UNIVERSITY *of* NICOSIA

Week 2 – Session 4

Hidden Incentivized Models & Game Theoretical Aspects

BLOC 512: Blockchain Systems and Architectures

Session Objectives

- This session will be about game theoretical aspects of Blockchain technology, a little bit more demanding topic, only slightly covered with research studies and even less in media. We won‘t be talking about the technology or business cases here, instead we will focus on the bigger picture of what makes blockchains work: social and economic incentivization structures.

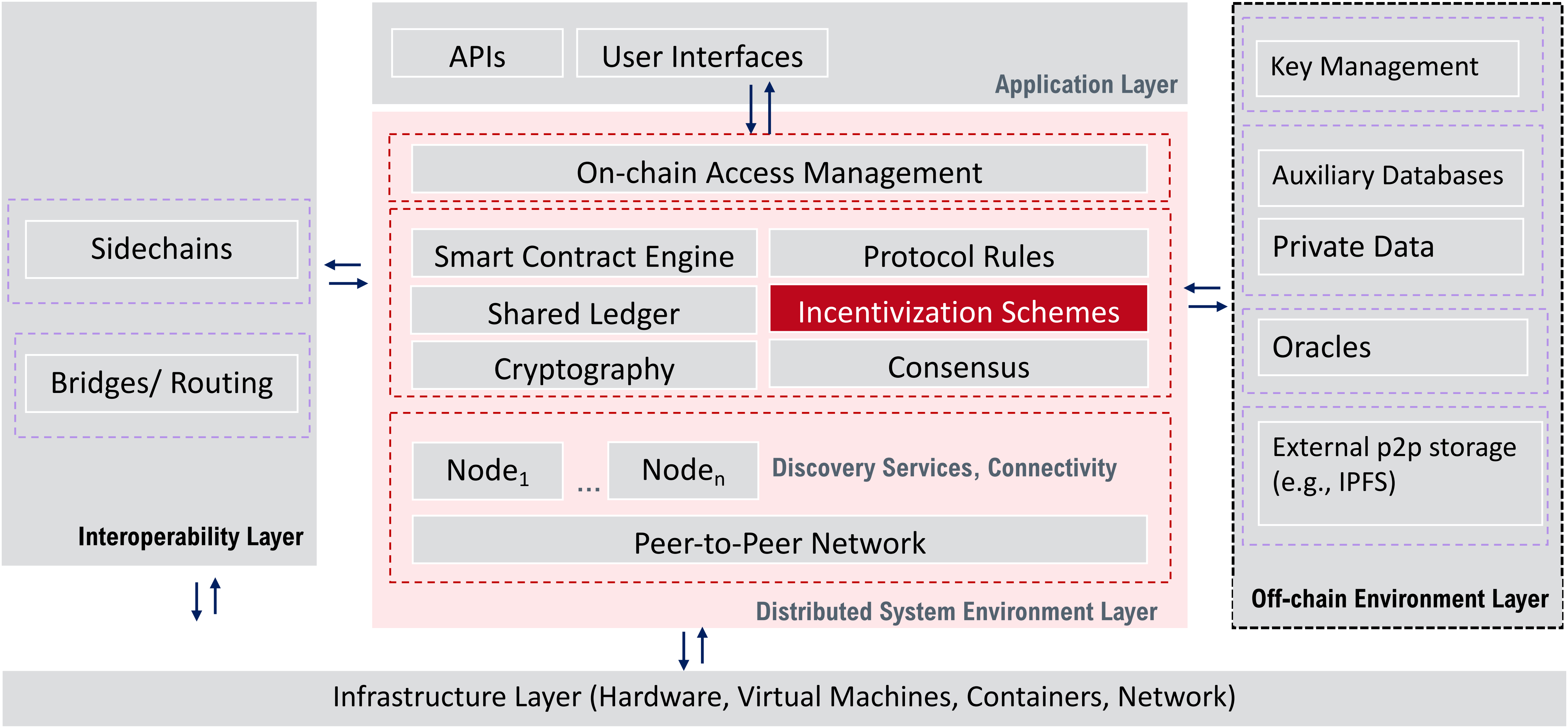
- Understand how a balanced incentivization in Bitcoin is fundamental to its operation
- Overview of basic concepts in the game theory
- Review currently known risks and mitigations in blockchain systems due to the delicate nature of rewarding honest behavior, punishing malicious actions and their influence on preserving reputation

Agenda

1. Blockchain incentive structures: The case of Bitcoin
2. Game theory basics
3. Risks to blockchain security
4. Mitigation methods
5. Conclusions
6. Self-Assessment Exercises and Further Readings

Flashback

DLT Layers & Architectural Components



Bitcoin Blockchain Incentive Structures

Introduction

- We have covered fundamental properties of blockchain and consensus mechanisms, we also have good knowledge of many technicalities that make Bitcoin tick and Ethereum tock.
- Byzantine Fault Tolerant consensus, Paxos, ECDSA, SHA-256, the size of blocks, public/private key pairs, signatures, ... These are not important for the big picture.
- It is important that we use these technologies for a good cause. They are shaping our lives already.
- But, **how** do we design them with that goal in mind? We can prepare various models, but how do we test them and how can we run simulations and see what works best?
- **Game theory** is a good fit for these kind of problems, as it is *about how participants interact among each other in order to achieve their preferred goals.*
- In this session we will make a high-level overview of the main concepts and will provide a list of sources which you can use to dig further into these topics.

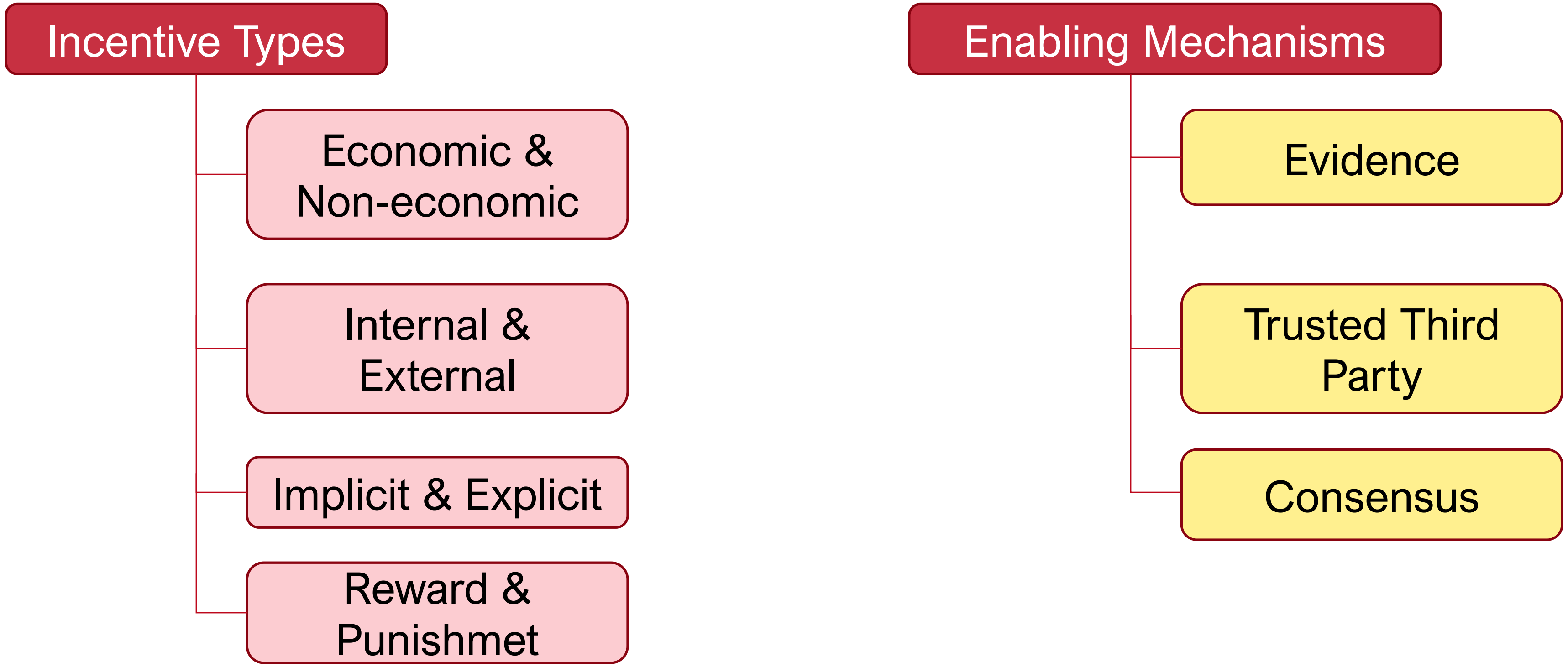
Types of Incentives

- Incentives come in various forms:
  - Such schemes incorporate both financial rewards (based on some token) and non-monetary incentives (e.g., reputation systems).

1. **Economic Incentives**
   - Various blockchains leverage on economics to design incentivization scheme for the actors participating to such systems. Embedding such schemes during the architectural design of a blockchain protocol are important in order to shape the behavior of the community so that the vision of the founders can be realized.
2. **Non-economic incentives**
   - Such schemes aim to foster cooperation within communities that theoretically share aligned incentives.
   - To promote anonymity e.g., the lack of economic incentives does not prevent the existence of Tor

- How security relates to incentives for the various actors participating? Do incentives produce unexpected results?
  - Consider DAOs, DeFi, even the smart contract engines

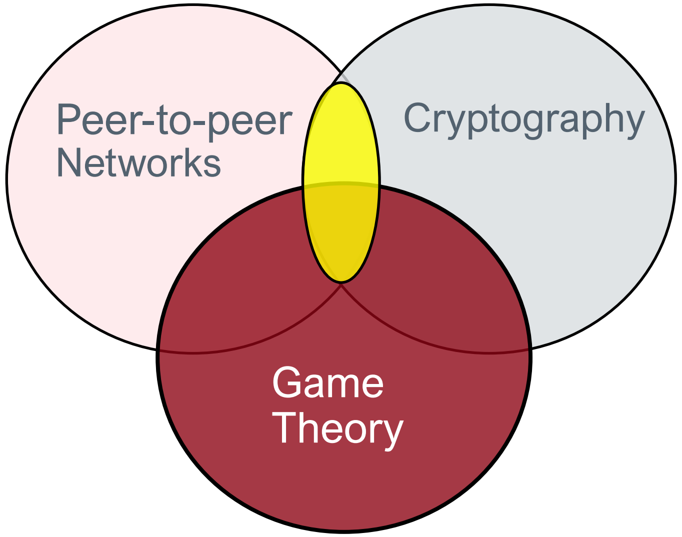
Types of Incentives – Part II



[1] Azouvi, S., Hicks, A., & Murdoch, S. J. (2018, March). Incentives in security protocols. In Cambridge International Workshop on Security Protocols (pp. 132-141). Springer, Cham.

