TechXplore

# Blockchain is useful for a lot more than just Bitcoin

May 10 2016, by Mark Staples

Blockchain technology is not just useful for creating digital currencies such as Bitcoin or developing new financial technologies.

Blockchains can be used for a wide variety of applications, such as tracking ownership or the provenance of documents, digital assets, physical assets or voting rights.

Blockchain technology was popularised by the Bitcoin digital currency system. But, essentially, a blockchain is just a special kind of database. The Bitcoin blockchain stores cryptographically signed records of financial transfers, but blockchain systems can store any kind of data. Blockchains can also store and run computer code called "smart contracts".

What makes a blockchain system special is that it doesn't run on just one computer like a regular database. Rather, many distributed processing nodes collaborate to run it. There can be a full copy of the database on every node, and the system encourages all those nodes to establish a consensus about its contents.

This boosts our confidence in the database and its contents. It's difficult, if not impossible, to meddle with the database without others finding out and correcting it. The global consensus among the nodes about the integrity and contents of the distributed database is why it's often called a "distributed ledger".

## Why all the hype?

In our society, we normally rely on trusted third parties, such as lawyers, courts, banks and governments to process and keep authoritative records about commercial transactions.

These transactions aren't just about financial transfers, but also include the creation or transfer of physical assets, shareholdings, certifications, digital rights, intellectual property or even votes.

These third parties are trusted because we rely on them. If they fail or lie, we suffer. We tend to trust the third parties for reasons that are external to the database; lawyers are accredited; votes are counted by independent monitors; and courts run to established laws for matters such as oversight and the possibility of appeal.

Blockchains are interesting because the integrity of the contents of the distributed ledger does not rely on any specific individual or organisation. So, rather than relying on trusted third-party organisations to facilitate these commercial transactions, we might instead rely on a trusted blockchain system.

This means blockchains give us new opportunities to rethink how parts of our society work. Innovation here might reduce friction in the economy, or create new kinds of services and ways of doing business with each other.

Whether or not blockchain systems are trustworthy is an interesting question. The reasons for believing that blockchain systems won't fail or lie would be based on our understanding of the underlying software technologies. It also depends on our understanding of market incentives that influence behaviour of the many distributed processing nodes that run blockchains.

However, blockchain technologies are still new in the scheme of things, and the community is still discovering their risks, limitations and potential economic and social impact.

## How will blockchains be used?

Because blockchain technology is so new, it's difficult to predict exactly how they will end up being used. This is why we at Data61 in CSIRO are exploring new ways blockchains can be used across industries.

To understand the economic and societal opportunities presented by blockchain technology, we also need to understand its technological risks and limitations. At Data61, we plan to identify, develop and evaluate some "proof of concept" systems using blockchains to investigate them.

A recent UK government report on blockchain technologies provides a good overview and examples of the use of blockchain.

One of these is Everledger, a company founded by Australian woman Leanne Kemp.

Everledger uses a blockchain to record information about the provenance and ownership of individual diamonds and other valuables. Here, rather than the blockchain recording transfers of digital currency, it records transfers of ownership of identified physical assets.

This globally accessible provenance trail could reduce fraud and theft, and enable new or improved kinds of insurance and finance services.

The same general idea could be used for any supply chain, such as in retail, agriculture or pharmaceuticals.

The drivers for improving assurance of supply chain quality vary in different industries. It could be brand reputation in retail, or safety in pharmaceuticals, or a combination in agriculture.

It is worth observing that blockchains don't totally do away with the need for trusted third parties. A blockchain is only a digital record, but we need others to determine if those records actually match the corresponding physical assets in the real world.

Everledger relies on major diamond certification companies to measure identifying information about individual diamonds. These measurements can be independently cross-checked. But in some sense, companies such as these become trusted third parties for this blockchain-based system. One can imagine the adoption of blockchain technologies creating opportunities for new kinds of trusted third-party organisations.

Underlying all of these applications is the need for data integrity, which is the key security property for commercial systems, and the primary property for blockchain technologies.

For financial transactions, data integrity means you can't spend money you don't have, and you can't spend money twice. For physical supply chains, this means you can't fraudulently acquire record of ownership for an asset.

However, other security properties, such as privacy and confidentiality, are also important in many application areas. To achieve confidentiality, other mechanisms such as cryptography must be used in conjunction with the blockchain.

Part of our software architecture research at Data61 is to seek to understand how design choices for software-based systems affect tradeoffs for qualities including security (integrity, confidentiality, privacy), performance (latency, throughput and scalability), and others.

Good design choices can control risks to achieving these qualities, and this is part of what is evaluated in our research using proof-of-concept systems.

## Smart contracts

Computer programs are a special kind of data and so can be stored in a database. That means we can store programs in the distributed ledger of a blockchain system, and execute those programs while later transactions are being processed.

In the Ethereum blockchain, these programs can be highly complex.

These programs are normally called "smart contracts".

Smart contracts can carry value, and can conditionally transfer that value according to complex business conditions based on the latest state of the distributed ledger.

This means blockchain systems can do more than store information about commercial transactions; they can also process commercial transactions too. This greatly expands the opportunities for using blockchain systems.

Although smart contracts are often thought of as standing for self-executing legal contracts, they are written in a general purpose programming language and can be used to implement a wide range of business logic.

Can smart contracts actually stand as legal contracts? This is an interesting question. For legal contracts to be enforceable, they need to be understandable by reasonable persons.

Can the bytecode of a program stored on a blockchain really be understood by any human? Perhaps only obsessive hobbyists might be able to develop that skill! Another thread of research in Data61 is investigating new ways of representing and analysing smart contracts, using recent results from legal informatics.

Blockchain technology is still in its infancy. There are a wide range of plausible future scenarios for their future impact, ranging from efficiency improvements for commercial transactions through to a complete reinvention of the economy.

As with any disruptive technology, understanding the plausible, possible and probable impacts – the opportunities and risks – will be vital for wise policy, strategy, and design choices by Australian governments and companies.

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

Source: The Conversation

Citation: Blockchain is useful for a lot more than just Bitcoin (2016, May 10) retrieved 26 April 2024 from https://techxplore.com/news/2016-05-blockchain-lot-bitcoin.html