insight.tech

POWERING IoT AND EMBEDDED INNOVATION

Blockchain: The Key to IoT Cybersecurity

If you're a hacker, the equation is simple: Commandeer a lightly protected IoT endpoint, then use it to gain access to higher-value targets elsewhere on an enterprise network. It's no surprise that cyberattacks targeting IoT devices tripled in the first half of 2019.

Such attacks are possible, at least in part because most IoT networks are based on centralized communications and security architectures like public key infrastructure (PKI). When dealing with thousands of distributed systems in the wild, PKI presents a number of challenges that leave IoT deployments susceptible to man-in-the-middle attacks, as well as single points of failure across a distributed network.

Trent Poltronetti, vice president at blockchain security company SmartAxiom, explains.

"The problem is that PKI involves a lot of certificates and this chain of trust back to the root certificate," says Poltronetti. "If it's well implemented, it's quite secure, but if you've got these endpoint devices that are user-facing in the real world, then you've got to talk to some server far away that maybe has millions of devices hitting it.

"If a key is captured, you could do a man-in-the-middle attack and give fake data to the servers or to the devices. And then you've got this issue with whether to design the system to fail open so it still keeps running and the users are happy but the security is turned off, or just lock the whole thing down."

So rather than trying to force a centralized security architecture onto distributed systems, why not just leverage a distributed security architecture like blockchain?

Blockchain: Distributed Edge Security

Blockchain provides an alternative to PKI. As a distributed database technology, blockchain eliminates the single points of failure associated with traditional security architectures by establishing trust among nodes on a peer-to-peer network.

Because multiple, decentralized nodes are used to verify transactions, blockchain-based networks provide several advantages:

- **Redundancy:** Even if an individual server or network goes down, other blockchain nodes can continue to verify transactions. And because transactions are stored on multiple nodes, compromising one node does not compromise the entire system.
- **Resiliency:** Because cryptographic hashes tie each block to previous blocks, transactions are authenticated using a shared history, which is another dimension of protection against man-in-the-middle attacks.
- **Scalability:** The more nodes on a blockchain network, the greater the security becomes because more compute resources are applied to transaction verification.

"While they're individually simple and breakable, as a group the nodes can work together to replace the security server for authentication and approval," Poltronetti says. "They're reliable because they're redundant. Because it's a majority consensus."

Better than Bitcoin for IoT Systems

Despite these advantages, most blockchain technologies are designed for enterprise deployment. In these applications, blockchain nodes typically have data center-class compute and memory resources at their disposal. And since generating and verifying a block becomes more complex and time-consuming as the chain grows and more nodes are added to the network, a large amount of latency is expected in many enterprise blockchain use cases.

Of course, IoT edge nodes don't contain anywhere near data center-class compute. And they are extremely time sensitive, as users can't wait 10 minutes for a light to turn on or the air conditioning to kick in.

To offset these drawbacks, SmartAxiom developed its own multi-chain blockchain called BlockLock that helps protect IoT networks from endpoint to cloud. BlockLock splits the conventional blockchain architecture in two with a Device Chain that controls node provisioning, authentication, and identity management, and an Event Chain that records transactions **(Figure 1)**.

This approach benefits IoT systems in a couple of ways. First, because the Device Chain accounts only for the devices and not the transactions they conduct, it can fit within an endpoint small-capacity, high-speed SRAM. Second, the architecture drastically reduces storage requirements because device data does not have to be duplicated with every new transaction. And transactions that fall outside of the buffer needed for shared-history authentication can be discarded or archived in cloud storage.

BlockLock is hardware, OS, and network agnostic. It can run on Intel® Atom® processor-powered IoT gateways with less than 512 MB of memory and consume less than 5 percent of the system's total resources.

Still, its performance requirements are too high for the resource-constrained IoT sensor nodes powered by simple microcontrollers. And the gateways BlockLock runs on are not efficient enough to support a full-scale enterprise blockchain.

