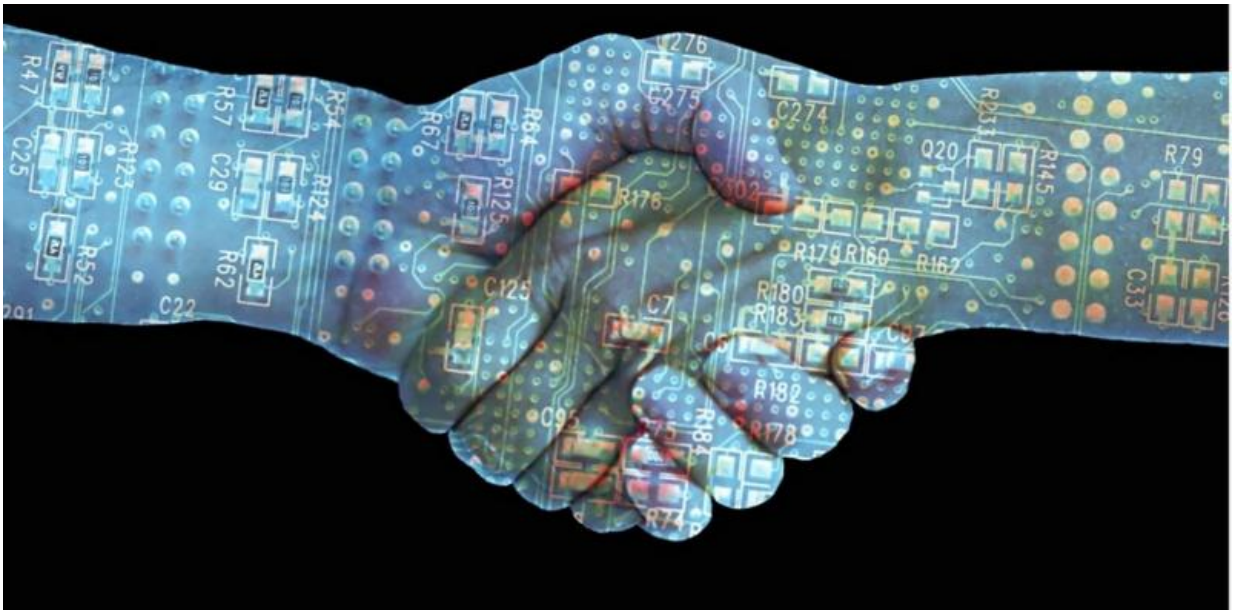
Blockchains—focusing on bitcoin misses the real revolution in digital trust

July 18 2016, by Ari Juels And Ittay Eyal



Ensuring trust in digital records and transactions is hard; the blockchain is an important solution. Credit: Robert Bagnall/YouTube, CC BY

In 2008, short of sending a suitcase full of cash, there was essentially just one way for an individual to send money between, say, the United States and Europe. You had to wire the money through a mainstream financial service, like Western Union or a bank. That meant paying high fees and waiting up to several days for the money to arrive.

A radically new option arose in 2009 with the introduction of bitcoin. Bitcoin makes it possible to transfer value between two individuals anywhere in the world quickly and at minimal cost. It is often called a "cryptocurrency," as it is purely digital and uses cryptography to protect against counterfeiting. The software that executes this cryptography runs simultaneously on computers around the world. Even if one or more of these computers is misused in an attempt to corrupt the bitcoin network (such as to steal money), the collective action of the others ensures the integrity of the system as a whole. Its distributed nature also enables bitcoin to process transactions without the fees, antiquated networks and (for better or worse) the rules governing intermediaries like banks and wire services.

Bitcoin's exciting history and social impact have fired imaginations. The aggregate market value of all issued bitcoins today is roughly US$10 billion. The computing devices that maintain its blockchain are geographically dispersed and owned by thousands of different individuals, so the bitcoin network has no single owner or point of control. Even its creator remains a mystery (despite many efforts to unmask her, him or them). Bitcoin's lack of government regulation made it attractive to black markets and malware writers. Although the core system is well-secured, people who own bitcoins have experienced a litany of heists and fraud.

