Could **blockchain** secure IoT?

In the face of all the hype, it's hard to understand what's really worth knowing about blockchain. Here, we part the smokescreen and examine the true potential of when blockchain and IoT combine.

It's a packed Thursday night in London's trendy Shoreditch and a man waiting at the bar wears a black t-shirt emblazoned with the words "CRYPTO FOR GROWN UPS" in huge neon white text. Twelve months ago, this would have been unheard of, but over the last year – with Bitcoin's value hitting a record high of $1,943 in December 2017 – crypto has become big business.

This has many implications, not least of all for blockchain, the distributed ledger technology discovered inadvertently through Bitcoin, which underpins the growing list of all *1,700-odd cryptocurrencies*. Yet it is a totally separate standalone technology. It doesn't need a cash component to function. And it has its own steadily ramping hype – with dozens of industries *outside finance* – being tipped for transformation. These factors have led to a maelstrom of confusion around the technology.

One *independent C-suite guide* [PDF] suggests that nothing has ever proved so polarising in the history of tech. Individuals at the forefront of the movement – *like Brian Behlendorf*, a primary developer of the original Apache Web server, and instrumental in the formation of the internet – believe it is on the brink of changing our world. While many well-respected CIOs openly dismiss it as a joke.

> ***Blockchain technology could potentially allow billions of connected IoT devices to communicate in a secure yet decentralised ecosystem which also allows consumer data to remain private and also remove the centralised weak aspect.***
>
> **Kevin Curran,**
> *professor of cyber security at Ulster University*

Business: The value of blockchain and IoT combined

It's important to add some context here. Blockchain technology is a decentralised database – akin to a Google Docs version of Excel. It adds unique value to certain tasks but is also slower and more expensive than a regular database, such as MSQL. This means it will never be the answer to every business problem going, but in the areas where it does come into its own – to securely connect distributed systems – it can deliver something brand new.

The Internet of Things – and the resulting need to process all that sensor data – is one such area. As Tiana Lawrence, author of *Blockchain for Dummies*, put it in a recent article titled "*Blockchain set to converge with other trends in 2018*": the combination of AI, IoT and blockchain technology "represents the future of our interconnected society".

Lawrence provided a simple consumer example. An IoT device will use sensor data to help with your daily life. A machine learning algorithm will control that device to learn your habits and patterns. Blockchain technology will then become important to store and access that information immutably, permanently and transparently.

"All three of these technologies are moving to the point of convergence, and 2018 should be the first year these webs start intertwining," she wrote.

Security: The enhanced protection in IoT meets blockchain

"Blockchain technology could potentially allow billions of connected IoT devices to communicate in a secure yet decentralised ecosystem which also allows consumer data to remain private and also remove the centralised weak aspect," *Kevin Curran*, professor of cyber security at Ulster University, tells us.

This would help mitigate the single centralised model currently used in IoT and would provide a solid cryptographic foundation to help prevent data tampering. Both of these have become especially important with the *rise of IoT botnets*, which once active, can be hard to disable.

"A decentralised blockchain also provides a method for IoT devices to form group consensus regarding network threats and take appropriate mitigating actions," says Curran. "This adds layers of access to keep out unauthorised devices from the network. Blockchains can manage all local network transactions to control communication between home-based IoT devices and the outside world. They can authorise new IoT devices and cut off hacked devices." »

Industry: Some specific examples on how this could work

This could have huge implications in industry – especially for the supply chain [PDF] – where pretty much any product is a 'thing' in the IoT that can be tagged and tracked to deliver a variety of services. Put simply, this would allow IoT suppliers to guarantee whatever is important to their consumers. This could be that their tuna has been sustainably fished, their coffee beans organically grown or their diamonds come from ethical sources.

In the building industry, which probably gets talked about less than others, "one of the greatest challenges is linking the idea created by the architect to the pragmatic implementation on the ground, and the future operation of the building," explains Joe Pindar, director of strategy at digital security company Gemalto. In other words, things go wrong and take longer than planned in the process of building.

A new breed of IoT companies are working to solve this problem. InteliTaap, for example, is deploying proximity and activity sensors on building sites to help identify what's going on, then using the data to deliver more realistic completion dates. Meanwhile Open Sensors is monitoring and optimising room occupancy rates – along with noise, temperature, and CO2 levels – through IoT devices, Pindar tells us.

"In both cases, maintaining the accuracy of the data is essential as it is used to make costly business decisions. This is where blockchain comes in – providing an auditable log and p roof that the data has not been tampered or changed," he says.

Reality check: An overview of the practical limitations

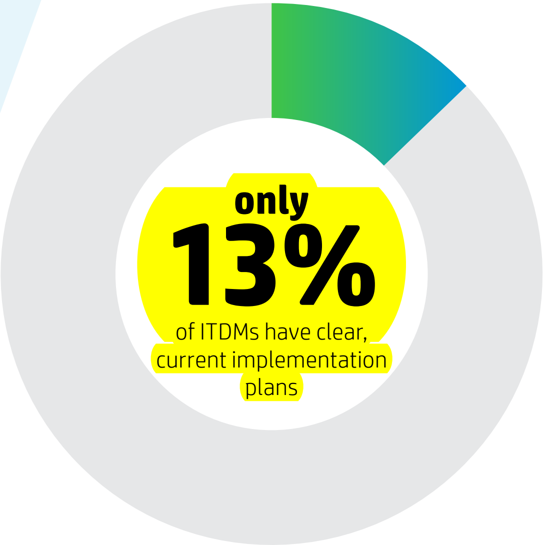
Lack of security baked into IoT devices from the outset has long been "a ticking time bomb" – and this advanced model requires even more from manufactures. To make this work in practice they must adhere to "the principles of Ethical Design" explains Curran. "This inherently demands that IoT manufacturers take strides to ensure their devices are secure and have planned roadmaps for security

updates to protect society from the problems which arise when compromised devices join the global network."

In addition to this, some of "the existing blockchains are simply not suited for IoT devices due to high energy consumption and processing overhead involved," he adds. "There is perhaps more potential in proof of stake blockchains as opposed to proof of work in the future Internet of Things.

"To arrive at large-scale integrated IoT blockchain(s), we need to overcome challenges such as proof of work high resource demands, the large latencies in transaction confirmation and the very small scalability involved in broadcasting transactions to the blockchain," he concludes.

The real challenge for many organisations, though, is likely to be education and implementation. Recent IDG Connect research of over 7,000 global IT leaders showed that only 13% of those surveyed have clear, current plans to implement this technology. However, like most of the smoke and mirrors surrounding the topic, this may lack nuance. In practice, much of this technology may come inadvertently through third party suppliers who manage the nuts and bolts – and ultimately – its reputation. ■



find out more visit THE HP BLOG

c06299058,April.2019