as little as $1 today.

NUMBERS | ECONOMICS

The Bitcoin Paradox

Why cryptocurrency will always be political.

BY SIMON DEDEO
DECEMBER 14, 2017

You are an inmate in a luxury hotel. Locked in your soundproof suite, you hear nothing and see nothing. Liveried butlers bring you meals on silver carts. You have plenty of time to read, think, and listen to music. All the riches of culture can be called down at your whim. But you are trapped, too, and desperate to talk.

One day, you look under your dinner service and discover a note. ARE YOU THERE? You write back, tucking your reply under the plate. YES, WHO ARE YOU, WRITE SOON. In the morning you find replies. It doesn't take long before you realize that notes are being shared, passed, and shuffled, among perhaps dozens of inmates being held in dozens of rooms.

BEFORE BLOCKCHAIN: The common knowledge enabled by the blockchain used to be created in spaces like the Kiva, a reconstructed version of which is shown here.

Communication is easy, but it's hard to tell who knows what. Messages pass one another in corridors; conversations fragment. When A replied to B, had she received your message yet, or was she reading C's? Did she ignore what you said because she didn't like it, or because it had yet to be delivered? When D proposes a simultaneous attack on the wardens as they deliver dinner, how many people received it? When A confirms to D that she's in, will D see the message in time? Will D know that B saw it?

Here's one solution, if a strange one. Write a message with a very difficult mathematical problem on it—a problem so hard that it would take a month of concentration to solve. Now wait.

Perhaps nothing happens. But perhaps, just perhaps, you find the answer under breakfast one morning.

There's a room sunk into the ground at the Bandelier National Monument, a few miles from Los Alamos, New Mexico. In plain view for seven centuries, among the ruins left behind by the native peoples who lived there, the circular room, about the size of a high-school classroom, is called a Kiva. A bench formed out of straw and mud used to run around the perimeter.

One thing Kivas were used for is politics. The circular floorplan made it possible not just for everyone to be heard, but to be seen. When someone spoke in the Kiva, he could see his fellows and his fellows could see him. The circle also meant that his fellows could see each other seeing him; at a glance they could take in not only the speaker, but the faces of their colleagues doing the same.

It is not enough to dislike a government; you need to know that others do too.

That matters because politics is not just what you think and believe. If I'm trying to do something that requires your cooperation I need to do more than say I'm willing. I need to know that you know I'm willing.

In cognitive science, we call this common knowledge. To know something is one thing; but to know it with others, know that others know it, and know that they know that you know it, and all the way up the tower—this is another thing altogether. It's what you need for costly cooperation. What teammates on the field and business partners in the boardroom signal when they look each other in the eye is a mental moment at the origin of society.

Common knowledge is power. It is not enough to dislike a government; you need to know that others do too. When you've built that common knowledge in secret meetings and basement cafes you might go out into the street. In a crowd, common knowledge is obtained without needing to look: The roar of a crowd is the roar an entire crowd can hear.

Totalitarian societies know the power of common knowledge very well. When Gary King's Institute for Quantitative Social Science reverse-engineered the Internet censorship practiced by the Chinese government, they found that the government cared less about insults and criticisms than one might expect. What it censored aggressively were social media posts making plans to meet in person. Online, talk is cheap: but face-to-face people can build common knowledge.

Back in your luxury hotel prison, the moment comes: You see an answer to your mathematical problem under your dinner. What does that tell you? At the very least, your message must have reached someone else.

You ponder a bit, and write down a different problem. More than a brainteaser, this one has a funny property: It's impossible to solve except by guess-and-check. And, while it's easy to check whether your guess is correct, it's very hard to find the right guess. If you guessed once a minute it would take you 10 years, say, before you got the answer.

A week later, a solution arrives. What does that tell you? For the answer to be struck so quickly, there must have been many people who saw your problem and worked on it. Indeed, somewhere around 500.

Collage: De Agostini Picture Library / Contributor / Getty Images; Pixabay

Now you're in business. You make a second problem. It has the same properties as the first, plus it incorporates the solution to the first problem. (If you like, imagine that the problem involves a collection of numbers; the new problem takes as one of its numbers the solution of the first.)

You send it back out. You wait. A week later, an answer to the second problem comes back.

What do you know now? Well, as before, you know that a large number of people saw the second problem. And, since the problem included the message from the first problem, you know that everyone saw that as well, and can reason in a similar fashion. A rough, statistical form of common knowledge has emerged.

The luxury prison of voices is the Internet.

As long as you're willing to keep solving problems like this, you can thread together a conversation. If someone wants to reply to you, they can add the solution to your problem to their message. Now you know that the message really is responding to yours, since it couldn't have been written by someone until your message was shared and solved, and when the problem is solved, you know others know it too.

You have started a chain. And every element of that chain, as well as the existence of the chain itself, is common knowledge.

The luxury prison of voices is the Internet. Messages are passed back and forth as Internet packets. Problems are solved by custom-built computing machines. The use of these problems to solve the common knowledge problem is called "Proof of Work." And the string of messages threaded from one problem to the next is the blockchain.

When common knowledge becomes possible, what will be the first order of business in your communication with your fellow inmates? It will be how to get out, and who will lead the effort. It will be politics.

When I was a graduate student, I was, for a time, in charge of taking lunch orders for a Thursday seminar series (called Thunch, or Thursday Lunch). Students would log onto the central mainframe and use a specially-written command to place an order. Around 11:30 I would print out the order database and ride my bicycle over to the sandwich shop to place it. Accounts were kept in a text file in the mainframe, and once every few weeks I would stroll the halls collecting debts.

