Researchers link realism to blockchain's promise

December 28 2018

Princeton researchers are answering fundamental questions about blockchain to explore its full potential. Credit: Beatrice Trinidad

Depending on who you ask, blockchain technology is poised to revolutionize the world—from creating a universal currency to building a free and truly private internet. Or, the new technology, built with a combination of encryption and transparency, is a solution in search of a problem.

The reality likely falls somewhere in between. While a growing number of startups and researchers are devoting themselves to exploring blockchain's full potential, experts caution that a healthy dose of skepticism is needed to fully evaluate the technology and its eventual place in society.

For many individuals, though—including some looking to invest—blockchain technologies and their limitations remain poorly understood, leaving people vulnerable to being exploited by bad actors. Researchers at Princeton University's School of Engineering and Applied Science are striving to change that through education, outreach and research.

"Early on we realized this was a technology that was not well understood but that a lot of people were interested in," said Ed Felten, the Robert E. Kahn Professor of Computer Science and Public Affairs at Princeton. "There wasn't a coherent, high-quality way of teaching about this technology or explaining it, so we've tried to systematize the knowledge and unsolved problems underlying it."

Simply put, a blockchain is a ledger. But unlike an old-time hotel register gathering dust on a counter, a blockchain ledger is held electronically in multiple locations across the internet. It is visible to any member of the community participating in that particular blockchain. Each copy of the ledger is held on a computer called a node; when someone makes a transaction using the blockchain—say using virtual currency to order a pizza—the operators of the nodes run through calculations to create a new entry, or block, in the ledger. Each new block is encrypted using a private, numeric key from the person who bought the pizza; the new blocks are also linked to the previous blocks using additional encryption.

The combination of encryption and visibility makes entries extremely difficult to fake. Because the calculations are carried out on multiple

nodes and the results are visible to participants—varying results would be an immediate red flag. The distributed nature of the system means it is hard for a single entity to control. It also makes transactions extremely difficult to track back to a user.

The initial use of blockchain technology was in new forms of currency such as Bitcoin. More recently, the ability to track decentralized transactions reliably has attracted other sectors. Businesses are exploring its use for contracts, app development and international finance.

"I think this will be a story of gradual integration, rather than a story of a revolution," said Arvind Narayanan, an associate professor of computer science at Princeton. "It's an interesting new technology, and a number of us here are working to make that technical footing even stronger."

In 2014, Narayanan began teaching one of the first university courses on blockchain, which he and Felten soon expanded into an online Coursera series and a popular textbook. At the same time, with colleagues and former and current students, they began innovating ways to maximize the benefits of blockchain and minimize the risks. "There's a lot at stake, and a lot not understood about this technology," Felten said. "As independent academics, the role we try to play is to be explainers, interpreters and B.S. detectors."

That said, Felten and Narayanan believe that blockchain does have a significant role to play—although, most likely, we have yet to imagine what it will be. "In some sense, we're still in search of its major application," Felten said.

Numerous Princeton alumni are attempting to fill that unknown by becoming early innovators in the field, including a co-founder of the cryptocurrency Ethereum and founders of several high-profile companies, such as Blockstack (see list below). Where they will take

these and other ventures depends not only on technical finesse, but imagination.

The decentralized network

Blockchain's most prominent use so far has been in creating cryptocurrencies, such as Bitcoin and Ethereum, that are not controlled by a central bank. These currencies are not blockchains themselves—they are abstract tokens—but trades of their coins are recorded on blockchains. Because ownership and any transfer of ownership is recorded on the public ledger, participants in the Bitcoin system do not need to trust any one entity. Instead, they place their trust in the distributed ledger technology, which is maintained by a large number of participants around the world.

Each cryptocurrency offers a limited number of coins, although new ones are regularly created and doled out as payment to users, called miners, who are the first to solve the difficult computational problems—the harsh puzzles—added to the chain. Miners' computers run algorithms that perform the difficult task of building blockchain records and solving mathematical problems. In exchange, they receive coins.

While this sounds abstract, Felten points out that the system actually has much in common with conventional currencies. "Most money we have exists in numbers on some computer somewhere," he said. "If you go into a sandwich shop, they give you a sandwich in exchange for you telling a bank to move numbers from one account to another." Like paper money, he continues, cryptocurrencies have value because their supply is limited, and because users can be confident that they can exchange them for goods and services. Cryptocurrencies now trade against the dollar, and their combined market cap is over $100 billion.

Among their biggest attractions, cryptocurrencies offer a way to transfer money over distances and borders without involving intermediaries that may charge high fees. In other cases, certain cryptocurrencies possess advanced features, including the ability to create smart contracts, or self-enforcing rules that govern escrow arrangements and other interactions.