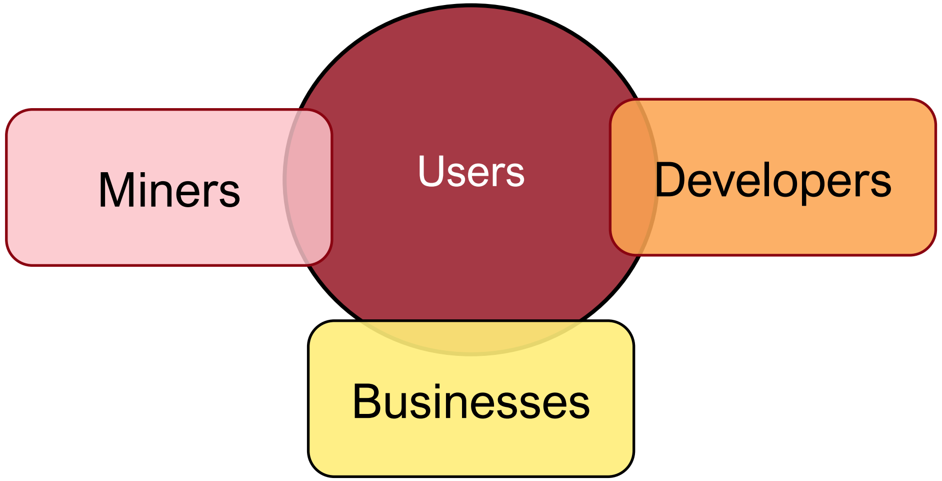
Actors (Players) – Part I

- Regarding ***game theoretical aspects*** of Bitcoin, we are observing strategies of operation for different sets of actors in the system.
- When discussing peer-to-peer blockchain networks, we usually classify actors to full nodes, light nodes and mining nodes (or validators or block generators, more generally).
  - If we look at the whole ecosystem from a social point of view, we can instead classify them into users (can be end-users who use Bitcoin as a currency for payments and/or investors, traders etc. who use Bitcoin more indirectly), miners, developers and businesses. **They can cooperate to a greater or a lesser extent.** They can even be in several or all categories at the same time.
- Evaluating interactions is much simpler for actors of the same type, like between miners only, but in reality, all permutations of relations should be considered as one without another can hardly exist.



Actors (Players) – Part II

- Within a public blockchain we have different actors:
  - **Miners** (block producers, validators),
  - **Developers** (scientists, pioneers),
  - **Businesses** (that use the software),
  - and **end-users** that are using the network, running their nodes, or acting as investors
- At any given time in the network, these different actors are either cooperating or engaging in other activities or even prone to attacks.
- We need a way to study and understand their interactions.



Incentives in Bitcoin (Cont.)

- There are multiple ways of *securing consensus in blockchain systems* as we have learned so far. A set of economic, development, mining, and adoption **incentives** makes **Nakamoto consensus** a novel approach (and, to a degree, easier to implement and understand, too) than a complex Paxos-like system, which in BFT variant has tolerance to 33% of bad actors, compared to Bitcoin‘s 49%

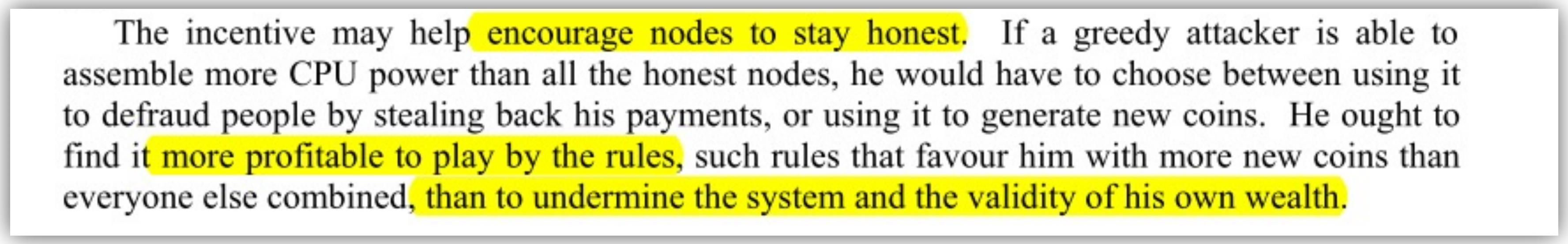
  (what we will actually discover later is that following a certain strategy, even in Bitcoin 33% of malicious miners have a chance in performing a certain type of attack).

- Incentives in Bitcoin-like systems lay in their native currency. Elsewhere, the incentives can be less direct (like costs savings, relaxing trust issues or support for new products).

Incentives in Bitcoin (Cont.)

- There are two types of direct incentives in Bitcoin, that miners receive for their work:
  - **coinbase reward**, which is a first transaction in every block, which creates new coins for the creator of the block; they also serve as the initial („fair“) distribution of coins
  - **transaction fees**, which are the difference between input values and output values of each transaction in the block and are also added to the mining reward.

- **Why do we need these in Bitcoin?** A simplistic answer is to pay miners for securing the network. But there is more underneath it which becomes obvious if we just take a look at the Bitcoin whitepaper:

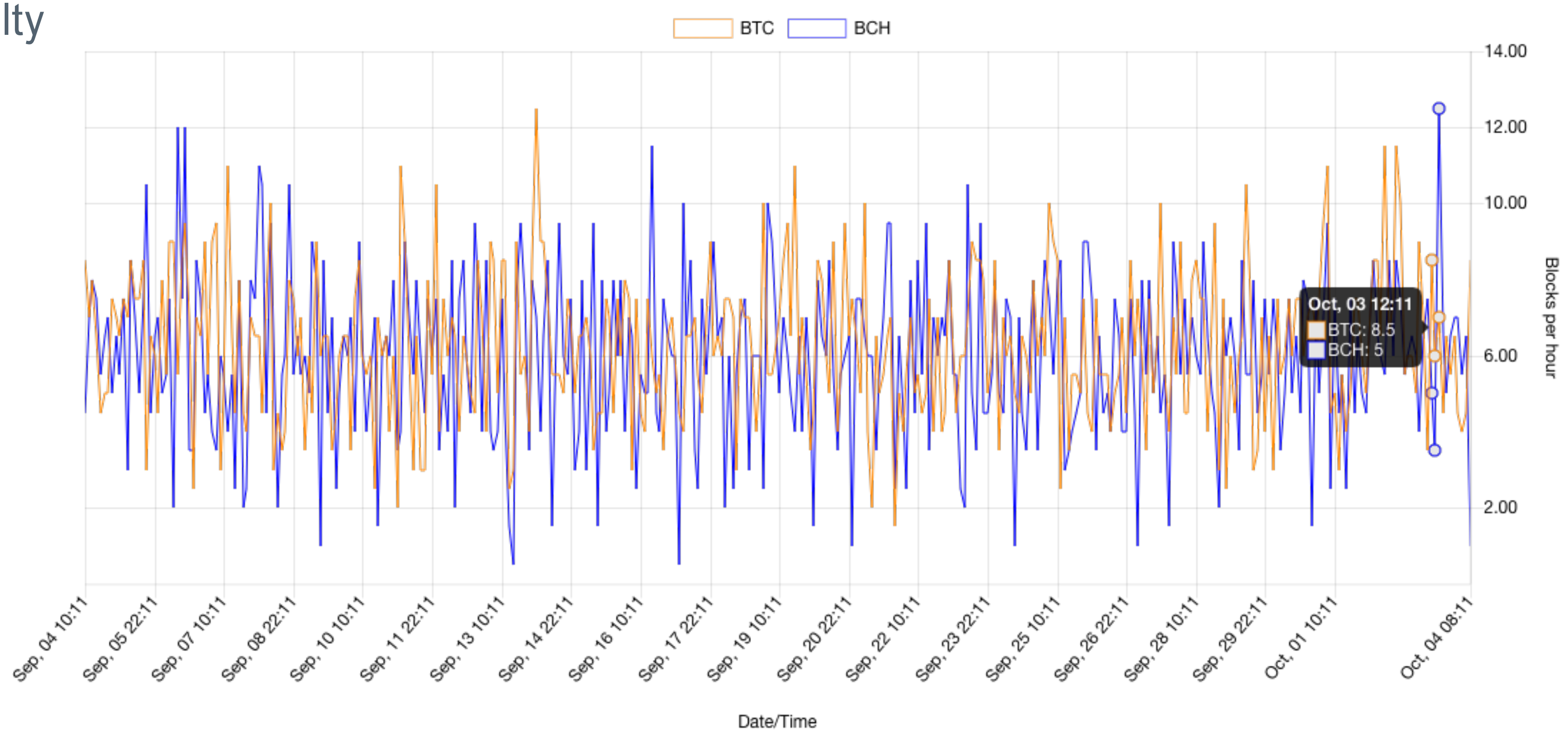


The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to 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.

Incentives in Bitcoin (Cont.)

Example: https://fork.lol/blocks/time

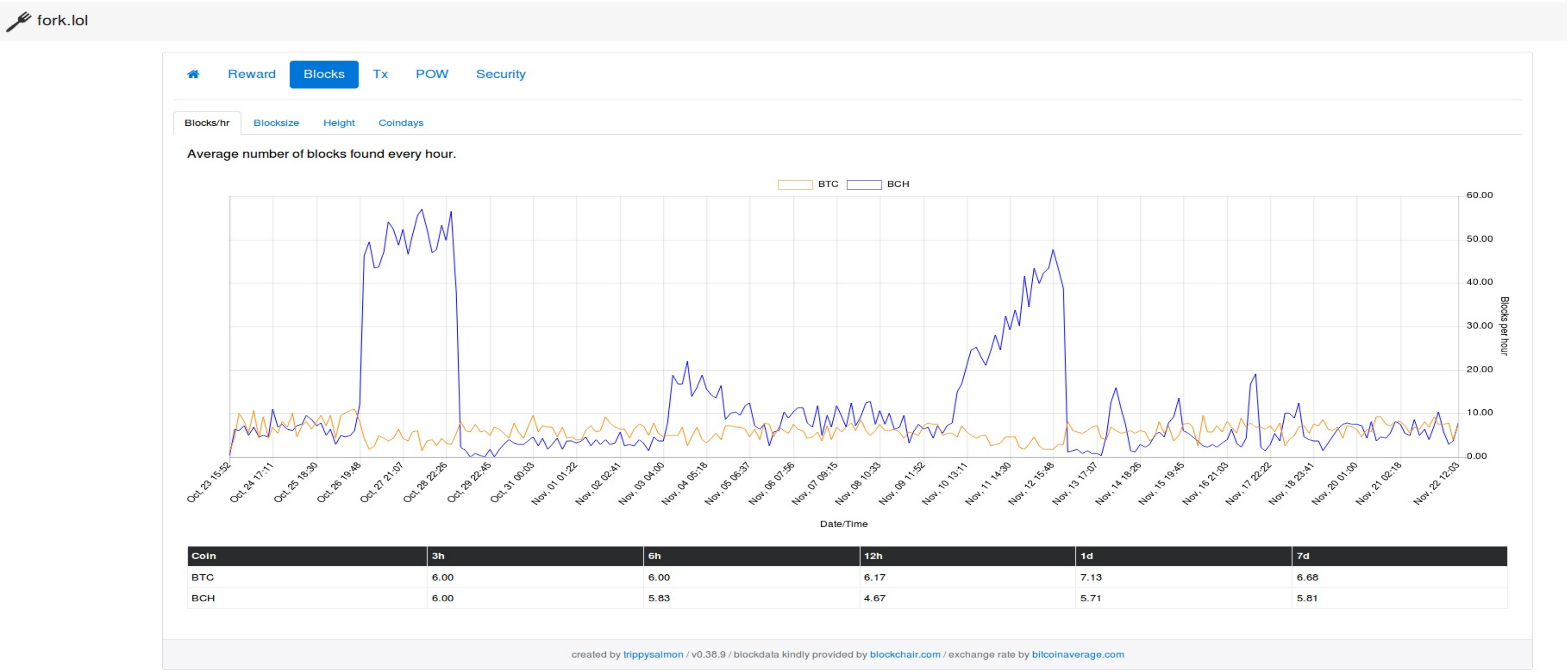
- Bitcoin Core and Bitcoin Cash behavior
- Block, Hashrate, Difficulty
- Miner’s Games



