Newsletter

9th Jan 2020

A regular newsletter prepared for technology enthusiast and others interested to know how blockchain can make IoT firmware upgrades more secure.

Whether you are a current client, investor, contractor, or simply someone who wants to keep up to date with this fast-moving field, we hope this will be a useful source of information for you.

Focus for this edition – **IoT Security Threats and Blockchain Defence**

Dear Readers!

A warm welcome to 2020 from the whole of the Sprytech team! We're very excited to be starting a new year searching for and implementing solutions to your real-world business problems with our patented blockchain technology.

Indeed 2020 stands to be an auspicious year, both for Sprytech and for the rapidly evolving blockchain sector in general. With Brexit-derived uncertainty starting to clear up following the decisive election result from the end of last year, companies large and small who had been postponing investment decisions are starting to act on pressing issues and considering which systems to upgrade and how. Never have the operational problems of supply-chain data management been more crucial than now, given the UK's immanent departure from the EU at the end of the month.

For those who are interested in the possibility of applying blockchain technology to your own business model, please feel free to get in touch with us via the details below. We're always happy to provide advice and information about how our platform can be tailored to suit multiple needs.

IoT Security Threats and Blockchain Defence

This newsletter's specific focus is on the ability of blockchain to make IoT firmware upgrades more secure.

SPRYTECH LTD, London UK
Tel: +44-2086140787 E-mail: info@sprytech.uk Website: www.sprytech.uk & www.pharmachain.net

The often underappreciated vulnerability of IoT devices to malware attacks and other forms of security breach has been a growing concern for several years now, but has been thrust further into the spotlight recently when the World Economic Forum listed it as one of the main cybersecurity threat themes of 2020.

This ominous message has been echoed by the Information Security Forum, and as such both companies and individuals are looking for advice on how they can better secure their own devices against attacks.

But what exactly is the nature of the threat, and how can blockchain help the alleviate this danger?

The Threat to IoT devices

The ubiquitous presence of electronic devices, coupled with the fact that for many of us daily life, both professional and personal, would start to seem all but impossible without them, makes the threat to IoT networks seem even more menacing.

Essentially, IoT devices and their connections to networks and the Cloud are a security weak spot which has been known to be vulnerable for years, but easily implementable and economically efficient solutions have been hard to find.

These connections can be hijacked by either malware or organised criminal organisations, and the vast masses of personal data stored and accessed via our devices are accordingly exposed to theft, leakage and manipulation much more often than we normally like to acknowledge.

Even more worryingly, it is far from immediately obvious to a user or even a system administrator when a connection or a device has been compromised, thus making the detection of and defence against such threats exceedingly difficult to execute in real time.

How can Blockchain Help?

For several years now there have been ongoing attempts to leverage blockchain technology to improve the security of IoT devices. What these attempts have in common is they attempt to use blockchain as a fool proof and significantly more watertight method of identifying devices connecting to a decentralised network, and therefore to minimise the danger of devices being 'spoofed' or impersonated in order to access data illegitimately.

SPRYTECH LTD, London UK
Tel: +44-2086140787 E-mail: info@sprytech.uk Website: www.sprytech.uk & www.pharmachain.net

By registering every IoT node in the system into the underlying blockchain, each device gets a unique generated ID which is much harder to hack or replicate, therefore ensuring devices can be identified and permissioned or rejected from the network accordingly.

In this way one of the key strengths of blockchain-based system – that the decentralised ledger is by definition much harder to hack or 'cheat' than a single centralised one – combined with the fact that blockchain applications often enjoy considerable synergies with complex cryptographic identifiers means software upgrades can be undertaken in a much more secure manner, providing peace of mind for both the user and the company providing the update.

Sprytech Blockchain as a Solution to IoT Security Threats

One of the strengths of S-Blox, Sprytech's patented private blockchain platform, is the availability through our system of unique Quantum Ready Cryptography (7 discrete types), which provides an extremely high barrier to any attempted cybersecurity threat from either malware or hacking.

In addition to security concerns, the distributed nature of S-Blox and applications for automated firmware upgrades based on this platform also make the upgrade process more resilient to systems failure, and even reduce the time needed for the data transfer to take place.

We hope that this brief note serves as an illustration of how S-Blox in particular and blockchain technology in general can play a major role in making IoT systems more secure, and we hope you are as excited as we are to see what dynamic changes to the tech and business world are on the way for 2020!

Belated Happy New Year!

Until next time,

The Sprytech Team

SPRYTECH LTD, London UK
Tel: +44-2086140787 E-mail: info@sprytech.uk Website: www.sprytech.uk & www.pharmachain.net