Blockchain and the IoT Hype or reality?

Every so often a technology concept appears, seemingly out of nowhere, that, in the jargon of our industry, might be said to 'challenge the existing paradigm', writes IoT Now's editor, Alun Lewis. We've seen it recently with NFV/SDN, effectively deconstructing traditional telecom architectures to turn the planet's networks into what looks like one giant motherboard.

Christian Cachin, IBM Research

Gareth Stephens, GBG

The latest new 'new' idea to start filtering into the IoT community's collective mind involves the application of Blockchain technologies to the IoT/M2M world – and it's currently causing a lot of the individual heads that make up that collective mind to do some intensive scratching.

While most coverage of blockchain implementations so far has focused on their role in supporting the so-called cryptocurrencies such as Bitcoin, the concept itself represents another step in our journey towards decentralisation, initiated by the peer-to-peer worldview of the internet. Rather than having one central system tracking and authorising transactions, blockchain technologies work as 'a programmable distributed trust infrastructure', with built-in features providing trackable audit trails that all users can see and share – hence the term 'Public Ledger', which is also sometimes used.

This in turn is leading to the evolution of a number of other concepts that should definitely be of interest to the IoT world, such as Decentralised Autonomous Organisations, an idea promoted by **Slockit** who envisage a world where we can rent, sell or share anything – without middlemen. There's also growing interest in the possible role that blockchain might have in dealing with the increasingly critical issue of security in an IoT world.

So what is it?

Blockchain has started on a familiar journey: initial debate in odd corners of the technology blogosphere; trial projects by the R&D operations of a few large companies; a wave of innovation and start-ups; and the appearance of dedicated conferences on the topic. As a result, this got the editorial whiskers of IoT Now twitching a few months ago and we decided to canvas some opinions on how things might play out from a few experts. Now read on...

One of the companies that has been pioneering research into blockchain has been IBM, as Dr. Christian Cachin, cryptographer, at **IBM Research** in Zurich explains: "Blockchain is a promising new method for securing online transactions among mistrusting entities. A blockchain is a distributed ledger shared via a peer-to-peer network that contains an ever-expanding and immutable list of data records. Each participant has a copy of the ledger; additions to the chain are propagated throughout the network and agreed on by the participants. Even if some participants try to influence the system and gain an advantage for themselves, a cryptographic protocol ensures that one commonly agreed blockchain emerges, which holds only valid records, reducing the need to establish trust using traditional and expensive methods. At IBM's Zurich lab we're developing cryptographic protocols for the Hyperledger Project to create an open blockchain for business using Byzantine fault tolerant replication."

With us so far, dear layman reader? Don't worry, Dr Cachin now makes it tangible. "One of the more intriguing blockchain applications is supply chain management," he adds. "This involves managing many relationships with direct suppliers of goods—and companies also have to be aware of what's going on with their suppliers' suppliers. It's not just financial transactions, but also planning and managing each step in the process of going to market. Because of these separate but related interactions, there's a tremendous amount of overhead—time delays, pile-on costs, and the potential for mistakes to be made.

"Imagine instead supply chains where blockchain is used," he suggests. "An aircraft manufacturer might create a blockchain-based system for holistically managing all of its relationships with its suppliers. These will all share the exact same information about a new aircraft model – every step in the process of planning, designing, assembling, delivering and maintaining it. At the same time, the manufacturer will use other blockchain-based systems for managing financial transactions connected to each step. Trust, accountability, compliance with government regulations, and internal rules and processes get built into supply chains. The result: reductions in cost and time delays, improved quality, and reduced risks."

Making sure who is who – and what is what

Another critical building block of the IoT – identity – is also apparently ripe for blockchain. Gareth Stephens, head of Proposition Development at identity management company **GBG**, says, "With its highly secure and decentralising characteristics, blockchain can enable a single digital identity, allowing people to verify themselves once and then use this many times. But this also extends into 'things'. Think of a chair that could relay data about the person using it to reflect the length of time in use, weight,

movement, etc. and assigns it to the individual sitter. How do we stop people intercepting this information and how do we know it was the right chair/thing sending that information?