Average number of blocks found every hour

Incentives in Bitcoin (Cont.)

Example: Screenshot goes back to BitcoinCash fork
Miners' games? Hashing races?



Average number of blocks found every hour.

Coin	3h	6h	12h	1d	7d
BTC	6.00	6.00	6.17	7.13	6.68
BCH	6.00	5.83	4.67	5.71	5.81

created by trippysalmon / v0.38.9 / blockdata kindly provided by blockchair.com / exchange rate by bitcoinaverage.com

Chart source: https://fork.lol , screenshot made in2017

Incentives in Bitcoin (Cont.)

- Only **miners** receive direct rewards for their work in Bitcoin.
- **End-users** that actually create new transactions and are necessary for the system to have any purpose at all, can at the same time also be miners, full nodes, developers or investors. They are encouraged to use the system for the reasons we mentioned in the first session.
- **Investors and developers**, who speculate that their contributions will eventually make the system more successful, are not receiving any dividends from the protocol itself.

All these actors hope to be better off by following one strategy or the other. Sometimes they cooperate, sometimes they compete, in some cases they might even engage in cyberattacks against others.

Full nodes that help relay transactions, are also supporting the network and their work is not costless (paying for internet bandwidth, dedicating enough storage on disk, having a computer powered on *etc.*). Currently, they receive no direct compensation for their work.

Should they? – Stay tuned to see what game theory says about it!

Incentives in Bitcoin (Cont.)

What motivates actors in Bitcoin and other public blockchain networks in general? – There is an *ideology*, but ideology alone can carry you only until you need to pay for food and bills.

- Miners
  - are investing large amounts of money for mining rigs, using lots of electricity, as cheap as they can get it
  - are narrowly focused on optimizing the operation of chips made for one purpose only: calculating SHA-256 hashes
  - they hide their infrastructure (mostly), but announce their mining results (honestly?)

  → sell only as much cryptocurrency as needed for operating, interested in preserving its value, so they keep their job

  † in case the project fails, they end up with unusable equipment and worthless cryptocurrency
- Businesses
  - are investing large amounts of money into various (sub)projects, sometimes publicly, sometimes hidden

  → investors and business using the blockchain both look for return on investment

  † in case the project fails, they lose their investment, occasionally their reputation as well
- Developers
  - are investing large amounts of time to build the protocol, trying to find financing for their work as best as they can
  - are concerned with holistically evolving the protocol itself
  - their work is completely in the open (mostly), all changes in the code are “permanently” public

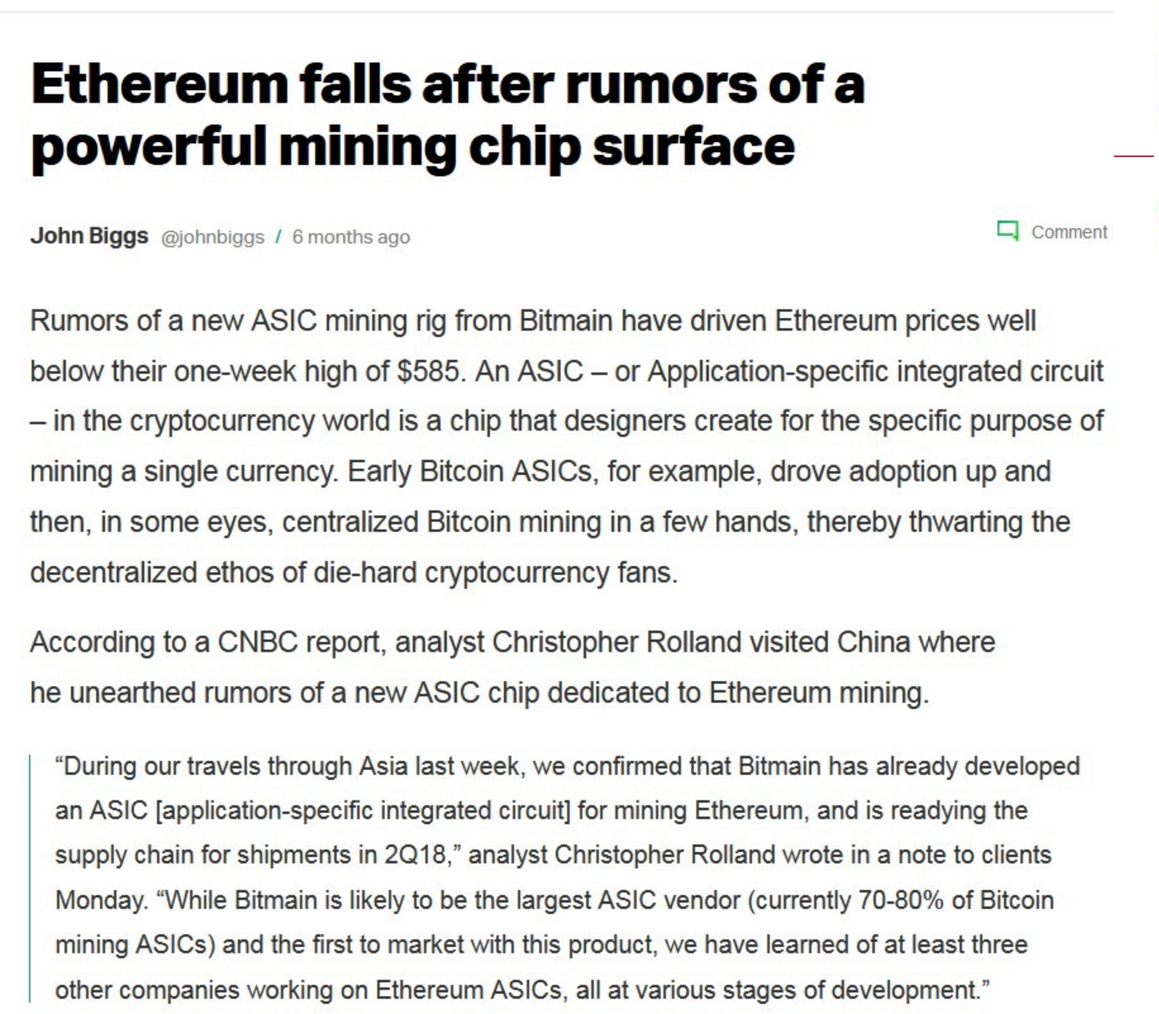
  → try to get funding for their work, interested for cryptocurrency to preserve its qualities, so they keep their job

  † in case the project fails, they move elsewhere, preserving their knowledge and reputation
- Users
  - use cryptocurrency for the claimed features, but a large part of usage is currently still investment speculation
- *What about external adversaries, who want to stop this train altogether?*

Disagree? Share on forums!

Incentives in Bitcoin (Cont.)

- Combining punishments with rewards strengthens the protocol security features.
- Ethereum takes this to a new level:
    - Rewarding “good” behavior (for actors that play by the rules)
    - Punishing “bad” behavior (for actors that attempt to manipulate the system)
- **How?** With an upgrade to the consensus protocol
- Consensus is secured through Proof-of-Stake (PoS) - PoS affects game design differently than PoW by examining real world behavior



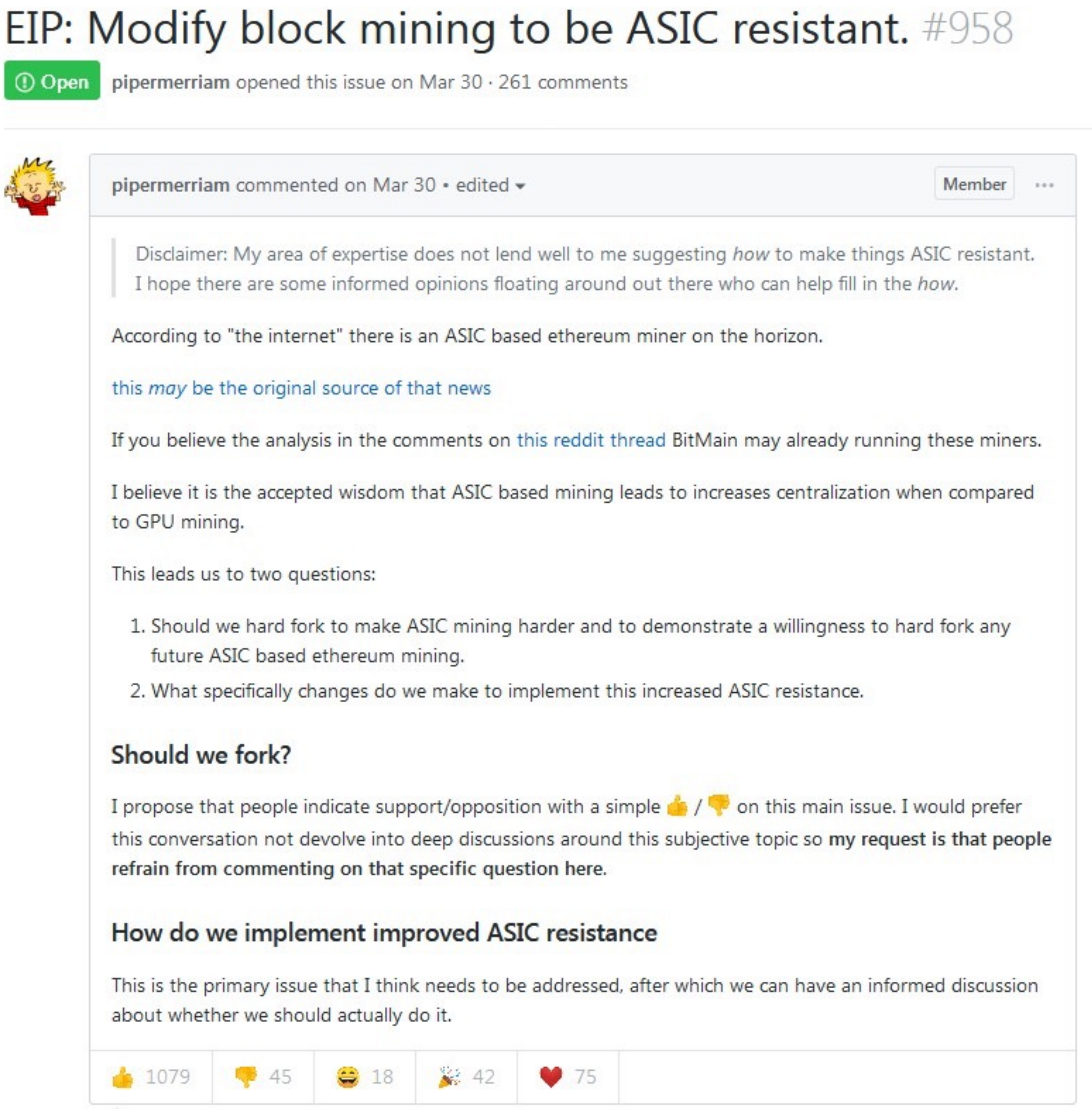
Ethereum falls after rumors of a powerful mining chip surface

