FEDERAL RESERVE BANK *of* ST. LOUIS
CENTRAL TO AMERICA'S ECONOMY ®

How a Blockchain Can Keep People Honest (and Log Uncooperative Behavior)

Andrew Spewak

By Andrew Spewak, Senior Research Associate

Helping others is hard work. In an episode of NBC's *The Good Place*, Eleanor Shellstrop promises to take care of her friend's dog for a couple days, then unexpectedly scores tickets to see Rihanna in Vegas.

She decides to blow off her dog-sitting duties in favor of a road trip to Sin City, highlighting a key societal problem: Our self-interest often conflicts with the interests of those around us.

Blockchain technology can alleviate the issue. At its core, blockchain is a recordkeeping system in which each member of a community keeps tabs on one another. It can align one's self-interest with the interests of one's community, leading to group cooperation.

Allow me to illustrate how it works.

The Primitive Blockchain: A Network of People and Their Memories

Cryptocurrencies like bitcoin utilize blockchain, but the concept actually predates modern civilization. Thousands of years ago, a primitive form of blockchain ensured that members of hunter-gatherer societies would put the needs of the group ahead of their own wants.

Since these early humans didn't have Netflix, they gossiped to pass the time. *Who had a crush on whom? Who swiped seconds at dinner last night?* Most importantly, *Who went to work in the morning?* It all became public record.

That's bad news for the slackers. If the village fisherperson hit snooze on the alarm rock, everyone heard about the slugabed's indolence by lunchtime. And with survival hanging in the balance every day, they wouldn't forget a transgression so quickly.

We can think of one of these communities as a network of people (see figure). Every action—positive or negative—is saved as a block of information in each person's memory. On everyone's brain, there is thus a chain of blocks detailing the history of actions in this community. In other words, a blockchain.

What a Primitive Blockchain Looks Like

Blockchain is a record-keeping system that enables members of a community to "keep tabs" on one another, leading to group cooperation. People in small groups have been tracking each other like this mentally for millennia, but it takes technology to scale globally.

FEDERAL RESERVE BANK *of* ST. LOUIS
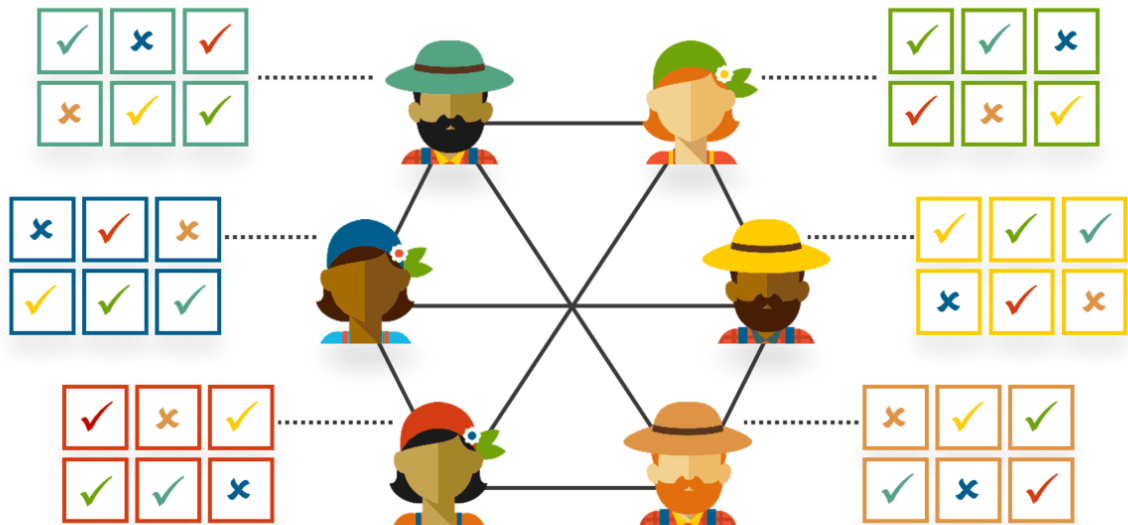
Icons: Thinkstock / Bluebearry

Tap figure to enlarge

They Knew You Were Trouble When You Walked In

If somebody were to repeatedly free ride off the community without doing any hard work, the blockchain would reflect that. Every member of the community would be able to recall several instances in which this person shirked on their responsibilities. The loafer would earn a bad reputation.

Reputation is not only Taylor Swift's latest studio album, it also can serve as social currency:

- Hunter-gatherers who built a good standing through their efforts "cashed in" their reputation, enjoying the benefits of belonging to the group.
- The free riders, who had little social credit, were outcast.

Since no sane person would want to live in the wild where a Balverine might eat them, even the laziest of the bunch would do their jobs. Thanks to the blockchain, it was in everyone's self-interest to cooperate by contributing to the group's survival.