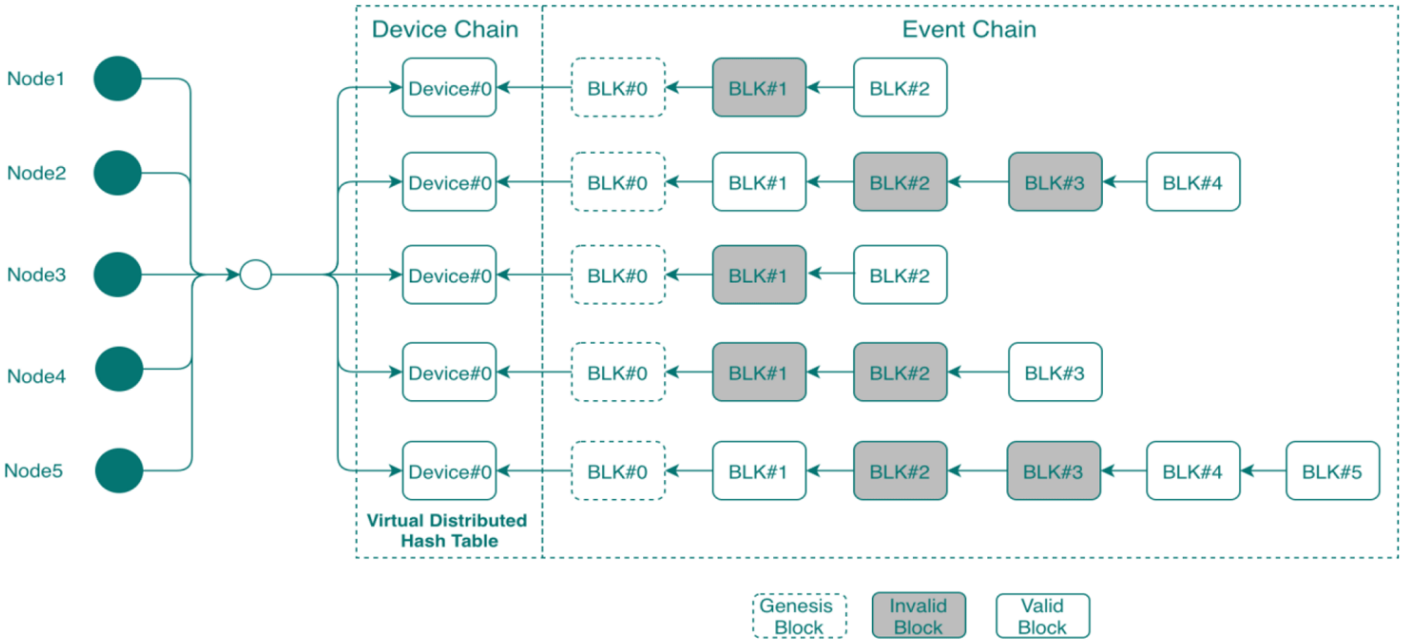

Figure 1. The blockchain verification process is split into Device and Event chains to improve memory utilization and system latency. (Source: SmartAxiom)

To enable a full edge-to-cloud blockchain architecture that capitalizes on the speed and storage benefits of the multi-chain architecture, SmartAxiom developed two additional components that complement the BlockLock stack:

In endpoints, Beachhead Microcode provides a small-footprint blockchain library that helps facilitate the generation of encrypted blocks. It also implements a micro-ledger where transactions are temporarily stored.

In the cloud/datacenter, the company's Tenacious Service integrates with INFORMIX for longer-term storage of time-series and spatial/GIS data, allows users to sync local IoT blockchains with other distributed ledgers, and includes additional anomaly detection and security analysis tools.

A holistic picture of the SmartAxiom blockchain portfolio, referred to collectively as Fortress, can be seen in **Figure 2**. Even with all of this infrastructure in place, SmartAxiom multi-chains are able to approve blockchain transactions in 100 ms or less—at least 5x faster than traditional PKI authentication.

IoT Security in the Wild

It typically takes years before new technologies are successfully deployed into the market, but IoT security is already behind the curve. To keep pace with the ever-evolving IoT threat landscape, organizations are implementing blockchain-based security solutions today.

For instance, one major auto manufacturer leverages SmartAxiom's multi-chain security architecture at one of its plants. Here, the technology is used to enhance network security for real-time sensors, actuators, and control systems. Plus, it is a method of removing silos between warehouse IT, operations, and analytics platforms so that plant data can be synchronized into one overarching system.

In this case, the SmartAxiom deployment was able to achieve latencies of less than 10 ms.

But the opportunity for blockchain extends beyond enhanced security and automation efficiency. It can be extrapolated to a vehicle or its electronic control units (ECUs), potentially securing the connection between "edge devices" and enterprise applications that make the IoT go.

"You have 200 processors in a car. If you run light blockchain among the biggest six or seven—and make them trust each other, make them work together, now the car can defend itself," says Poltronetti. "If they trust the car, it can be an endpoint in a larger system. Now for your ride hailing, your car sharing, your deliveries, it's a beautiful thing."

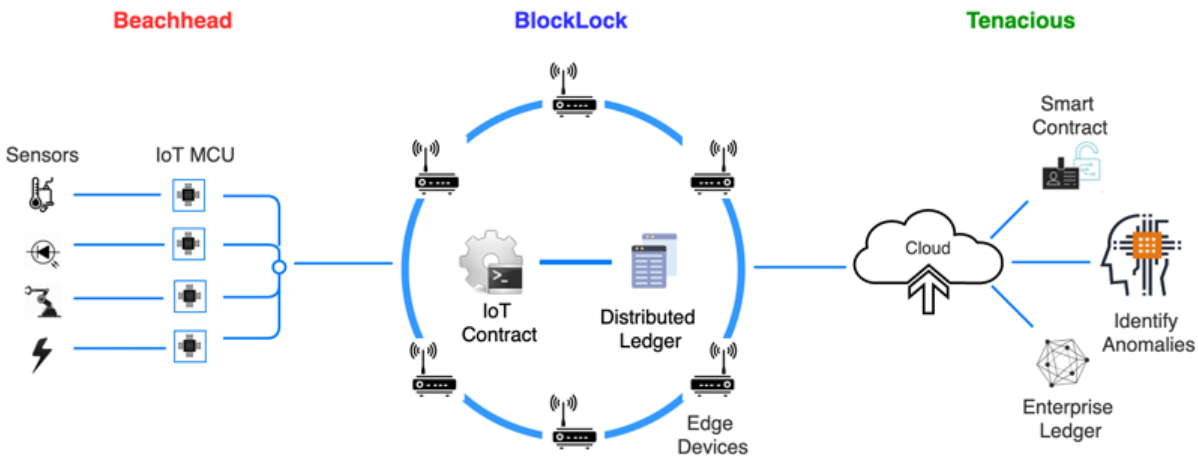

Figure 2. Fortress contains three blockchain components, extending multi-chain architecture from edge to cloud. (Source: SmartAxiom)