John Biggs @johnbiggs / 6 months ago

Rumors of a new ASIC mining rig from Bitmain have driven Ethereum prices well below their one-week high of $585. An ASIC – or Application-specific integrated circuit – in the cryptocurrency world is a chip that designers create for the specific purpose of mining a single currency. Early Bitcoin ASICs, for example, drove adoption up and then, in some eyes, centralized Bitcoin mining in a few hands, thereby thwarting the decentralized ethos of die-hard cryptocurrency fans.

According to a CNBC report, analyst Christopher Rolland visited China where he unearthed rumors of a new ASIC chip dedicated to Ethereum mining.

> "During our travels through Asia last week, we confirmed that Bitmain has already developed an ASIC [application-specific integrated circuit] for mining Ethereum, and is readying the supply chain for shipments in 2Q18," analyst Christopher Rolland wrote in a note to clients Monday. "While Bitmain is likely to be the largest ASIC vendor (currently 70-80% of Bitcoin mining ASICs) and the first to market with this product, we have learned of at least three other companies working on Ethereum ASICs, all at various stages of development."



EIP: Modify block mining to be ASIC resistant. #958

pipermerriam opened this issue on Mar 30 · 261 comments

pipermerriam commented on Mar 30 • edited

> Disclaimer: My area of expertise does not lend well to me suggesting *how* to make things ASIC resistant. I hope there are some informed opinions floating around out there who can help fill in the *how*.

According to "the internet" there is an ASIC based ethereum miner on the horizon.

this *may* be the original source of that news

If you believe the analysis in the comments on this reddit thread BitMain may already running these miners.

I believe it is the accepted wisdom that ASIC based mining leads to increases centralization when compared to GPU mining.

This leads us to two questions:

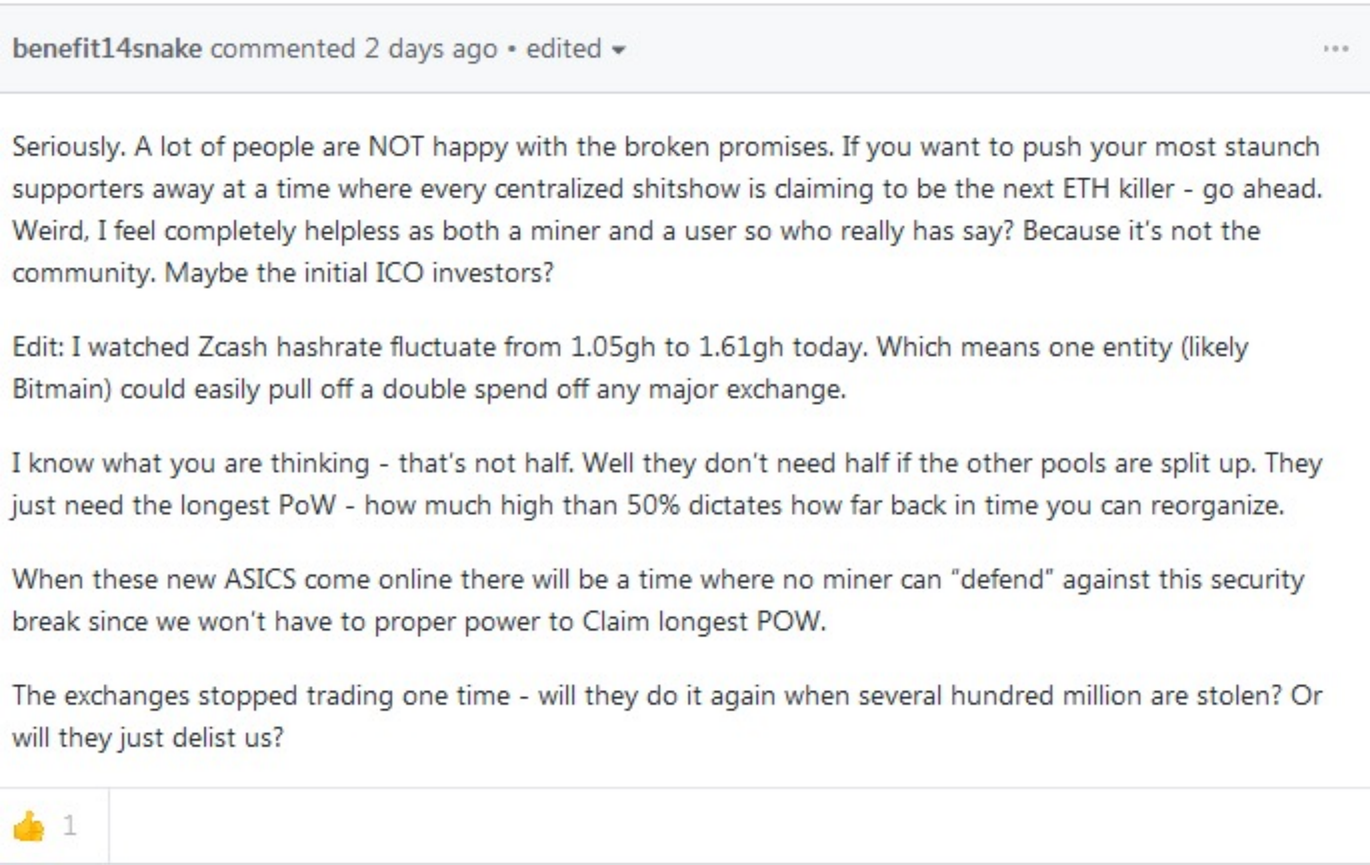
1. Should we hard fork to make ASIC mining harder and to demonstrate a willingness to hard fork any future ASIC based ethereum mining.
2. What specifically changes do we make to implement this increased ASIC resistance.

Should we fork?

I propose that people indicate support/opposition with a simple 👍 / 👎 on this main issue. I would prefer this conversation not devolve into deep discussions around this subjective topic so **my request is that people refrain from commenting on that specific question here.**

How do we implement improved ASIC resistance

This is the primary issue that I think needs to be addressed, after which we can have an informed discussion about whether we should actually do it.



benefit14snake commented 2 days ago • edited ▾

Seriously. A lot of people are NOT happy with the broken promises. If you want to push your most staunch supporters away at a time where every centralized shitshow is claiming to be the next ETH killer - go ahead. Weird, I feel completely helpless as both a miner and a user so who really has say? Because it's not the community. Maybe the initial ICO investors?

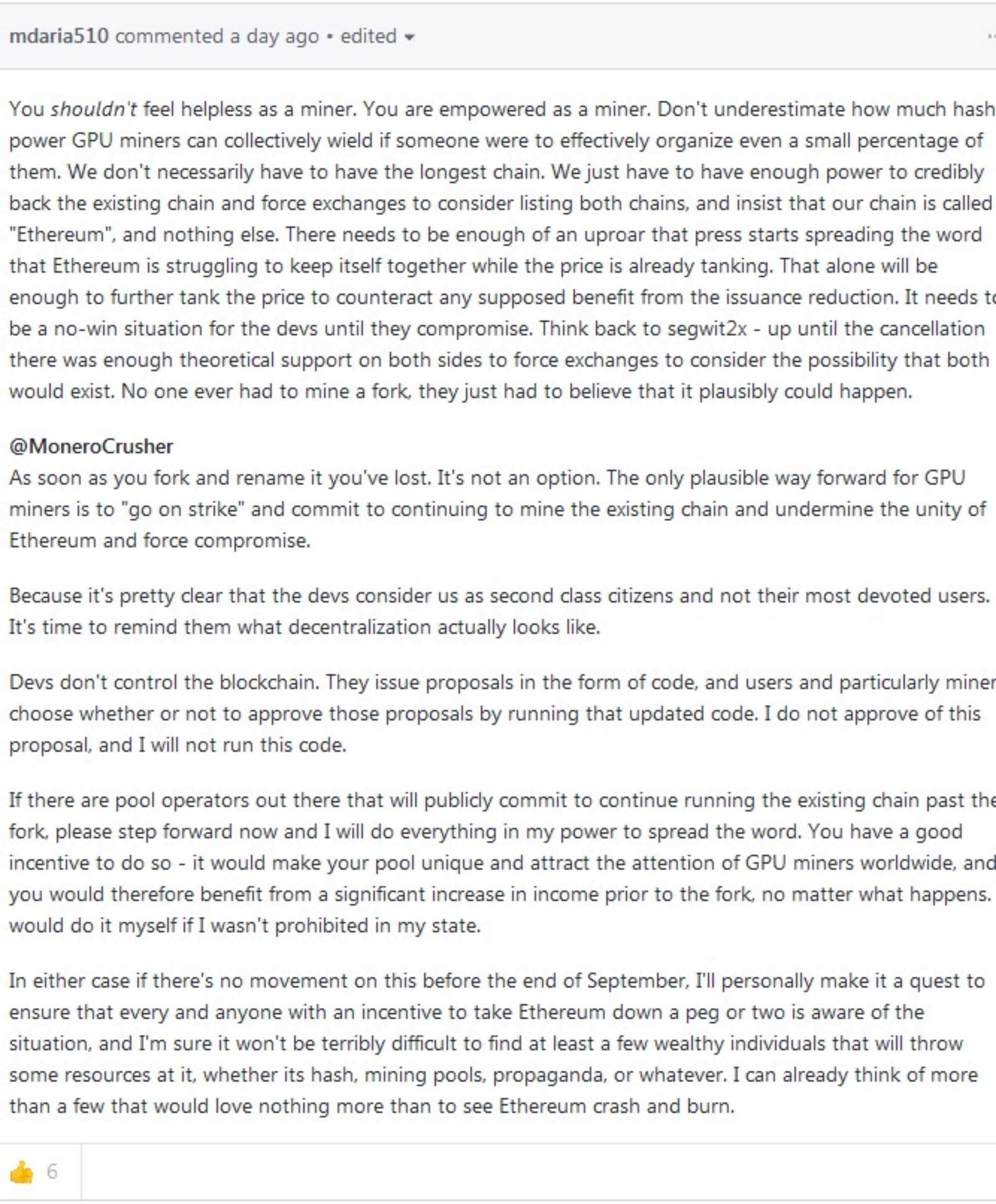
Edit: I watched Zcash hashrate fluctuate from 1.05gh to 1.61gh today. Which means one entity (likely Bitmain) could easily pull off a double spend off any major exchange.

