THE CYBER-SECURITY SOURCE

by Adam Palmer and Michael Palage
June 26, 2017

Blockchain: A multi-functional 'Swiss Army knife' for cyber-security

> Blockchain is known for powering cryptocurrencies, but developers are finding many other innovative uses for crypto-secure transactions, write Adam Palmer and Michael Palage.

Over the past several years, more than a billion dollars have been invested in blockchain startups by investors seeking to capitalise on what is estimated to be an $US 8 billion market by 2024.

This private sector investment has also been coupled with several public sector initiatives from various governments. This article examines the aspects of blockchain technology that make it uniquely situated to support cyber-security capacity building.

It is important to note that blockchain is not a ‘silver bullet' solution. However, it will be a critical tool for improving cyber-security.

Blockchain 101

Blockchain is a peer-to-peer distributed ledger technology that provides for the secure archival of information (transactions) in a dynamic repository comprised of a never-ending series of sequential data blocks chained together using public/private key cryptography. Through the use of cryptography and consensus protocols associated with the writing of data blocks to the chain, the information stored in the repository is tamper resistant and immutable. It is this combination of features which provides the level of transparency, trust and accountability among users of that blockchain.

There are two general classifications of blockchain technology: permissioned and permissionless. The original Bitcoin blockchain was built to create a ‘permissionless' peer-to-peer network for transferring a virtual currency from any one party on the network to any other party on the network. It is permissionless because there is no trusted authority (such as a bank or clearing house) verifying that the transactions are legitimate and that the record for the transactions is, and

remains, correct. Instead, transactions are verified by a consensus protocol among the miners. Trust is linked to the degree of difficulty set for the miners, and each change is recorded on the blockchain transaction record.

Unfortunately, the computational demands of a permissionless system, like Bitcoin, make it very inefficient. As a result, many blockchain applications being investigated in the financial and digital identity sectors are ‘permissioned' networks. A trusted authority manages access to the networks by users, and is authorised to perform verification of the transactions.

Permissioned blockchains can establish a consensus protocol that is not as computationally demanding, but is still secure through the management of the parties on the network. Permissioned blockchains then have greater potential to be utilised to support other functional applications of blockchain (eg, decentralised, secure cryptography) and the application to digital identity where the economic incentive model of cryptocurrency is not needed.

Permissioned blockchains also permit a more formal governance structure to provide a framework for resolving disputes between users – this is more challenging on permissionless blockchains, which are autonomous by nature.

Cryptocurrency Going Mainstream

Blockchain is the underlying technology enabling Bitcoin, the world's most popular ‘cryptocurrency'. Blockchain's early association with Bitcoin and the dark web created an initial stigma for the technology in some sectors. However, Bitcoin has recently gone mainstream, with a growing number of established companies accepting Bitcoin as legal tender. This list includes not only technology-centric companies such as Microsoft and Dell, but also traditional companies such as SBB, the Swiss rail operator.

Several recent developments show the potential for a much wider adoption of blockchain cryptocurrencies. Alipay is currently the most popular mobile payment application in the world, with over 450 million users just in China.

Eric Jing, the CEO of Ant Financial, was recently quoted as saying he ‘definitely' sees blockchain being a foundation to its popular mobile application. With Ant Financial's pending acquisition of MoneyGram, Alipay may soon be able to leverage MoneyGram's existing network of 350,000 outlets in nearly 200 countries and territories. These developments are in addition to the People's Bank of China (PBOC) that has recently completed a proof-of-concept testbed and appears to be one of the first major central banks positioned to begin a wide-scale use of cryptocurrencies.

FinTech Embrace of Blockchain

A broader use of blockchain technology is likely to occur in the financial technology (FinTech) sector, providing the ability to speed transactions and remove intermediaries as well as to potentially provide billions of dollars in cost saving and efficiencies for the financial services industry.

The Depository Trust & Clearing Corporation (DTCC), which is one of the world's largest financial service companies for clearing and settlement services, has recently announced that it selected

IBM, in partnership with Axoni and R3, to re-platform DTCC's Trade Information Warehouse (TIW) with distributed ledger technology (DLT). Interestingly, DTCC in their press release made no specific reference to blockchain and instead only mentioned DLT. This appears to be a growing trend in the FinTech sector to avoid using the moniker blockchain and instead use DLT. R3, a leading consortium of 70 global financial companies, in a blog post has recently stated that its Corda product is a distributed ledger and not a blockchain.

For the purposes of this article, blockchain and DLT are intended to be used interchangeably, but it is important to understand that there are those that view them as distinct terms. While DTCC avoided using the term blockchain in its press release, it did state that its distributed ledger protocol "will be submitted to Hyperledger when the solution goes live". Hyperledger is an open source collaboration initiative hosted by the Linux Foundation whose objective, according to its website, is "to advance cross-industry blockchain technologies" in the finance, banking, Internet of Things, supply chains, manufacturing and technology sectors.

Healthcare

My Health – My Data (MH-MD) is an initiative launched in November 2016 with funding from the European Commission and designed to enhance the privacy of individual healthcare records. In January of this year, the US Food and Drug Administration announced an initiative with IBM to use blockchain technology to facilitate the secure and scalable distribution of health records.

Currently, these records are often stored centrally across numerous data repositories with varied levels of security. Because of the highly sensitive nature of this data, these repositories are a frequent target of massive data breaches.

Blockchain technology provides a framework in which this data can be securely stored in a decentralised manner, while enabling access to the data when authorised.

Digital Identities

Digital identities are broadly defined as any set of information used by computer systems to represent some entity (a person, organisation, application or device). Common forms of digital identity are password-based access credentials and user profiles, which can include various identity credentials used to verify that the entity is authorised to engage in a transaction.

There are three fundamental aspects of digital identity: identity creation (creation of valid identity credentials), authentication (verification of those credentials) and authorisation (verification of rights provided by those credentials).

The current model for digital identities typically involves users having separate identity credentials stored across different providers. However, the distributed nature of blockchain technology provides for a fundamental paradigm shift regarding digital identities, in which identity credentials are controlled by the individual user instead of the provider.

The Sovrin Foundation, a US not-for-profit organisation, has recently proposed a model for 'self-sovereign' identity, in which users manage and control their own identity credentials. Individuals create a digital identity with various identity credentials on a public-permissioned blockchain

managed by Sovrin. These credentials are then accessed and verified by service providers globally as needed, but the individual's personal information remains in the blockchain under the control of the individual.

Participants can use their digital identity across multiple service providers, but their identity is not tied to any service provider – it is completely portable and remains under the participant's control. The Sovrin Foundation recently contributed it code base to Hyperledger which now operating this under the project name Indy.

Blockchain IoT

While the use of blockchain in promoting individual digital identity is exciting, its potential use in the continued evolution of the Internet of Things (IoT) could truly be transformative.

The amount and type of data that IoT-connected devices are exchanging has the potential to both enhance and frustrate users. As the number of connected devices continues to grow exponentially, it is critical that there be a fundamental re-evaluation of the underlying security of these devices and the threat that they pose to the Internet's greater security and stability.

A group of Chinese companies including China Unicom, ZTE and Alibaba Group have recently joined with the Egyptian National Telecom Regulatory Authority in submitting a paper to the ITU's Internet of Things (IoT) Study Group. This paper, entitled ‘Framework of blockchain of things as decentralized service platform', recognises how blockchain can provide a unique framework for the future growth and evolution of the IoT.

Governmental oversight

The excitement surrounding the potential of blockchain and DLT has not only caught the eye of the private sector, but also the public sector.

Poland's Ministry of Digital Affairs has been active in promoting blockchain adoption. In 2016, the Ministry announced ‘From paper to digital Poland', an effort to promote digital public services, the development of cashless solutions and the implementation policies to promote blockchain-based security systems.

This acceptance of blockchain appears to represent a shift in attitude of Polish regulators from earlier silence on cryptography-based systems such as Bitcoin and blockchain. Poland's Ministry of Digital Affairs, however, has now identified blockchain as a technology that can accelerate national growth.

Poland's moves have been echoed in Ukraine where blockchain conferences, such as the ‘Blockchain Incredible Party' (BIP) events held in Odessa and Lviv, have highlighted distributed crypto-security programmes system focus in Eastern Europe.

Applications of blockchain have also quickly spread beyond the financial sector. A blockchain-based voting system project has been launched near Kiev to address concerns about voting fraud. Additionally, an Odessa-based group is developing a system for state auctions, seeking to make privatisation more transparent and less corruption-prone with the use of a distributed ledger.

With the recent passage of the new European National Information Security Directive (NIS), EU regulators and national governments are likely to begin focusing on blockchain regulation.

Blockchain, and cryptocurrency such as Bitcoin, are largely unregulated across Europe. They are not generally accepted as legal tender by governments. In 2015, the Polish Ministry of Finance explicitly stated that virtual cryptocurrencies do not fall within the scope of the Polish Payment Services Act, nor can they be considered financial instruments. These limitations, however, have not generally affected their trade in Internet forums and exchange as an accepted online currency.

Forward thinking

It is important to remember that blockchain is still an emerging and developing technology. However, when considering some of the proof-of-concept pilots currently underway and other mainstream applications coming to the market, the future appears bright for this technology.

Open source initiatives such as Hyperledger have the potential to make blockchain a truly transformative technology, much like Linux transformed the growth of the web. Efforts underway to develop standards for this distributed ledger technology will enable businesses of any size and across many industries looking to integrate this technology.

It is important for the IT professional community to determine how to best leverage this technology to increase the security, stability and resiliency of the broader Internet and enhance users' online experience.

Authors:

Adam Palmer

Adam Palmer is a former US Navy Officer, Prosecutor and Manager of the UN Global Programme Against Cybercrime. He is a Senior Research Fellow of the Kosciuszko Institute and a global consultant for CyCap, an EU and Singapore-based cyber-security consulting firm.

adamppalmer@gmail.com.

Michael Palage

Michael Palage holds a BSc in Electrical Engineering and JD in Law and is a founder of InfoNetworks. He has provided consulting services to both the public and private sector in connection with a broad range of governance issues involving the Internet's unique identifiers. mpalage@infonetworks.global.

InfoNetworks is a recently created company that I co-founded to focus on Blockchain related matters while Pharos Global will remain focused mainly on the domain name industry.

About the Kosciuszko Institute:

The Kosciuszko Institute is an independent, non-governmental research institute that was founded in 2000 as a non-profit organisation. The institute drafts expert reports and policy recommendations for European and Polish decision-makers. The Kosciuszko Institute is the organiser of the European Cybersecurity Forum – CYBERSEC, an annual public policy conference dedicated to the strategic aspects of cyber-security. The third edition of the forum will be held on 9-10 October 2017 in Krakow, Poland.

Topics:

- Bitcoin
- Blockchain