

Privacy Tech

Exploring the technology of privacy

Unravelling the mystery of blockchain – Should privacy professionals be concerned?

Annelies Moens, CIPT
Privacy Tech | Jul 28, 2016



“I am in the process of booking an apartment in Stockholm and I have the option of paying through a company that purports to be able to send money with the real exchange rate (not marked up), which sounds great, until I start to read the privacy policy... which essentially says that all my information including account information could be shared with a wide ranging number of third parties.”

I thought this practical scenario was a good lead in to my participation at the European Identity and Cloud conference in Munich in May, which included a full day on blockchain and where I raised my Stockholm booking scenario. Blockchain is an electronic distributed ledger system designed to cut out costly middle agents to enable faster and cheaper processing, not dissimilar to the company I was going to use to transfer money to pay for the apartment in Stockholm.

This technology is being talked about everywhere, but how new is it and do we really understand it?

The original intent of blockchain was to conduct trusted transactions between parties over untrusted networks. Blockchains involve a large number of parties that see the data within blocks and use consensus algorithms to reach agreement on the integrity of the distributed blockchain. The revolutionary factor in blockchain is that it locks down an event in real-time.

Blockchain is not a new concept and is derived from a 1979 patent on merkle trees. Each block in a blockchain contains a summary of all the transactions in the block, using *merkle trees*, which are binary hash trees used for efficient verification of data integrity.

Blockchain's strength lies in determining the provenance and trackability of transactions. As such, it works well where there are:

- Brokers and intermediaries involved which can be eliminated;
- Highly regulated businesses with strong audit and governance requirements;
- Lengthy processes and settlement of deeds;
- Shared businesses with multiple parties involved.

Blockchain can be used in many situations including, identity and authentication, finance, internet of things, cryptocurrency, smart contracts, government, and legal record keeping. There are many businesses starting to use blockchain technologies. A few examples include:

- International payments – **Ripple** – the first global decentralised transaction settlement network designed to reduce clearance and settlement time
- Cryptocurrency – **BitStamp** – first EU bitcoin exchange platform with a banking licence in Luxembourg
- Real estate financing – **Ubitquity** – securely, recording, tracking and transferring of title
- Digital content – **Ascribe** – sharing and tracing digital work
- Smart contracts (or not so smart contracts) – **Ethereum** – platform which runs contracts

So what, from a privacy view, do we need to think about as the blockchain technology rolls out in various different applications and sectors? Keep in mind that this is a new field of technical activity with a lack of standardization (though National Standards Bodies, including Standards Australia are keen to address this through international standards setting).

Responsibility and governance

Who would be regulated and responsible if there was a data breach?

Earlier, I mentioned that blockchains use consensus algorithms to reach agreement on the integrity of the distributed blockchain. In a decentralised model there is a shared responsibility, so changes can only occur with “consensus,” which generally means that more than 50% of participants in the network need to agree. Consequently, when there is a data breach, it is not necessarily clear how responsibility is going to be allocated.

For example, in mid June, Ethereum - a platform which runs smart contracts - was subjected to a multi-million dollar hack which exploited a loophole in its code. The code was being rigidly followed but produced unforeseen and undesirable outcomes. “Unlike normal contracts which can be interpreted by smart people,” Motherboard reported, “smart contracts are interpreted by computers. Computers are dumb. They can only do what they are told.”

It remains to be seen how the Ethereum hack will play out and be resolved. Broadly speaking, the governance of blockchain still needs to mature.

Trust

Can we trust blockchains?

Trust is an integral component to effective privacy and takes significant effort to establish and takes seconds to undo. The original permission-less, public model of blockchain was intended to overcome the problem of not trusting third parties. However, it is impossible to eliminate trust, as it is:

- An unavoidable element of human life;
- We don't know the future but plan for it;
- We don't know to what extent our perceptions are true; and
- We don't know to what extent our memories are real or not.

Permissioned, private blockchains have been set up to limit users and ironically attempt to assure trust at the expense of resilience and robustness which a permission-less model provides.

Again, it remains to be seen how trustworthy blockchains will be and, in my view, their level of trustworthiness is, in part, dependent on the quality of their governance framework.

Right to be forgotten

Can we delete information?

Internationally, relatively new privacy concepts, such as the right to be forgotten are being introduced. That will sit rather uncomfortably with blockchain technology which is designed to keep transactional information in perpetuity. The extent to which this encompasses personal information remains to be seen. However, the global trend towards information being more easily attributed to individuals suggests to me that this will eventually become a thorny issue.

Transparency

Can we keep our privacy?

Transactions in blockchain are recorded in a decentralised model in such a way that there is complete transparency as to all the transactions that have taken place from first to most recent – hence why its strength lies in determining provenance and trackability of transactions. This means that information, including potentially personal information, will be widely accessible and is why I didn't go ahead with my Stockholm booking as outlined at the beginning.

So, let me leave you with another quote, this time from a discussion about the Bitcoin blockchain from a UK government report.


 “Unlike traditional online payments, which are only visible to transacting parties and financial institutions, Bitcoin payments — including the wallets involved, the approximate time of the transaction, and the transaction values — are recorded in a publicly visible block chain. Anyone can process the block chain and draw inferences about, for example, the turnover of an on-line merchant, the buying profile of a particular user, or even the many transfers between private individuals — a capability that was restricted in the past to financial institutions and law enforcement.”

photo credit: Bitcoin Chain IMG_9197 via photopin (license)

Comments

Logged-in as: John Wunderlich

Share your thoughts