I know what you are thinking - that's not half. Well they don't need half if the other pools are split up. They just need the longest PoW - how much high than 50% dictates how far back in time you can reorganize.

When these new ASICS come online there will be a time where no miner can "defend" against this security break since we won't have to proper power to Claim longest POW.

The exchanges stopped trading one time - will they do it again when several hundred million are stolen? Or will they just delist us?

👍 1



mdaria510 commented a day ago • edited ▾

You *shouldn't* feel helpless as a miner. You are empowered as a miner. Don't underestimate how much hash power GPU miners can collectively wield if someone were to effectively organize even a small percentage of them. We don't necessarily have to have the longest chain. We just have to have enough power to credibly back the existing chain and force exchanges to consider listing both chains, and insist that our chain is called "Ethereum", and nothing else. There needs to be enough of an uproar that press starts spreading the word that Ethereum is struggling to keep itself together while the price is already tanking. That alone will be enough to further tank the price to counteract any supposed benefit from the issuance reduction. It needs t be a no-win situation for the devs until they compromise. Think back to segwit2x - up until the cancellation there was enough theoretical support on both sides to force exchanges to consider the possibility that both would exist. No one ever had to mine a fork, they just had to believe that it plausibly could happen.

@MoneroCrusher
As soon as you fork and rename it you've lost. It's not an option. The only plausible way forward for GPU miners is to "go on strike" and commit to continuing to mine the existing chain and undermine the unity of Ethereum and force compromise.

Because it's pretty clear that the devs consider us as second class citizens and not their most devoted users. It's time to remind them what decentralization actually looks like.

Devs don't control the blockchain. They issue proposals in the form of code, and users and particularly miner choose whether or not to approve those proposals by running that updated code. I do not approve of this proposal, and I will not run this code.

If there are pool operators out there that will publicly commit to continue running the existing chain past the fork, please step forward now and I will do everything in my power to spread the word. You have a good incentive to do so - it would make your pool unique and attract the attention of GPU miners worldwide, and you would therefore benefit from a significant increase in income prior to the fork, no matter what happens. would do it myself if I wasn't prohibited in my state.

In either case if there's no movement on this before the end of September, I'll personally make it a quest to ensure that every and anyone with an incentive to take Ethereum down a peg or two is aware of the situation, and I'm sure it won't be terribly difficult to find at least a few wealthy individuals that will throw some resources at it, whether its hash, mining pools, propaganda, or whatever. I can already think of more than a few that would love nothing more than to see Ethereum crash and burn.

👍 6

The Importance of Economic Ideas

*„**The ideas of economists and political philosophers**, both when they are right and when they are wrong, **are more powerful** than is commonly understood. Indeed, the world is ruled by little else. Practical men, who believe themselves to be quite exempt from any intellectual influences, are usually the slaves of some defunct economist. Madmen in authority, who hear voices in the air, are distilling their frenzy from some academic scribbler of a few years back.“*

– *John Maynard Keynes,* The General Theory of Employment, Interest and Money (1936)

Game Theory Basics

Terminology

- **Game theory** – „the study of mathematical models of conflict and cooperation between intelligent rational decision-makers“*, that has its beginnings from centuries ago, but became more recognized since John von Neumann published a paper on it in 1928.

  *Myerson, Roger B. (1991). Game Theory: Analysis of Conflict

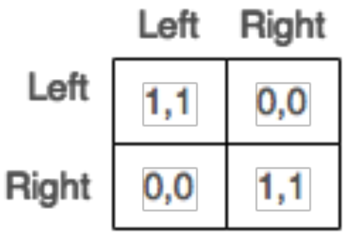
- **Self-interested agent** – each agent (player) has his own preference of which outcomes he likes
- **Strategy** – a description of actions defining how a player plays in a game, at the same time also accounting for other players
- **Utility function** – a generalized metric of „happiness“ of a self-interested agent for a particular preference among all available alternatives, for instance in Bitcoin the function would prefer outcomes where an agent receives more coins; however not all utilities are about „money“
- **Rational user** – aims at maximizing his own utility function, hence he is primarily concerned with his own profit and doesn‘t care about happiness of others (selfish, non-communicating, intelligent, purely economic → *rational fool*)

Non-cooperative Games

- **Non-cooperative games are about conflicts**. They help us understand *why* a certain strategy would be played, often seeking Nash equilibrium.
- In non-cooperative games, there is no agreement between parties, no communication, no negotiation.
- **John von Neumann** published a pioneering book in 1944 with Oskar Morgenster, titled: Theory of Games and Economic Behavior, which described the basics of classical game theory.
- The book is in public domain, available here: https://archive.org/details/in.ernet.dli.2015.215284

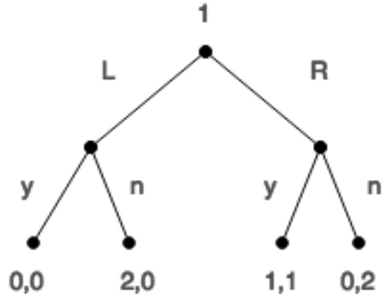
Non-cooperative Games

- Non-cooperative games are said to be in **normal form**, meaning that their representations are usually made with *n-dimensional matrix* of all possible actions and payoffs for players.
- They cover games where all actions of players are played simultaneously. Usually, they consist of only 1 step. Many other games can be reduced to normal form, therefore this is **one of the most fundamental concepts in game theory**.



	Left	Right
Left	1,1	0,0
Right	0,0	1,1

- **Extensive form** games represent situations where players do not always act simultaneously, but instead perform sequential actions. They can be presented for instance with *trees*, where nodes are denoting choices of players and edges represent possible actions.
  The leaves represent final outcomes of player‘s utility function.



Solution Concepts

- Which game outcomes are better than others, how do we analyze different strategies?
- An **optimal strategy** (absolute best) is the one that gives maximum utility to the agent. Finding it is practically impossible due to uncertainties and unknowns in the environment.
- Therefore, game theory suggests reducing the problem by focusing on certain interesting subsets which are called *solution concepts*. It is not so much about finding the best strategy, but finding outcomes that are better than others (lesser outcomes can then be eliminated to get us closer to the solution).

- The two most common solution concepts range from optimality to equilibrium:
  - **Pareto optimal** (efficient) – a strategy profile that gives the best outcome to any of players without hurting others
  - **Nash equilibrium** – if each player knew the strategies of others and wouldn't be able to increase his gains by changing his strategy, such actions would be in Nash equilibrium.
    „*If a player acted differently, he would not be better off, but likely worse*.“

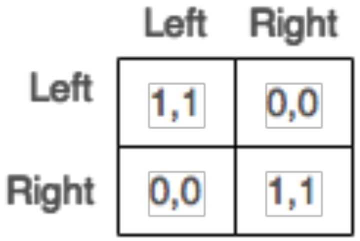
John Forbes Nash, Jr. proved in 1951 that at least one Nash equilibrium exists for any finite game. So players are deciding on their actions while also taking into account the decision-making of others.

Examples

Some of the games that you will most often read about in connection to game theory are:

- **Common-payoff games** – team games, where there are no conflicting interests, the goal is to coordinate towards max payoff overall [*pure-coordination*]

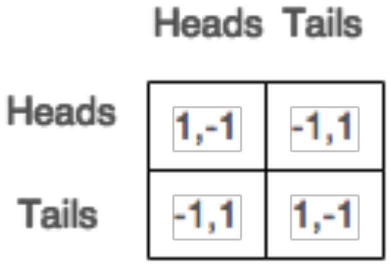
See the example of drivers driving towards each other. They both get 1 point (they are safe) if they both drive on either their left or their right side, otherwise they both get 0 (they crash).
In other words, they have maximum utility when they chose same sides.



	Left	Right
Left	1,1	0,0
Right	0,0	1,1

- **Zero-sum games** – one's gains are balanced by other's loses [*pure competition*]. They are played between 2 players, because games with more can be transformed to a game of pairs.

An example is matching pennies game, where players throw coins and if both coins land on the same side, the first player takes both, otherwise the second player takes them.



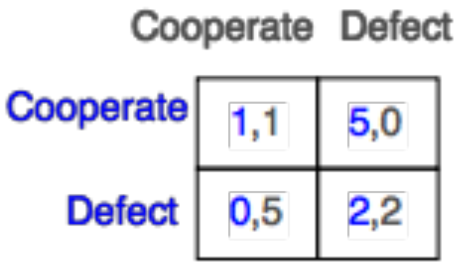
	Heads	Tails
Heads	1,-1	-1,1
Tails	-1,1	1,-1

Examples (Cont.)

- **Prisoner's dilemma** – a standard game used for representing ***non-cooperative rational players***. It was designed in 1950 within RAND corporation, in a time of Cold War dilemma of arms race – should the opposing alliances arm or disarm? From each side, arming seemed rational and so it really did happen. If they would cooperate, disarming would be the „best“ option to prevent war and save a lot of costs. Furthermore, Prisoner‘s dilemma has many real-life applications and is of interest in many sciences, from biology to economics.

We observe the actions of two prisoners suspected of a crime they did together. Each of them can confess to the crime (Cooperate) or betray the other prisoner (Defect). Based on their actions, they get different jail term as can be seen in the table.

They would each get only 1 year in prison if they would cooperate (2 years prison time altogether). But if they are rational, they want to get as little jail time as possible → they both defect (4 years altogether), because each of them knows that the best decision of the other is to defect and so they must also defect or otherwise face the highest penalty. → That is Nash equilibrium, but it is not Pareto optimal ☺



	Cooperate	Defect
Cooperate	1,1	5,0
Defect	0,5	2,2

- Note: actual numbers don‘t matter, it is only required that they follow some rules.