Even more than the currency itself, though, what has drawn the world's attention are the unprecedented reliability and security of bitcoin's underlying transaction system, called a *blockchain*. Researchers, entrepreneurs, and developers believe that blockchains will solve a stunning array of problems, such as stabilization of financial systems, identification of stateless persons, establishing title to real estate and media, and efficiently managing supply chains.

Understanding the blockchain

Despite its richly varied applications, a blockchain such as bitcoin's aims to realize a simple goal. Abstractly, it can be viewed as creating a kind of public bulletin board, often called a "distributed ledger." This ledger is public. Anyone – plebeian or plutocrat, baker or banker – can read it. And anyone can write valid data to it. Specifically, in bitcoin, any owner of money can add a transaction to the ledger that transfers some of her money to someone else. The bitcoin network makes sure that the ledger includes only authorized transactions, meaning those digitally signed by the owners of the money being transferred.

The key feature of blockchains is that new data may be written at any time, but can *never be changed or erased*. At first glance, this etched-in-stone rule seems a needless design restriction. But it gives rise to a permanent, ever-growing transactional history that creates strong transparency and accountability. For example, the bitcoin blockchain contains a record of every transaction in the system since its birth. This feature makes it possible to prevent account holders from reneging on transactions, even if their identities remain anonymous. Once in the ledger, a transaction is undeniable. The indelible nature of the ledger is much more powerful and general, though, allowing blockchains to support applications well beyond bitcoin.

Consider, for example, the management of title to a piece of land or property. Property registries in many parts of the world today are fragmented, incomplete, poorly maintained, and difficult to access. The legal uncertainty surrounding ownership of property is a major impediment to growth in developing economies. Were property titles authoritatively and publicly recorded on a blockchain, anyone could learn instantly who has title to a piece of property. Even legitimate anonymous ownership – as through a private trust – could be recorded on a blockchain.

Such transparency would help resolve legal ambiguity and shed light on

malfeasance. Advocates envision similar benefits in blockchain recording of media rights – such as rights to use images or music – identity documents and shipping manifests. In addition, the decentralized nature of the database provides resilience not just to technical failures, but also to political ones – failed states, corruption and graft.

Smart contracts

Blockchains can be enhanced to support not just transactions, but also pieces of code known as *smart contracts*. A smart contract is a program that controls assets on the blockchain – anything from cryptocurrency to media rights – in ways that guarantee predictable behavior. A smart contract may be viewed as playing the role of a trusted third party: Whatever task it is programmed to do, it will carry out faithfully.

Suppose for example that a user wishes to auction off a piece of land for which her rights are represented on a blockchain. She could hire an auctioneer, or use an online auction site. But that would require her and her potential customers to trust, without proof, that the auctioneer conducts the auction honestly.

To achieve greater transparency, the user could instead create a smart contract that executes the auction automatically. She would program the smart contract with the ability to deliver the item to be sold and with rules about minimum bids and bidding deadlines. She would also specify what the smart contract is to do at the end of the auction: send the winning bid amount from the winner to the seller's account and transfer the land title to the winner.

Because the blockchain is publicly visible, anyone with suitable expertise could check that the code in the smart contract implements a fair and valid auction. Auction participants would only need to trust the correctness of the code. They wouldn't need to rely on an auctioneer to

run the auction honestly – and as an added benefit, they also wouldn't need to pay high auctioneer fees.

Handling confidentiality

Behind this compelling vision lurk many technical challenges. The transparency and accountability of a fully public ledger have many benefits, but are at odds with confidentiality. Suppose the seller mentioned above wanted to conduct a sealed-bid auction or conceal the winning bid amount? How could she do this on a blockchain that everyone can read? Achieving both transparency *and* confidentiality on blockchains is in fact possible, but requires new techniques under development by researchers.

Another challenge is ensuring that smart contracts correctly reflect user intent. A lawyer, arbiter or court can remedy defects or address unforeseen circumstances in written contracts. Smart contracts, though, are expressly designed as unalterable code. This inflexibility avoids ambiguity and cheating and ensures trustworthy execution, but it can also cause brittleness. An excellent example was the recent theft of around $55 million in cryptocurrency from a smart contract. The thief exploited a software bug, and the smart contract creators couldn't fix it once the contract was running.

Bitcoin is a proof of concept of the viability of blockchains. As researchers and developers overcome the technical challenges of smart contracts and other blockchain innovations, marveling at money flying across the Atlantic will someday seem quaint.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation