



Gilles Sabrie / The New York Times

This Bitcoin farm in Guizhou, China requires a tremendous amount of cooling power.

BITCOIN

February 5, 2018

Cornell Tech Professor Explains Hype And Pitfalls of Cryptocurrencies

By **Amol Rajesh**

Chances are you know someone who's mined bitcoin. However, cryptocurrencies are not everything they appear to be. Drawing the ire of governments and financial institutions alike, questions about its reliability are on the rise.

Prof. Ari Juels, computer science at the Jacobs Technion-Cornell Institute at Cornell Tech, discussed the impact, technology and regulatory environment of cryptocurrencies.

Co-director of the Initiative for CryptoCurrencies and Contracts — a collaboration between Cornell, the University of California, Berkeley and the University of Illinois at Urbana-Champaign, based at Cornell Tech — Juels helps lead research on blockchain technology and its applications.

Cryptocurrencies are one of the most notable applications of blockchain technology. Blockchain is a digitally-secured distributed ledger of transactions. Juels talked about possible reasons behind the surge in popularity of cryptocurrencies such as Bitcoin.

“Cryptocurrencies are digital assets created and managed in decentralized or peer-to-peer systems,” Juels said. “Bitcoin is so popular now because it points the way to new and interesting models of digital trust. But of course the main reason is simply that its price has skyrocketed.”

According to CoinDesk, the price of one Bitcoin today is \$7,011.

Bitcoin are created through a “mining” process in which certain computers solve complex math problems. Every time a computer “mines” a new Bitcoin, it becomes harder to mine more Bitcoins. The increase in Bitcoin mining has taken a large toll on overall electricity consumption.

“The Bitcoin network consumes as much electricity at this point as a small nation. This is unconscionable and unsustainable. Happily, less wasteful alternatives are the subject of active research and deployment,” Juels said.

In the past few years, there have been many instances of cryptocurrency exchanges getting hacked. Bitcoin has been subject to thefts with damages often exceeding tens of millions of dollars. Cryptocurrencies, despite being a relatively new development, have the same security lapses as the general internet, according to Juels.

“The difference is that cryptocurrencies are a particularly rich and juicy target and their partial anonymity helps black-hat hackers,” Juels said, referencing groups of illegal hackers.

Juels elaborated on security concerns and other drawbacks which are associated with fully decentralized cryptocurrencies.

“Price volatility is only one problem. High and volatile transaction fees are another. And the perennial challenge of managing private keys, i.e., the secrets needed to hold and transact with cryptocurrencies, is yet another,” said Juels.

Juels added that securing private keys are even challenging for security experts.

He expressed doubt on the ability of current cryptocurrencies to be widely used as a means for exchange.

“Whether ‘permissionless’ cryptocurrencies can function effectively as true currencies remains to be seen,” Juels said.

Juels gave his thoughts on the current regulatory environment for cryptocurrencies.

“I’m a computer scientist, not a regulator. But I’ll point out that cryptocurrencies and decentralized systems more generally were intended to spark a revolution and throw off the yoke of institutional and governmental oppression,” Juels said.

An Initial Coin Offering is a method by which the organizations behind an upcoming cryptocurrency can raise funds. ICOs have come under scrutiny from the Securities and Exchange Commission and they have been a topic in an ongoing debate over whether cryptocurrencies should be legally treated as currencies or as securities, like stocks.

Despite the current controversy surrounding cryptocurrencies, Juels hopes for positive regulation in the future to ensure stability and foster innovation.

“I’d like to see regulation that effectively brings the best of the old and the new, removing corrupt players in the traditional financial industry, but preventing new and worse unscrupulousness,” Juels said.

Although cryptocurrencies are contentious, Juels emphasized the importance of the variety of applications behind blockchain, the technology which serves as a backbone for cryptocurrencies.

“Blockchains and smart contracts promise to strengthen trust relationships and automate business processes in areas ranging from humanitarian aid to food supply chains,” Juels said.

