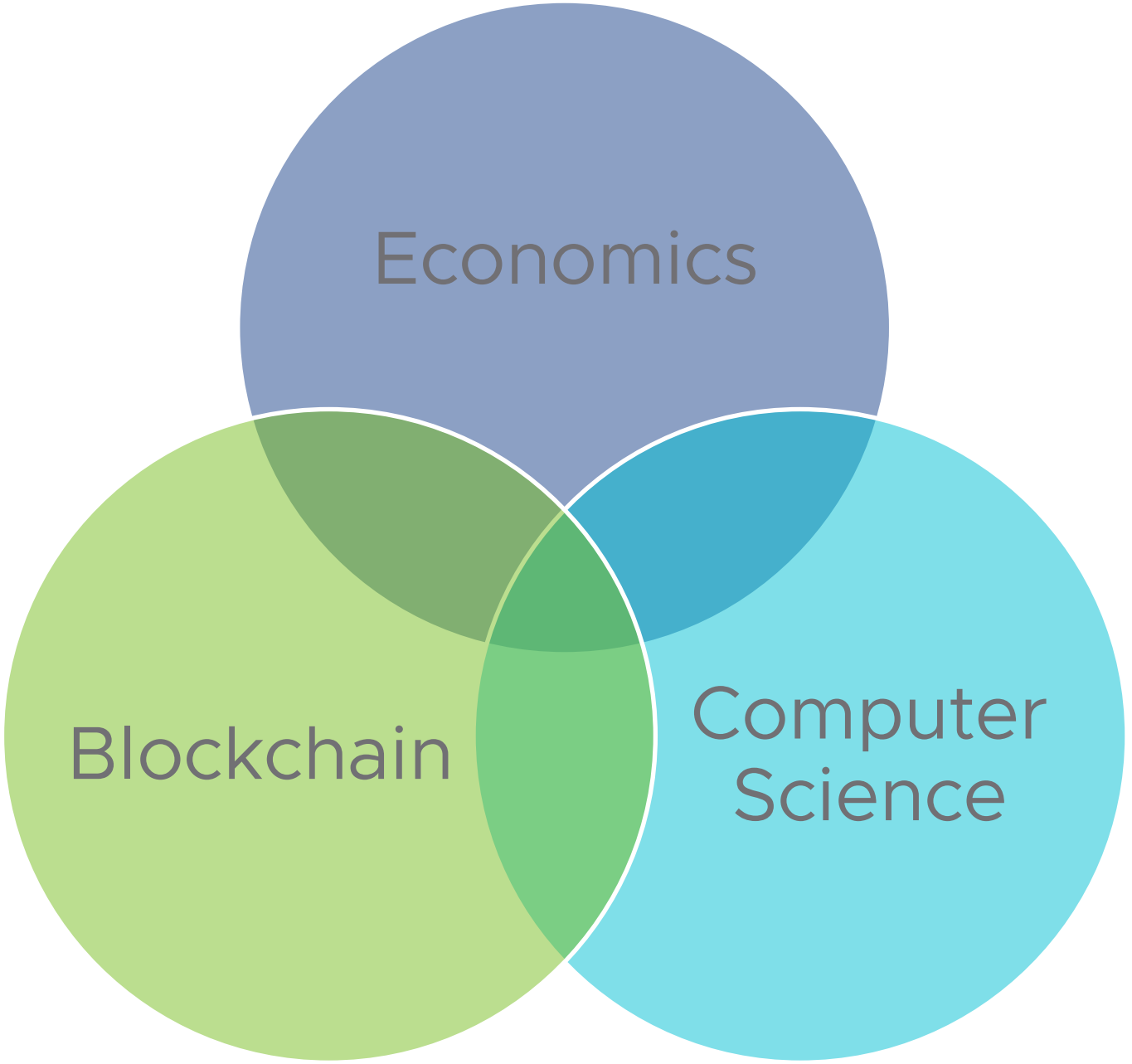
When Nakamoto meets Nash

Blockchain breakthrough through the lens of Game Theory

October 2020

vmware®



Plan: Money, Trust, Fairness, and Welfare

1. Modeling Money Endogenously
2. Incentivizing Trust (how, who, scale)
3. Incentivizing Fairness
4. Incentivizing Welfare

1: Modeling Money Endogenously

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a **trusted third party**"

Satoshi Nakamoto, bitcoin whitepaper, 2008

Traditional: Defining Money Exogenously

1. Money is a medium of exchange
   - “electronic payment system”
2. Money is a scarce resource
   - “21 Million Bitcoins”
3. Money is a store of value
   - “replace trust third party”