The Old-School Blockchain Is Still at Work Today

This form of blockchain didn't go extinct with the woolly mammoth. In each of the examples in the table below, members of a small community collectively monitor one another and punish uncooperative behavior, leading to cooperation. That's the blockchain at work. (Keep in mind, however, that blockchain is morally neutral; the objective "cooperation" it encourages isn't necessarily subjectively "good.")

Community	Uncooperative Behavior	Communal Punishment	Resulting Cooperation
Friends	Someone always claims to be "sick" when asked for a ride to the airport.	Conveniently "sick" friend is no longer welcome at happy hour.	Everyone provides favors for each other.
Neighborhood	A couple gives out healthy snacks on Halloween.	Trick-or-treaters egg their house.	Every house gives out sugar-filled candy.
Co-workers	A colleague takes credit for others' work.	Peers prank the credit-taker with a fake memo.	Everyone takes responsibility for their work only.

But that Kind of Blockchain Doesn't Scale

That type of blockchain only works for small communities. In large societies, we don't have the brainpower to remember everyone's actions. Hence, we have money. Unlike the primitive blockchain, money doesn't require us to keep track of what everyone else is doing. Nevertheless, it leads to the same result: It is in one's self-interest to serve society's common goals.

For instance, if Squidward didn't show up for his shift at the Krusty Krab, few people in town would notice. But he wouldn't get paid. And without money, he couldn't afford a big-screen TV. So he contributes to society by showing up to work every day.

Enter a Digital Blockchain Based on Data

All record-keeping systems, including payments systems, must deal with issues of trust and how to organize historical information. Traditional payments systems don't use blockchain. Instead, they rely on a central institution such as a bank to keep track of everyone's money.

Unlike traditional money, cryptocurrencies—digital currencies that operate independently of a central bank— harness the power of blockchain. The overall concept is analogous to the primitive blockchain. However, instead of a network of *people* saving information as *memory*, a network of *computers* saves information as *data*.

Whenever a cryptocurrency transaction takes place, a block of information with details on the transfer is saved on the network.

These blocks together form a chain that contains the entire history of transactions.

Because computers have more processing power than the human brain, this version of blockchain does scale to large communities, such as the millions of people using bitcoin.

This setup is essential because digital money can be easy to counterfeit—after all, it's just computer files. When a trusted authority like a bank presides over our accounts, we don't need to worry about this. The blockchain makes it so that, even without a central record-keeper, one has no incentive to counterfeit cryptocurrency.

An Example: Will I Get My Coffee?

Let's say I try to buy a cup of coffee with bitcoin. My purchase triggers a process in which all the computers on the network communicate with each other to determine if I forged my bitcoin or not. Basically, digital gossip.

Eventually, the computers reach a consensus:

- If they can trace my bitcoin through its transaction history all the way back to its origination, they verify the transaction. I enjoy my latte.
- If at some point this bitcoin appears in the chain with no data about its previous transaction—indicating that it's fake—the computers deny the sale. If I try to cheat the coffee shop, I don't receive my latte, so it's in my self-interest to play by the rules.

SCENARIO 1:
Bitcoin history traced to origination. Transaction verified.
Andrew enjoys his latte.
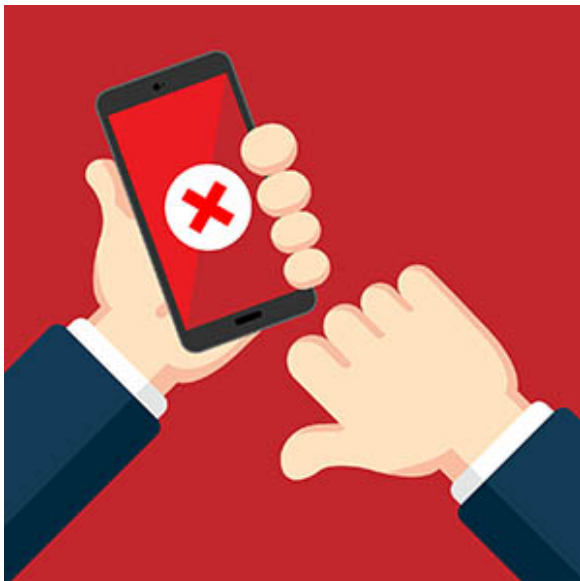
SCENARIO 2:
No data about Andrew's bitcoin, indicating it is fake. No coffee for this cheater.

Conclusion

In the literal sense of the word, cryptocurrencies like bitcoin are a revolution. The same technology that propelled the survival of primitive humans now allows us to buy coffee with the touch of a button. We have come full circle. With more technological innovations surely to come, who knows what blockchain will look like in the future? But we do know that, no matter its form, blockchain has the capability to induce self-interested people to partake in actions that serve a common goal.

Additional Resources

While this post illustrated the basic concept of a blockchain, the St. Louis Fed offers a collection of in-depth economic research on cryptocurrencies and fintech.

Also see:

- Dialogue with the Fed: Blockchain, Cryptocurrencies and Central Banks
- Podcast: Bitcoin: Beyond the Basics
- *Open Vault:* Three Ways Bitcoin Is Like Regular Currency