Prisoner‘s Dilemma (Cont.)

- Let‘s recap everything we‘ve learned so far on the example of prisoners: players are selfish, „rational fools“, can‘t communicate and have only one action available, so they focus on maximizing their utility function, that is: minimum jail time.

- Would prisoners act differently if they knew they would meet later in life? The betrayed prisoner might revenge! → This situation can be modelled with so called **Iterated prisoner‘s dilemma**, where there are more than one sequential steps among players.

- But it turns out the „best“ strategy is not so easy to find then:
- For finite number of rounds, the dominant strategy is still to defect.
- However, if games are *repeated infinitely* (such are the games we play in real-life: we are constantly deciding and acting, up until our death), it is not clear what strategies of rational agents would be chosen. A concept of *punishment* for pas bad behavior becomes important.

- Computer simulations made by Axelrod in late 70‘ suggested that **cooperation won over cheating**!

Iterated Prisoner‘s Dilemma

- Axelrod‘s tournaments found that the winning strategy, that performed the best overall (not in every game, but on average), was „Tit-for-Tat“, also called **look-back strategy** or **reciprocal altruism**.
- It worked simply by starting the first iteration with Cooperation, then looked back at the opponent last move and copied it in the next iteration.

- In summary, the best strategies were found to have these surprising properties:
  - Be nice – don‘t be the first to defect
  - Be provocable – return actions, both retaliation and forgiveness
  - Don‘t envy – don‘t focus on beating the opponent, but on maximizing your own score
  - Don‘t be tricky – anytime you try to exploit the opponent, you will provoke revenge

- What‘s more, rationality of players was found not to be necessary if there is a path for satisfaction of both players and probability of their future interaction.

Cooperative Games

Axelrod showed that cooperation can be evolutionarily advantageous. In the extreme, his

„... *dramatic results showed that in a very simple game the conditions for survival (be nice, be provocable, promote the mutual interest) seem to be the essence of morality. While this does not yet amount to a science of morality, the game theoretic approach has clarified the conditions required for the evolution and persistence of cooperation, and shown how Darwinian natural selection can lead to complex behavior, including notions of morality, fairness, and justice*.“ [see Wiki article about The Evolution of Cooperation]

- In **evolutionary game** theory, users are not necessarily rational, they just follow a strategy, perhaps unknowingly, and the results of all these strategies will eventually, through iterations, determine the best one (spread / reproduce / not die).

- **Evolutionary stable strategy** – an evolutionary strategy that successfully defends against attempts of take-overs by competing strategies (it is a „stable“ refinement of Nash equilibrium for evolutionary strategies).

Cooperative Games (Cont.)

By way of example that John Maynard Smith presented in 1973, imagine a world with doves and hawks. If there would be only hawks, their fights would be devastating to their population. If there would be only doves, they would be susceptible to any intruders, therefore such a population would also not be stable. But the right combination of hawks and doves would be evolutionarily stable.

- This brings us to *cooperation versus competition* and *rationality versus altruism*.

- As with many situations in real-life, the games are often not zero-sum, but by cooperative efforts all players can be better off. Think of peer-to-peer file sharing.

- Can you picture such a situation with regards to digital currencies and blockchain systems?

Mechanism Design

Mechanism design is a reverse game theory concept, where the goal of the system is known first, and only then a system is designed that would lead to that goal. It aligns incentives of rational players in advance so that they follow the desired strategies. The authors of mechanism design theory (Leo Hurwicz, Eric Maskin and Roger Myerson), were awarded a Nobel prize for it in 2007. Practical uses of MD are found in the operation of health care, auctions, voting *etc*. however it relies on complex and highly abstract calculations.

- The initial distribution of a cryptocurrency is an example of mechanism design in practice …
- Satoshi Nakamoto had a far-reaching problem in how to distribute bitcoins so that it would be fair and rewarding for those that support the project. As it started with “one CPU, one vote”, the distribution of bitcoins was within reach of anybody who would bother installing the node and run/test/review it.
- Vitalik Buterin decided differently, allocating vast amount of ether to the founders and developers, with the goal to ensure a long-term dedication of the team.
- Finally, the market decides on the spot price *and* allocation, reaching an equilibrium that lasts as long as the corresponding ecosystem circumstances hold.
- → *Cryptoeconomics* is born and we will witness a lot of research in this field in the following years.
- A good, if somewhat involved, introduction to the mechanism design was made from BlockChannel in 2017 and is available here: A Crash Course in Mechanism Design for Cryptoeconomic Applications

Crypto-Economics

Cryptoeconomics is yet another confusing term, but what it is actually supposed to be about, is about ***open blockchain systems*** that use native currency as a mechanism ***to encourage honest behavior*** of participants. The "crypto-" part of the expression then pertains to the cryptographically secured protocol.

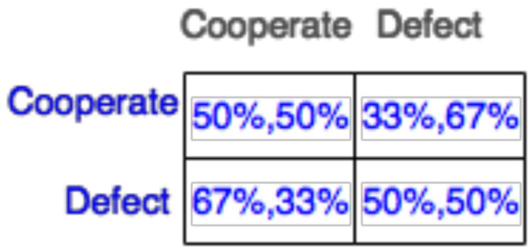
> *"Cryptoeconomic approaches combine cryptography and economics to create robust decentralized P2P networks that thrive over time despite adversaries attempting to disrupt the network."*
>
> – Nick Tomaino, June 2017

- Cryptoeconomics: Paving the Future of Blockchain Technology by Kyle Wang, July 2017:
  - An excellent overview of security models taking incentives into focus. Good description of bribing a.k.a. the P+ε attack and how it (doesn't) affect Casper.
- Making Sense of Cryptoeconomics by Josh Stark, August 2017:
  - Nice introduction to the becoming of cryptoeconomy, with some examples of its use in consensus protocols that we have covered already, application design (like in a decentralized prediction markets, where the functioning of the applications is dependent on users telling the truth, so they are rewarded for that in a native application token) and the use of cryptoeconomics with state channels, that relieve on-chain processing off the blockchain.

Hashing Race in Bitcoin

Here is an exercise in what‘ve covered ...

- **Should miners upgrade their hardware?** Let‘s consider 2 rational miners in Prisoner‘s dilemma, where they each have 50% of the total hashing power initially and are thinking about doubling their mining rigs. If only one of them upgrades, his percentage of hashing power would rise to 67%, but if they both upgrade, they would stay at 50%.
- We expect that they would not cooperate and instead try to beat the other with upgrading their equipment, because that is Nash equilibrium.



	Cooperate	Defect
Cooperate	50%,50%	33%,67%
Defect	67%,33%	50%,50%

Both increase the hashrate!
2x hashrate overall, but
percentage the same.

- Indeed, this is what is happening, if only we remember about the difficulty target ever increasing.
- Also note that this is not Pareto optimal, as such an outcome is not efficient due to huge costs for both of them (of course, the good side of it is that the security of Bitcoin is increasing because of it).

Bitcoin Core vs. Bitcoin Cash

Let's think about many proposed hard-forks in Bitcoin in the past years and try to recognize the game.

- More often than not, these forks dealt with raising the maximum size of the blocks. The most notable are:
  - Bitcoin XT in 2015,
  - Bitcoin Classic in 2016,
  - Bitcoin Unlimited also in 2016 but gaining a lot of steam in 2017,
  - Bitcoin Cash that was materialized on August 1st 2017.
  - There are several known current and historic Bitcoin fork projects.
- It took many hesitant years before the hard-fork actually happened. Despite heated discussions, nobody dared to "pull the trigger" with one of the proposed forks.
  - **Miners** didn't do it because of fear of losing their investment to a possible failure with a new currency, but were tempted as it would possibly increase their profitability and their position in general.
  - **Businesses** want to do whatever is available to increase their profitability, but their power is mostly indirect.
  - **Developers** mostly preferred not to interrupt a running engine and also weren't expecting any benefits to their side.
  - **Users** usually prefer things to stay as they are so as to not having to change their habits and they are usually not interested in technical details at all.
- So when the SegregatedWitness upgrade inched ever closer, suggesting scaling would (at least partly) move to layers above blockchain, miners finally pulled the trigger in order to defend their goals.

Bitcoin Core vs. Bitcoin Cash (Cont.)

- Bitcoin Classic and Bitcoin Unlimited *both* currently have special editions that support Bitcoin Cash.
- The next incoming hard-fork "SegWit2X" was planned for November 2017 and it *also* attempted to increase the block size – its lead developer Jeff Garzik was following his intentions from way back in 2010.
- As the *cooperation* has clearly ended for the moment, a Tit-for-Tat strategy suggests competition to escalate. Indeed, there are motions for legal actions, draconian steps in social/development websites, media propaganda … naturally, from all sides of the players … Bitcoin Core developers are under pressure to provide 2nd layer scaling solutions, opposing developers are consolidating competing clients, while miners are naturally maximizing their profits by switching mining between Bitcoin Core and Bitcoin Cash.
- **What follows?** With a little bit of patience, a more forgiving Tit-for-Tat strategy might resolve the situation. Perhaps a **Tit-for-Two-Tats**. Or a third way will be taken, perhaps something in the likes of Bitcoin-NG. The game of Bitcoin did become much more complex, with developers against developers, businesses versus businesses, and miners jumping sides. However, the game is still the one and the same.
- See this article and at minimum read about the *grim strategy* or the "Grim Trigger": https://blockgeeks.com/guides/cryptocurrency-game-theory/

Bitcoin vs. Ethereum

- With many flavors of Bitcoin and ***two*** flavors of Ethereum, let’s not forget that Bitcoin serves a different purpose than Ethereum. So they are in a different game for all categories of players, except for investors who see this world as a game in whole.
- However, if we consider Ethereum’s split into two and how vastly different their ecosystems are, both in size and feature-wise, we might get some sort of a picture of what might come to Bitcoin in the following years.