For all of the complexity of our financial system, this is basically how money works. People have accounts: a set of numbers, kept in a text file, or a ledger, or a database somewhere at a bank. We agree on rules for how those numbers change. We serve Thunch.

BitCoin is a currency that lives on the blockchain. The only messages that can be sent are "transactions," transfers of a fictitious unit of money, or bitcoins, between accounts. Like any financial system, BitCoin has its own set of rules. No account can go below zero. People who take the time to solve the proof of work puzzle are awarded a unit of currency.[1]

ALSO IN ECONOMICS

Taming the Unfriendly Skies

By Allan Dodds Frank

When Rick Curtis, Chief Meteorologist for Southwest Airlines, walks down the hallway, he is often asked, "What does this week look like?" For Curtis, it's the universal question that comes to him from every level of management—frankly, just about everyone at Southwest has a stake...**READ MORE**

Currency is just one use of the blockchain. There are lots of others. Etherium is another blockchain that not only keeps accounts, but also allows users to upload fragments of computer code that govern transfers in increasingly complex ways. Basic government functions, such as the registration and transfer of automobile titles and real estate, the signing of public contracts, and even voting, can be done on blockchain. So can the establishment of new prediction markets that allow participants to bet an internal currency on real-world events.

These are all variations of the conversation at the Kiva. Which is to say, they are political. And that merger of technology and politics produces an unexpected paradox.

While blockchains are excellent at forming common knowledge according to a set of rules, those rules are set by hand at the very beginning. Blockchains in place to date do not include a process for amending their constitutions. That means participants are trapped in the logic set by their founders. As systems grow, this constraint leads exactly where you would expect: to disagreement, divergence, and, finally, revolution.

In the world of blockchains, that's called a "fork": when sufficiently many members of the chain want to change the rules, they can go rogue, publicizing a new set of rules and attempting to lure others to divert their computer power to solving proof-of-work problems for their new republic. Forks have happened repeatedly in both BitCoin and Etherium, usually over technical questions,

although Etherium has also forked over the question of how to respond to looting.

This process is familiar to us from political history. Tribes don't have constitutions, and neither did the monarchies of Europe. Change could be confusing, abrupt, and often violent.

It's easy to become enchanted with the dizzying profits being made with BitCoin, and with the elegance of the mathematics beneath it. But it's dangerous to forget that the point of these systems is to bring the political power of common knowledge into the Internet age, together with all of its potential for disruption and conflict. China's response to the blockchain exemplifies the uncertain landscape. On the one hand, they banned residents from trading on cryptocurrency exchanges—but, on the other, they invest large amounts of money into developing high-speed hardware custom-built to solve proof-of-work puzzles.

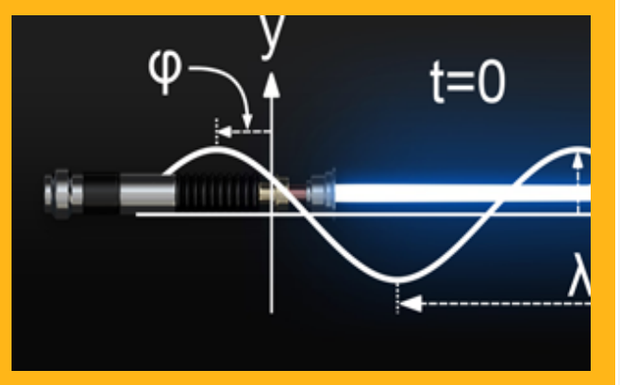
The blockchain is no less a social creation than the Kiva. We haven't outrun politics yet, and it doesn't look like we will.

Simon DeDeo is an assistant professor at Carnegie Mellon University, where he runs the Laboratory for Social Minds, and external faculty at the Santa Fe Institute.

Lead Image Collage Credits: Nastasic / Getty Images; Pixabay

JOIN THE DISCUSSION

NEXT ARTICLE:



MATTER

The Science of Star Wars Weaponry

By Patrick Johnson

RELATED ARTICLES:

CULTURE

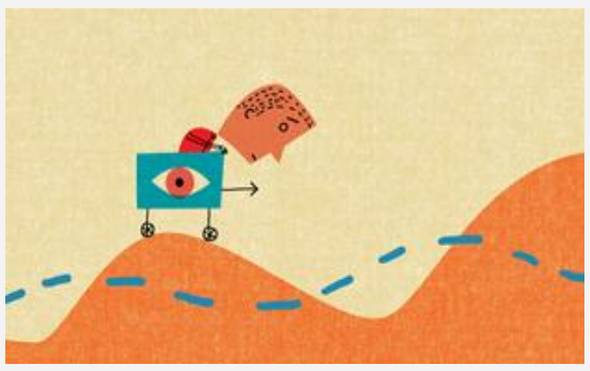
To Rescue Democracy, Go Outside

By Alex Pentland

CULTURE

Is Tribalism a Natural Malfunction?

By Simon DeDeo



NUMBERS

Don't Tell Your Friends They're Lucky

By Bob Henderson

NAUTILUS: SCIENCE CONNECTED

Nautilus is a different kind of science magazine. We deliver big-picture science by reporting on a single monthly topic from multiple perspectives. Read a new chapter in the story every Thursday.

 Matter, Biology, Numbers, Ideas, Culture, *Connected*