Game theory: players have preferences over outcomes (utility function)

Traditional: Modeling Money exogenously

- Money is singular, more money is better, Money is transferable utility

Reality: there are many Money Systems

- Some are better than others
- Need a microeconomic theory of competition between Money Systems

Breakthrough: Defining Money Endogenously

Utility of Money Systems:

1. **Friction**: How good they are as a medium of exchange
2. **Fairness**: How good they are as a scarce resource
3. **Trust**: How good they are as a store of value

Bitcoin (and later cryptocurrencies) offer a new Money System:

1. Electronic payments based on cryptography for reduced friction
2. Limited supply, circulation by participation with exponential decay for fairness
3. Byzantine Fault Tolerance for trust (more on BFT later)

Open Question 1:

A game theoretic endogenous theory of the utility of Money Systems

(that can model friction, fairness, and trust)

2: Incentivizing Trust

2a: trust there is no double spend

2b: who is maintaining trust?

2b: trust and scalability

"A common solution is to introduce a trusted central authority … The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank."

Satoshi Nakamoto, bitcoin whitepaper, 2008

vmware

“The proof-of-work chain is a solution to the Byzantine Generals’ Problem. I’ll try to rephrase it in that context”

Satoshi Nakamoto, email archive, 2008

vmware®

Distributed Computing Meets Game Theory

Distributed Computing:

- n-f Good guys, f bad guys
- Protocol (strategy) is tolerant to an adversary controlling f bad guys if:
  - no matter who the f bad guys are, if the good guys run (play) the protocol (strategy)
  - then the "properties" of the protocol hold
- Key notion of Byzantine Fault Tolerance in Distributed Computing and Cryptography

Game Theory:

- n players, all are rational
- Protocol (strategy) is robust to coalitions of size f, if:
  - No matter who the coalition of f are, if the other players run (play) the protocol (strategy)
  - **and the coalition plays a best response;**
  - then the "properties" of the protocol hold
- Key notion of Coalition Resistant Equilibrium in Game Theory

Rational player

A best response

"If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth."

Satoshi Nakamoto, bitcoin whitepaper, 2008

Play the equilibrium strategy

Open Question 2a:

A game theoretic theory of Consensus and a game theoretic analogue to Byzantine Fault Tolerance

2: Incentivizing Trust

2a: trust there is no double spend

2b: who is maintaining trust?

2b: trust and scalability

Blockchain: decentralized voting power

Who is allowed to vote?

France: All adult males (1793, 1848). Adult women (1944).

US Adult women (1920). Only citizens (today)

Choosing who is allowed to vote chooses how power is distributed

In Computer science we assume an adversary, want to restrict the voting power of the adversary

- In Bitcoin, assume the adversary controls less than 51% of mining (=voting) power
- “The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.”

Who is allowed to Vote? Power of the adversary

Who has voting power? How do you prove you possess this voting power?

- If the adversary controlled all the voting power, then we would be doomed

Proof of Membership: One member One vote

- Traditional ”permissioned” model, adversary controls fraction of the members

Proof of Work: One CPU One vote

- The bitcoin revolution, mildly hard cryptographic puzzles, adversary controls fraction of the CPU
- Called the “permissionless” model.

Proof of Stake: One coin One vote

- allows punishment via slashing, adversary controls fraction of the stake

Proof of Space: One GB of storage one vote

- Many new definitions along with new mildly hard cryptographic puzzles
- Proof of space-time, Proof of replication, etc

Who is allowed to Vote? Plutocracy?

Decentralization in Bitcoin and Ethereum Networks [Gencer etal 2018]

- Few (less than 15) large mining pools
- Very few large ASIC providers (monopoly power)
- PoW causes centralization
- PoW prefers certain geographic regions and taxation regimes
- PoW is wasteful

Macro economic thesis: One $ One vote

Open question 2b: how to avoid monopolies, centralization, prevent bribery

2: Incentivizing Trust

2a: trust there is no double spend

2b: who is maintaining trust?