Blockchain is still in its infancy, though, so the true scope of its usefulness is likely yet to be revealed.

"It's kind of an analogy to the early days of the internet, where some people were super excited and made a lot of claims about how it would change human existence forever, and some said it was just a fad," Felten said. "While it didn't solve all of humanity's problems, it did turn out to be pretty important."

But for all the interesting current and future uses for blockchain, he added, there is "an extraordinary amount of snake oil and exaggeration in the public rhetoric." Because some cryptocurrency transactions are anonymous, for example, they are particularly attractive for criminal groups, including those looking to exchange illegal goods. In other cases, less savvy users are exploited through "pump and dump schemes" in which unscrupulous investors artificially boost the price of a hot commodity and then quickly sell, causing a crash. "There are a huge number of scams going on," Narayanan warned.

Blockchain is also extremely energy intensive, mostly due to mining, which requires specialized equipment with a high demand for electricity. Bitcoin mining alone accounts for about 0.1 percent of total world energy use—more energy than certain countries, including Denmark and Ireland, consume. As Narayanan testified before the Senate Committee on Energy and Natural Resources in August, this represents a serious problem for energy use and the environment.

Coding the future

From the early days, Princeton researchers have been striving to mitigate some of these issues and to better understand the technology and its potential.

"Bitcoin is portrayed in the media as jumping into existence from the mind of one mysterious person, but I co-authored a paper on the component technologies of cryptocurrencies that cited literature from the early 1980s," Narayanan said. "Continuing to improve on cryptocurrency and blockchain will take a lot more computer science research."

BlockSci, for example, is a database that Narayanan and his colleagues built to analyze hundreds of millions of Bitcoin transactions. BlockSci allows them to investigate trends and to answer questions such as how much money is actually being transferred and how much privacy users truly have.

"There are lots of interesting scientific and commercial questions we can ask with these data," Narayanan said. A recent investigation revealed, for example, that bitcoins are changing hands less often than what was previously assumed—about 1.4 times per month—suggesting that individuals are using coins less as currency and more as investments.

Princeton students and graduates are also pushing the field forward, by creating apps and writing software to improve cryptocurrencies; founding companies based on blockchain; and funding such ventures. Joseph Lubin, one of the founders of Ethereum, graduated from Princeton in 1987 with a degree in electrical engineering and computer science.

One recent venture, Basis, founded by Princeton computer science

alumni Nader Al-Naji, Lawrence Diao and Josh Chen, recently raised $133 million for effort to build a cryptocurrency that maintains a more stable price than conventional blockchain-based "coins." The Basis system creates the virtual equivalent of a central bank, which automatically adjust the supply of currency, based on demand.

One recent Princeton alumni venture, Blockstack, aims to build a completely decentralized internet based on blockchain. According to co-founders Ryan Shea (2012 BSE in mechanical and aerospace engineering) and Muneeb Ali (2017 Ph.D. in computer science), Blockstack, which is registered as a public benefit corporation, was inspired by major issues they perceived in the way the internet works, including concerns about personal data and autonomy.

"We saw that a lack of competition and lack of control for the end user was really hampering freedom, security and privacy around the world," Shea said. "We wanted to build a new system that empowers the individual and allows each of us to own our data."

Rather than Facebook storing and controlling all of a person's data on its servers, for example, a Blockstack user could easily migrate his or her digital identity from app to app, if desired. Blockstack software for managing profiles and securing accounts is already available, as are decentralized messenger and document editor apps. Next year, the company plans to release its own blockchain in tandem with a Blockstack token, and discussions are underway for creating a decentralized Twitter.

"We're working with lots of teams to help them build whatever apps they desire on the platform," Shea says. "The most exciting things are less around the exact details of the underlying infrastructure we provide and more around how we enable developers to create new experiences."

Blockstack is already coming full circle by inspiring and enabling other Princeton scholars to create new technologies. At the Keller Center for Innovation in Engineering Education's eLab Summer Accelerator Program in August, a team of new Princeton graduates launched Afari, a Blockstack-based social media platform meant to give data privacy back to the people by returning data ownership and privacy to users, and by giving everyone an equal chance for their voice to be heard and rewarded.

"Social media is so broken in our opinion that you need to redesign it from the ground up," said Avthar Sewrathan, co-founder of Afari and a 2018 graduate in computer science. Blockchain, the team said, makes that possible. "When you make a post on Afari," said co-founder Felix Madutsa, "your data is not stored with us but rather is stored on a decentralized system that you, the user, controls and owns."

Provided by Princeton University

Citation: Researchers link realism to blockchain's promise (2018, December 28) retrieved 25 June 2024 from https://phys.org/news/2018-12-link-realism-blockchain.html