Bitcoin-Based Blockchain Breaks Out

Virtual currencies such as bitcoin rely on this digital public ledger system to guard against fraud, an approach that could likewise secure the coming Internet of things.

April 1, 2015 | By Larry Greenemeier

The Bitcoin Network’s so-called “blockchain” digital public ledger system records all transactions once they have been deciphered and validated. Adapted for other uses, such a system could serve as a gatekeeper and auditor to defend against, say, a cyber prankster looking to turn off your freezer via the Internet. Moreover, it could enable two autonomous automobiles to exchange data, ensuring that one stops at a traffic light while the other crosses the intersection.

These are just a few opportunities that big tech companies and start-ups alike envision when they consider applying the blockchain approach outside the realm of virtual currency. Blockchains are appealing from a security and privacy standpoint because they rely on information stored across a decentralized network of computers, so there is no central repository to serve as a juicy target for cyber attackers.

The Bitcoin Network serves as the best example to date of blockchain technology in action, although some other digital currencies—including litecoin and dogecoin—also use blockchains. Bitcoin operates on a peer-to-peer network that consists of computers—run by “miners” set up specifically to verify the validity of a transaction and record it in the blockchain. The first computer to solve a cryptographic puzzle accompanying each transaction is awarded bitcoins. Other computers in the network check the solution, creating a redundancy designed to guard against transaction fraud.
Once a transaction is entered into the blockchain ledger, it cannot be deleted or changed. “To change history, an attacker needs more computation power than all honest parties combined,” says Ittay Eyal, a distributed systems researcher in Cornell University’s Department of Computer Science.

This system is well-suited to operate as an online payment network because it does not require a central bank or transaction clearinghouse that would take a healthy cut of each transaction, as is the case with debit and credit card transactions, says Campbell Harvey, a Duke University professor of finance. The computer that successfully validates a bitcoin purchase or transfer does receive a small piece of the currency changing hands, but this is generally a fraction of a percentage. Stripe, a payment processing service that enables businesses to accept different methods of online payment, announced in February that it will charge customers 0.5 percent per successful bitcoin transaction. The service charges more than 2.9 percent per credit card transaction.

IBM has thrown its considerable weight behind blockchain technology as part of its strategy to help its customers establish networks of interconnected devices—aka the Internet of things. In January the company unveiled a proof of concept for ADEPT, its “autonomous decentralized peer-to-peer telemetry” system developed with Samsung.

In a report IBM released earlier this year the company described ADEPT as being able to use blockchains to provide a ledger of transactions among billions of devices that would autonomously exchange commands and other messages.

As with bitcoin transactions—although no money would be exchanged—encrypted commands exchanged between devices would be validated and recorded as a measure of protection against hackers inserting malicious software that might damage an Internet-connected washing machine or use it to gain access to a home computer network and steal personal information. In IBM’s vision smart appliances could even be programmed to autonomously execute digital contracts with other devices on their network to access software updates, pay utility bills or share resources—such as processor cycles, network bandwidth or power.

Blockchain technology could also revamp automotive security systems. In a blockchain network, when a car’s owner approaches his or her vehicle the car’s onboard computer would exchange data with the owner’s key fob or smartphone app to verify and authorize entry and operation, Harvey says. A blockchain would have information about the car’s ownership provided by, for example, the dealer who sold the car or the state that registered it. A blockchain ledger could likewise be used to create digital contracts with embedded intelligence that perform transactions based on how they are programmed.

Start-ups are looking to apply this distributed ledger setup to cloud storage services (so that all of a user’s data is not housed in the same vendor’s data center) as well as electronic voting systems. A political party in Denmark last year claimed to have used blockchain technology to create a digital ballot for internal use at the party’s annual meeting. Smart contracts are another example. “The simplest example perhaps is requiring two out of three cryptographic signatures to transfer money out of a wallet—this can be done without trusting any single entity to enforce the contract,” Eyal says. Another example is Ethereum, a virtual currency that plans to allow arbitrary computation on top of a blockchain structure, facilitating more complex contracts, he adds.
One criticism of virtual currency is that, despite claims of superior security, it has been vulnerable to cyber attacks. Last year's collapse of Bitcoin's largest exchange, Mt. Gox, typically serves as the poster child for Bitcoin's growing pains. Hackers infiltrated the network and made off with more than 744,000 bitcoins, a haul of about $386 million. Harvey points out that an exchange does not control transactions on the Bitcoin Network, however. Rather it communicates with the network to send and receive data. Although the details of Mt. Gox's undoing are still hazy, the problem was in their software communicating with the Bitcoin Network as opposed to flaws in the network itself, he adds.

Mt. Gox's fate indicates that even blockchain-based systems are not infallible, as does research Eyal has done with Cornell associate professor Emin Gün Sirer. Still, if high levels of cryptography are used to send and store transactions throughout the network, blockchain can be a successful model for the secure exchange of online payment and other information.

**Recommended For You**

1. **10 Original Gifts for Science (and SciArt) Geeks** 3 months ago
   blogs.scientificamerican.com ScientificAmerican.com chalkboard

2. **Intelligent Robots Must Uphold Human Rights** 2 days ago scientificamerican.com ScientificAmerican.com Society & Policy

3. **Beauty in Math and Art Activate Same Brain Area** 6 months ago scientificamerican.com ScientificAmerican.com Mind & Brain

**Comments**

NPalmquist
April 1, 2015, 10:15 AM

Every day is April Fool's Day for people who buy Bitcoins!

Report as Abuse | Link to This

coinsketch
April 1, 2015, 12:05 PM

"Mt. Gox's fate indicates that even blockchain-based systems are not infallible" In the name of science who wrote this?

(Hi Neal!)

Report as Abuse | Link to This
Many companies such as Dell Computers, Microsoft, Tiger Direct, Dish Network, Overstock.com now accept Bitcoin for online payments as cutting out the middle man (paypal, banks, credit cards) allows them to reduce their transaction fees and even offer discounts back to the customer.

Just like how email revolutionized communications, think of Bitcoin as cash for the internet whereby value can sent anywhere in the world instantly for negligible fees. It is secured by cryptography, each bitcoin is divisible by 100 million units, and there will only ever be 21 million bitcoin created.

I strongly suggest reading up more on Bitcoin and Blockchain technologies such as Ethereum that have the potential to be a game changer allowing individuals to transact one-to-one without requiring 3rd parties.

Mt. Gox was a 3rd party exchange that was holding onto people bitcoins. The great thing about Bitcoin is that you can be your own bank and don’t need to reply on third parties that might be susceptible to security breaches (like Mt. Gox).

In the history of Bitcoin, there has never been an attack on the block chain that resulted in stolen money. Neither has there ever been a reported theft resulting directly from a vulnerability in the original Bitcoin client, or a vulnerability in the protocol.

Bitcoin is secured by standard cryptographic functions. These functions have been peer reviewed by cryptography experts and are considered unlikely to be breakable in the foreseeable future.