2c: trust and scalability

Scalability of Blockchains

One of the biggest technical challenges

1. Consensus (better consensus protocols like PBFT/Tendermint/Casper/SBFT/HotStuff)
2. Data availability (record transactions in an open and accessible ledger)
3. Execution (validate the execution of the transactions)

By far, execution (validation) is the bottleneck:

- Today: every miner and every validator must execute all transactions
- Promising solution: Optimistic Rollups
  - Few bonded validator execute (aggregate transactions)
  - Anyone can post a challenge (proof of fraud) and get a reward if correct
  - Classic Principle-Agent problem with deep ties to computer science
  - Principle wants transactions to the aggregated, agent may be lazy or malicious

Open Question 2c:

A game theoretic framework for scalable validation

3: Incentivizing Fairness

“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”

Satoshi Nakamoto, bitcoin whitepaper, 2008

Rich get richer and the poor get poorer

”To him that hath, more shall be given; and from him that hath not, the little that he hath shall be taken away”
Percy Bysshe Shelley, 1821

Good Money System should be fair

- Fairness is challenging to define
- Chain quality: your fraction of reward is proportional to your fractional voting power

How do you allocate money?

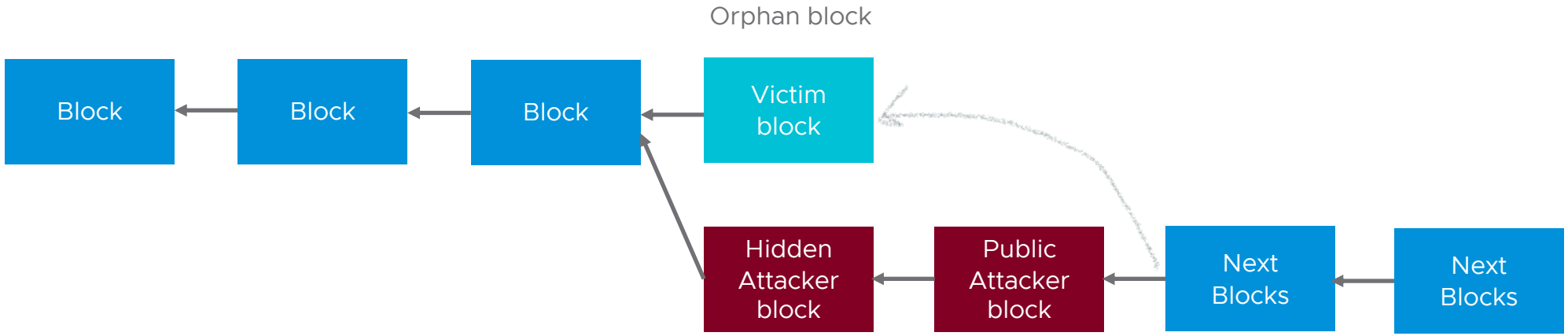
Bitcoin: new coins for the miner of a block

- A block that actually becomes part of the longest chain!!
- Orphan blocks get nothing!!

Selfish Mining:

- Cause other blocks to become orphans
- Decreasing the fair share of others -> implicitly increases your share (unfairly)
- Requires a large coalition to succeed
- The larger the coalition, the larger their advantage from Selfish Mining
- Selfish Mining: incentivizes centralization, rich get richer

Selfish Mining



- Ethereum: Uncle rewards
  - Add links to orphans
  - Still susceptible to Selfish mining
- FruitChain [Pass, Shi, 2017]:
  - Playing honest is an epsilon best response, deviating is always profitable
  - Protocol differs from just adding uncle links
- ColorDag:[Abraham, Dolev, Eyal, Halpern, 2020]
  - Playing honest is an epsilon best response, deviating is almost always not profitable
  - Add links to orphans (and a new probabilistic reward scheme)

Open Question 3:

A game theoretic framework for fairness and chain quality

4: Incentivizing Welfare

“The incentive can also be funded with transaction fees. 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”

Satoshi Nakamoto, bitcoin whitepaper, 2008

Blockchains as a public good

Clients (buyers) need to submit transactions to a trusted Money System

- Clients are paying for trust (security)

Miners (sellers) need to maintain the Blockchain

- Blockchain provides trust (security)

What mechanism does Bitcoin use to allocate buyers to blocks?

- Essentially a first price auction with a fixed limited block size
- The block size debate is beyond the scope of this talk ☺
- Classical mechanism design and auction theory: second price auction
- Not robust to collusion
  - Between buyers; Between buyers and sellers
- Fixed price?
- EIP 1559: burn a fixed price (that depends on congestion), then pay an optional tip
  - Burning: tax policy!

Open Question 4:

A theory of blockchains as public goods and incentivizing social welfare

Conclusion and Open Questions

When Nakamoto meets Nash

1. Modeling Money Endogenously
   - A theory of money that can capture the utility of fairness, trust, and friction
2. Incentivizing Trust
   - For Consensus
   - For Voting rights
   - For Scalability
3. Incentivizing Fairness
   - Avoiding selfish mining
4. Incentivizing Welfare
   - Blockchain as a public good

Thank You