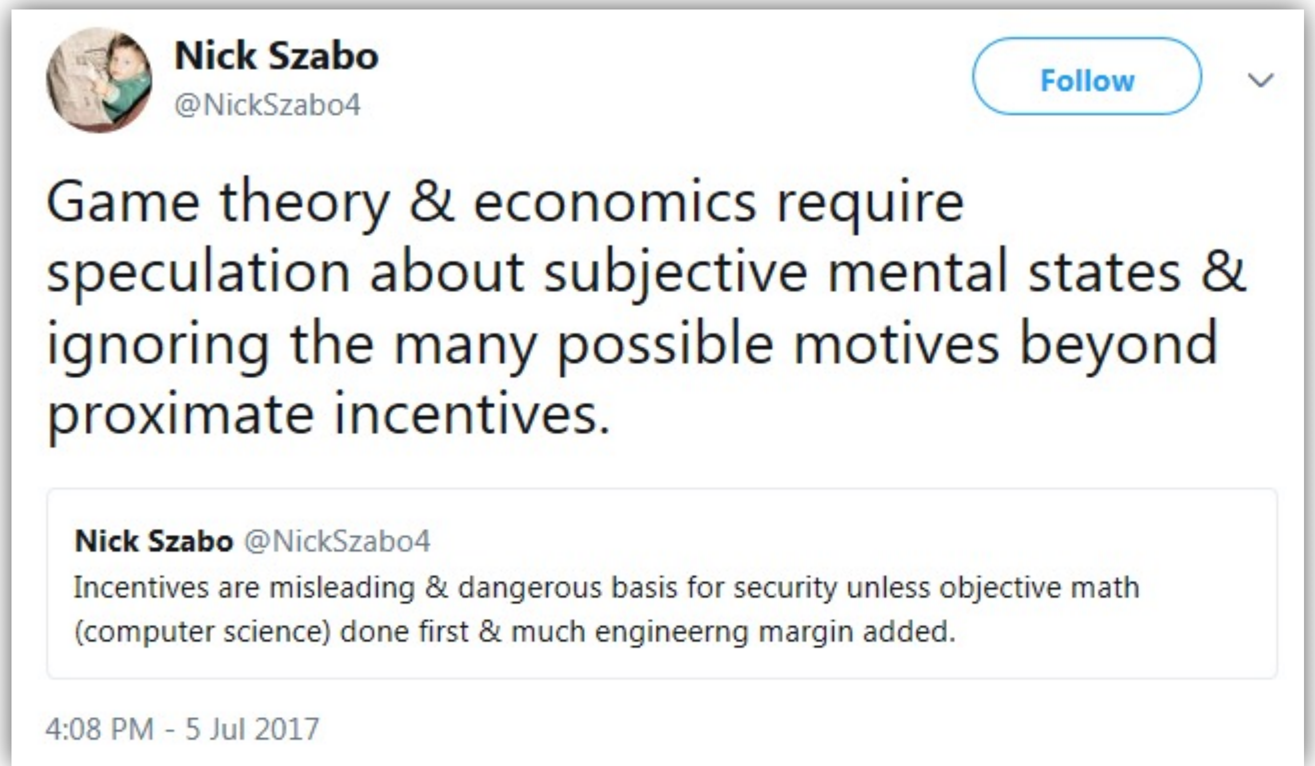
Recap – Bitcoin Incentives

To backtrack a little, let‘s revise the situation in Bitcoin with projections to the real world (Tapscott, 2016: Blockchain revolution) – **Value as Incentive**:

- Principle – alignment of incentives of all stakeholders with value token, so they care for it (the ultimate Tamagotchi)
- Problem to be solved – concentration of power in corporations with disproportionate extraction of value from the very networks that endowed them with rights („If you give people bad incentives, they behave badly, and they behaved just as one would have expected.“, J.E. Stiglitz on 2008 crisis)
- Breakthrough – in Bitcoin, participants are expected to be rational, acting in their own interest, the strategy is that no matter how selfish they acted, their actions would benefit the system overall – making people trustworthy in the sense that they are predictable (miners consume a resource external to the network, the electricity, if they want to compete for rewards)
- Implications for the Blockchain Economy – only now can the Internet be used fully as a tool for proper financial incentives to collaborate effectively, from secure money without counterfeiting, physical thefts and uncapped supply, to finally be able to use multifaceted identity and reputation placeholders, to smart contracts, Internet of Things and, well, no nation state countries.

Risks to Blockchain Security

“Magic money” vs. Engineering



Nick Szabo
@NickSzabo4

Game theory & economics require speculation about subjective mental states & ignoring the many possible motives beyond proximate incentives.

Nick Szabo @NickSzabo4
Incentives are misleading & dangerous basis for security unless objective math (computer science) done first & much engineerng margin added.

4:08 PM - 5 Jul 2017

- Source: https://twitter.com/NickSzabo4/status/882738070616809472

Some Concrete Examples

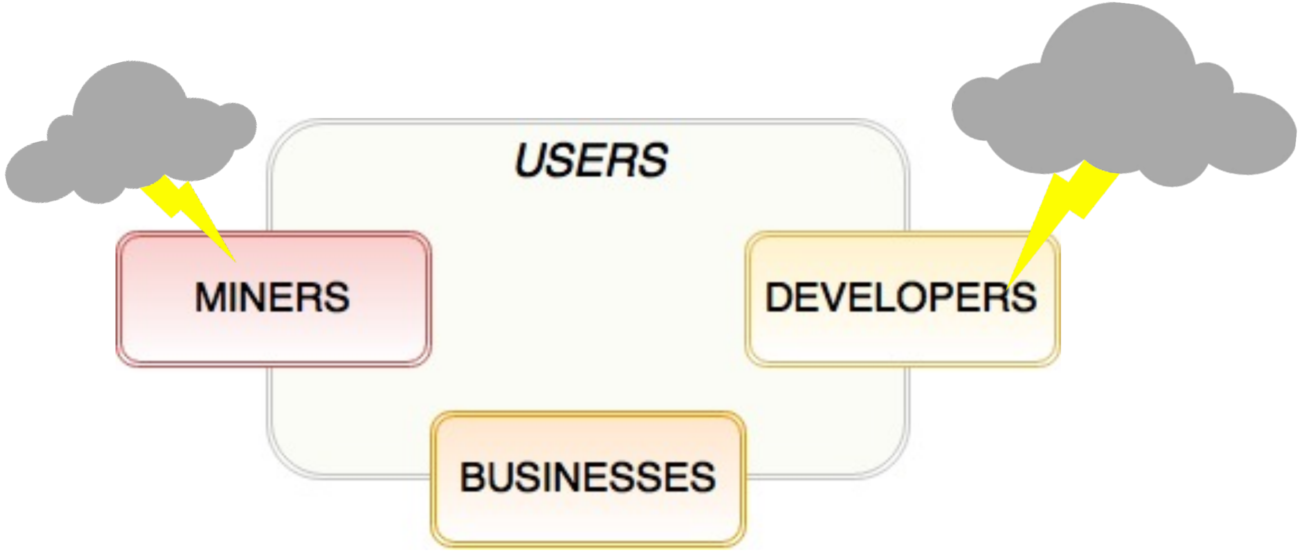
- In Bitcoin, what is the formal protocol specification? How can then different implementations be made? How would a challenger idea be implemented? By forking the code under another name, by pressuring the existing development process, by attacking the existing implementation? Not very trivial questions.
- Pool switching, either to increase the success of selfish mining or to disrupt reward systems.
- Majority is not enough: Bitcoin mining is vulnerable - In 2013, Ittay Eyal and Emin Gun Sirer showed that a block-witholding attack could be successful with only 33% of hashing power (not 51% as usually thought).
- Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools – In 2014, Benjamin Johnson, Aron Laszka, Jens Grossklags, Marie Vasek, and Tyler Moore presented results of their game theory models, showing that economically-motivated DDOS attacks do have a certain threshold when they become profitable.
- On Bitcoin and red balloons – In 2012, Moshe Babaioff, Shahar Dobzinski, Sigal Oren, and Aviv Zohar presented a paper showing that full nodes are actually disincentivized to relay transactions and therefore they proposed a model that aligns the protocol with a broader incentive scheme.

Reality and Rules are Subjective

With our basic knowledge of game theory, we can now more confidently delve into challenges that face Bitcoin and other blockchain systems. A deeper understanding of the theoretical background would of course help us even more, but these topics quickly get very complex and our aim here is just to be able to follow current events and be better informed when acting upon them.

The two main points to make about game theoretical incentive structures in Blockchain related motives and rewards are the following:

- **Not every actor may end up being rational**
- **Several collusion variables may exist „out“ of the game environment**



When „losing“ may actually be winning

Imagine a government that wants to take drastic steps against Bitcoin or any other related technology for their own reasons (monetary stability, experimentation for future use, attacking another state that may be heavily invested etc.), realizing they can’t „ban“ it.

When the stakes are higher in *another* (longer, bigger) game, it may be economically rational to justify a temporary loss for a future win. Keep in mind that this might appear irrational in the subset game! Undermining Bitcoin via investing hugely in hashing power, and then performing any of the high powered attacks possible, **just to undermine confidence in the network**:

- Reverse transactions that they send while in control. This has the potential to double-spend transactions that previously had already been seen in the block chain.
- Prevent some or all transactions from gaining any confirmations.
- Prevent some or all other miners from mining any valid blocks.
- Raise the difficulty significantly, and then completely switch their mining off, making block issuance more scarce and creating congestion in the system.
- DDOS-ing the network in any economically expensive multitude of ways (more here) or congest the network with high fee transactions to eclipse normal transactions, raise fees and create delays in confirmations and loss of use in the system …

But wait, there is more!

Even without going into mining, adversaries can attack via a large number of different ways that take advantage of **wider games** and their PAPI (players, actions, payoffs and information) [Rasmusen,2005] Without solidly defining these larger „games“, it may well be nigh **impossible** to verify the long term, game theoretical viability of Bitcoin or any large blockchain-based system in a cohesive manner, that takes under consideration its external environment as well.

This intertwining of incentives is practically impossible to map out, because it would have to take under consideration the broadest spectrums possible. In these scenarios, **mapping out sets and subsets of PAPIs would be the best indication to what we can expect**:

- Players: How large or how rational can we expect them to be if Bitcoin may end up being viewed as a serious threat to them (financial institution, bank, or even a small state)
- Actions: Would a country prefer to chase miners, shut down the internet or some other action (out of the system) to influence it?
- Payoffs: What's the cost vs. benefit of allowing Bitcoin to proliferate, esp. in relation to the specific payoffs desired by e.g., a company (market shares), a country (monetary policy control), etc.
- Information: What information about other players would allow them to collude against said system (could we consider that Hyperledger and R3 may be such attempts?)

Gaming Transparent Systems

- Collusion of players towards a set of actions could mean that even though e.g., mining pool hashrate seems adequately distributed, this might not be the situation under the surface. We have no ways outside of Bitcoin to ensure the same degree of (information) transparency we can all evaluate via the blockchain. And it's not just mining, it’s governance, development, discussions and information „watering holes“ that we need to safeguard against collusion and special interests, that may be taken advantage of, by rational or (seemingly) irrational actors.

- Bribes, coercion, manipulation, even threats and special interests (large investors, companies, state agencies, *etc.*) are not so easy to define theoretically as actors (and they don’t have to be rational either) and the repercussions of their actions to the closed system of Bitcoin, should **not be discounted** as an action of a player acting according to the rationality of their own game.

- **For instance**, in the case that fees for transactions rise beyond „acceptable“ levels, what would stop a large exchange from entering in an agreement with a mining pool or miner to **always** include their transactions with a smaller fee (than the market’s) for a monthly subscription fee, and in this way avoid the unpredictability of the (current) fee market? (This might already be happening …)

The Art of War

- In 5th Century BC, the great Chinese military strategist Sun Tzu wrote in his legendary work, the Art of War:

"All warfare is based on deception."

