Protecting the 'right to be forgotten' in the age of blockchain

31 October 2018, by Raja Jurdak, Ali Dorri And Salil S. Kanhere

A new framework gives you full administrative control of your blockchain-stored data. Credit: Shutterstock

There's been a lot of hype about blockchain over the past year. Although best known as the technology that underpins Bitcoin, blockchain is starting to disrupt other industries, from supply chains to energy trading.

One of the key selling points of blockchain is that once data is added to the chain, it can't be changed or removed. This makes blockchain trustworthy.

But this same immutability makes blockchain problematic in a world where privacy laws require companies to delete your data from databases once it has served its purpose. This is known in some jurisdictions as the "right to be forgotten".

We have designed a blockchain in which users can remove their data from the database without violating blockchain's consistency.

There is currently a growing market of Internet of Things devices, from smart homes and self-driving cars to voice assistants and smart energy meters. These devices continuously collect digital biographies of our lives. As this data is increasingly being stored on blockchains, the tension between blockchain and the right to be forgotten will only increase. Our tool could help.

How blockchain works

At its core, blockchain is a database that is jointly managed by a distributed set of participants. Whenever new data is added to the database, all the participants must agree to verify it. In this way, blockchain removes the need for a third-party, such as a bank, to verify transactions.

The blockchain ledger is organised into blocks, where each block is linked to the previous block through cryptographic hash functions. These functions create a short code based on the content of the previous block, and it is not possible to guess this code without trying all possible codes. Chaining the blocks in this manner ensures that the data stored in them cannot be altered, as any changes made would break the blockchain consistency.

This makes blockchains immutable. It also makes blockchain data easy to trace and audit, particularly for large networks like the Internet of Things. These features are highly attractive for organisations operating across organisational boundaries, and in environments where participants may not fully trust each other.

Regulatory challenges

The European Union's recent General Data Protection Regulation (GDPR) is a significant piece of legislation that is at odds with a digital economy underpinned by blockchain.

The GDPR requires companies that hold people's data to erase that data once the original purpose they needed it for is complete. That means that people must be able to remove their data from third party databases after a certain period of time.

Blockchain – being unchangeable – presents an obstacle to exercising that right.

Risks to privacy

Let's say you live in smart home that uses sensor data to monitor your home security. You have a home insurance policy and, in order to receive lower premiums, you allow your smoke alarm and security sensor data to be recorded on a blockchain.

The blockchain data can be accessed by the police, the fire department and the insurance company so they can audit any smoke alarm or security events. Once your insurance period has ended, you should be able to remove your security data from the blockchain to enhance your privacy.

If you left your data on the blockchain indefinitely, that would increase the risk of your data being identified as yours, and your activities being tracked by any entity with access to the blockchain.

A blockchain participant typically uses one or more public keys as its identities. The transactions in blockchain are stored anonymously, as there is no direct link between the public keys and the real participant identity. But a breach in identity in any of the transactions, for instance by linking the transaction content to other known data about the user, leads to all interactions of the users's devices, stored in blockchain, to be tracked by all blockchain participants.

Removing data without breaking the chain

So being able to the remove data from the blockchain without "breaking the chain" would be beneficial for user privacy. It would also be beneficial to save storage space on the servers that store blockchain ledgers.

But currently, removing data from a blockchain is not possible without breaking the blockchain's consistency.

We have come up with a solution that makes it possible to remove your detailed transaction data from a blockchain database, without removing the auditable trace that the transaction took place.

As described in our peer-reviewed publication this month, Memory Optimised Flexible Blockchain allows you to temporarily store, summarise, or completely remove your transactions from blockchain, while maintaining the blockchain's consistency.

The remaining trace of the data (its hash) on the blockchain can still be used in the future, in case disputes over what happened arise. For instance, if a home owner wanted to verify that a break-in took place at their house under a previous insurance policy, they could provide a private copy of the data with its associated hash. A legal authority could then compare the hash of the person's data with the hash that is still stored on the shared blockchain and thereby validate the authenticity of the person's claim.

This approach provides you with full administrative control of your blockchain-stored data. It makes it possible for you to remove or summarise this data, without sacrificing the ability to audit the data in the future.

Reclaiming privacy and control

It is important to note that our published approach can run atop any existing blockchain solution, and does not affect the blockchain consistency. The links among blocks through hash functions are preserved, even as specific blocks are removed or summarised from the chain. In other words, the link of any blockchain entry remains, but the bag containing some data can be cut loose.

In fact, as long as the removed content is stored privately outside of the blockchain, the data's authenticity can be independently verified at a later time by comparing it against the hash in the blockchain. In this way, you can reclaim control of any previously shared data and exercise your right to be forgotten in the age of blockchain.

Provided by The Conversation