Cutting through the blockchain hype

Your expert guide to blockchain technology

In this e-guide:

Despite having pockets of adoption, blockchain technology is still in its infancy, with consolidation in the supplier market expected to take place over the coming years. While blockchain applications focused on the supply chain are fast maturing, the same cannot be said of other blockchain applications, many of which remain in the experimental stages. In this e-guide, read more about blockchain's potential beyond the supply chain, such as securing the internet of things and telco voice wholesaling.

How blockchain can secure the IoT

Aaron Tan, executive editor, APAC

The unprecedented distributed denial of service (DDoS) attack involving as many as 100,000 compromised devices in the Mirai botnet that nearly brought the internet to its knees in 2016 was a stark reminder of the sorry state of internet of things (IoT) security.

At the heart of the problem is the security architecture of the IoT, an inherently distributed client-server model that uses a central authority to manage IoT devices, along with all the data generated across an IoT network.

For IoT data to be trusted, all trust requests are aggregated into a single location, creating a single point of security intelligence that has, at times, compromised IoT security, leading to Mirai-style botnet attacks, according to Joseph Pindar, director for strategy in the CTO office at Gemalto, and co-founder of the Trusted IoT Alliance, a non-profit group that advocates the use of blockchain to secure IoT ecosystems.

In these attacks, IoT devices are unable to adapt their behaviour because they are not considered "smart" enough to make security decisions without the help of the central authority.

Pindar said blockchain removes this single point of decision-making that leads to failure, by enabling device networks to protect themselves in other ways, such as allowing devices to form group consensus about what is normal within a given network, and to quarantine any nodes that behave unusually.

The second aspect, he said, is to form trust in IoT data by enabling what he called the five digital security primitives: availability, auditability, accountability, integrity and confidentiality.

In blockchain, data is automatically stored in many locations and is always accessible to users. For auditability and accountability, a private, permission-based blockchain is used – where all users are authorised to access the network – and because all data stored on the blockchain is signed, each device is accountable for its actions.

For integrity, blockchain is, at its core, a public ledger of data entries – every deletion or correction of data is entered – and as the entries are confirmed by the network, a complete chain of events is created, said Pindar.

Blockchain is already being used in industries such as retail, where blockchain startup BitSE's Vechain platform is being used to demonstrate the provenance of high-value goods, including premium wines and Louis Vuitton handbags, to Chinese consumers who have a particular need to understand the authenticity of goods.

Pindar also gave the example of San Francisco-based Chronicled, which has applied blockchain to pharmaceutical supply chains to ensure tailored gene therapy drugs are delivered to the right person.

"By utilising a secure IoT platform, they are also able to attest to the quality levels of the drugs and to ensure that these drugs do not fail during the supply process, which could impact the efficacy when taken by the patient," he said.

Securing operational technology

Blockchain can also help to overcome the prevalent mindset in managing and securing industrial IoT and operational technology (OT) devices: once a sensor, device or controller has been deployed and is working, it cannot be touched.

"Even if there is a known security vulnerability, it is not worth fixing it, because there is a chance that the security patch would cause problems elsewhere in the system that no one knows how to fix," said Pindar.

"But as cloud computing has demonstrated, there are continual failures of devices and systems when operating at very large scale. Simply put, it is not possible to manage large-scale systems that are fragile and not resilient to failure – as is the case with many current industrial IoT and OT systems."

Pindar said the solution is to allow continuous deployment of software updates, as well as blockchain technology after devices have been deployed, with little or no downtime through an over-the-air update system.

"This has been shown to actually increase the availability of systems compared to an 'avoiding failure' approach," he said. "Therefore, a cost and operationally efficient way of providing over-the-air updates and patching to IoT devices and sensors would greatly benefit the industry as a whole."

According to market research firm Netscribes, the global blockchain technology market is expected to grow at a compound annual growth rate of 42.8% and reach $13.96bn by 2022.

The North American region accounted for the largest share of blockchain adoption in 2016, and is expected to dominate the overall market in the near future. However, the Asia-Pacific region is expected to adopt this technology at a faster rate owing to its wide adoption in China and India.

Next Article

In this e-guide

Blockchain is no 'magic wand' for cyber security

Aaron Tan, executive editor, APAC

The unprecedented distributed denial of service (DDoS) attack that disrupted the internet in October 2016 was a stark reminder of the sorry state of cyber security.

At that time, the Dyn Domain Name System (DNS) being used by a majority of websites to provide access to online services was hit with massive volumes of internet traffic unleashed by as many as 100,000 compromised devices in the Mirai botnet.

Although DNS is a decentralised system with servers around the world, its distributed components operate in reference to a central authority. Some cyber security experts have suggested that operating DNS on a blockchain would fully decentralise the system, preventing attacks aimed at a single, centralised source, and avoiding the flood of traffic that ultimately crashes websites.

"It also means that a hacker would have to gain access to multiple nodes in the system at the same time in order to implement the attack," said Eugene Aseev,

vice-president of engineering at Acronis. "That is much harder, more expensive and more time-consuming to carry out."

Indeed, the decentralised nature of blockchain has been part of the technology's appeal. As an open network that encrypts data and transactions on a distributed ledger, it makes all information publicly available. All participants in a blockchain network may verify the data, ensuring the information cannot be forged or removed.

In fact, blockchain has the potential to increase trust between parties as well as the accuracy of information. Examples include parties along a supply chain or government departments agreeing on the validation of records. If a copy of one's driving licence is distributed across trusted organisations in the ASEAN region, there would be many entities vouching for the integrity of that piece of identity.

"All actions are accurately recorded into blocks which are interconnected to previous blocks," said Sherif El Nabawi, security advocate at Symantec Asia-Pacific and Japan. "This means that the data is replicated in every subsequent block, enabling the system to compare the new block with the whole chain. If a block contradicts the other blocks, it will be recognised as false and will alert the entire system."

In addition, because all transactions are time-stamped and given a digital signature, any participant can trace the chain of actions back to a particular time period, finding the location of a party that initiated the transactions.

A recent IDC study suggests that worldwide spending on blockchain could reach $11.7bn by 2022 – the technology is clearly going through a hype cycle. There is no shortage of bold claims for what blockchain can do, but they often seem to be oversold.

"When people talk about blockchain use cases, they typically refer to data storage or exchange that is not streamlined or well-addressed by having a single or centralised database," said Bruce Davie, vice-president and chief technology officer at VMware Asia-Pacific and Japan. "By having the database distributed among several actors, it may offer a better solution."

In cyber security, high-potential use cases include identity management, data stores and smart contracts underpinned by a permissioned blockchain, by which known, authorised entities (agents or nodes) are invited to participate – unlike the permissionless blockchains used by most cryptocurrencies.

Although the immutability of the blockchain ledger makes it very hard to rewrite history by preventing anyone from tampering with data and information, it is arguably only a small part of the overall cyber security puzzle.

No magic wand

There are two things that make a blockchain theoretically tamperproof – a cryptographic fingerprint unique to each block, and a consensus protocol where the nodes in the network agree on a shared history.

But there are ways to subvert a blockchain, and there have been cases where flaws in code have been exploited to steal large sums of money.

An example of this is the DAO (decentralised autonomous organisation) attack that led to the theft of $50m worth of cryptocurrency Ether. "Bugs in smart contract code cannot necessarily be easily prevented, much like other software," said VMware's Davie. "There is a need to make the contract layer more resilient."

Individual blockchain nodes can also be compromised. In blockchain environments, just because one bad node cannot bring down the whole system does not mean you should not care about the security of that node.

Davie added: "Various forms of human error, including reusing passwords, falling victim to social engineering, and failure to operate with best practices such as patching known security vulnerabilities, continue to be the major issues for security – and these aren't immediately solved by blockchain."

It is therefore important for organisations to pay attention to the security of blockchain infrastructure by doing all the basics, such as applying micro-

segmentation, automated patch management, native data-at-rest encryption, and monitoring for changes to an application's intended state and behaviour.

"Blockchain is not a magic wand that fixes all security concerns," said Davie. "While there will be blockchain applications that prove valuable outside the world of cryptocurrencies, there is currently a lot of overpromising regarding the technology's application in cyber security.
"You still need to secure the infrastructure and environment on which your blockchain code runs, which brings us back to the core principles of applying good cyber hygiene and defence in depth."

That said, Acronis' Aseev believes enterprise adoption of blockchain in cyber security will happen in tandem with cryptocurrency developments – but only when there are industry-wide best practices or benchmarks for implementing blockchain.

"Today, the benefits of decentralised networks are often outweighed by high, unpredictable cost and time-consuming integration and deployment processes," he said. "The market is waiting for the solutions that are intuitive, cost-efficient, universal and collaborative. And they have yet to come."

Next Article

Cutting through the blockchain hype

Aaron Tan, executive editor, APAC

Despite having pockets of adoption, blockchain technology is still in its infancy, with consolidation in the supplier market expected to take place over the coming years, according to an industry expert.

Speaking to Computer Weekly in an exclusive interview, Tom Sprenger, CTO of AdNovum, a Swiss IT security company with offices in Asia, noted that many startups and investors are jumping on the blockchain bandwagon, but it is not always clear whether the use of the technology is really necessary.

Of the three main classes of blockchain applications – cryptocurrencies, transactional use cases such as smart contracts and business functions such as logistics – Sprenger noted that cryptocurrencies are overrated, volatile and have no real value behind them.

Sprenger said the transactional applications could make sense, but there is still a need to prove that blockchain is the right technology to use.

"If you look at all the proof-of-concept and innovation projects on blockchain, you have to be really critical and ask if blockchain is really needed," he said.

"My guess is that in half of those projects, blockchain is used because it is easy to get money, not because there is an added value."

Asked about the issues that have led to the current situation, Sprenger singled out three main areas. First, he said that although blockchain technology is developing quickly, many projects struggle to ensure stability in large-scale deployments.

"For example, if you are using smart contracts, you can't replace them like regular code," he said. "So you have to think about how to patch a production blockchain of smart contracts at scale.

"And if you run a blockchain in your datacentre alongside your core systems, the network security layer is untouched, so there is a lot work to do to bring blockchain into a production environment."

Sprenger also highlighted challenges in motivating businesses – and their rivals – to join a blockchain network, which often results in the democratisation of information.

"Now, that is very attractive to smaller firms because they have a chance to come together to beat the bigger companies," he said. "But not so much for the market leaders, without which the blockchain ecosystem won't spin up fast enough."

Sprenger also touched on the security of blockchain systems that are deemed secure as far as the immutability of information is concerned. However, he said that notion would not apply to data privacy and access management.

Citing AdNovum's Car Dossier project, which uses blockchain as a technological basis to create trust and drive value within the used and second-hand car industry in Switzerland, Sprenger said details such as the location of a car that had been involved in an accident could be captured on a blockchain.

"So you have location information and you know who owns the car at a certain point in time – that's very sensitive information, at least in Switzerland," he said. "Data privacy is a big concern and it's not yet resolved by the blockchain frameworks in the market – and that's where we jump in as a security company to provide access management capabilities."

According to market research firm Netscribes, the global blockchain technology market is expected to grow at a compound annual growth rate of 42.8% and be worth nearly $14bn by 2022. The Asia-Pacific region is expected to adopt this technology at a faster rate because of its wide adoption in China and India.

Next Article

Tibco to tackle blockchain challenges

Aaron Tan, executive editor, APAC

Tibco has started a research lab to develop new products and services in emerging areas such as blockchain, machine learning, artificial intelligence (AI) and the internet of things (IoT).

In blockchain, for example, the integration and analytics software company has formed a project dubbed Dovetail to address the challenges of implementing the technology.

Noting that the blockchain ecosystem is fragmented with a lack of tooling and standardisation, Tibco's global CTO Nelson Petracek told reporters at a company event in Las Vegas that Project Dovetail will make it easier to model smart contracts without deep programming experience.

Logic is abstracted from low-level code, and contracts can be deployed into different blockchain stacks with little or no change. Tibco said on-chain and off-chain computation can become more seamless, time-to-market is improved and the risk of technology lock-in is reduced.

Tibco's blockchain technology is also being applied in its AuditSafe tool, a cloud-based audit ledger that enterprises can use to store and audit events generated by business processes in Tibco Cloud and other third-party systems.

Project Dovetail and the formation of Tibco's new lab, which is open to participation by Tibco customers and partners, come at a time when interest in blockchain is growing across the Asia-Pacific region.

In July 2018, Singapore-based Global eTrade Services started an open trade blockchain network to boost cross-border trade between China and the rest of Asia.

Aligned with China's Belt Road Initiative and the Southern Transport Corridor, the permissioned blockchain network is run by trusted nodes hosted by accredited trade compliance companies.

By enhancing the security of trading documents, such as certificates of origin and commercial invoices, the blockchain network is expected to promote transparency and trust between shippers, freight-forwarders and customers.

In Australia, professional services firm Herbert Smith Freehills, Data61 and IBM are building a national blockchain to manage smart contracts from negotiation, through signing and across a contract's lifecycle. A pilot scheme is underway, and if the system works as expected, it will be offered first to Australian enterprises and then internationally.

According to market research firm Netscribes, the global blockchain technology market is expected to grow at a compound annual growth rate of 42.8% and reach nearly $14bn by 2022.

North America accounts for the largest share of blockchain adoption, and is expected to dominate the overall market in the near future. However, the Asia-Pacific region is expected to adopt this technology at a faster rate owing to its wide adoption in China and India.

In a separate EY poll in June 2018, 61% of senior professionals said regulatory complexity was the biggest barrier to widespread adoption of blockchain, followed by integration with legacy technology (51%) and a lack of general understanding of blockchain's capabilities (49%).

//

Next Article

More APAC consumer goods firms expected to adopt blockchain

Kimberly Chua

More consumer goods companies across the Asia-Pacific (APAC) region will follow on the heels of the financial services firms and adopt blockchain technology over the next five to 10 years, according to Ernst & Young.

Citing a CNBC article, Chandan Joshi, partner and global emerging markets leader for consumer products and retail at Ernst & Young, noted that blockchain technology would be rolled out across the financial industry in the next five to six years.

Joshi said the consumer goods industry was likely to follow suit due to the potential value that blockchain could bring in areas such as customer loyalty, retail and supply chain management.

Specifically, in markets where fraud is an issue, Joshi said blockchain would provide consumer goods companies with real-time information across their supply chains – from procurement and manufacturing to transportation and distribution.

Based on this information, consumer goods companies would be able to react faster and take proactive actions to identify and remove tainted or counterfeit products from their supply chain, for instance.

For now, Joshi said multinational companies in APAC were the forerunners in adopting blockchain – though many were doing so through trials and experiments, limiting the value of blockchain to a small scale.

Among small and medium-sized enterprises (SMEs), Joshi said the adoption rate of blockchain remained low, due to the lack of talent and their lower tolerance for failure. As blockchain is an emerging technology, some SMEs are waiting for it to become more mature before jumping on the bandwagon it, he noted.

That said, Joshi said governments could influence blockchain adoption through incentives that encourage adoption. The ultimate decision to adopt the technology, however, lies with the companies, which must overcome their fear of failure, he added.

For enterprises that are planning to adopt blockchain technology, Joshi said data privacy was a key factor to consider.

For example, while trading assets on an open blockchain may cut costs significantly, it may not be a practical solution for enterprises concerned with data privacy since every transaction is observable by all parties in the system, said Joshi.

Other than consumer goods, Joshi noted that other industries would increasingly adopt blockchain technology to enhance cyber security, and reduce or eliminate the roles of centralised authorities.

In securing internet of things (IoT) devices, for example, blockchain could help to address the inability of IoT devices to adapt their behaviour in response to security

threats without the help of a central authority, according to Joseph Pindar, director for strategy in the CTO office at Gemalto.

With blockchain, IoT devices can form group consensus about what is normal within a given network, and to quarantine any devices that behave unusually, Pindar told Computer Weekly earlier this year.

According to market research firm Netscribes, the global blockchain technology market is expected to grow at a compound annual growth rate of 42.8% and reach nearly $14bn by 2022.

North America accounted for the largest share of blockchain adoption in 2016, and is expected to dominate the overall market in the near future. However, the APAC region is expected to adopt this technology at a faster rate owing to its wide adoption in China and India.

//

Next Article

Colt pioneers blockchain in telco voice wholesaling

Alex Scroxton, networking editor

Network and datacentre owner Colt Technology Services and PCCW Global, the international arm of Hong Kong Telecom (HKT), have completed a successful trial of blockchain technology to manage inter-carrier settlements.

Simply put, inter-carrier settlements are the trading mechanism by which telecoms carriers are able to exchange services with one another to enable voice calls and other services to flow around the world across multiple networks. Due to the sheer number of carriers swapping services, these are often managed on a prearranged, wholesale basis.

"No carrier has 100% network coverage in a location where customers want service, so it's common to buy access rights to services from other carriers," says Colt chief of staff Louisa Gregory. "We often buy voice minutes from each other to meet customer needs."

"If you think about the amount of voice carried across the world, everybody tends to terminate calls on each other's networks on a constant basis. This is where the purchasing of minutes take place. On an annual basis we exchange

billions of minutes with other carriers," says Mirko Voltolini, Colt vice-president of technology and architecture.

However, this process is time-consuming, labour intensive, and prone to error. Colt, for example relies on a team employed in India to sift through millions of records every month – over 170 million of them in the case of a typical larger carrier customer.

"Every month, their sole responsibility is to take all the records and translate those into customer bills," says Gregory. "They have to manually identify any fraud and take any dispute from a customer that comes in. It is a full-time job just to manage this part of our revenues."

It was the desire to automate this process that led Colt and PCCW – which came on board through the firms' mutual involvement in the ITW Global Leaders' Forum – to consider how blockchain might streamline this process.

The objective of the trial was to find out if the advantages offered by blockchain technology – in particular data immutability – could maybe be used to make inter-carrier settlements more efficient, reliable and scalable.
Colt and PCCW enlisted blockchain startup Clear to help implement a bilateral private blockchain to record transactions, which could then be reported to a public blockchain. The trials then used smart contracts to rate call detail records, and record the settlement transactions.

The application of a decentralised, cryptographically enforced and immutable ledger meant that Colt and PCCW were able to analyse tens of thousands of call records, and settle up, in just a few minutes, eliminating hundreds of hours of manual work.

"Blockchain significantly reduced the need for that team," says Gregory. "[We saw] cost-efficiency gains through reallocating resources."

The extra layer of security and trust brought by blockchain means the trial has also potentially reduced the amount of fraud associated with voice, and has helped resolve disputes or discrepancies between Colt and PCCW, because the system can more easily detect problematic incidents and flag cases that may need human intervention.

"Today, two carriers need to compare their own records and discrepancies can take place," says Voltolini. "On blockchain, the same ledger is distributed and available to both [so] there is only one truth."

Blockchain 'viable' for wholesale

"Everyone is talking about blockchain but the use cases in the telecom industry have been fairly limited until now," says PCCW Global CEO Marc Halbfinger.

"While this deployment is currently only at the PoC stage, through our collaboration with Colt and Clear we are eager to demonstrate how the many

potential uses of blockchain across our industry can deliver exponential value by improving the ways we interoperate."

Although most current blockchain technologies lack solutions for scalability, contract privacy and enterprise-class business logic – all critical elements of an industry-wide settlement and clearing platform – the proof of concept did demonstrate the viability of a future blockchain-based wholesale trading system, says Colt.

This would be achieved through proprietary technologies such as multi-layer blockchain architecture, advanced cryptography and scalability enhancements to existing blockchain implementations.

The partners say the proof of concept could eventually herald a cryptocurrency-based wholesale model where, instead of exchanging cash to settle transactions, carriers could instead operate a token-based credit environment. Such a model could even be rolled out beyond the carrier community to other technology services providers.

Next Article

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 140+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively—and faster—than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; stock.adobe.com