- Thinking about the risks to the proliferation of Bitcoin and blockchain technology should acknowledge that.

Migration Methods

The Longest Games are the Most Open

Despite the uncertainty and developing nature of this field, in the fringes of Bitcoin as a closed system and the world at large as an open system, several observations can already be made :

- What we can argue with a degree of confidence, is that the more such a network is worth in total, the harder it is to undermine it with external pressure. This could emerge by increased liquidity of main trading pairs, that could otherwise enable speculative attacks.

- Taking control of concentrated hashing power, development, potential for coding bugs *etc.* could be mitigated by further decentralizing these elements and allowing for a larger plurality of options, which is somewhat done by market forces already.

- In a surprising case of the iterated Prisoner’s dilemma, even apparently irrational actors will almost always have adversaries and competitors, whether working purely in Bitcoin or in a larger „game“. This means a number of things long term (continued in the next page).

Big and bigger fish, in a wide ocean of global value

- The larger the value of the network, the larger the actors it will attract, and the more adversarial the relationship of competing actors **between them** is expected to become – but only **if** enough actors value decentralization and thus reject collusion, centralization and monopolization by a group of stakeholders. Whether in terms of liquidity, hashing power or investor influence, „bigger ponds attract bigger fish“, and while Bitcoin has always been very small in global terms, that is changing fast.

- More use cases, as those opened by a superior means of exchange or a store of value, or smart contracting platform generally, also mean a wider diversification to and from multiple rational actors.

- On the other hand, Bitcoin is not damaged by internal adversarial behavior since competition and market forces are at the center of not only consensus building, but price discovery and infrastructure development (exchanges, payment processors, service providers). Thus, an irrational actor may find an army of rational actors against them if the incentives are there to oppose him, someone shorting Bitcoin with a large amount of external fiat, may find market opposition very fast.

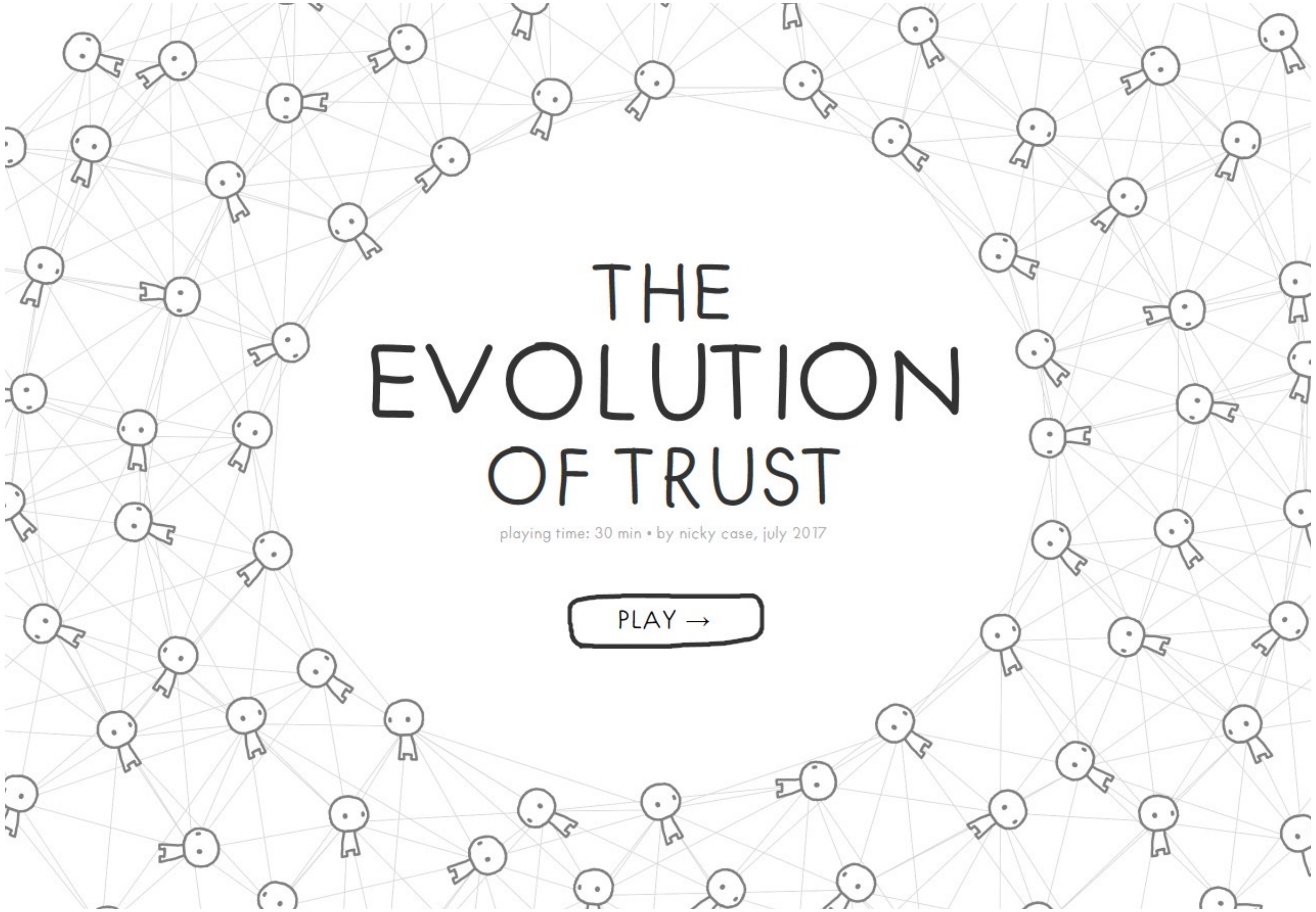
Race for scalability

- **The Scalability Factor:**
  - Considering the Blockchain Trilemma, the race for introducing the most scalable blockchain protocol is on. Many different blockchain protocols have been emerged claiming to be able to scale to millions of nodes and process thousands of transactions (high throughput).
  - This race has introduced several improvements to consensus algorithms and alternative governance models (though the idea of voting)
  - However, actors in such protocols are likely to identify more sophisticated attack vectors. ***Consider coalitional games between of different group of voters in a DAO?***

- From the game theory perspective, it seems that scalability is a factor that can linearly increase the complexity of the game dynamics. Especially for the next evolution of blockchains. As a result, these protocols are going to start exploding more advanced game theory scenarios in order to operate efficiently at scale.

  - *What do you think?*

The Evolution of Trust



http://ncase.me/trust/

Conclusions

Conclusions

- There are a lot of texts about how Bitcoin, Ethereum and many other blockchain systems work by utilizing a number of cryptographic and other technological constructs. A lot of ink is spilling on topics of optimizing user experience, scalability and regulatory challenges. However, at least as important question is how do we use all this for a good cause and for the long-term benefit of its users.
- Game theory offers a way to model interactions among participants and we can use its concepts to analyze the intricate incentives that make such systems operate even with a minority of malicious users.
- We conclude that there are still many open issues in blockchain designs, which are worrisome on the one hand and an amazing testbed for further research on the other. With these systems having larger and larger market evaluations, we can, and we must expect that any number of attempts to cheat the protocol will be made. Not the least because the actors can be rational and quasi-anonymous, and money literally lying in the open.

Glossary

Glossary

Utility function: a generalized metric of „happiness“ of a self-interested agent for a particular preference among all available alternatives, for instance in Bitcoin the function would prefer outcomes where an agent receives more coins; however not all utilities are about „money“

Rational user: aims at maximizing his own utility function, hence he is primarily concerned with his own profit and doesn‘t care about happiness of others (selfish, non-communicating, intelligent, purely economic -> rational fool)

Nash Equilibrium: if each player knew the strategies of others and wouldn't be able to increase his gains by changing his strategy, such actions would be in Nash equilibrium. „If a player acted differently, he would not be better off, but likely worse.“

Self-Assessment Exercises and Further Readings

Self-Assessment Exercises

- We have seen how competition drives the ever increasing hashing rates in Bitcoin, which has some negative connotations about its energy consumptions and positive ones for increasing the security of the system. However, short-term financial gains are not the only focus of miners, there are broader economic and social aspects that make Bitcoin interesting. How far do you think miners would be willing to support the network at a loss, paying more for the electricity than they receive rewards from mining?

You are welcome to share your thoughts on the forums!

Further Reading

A survey on applications of game theory in blockchain, Liu, Z., Luong, N. C., Wang, W., Niyato, D., Wang, P., Liang, Y. C., & Kim, D. I. (2019). arXiv preprint arXiv:1902.10865.

https://arxiv.org/pdf/1902.10865

(Excellent paper on providing a more extended view of the material we covered in this session. Table 2 presents a summary of Game Theoretical Applications for Security.)

Multiagent systems: Algorithmic, Game-Theoretic, and Logical Foundations, Yoav Shoham & Kevin Leyton-Brown, 2010

http://www.masfoundations.org/mas.pdf
(A very extensive description of game theory, if you are more interested in the topics we covered in this session)

The Miner's Dilemma, Ittay Eyal, 2014

https://arxiv.org/pdf/1411.7099v2.pdf
(Analysis of mining strategies for block witholding attacks among mining pools)

On Bitcoin and Red Balloons, Moshe Babaioff & Shahar Dobzinski & Sigal Oren & Aviv Zohar, 2012

https://www.microsoft.com/en-us/research/wp-content/uploads/2012/06/bitcoin.pdf
(On incentivizing full nodes)

Further Reading (Cont.)

Shelling Out: The Origins of Money, Nick Szabo, 2002

http://nakamotoinstitute.org/shelling-out/
(If you have not yet read it, it is highly recommended to bookmark it and read it when you have time. It is a deep exploration to the history of money, touching on the subjects of cooperation and altruism between humans.)

Bitcoin Mining as a Contest, Nicola Dimitri, 2017
https://ledger.pitt.edu/ojs/index.php/ledger/article/view/96
(An article about Bitcoin mining with interesting conclusions:
"The model suggests that the main motivation for active mining is given by the miners' cost structure, while the reward for solving the puzzle affects only the optimal level of computational power but not the decision to be active. Finally, the mining activity seems to be intrinsically monopoly-proof, in the sense that if only two miners were to be active, their profits would always be positive regardless of the marginal cost of the opponent.")

UNIVERSITY *of* NICOSIA

Questions?

Contact Us:

Twitter: @mscdigital
Instructor’s Email: christodoulou.kl@unic.ac.cy

Course Support:
Mark Wigmans - wigmans.m@unic.ac.cy
Marios Touloupos - touloupos.m@unic.ac.cy

IT & live session support: dl.it@unic.ac.cy