He adds, "In blockchain, people can create a single federated identity to authenticate themselves with services all over the globe, whether it be to login or to confirm a payment. Such solutions are decentralised, meaning that no companies hold all the keys to unlock these identities. Should a data breach occur, no one can take over an identity. We can also verify 'things' and their relationships to people. Each time they send/receive information from the IoT, the unique keys can be verified using the blockchain and only passed through when these match up. Blockchain alone often isn't the answer, but it is a key part of the overall solution."

An autonomous world of things

Matthew Coward, manager at **Sytel Reply**, also focuses on the role of blockchain in supporting the growing independence that we're assigning to things and systems: "Think about a production line able to talk with other production lines around the world, ordering parts and organising production on its own; think about networks able to reconfigure routing without human participation; think about machines communicating autonomously with the human world. The only grey point is security; IoT networks are huge, distributed and often built on top of existing unsecure protocols. Furthermore, they are built for interconnection and interoperation, dangerously linking different networks to each other.

"Blockchain, Coward proposes, "offers a compelling IoT solution as the greater the number of devices, the greater the inherent security. Why? Because the protocol acquires strength as the network grows, guaranteeing identity, security and provable information exchange. Reply has already designed some proofs of concept, based on blockchain, to accelerate our clients' own IoT development. Firstly, there's Blokcom, a messaging protocol based on blockchain, which transforms any untrusted environment into a trusted one where all data exchanged is verified and guaranteed against mutability and falsification. Then there's Securechain, a system to bring scalability and auditabilty to Software Defined Networks (SDN), using the **Ethereum** blockchain as a programmable security gateway to allow or reject changes on the SDN. Finally, there's Authentichain, a physical authentication protocol for the IoT world using any RF communication, providing secure access and mutual recognition for any smart device connected to every network."

He concludes, "Blockchain does however carry some challenges, like network growth management, process time to secure information and computational power. The last is one of the most important in an IoT context, since we deal with low-consumption devices with limited CPU power. Although a blockchain network requires a number of relatively 'heavy' miners to function correctly, very small and low-power IoT devices can participate as verifiers, providing a relatively light verification mechanism for the blockchain known as consensus."

"The IoT requires security from the edge to the enterprise", says Haydn Povey, founder of **Secure.Thingz.** and executive board member of the **IoT Security Foundation**. "We believe that security needs to be enhanced at every level of IoT implementation, from delivering confidentiality of data in transit and at rest, through to delivering high integrity and availability in the nodes - and blockchain is a potentially critical component in this. Providing transactional logs between nodes to prohibit non-repudiation and underpin financial interactions is going to be critical in building trust. For example, blockchain may enable adaptive white goods, where peak load on the electricity infrastructure demands that appliances pause to reduce load. This has real world benefit to the electricity utilities, but also may save costs for consumers if the transaction is formally captured and is non-repudiable."

Putting blockchain to work

One interesting initiative currently underway is **Chain of Things (CoT)**, a consortium of individuals, companies and organisations seeking to determine if blockchain can provide the best security solution for the IoT. In addition to security, the broader goal of CoT is to create a nexus for discussion and development at the intersection of IoT and blockchain.

Conor Colwell, one of CoT's founders explains, "Our initial focus is a use example that will document the layers of a full stack blockchain-based IoT solution for logging solar power generation to a distributed ledger. CoT will explore three segments critical to security: securely sending data from logger to ledger; maintaining ledger data securely; and, finally, securely sharing/transacting that data. This will be the first in a series which will use real world IoT deployments to both identify and explore potential security vulnerabilities while clearly establishing formulas for modular blockchain+IoT stacks. We're also actively seeking partnerships with a variety of groups - blockchain, IoT, security, or otherwise - who have an interest in testing real world implementations."

Matthew Coward, Sytel Reply

Haydn Povey, Secure.Thingz.

Conor Colwell, Chain of Things