Blockchain Technology: ‘Proof-Of-Work’ Versus ‘Proof-Of-Stake’ (http://www.lindau-nobel.org/blog-blockchain-technology-proof-of-work-versus-proof-of-stake/)

Posted on 26/08/2017 (http://www.lindau-nobel.org/blog-blockchain-technology-proof-of-work-versus-proof-of-stake/) by Demelza Hays (http://www.lindau-nobel.org/author/dhays/)

Bitcoins. Photo/Credit: skodonnell/iStock.com

Cryptocurrencies like Bitcoin and the blockchain technology that underpins them are gradually becoming household words. Although peer-reviewed research is only just beginning to develop on the topic, the cryptocurrency ecosystem is growing at an exponential rate. Everyday, new businesses, investors and researchers enter this dynamic space.

At the University of Liechtenstein, I have been working on an experimental blockchain project with Professor Dr Martin Angerer and Jonas Gehrlein, MSc from the University of Bern. Our research on blockchain technology has been an educational, demanding and exciting journey.

The terms ‘blockchain technology’ and ‘distributed ledger technology’ refer to a variety of different technologies that attempt to solve different problems. Cryptocurrencies and blockchain technology emerged after the 2007/08 global financial crisis. The most popular example of these technologies is Bitcoin.

Bitcoin is a decentralised and open-source digital currency that stores transactional data in a distributed database that is maintained by computers all around the world. The creator of Bitcoin, who is still unknown but goes by the pseudonym Satoshi Nakamoto, wanted to provide a decentralised, private and secure means of transferring value online that did not rely on trusting sovereign entities, central banks or financial intermediaries.

A major discussion in the cryptocurrency realm relates to the optimal algorithm for achieving a collective agreement on which transactions are valid and which are invalid within a distributed network. Currently, the two most popular methods are known as ‘proof-of-work’ and ‘proof-of-stake’.

Bitcoin’s proof-of-work algorithm uses large quantities of energy and hardware equipment, which have been estimated to cost (https://www.researchgate.net/publication/304781623_The_Fair_Cost_of_Bitcoin_Proof_of_Work) approximately $400 million per year. Proof-of-stake is a newer invention that has not been rigorously tested in the market.

When my colleagues and I began our research project, we wanted to investigate the differences between these two consensus mechanisms in a laboratory environment. Our motivation was simple: if both systems achieve the same outcome but one system (proof-of-work) incurs a negative externality on the environment, then why are people still using it?

Despite the seeming superiority of proof-of-stake, market participants prefer proof-of-work. Using market capitalisation as a proxy for demand, the highest market capitalisation coins all rely on proof-of-work. But proof-of-stake is gaining popularity: Ethereum, the second largest market capitalisation coin, is expected to switch from proof-of-work to proof-of-stake during the next year.

Our research uses game theory and behavioural economics to study the strengths and weaknesses of these two competing systems in a lab environment with students.

Our first step was to boil down the complex nature of these consensus mechanisms into abstract concepts that could be easily modelled in a lab. We spent months reviewing the research literature and brainstorming possible set-ups for the experiment.

The lab setup for proof-of-work was relatively straightforward. We planned to draw from the public goods literature on network externalities. Students would be given the option to use a medium of exchange that incurred an internal personal cost or a medium of exchange that incurred an external cost for the environment.

Essentially, this represented the current fiat system versus the energy-guzzling Bitcoin. At this point, we were very excited about the direction of our research and about the contribution that it could make to the fields of economics and information science.

Unfortunately, our research hit an insurmountable obstacle when we tried to model proof-of-stake: we could not find a way to do it easily in a lab. We discussed potential drawbacks of the proof-of-stake system such as 51% attacks, deflationary spirals and uncertainty stemming from ambiguity. But we came to the conclusion that Bitcoin's proof-of-work suffered from the same drawbacks, albeit to a lesser degree.

During my own reflection on the differences between proof-of-work and proof-of-stake, I came to the conclusion that these systems resemble our transition from a gold standard to a fiat standard. Like gold, Bitcoin uses electricity and capital equipment to mine new coins. The probability of randomly being chosen to create a block and receive a reward is equal to each miner's amount of mining power divided by the total amount of mining power on the network.

On the other hand, proof-of-stake allows the users with the largest holdings to create coins out of thin air. In a proof-of-stake system, the probability of receiving a reward is equal to the fraction of coins held by the user divided by the total number of coins in circulation.

Following this logic, proof-of-stake would appear to be superior to proof-of-work because economic theory argues that the fiat system is superior to the gold standard due to deflationary spirals caused by hoarding. (Note, however, that my late uncle, the American economist Larry Sechrest, argued in his 1993 book, *Free Banking: Theory, History, and a Laissez-Faire Model* that the problems associated with the gold standard actually stemmed from regulation and not from the scarcity of gold.)

To date, my reflections have not helped us find a suitable set-up for the lab experiment: we have been unable to find a major setback of the proof-of-stake consensus mechanism. The only problem that I could find was quite philosophical in nature and too complicated to be easily modelled in a lab.

The twentieth-century Austrian logician, Kurt Gödel, argued that no system can prove its own correctness from within itself. In reference to proof-of-work and proof-of-stake, the former appears to solve Gödel's incompleteness theorem while the latter relies on external truth to achieve consensus.

In a proof-of-work system, anyone can join the system and immediately determine the correct history of transactions in the blockchain because the correct chain is the longest chain by default. In comparison, proof-of-stake has not developed a method for ensuring that every computer in the network comes to the same conclusion on the correct history of transactions from within the system.

Instead, proof-of-stake relies on an external third party or host of third parties to establish agreement on the history of transactions. In plain terms: proof-of-stake establishes truth by appealing to an external anchor while proof-of-work establishes proof from within. Although the introduction of counterparties may not be a problem in every case, the original goal of the blockchain technology was to create consensus without intermediaries.

In the end, we could not find a suitable way to model proof-of-stake in a lab with humans. In our own analysis of this problem, we realised that there was a fundamental problem with the premise of our study: we were trying to model a lab experiment with humans based on a technology that was designed to minimise human interaction.

Although we have encountered this major setback in our study, we have learned a tremendous amount about blockchain technology and about our own strengths and weaknesses as researchers. Instead of giving up, we are going in a new direction with our blockchain research. After all, the journey for pioneers is never paved.

About Demelza Hays

Demelza Hays is a blockchain researcher at the Centre for Global Finance and Technology at Imperial College London, under the supervision of the former Chief Economist of the US Commodity Futures Trading Commission (CFTC), Professor Dr. Andrei Kirilenko. At the University of Liechtenstein, Demelza is completing her doctoral thesis on the role of cryptocurrency in asset management, and she teaches a course for bachelors and masters students on Bitcoin and blockchain technology. At Incrementum AG, Demelza is working on cryptocurrency research and a cryptocurrency fund for institutional investors.