Permissionless innovation with blockchain technology: computer says yes

April 2016

James Allen

Underneath Bitcoin is a distributed, persistent and encrypted public database called ‘blockchain’, which forms the ledger of Bitcoin transactions. It is in effect the guarantee that a given Bitcoin cannot be copied and spent twice by the current owner. The ‘miners’ who maintain this distributed database are paid for their efforts (in Bitcoin); the encryption protects both identities and the transactions that have been accepted.

A new era of permissionless innovation

There is currently an explosion of start-ups seeking to leverage blockchain technology. This is similar to the rush to find (and patent) new applications in all possible fields for the Internet in the late 1990s. It is true that blockchain shares some characteristics with late-1990s-era Internet Protocol (IP): it is publicly available, the relevant standards and payment mechanisms exist, it already has critical mass for the platform as a whole, and there is a developing ecosystem of support businesses building on it and offering related services. Just like IP was then, blockchain is now a technology allowing ‘permissionless innovation’ and, just like IP, it has attracted a mix of technologists, bankers, economists, venture capitalists, philosophers and artists.

Blockchain offers a flexible public co-operation mechanism

Blockchain offers an opportunity for groups to co-operate in database systems offering a ‘single truth’ without the complexity of all parties having to agree to trust a single master entity, which also represents a single point of failure. This property obviously has many potential use cases, which is part of the reason for the vast array of start-ups. Given that the Bitcoin blockchain is publicly accessible, matters of public record, such as public registers of copyright or land ownership,[1] are an obvious choice. The financial technology sector is currently in the vanguard in seeking applications. For example, settlement of stock market trades currently takes 3 days, when it could take much less time, offering the potential for substantial cost savings in IT and in capital held against counterparty risks. Considering the telecoms industry, number portability databases also offer an immediate potential application (these systems currently use a database held by a trusted party). Blockchain can also be applied to IoT – for example to register devices, authenticate users and support access and payment for data.

Blockchain is extensible

Not all blockchains have to be public: private blockchains also offer opportunities. Here, the participants can be controlled and it is easier to build something that exactly meets the needs of a particular situation. However, moving away from the existing platform, with its established critical mass, standards and payment mechanisms, has its own risks – in the end, a private blockchain is just a multi-user database (even if it uses a new and trendy

[1] The participants still have privacy, as they are identified by public keys.

technology). Of course, there is no need to reinvent everything: for example, blockchains can be linked together such that their payment mechanisms are convertible.

Beyond the ‘ledger’ or database function, there are already multiple attempts to increase the capabilities of the Bitcoin blockchain. For example, Ethereum (a more capable blockchain) builds in ‘contracts’, written in a programming language, that allow events (such as payments) to be triggered when other specified events occur. This addition makes the blockchain into an application and widens the scope to encompass everything software (or contracts) can achieve: from wills, through cooperative communities and electronic voting, to virtual nation states. While a future author will no doubt make great use of a blockchain-implemented will as a plot device, Neal Stephenson has already written a novel including virtual nation states (*The Diamond Age*).

Such an extension also enables practical solutions to some real problems. To give an everyday example, it would allow electronic equivalents of bank accounts where any two from six people have to approve a transfer or withdrawal, which in the current bank settlement world is achieved by two physical signatures on a cheque. It has already been used to demonstrate both a music market with no intermediaries between creators and consumers and the ability to trade electricity between producers and consumers. However, it also raises the possibility of distributed systems against which traditional enforcement mechanisms may struggle to gain purchase. For example, investigations of financial transactions will only find a public key, rather than a named individual.

These are exciting times. Some of these companies and technologies will be successful in niches, while some will become utilities and will form the basis of new and even more fruitful businesses. Regulators and governments will have to adapt and, in this case, as discussed above, they may also wish to adopt.

Analysys Mason has been observing connected ICT and advising operators, enterprises, government and regulators since 1985. For further insight into the implications of blockchain technology in terms of services, business models, regulation and policy, please contact James Allen at james.allen@analysysmason.com or David Abecassis at david.abecassis@analysysmason.com. For queries related to IoT, please contact Tom Rebbeck at tom.rebbeck@analysysmason.com.