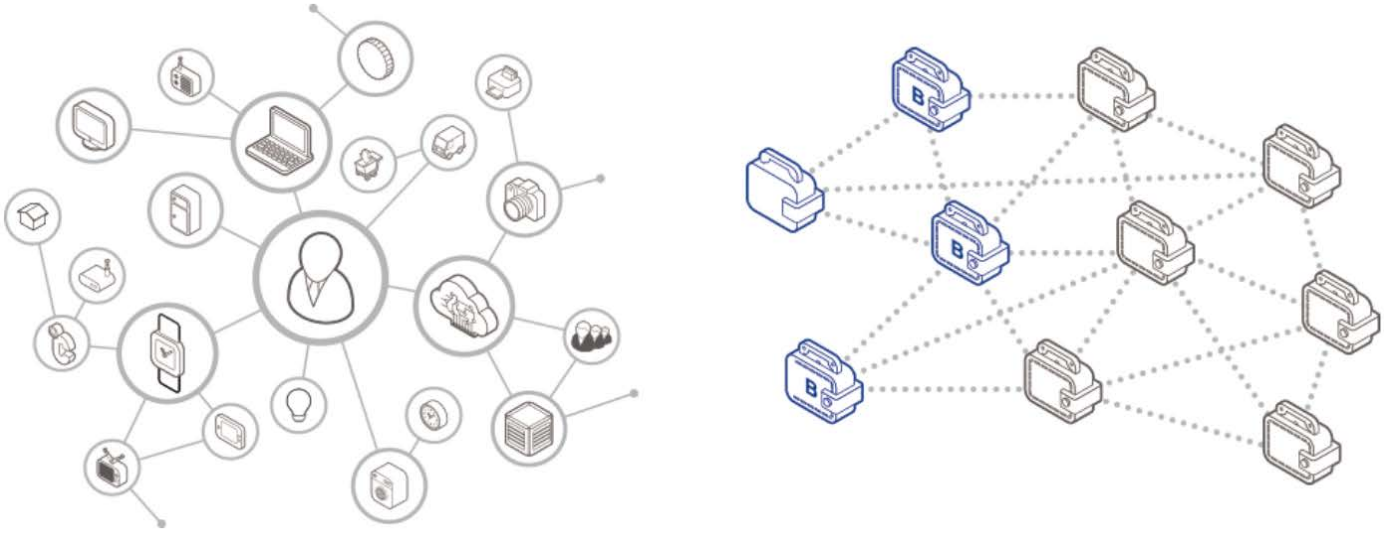
Calvin Price
Calvin is a student at UC Berkeley studying Economics, Computer Science, and Chinese.
Jan 22 · 7 min read

On Blockchain and the Internet of Things

Strengths, Weaknesses, and the Likely Road Ahead

The Internet of Things (IoT) is one of the most exciting paradigms in emerging technology. The principle of connecting billions of devices to automate networks is absolutely thrilling and has considerable applications in agriculture, manufacturing, consumer tech, and virtually all mechanically intensive industries. It also has a big problem: at its current stage, IoT is objectively infeasible and dangerous.

IoT connects a web of devices that typically operate with minimal computational power and are embedded with chips for the purpose of connectivity and little else. This is a major security flaw. Thus far, researchers have demonstrated horrifying capability and creativity in breaching IoT devices. Hackers have thus far managed to control implanted cardiac devices, entirely disable cars remotely, and launch the world's largest DDoS attack.



Source

The Case for Blockchain in IoT

IoT security flaws typically revolve around three areas: authentication, connection, and transaction. Devices improperly verifying, improperly connecting, or improperly spending with other devices are all major security concerns. (These are all software/protocol issues. Although is not the focus of this article, it is worth noting that IoT suffers from physical and hardware security flaws, too). A blockchain can alleviate all of these areas. Distributed ledgers seem like such a minor change to IoT networks considering how physically distributed the systems are, but the blockchain brings several killer apps with it.

Trustless: Fully operational IoT devices interact with known and (ideally) unknown devices. For example, autonomous machine repair is a big goal for the autonomous industry: when a mechanical failure or signs of deterioration is detected, the network responds by ordering new parts. In a trusted environment, such issues do not pose as a problem; in the real world, this is a major attack vector against the IoT network. But this otherwise thorny problem is solved by the trustless, consensus protocols of the blockchain, protecting from all but the most extreme malicious actors.

Auditable: Tracking the actions of network components and provably verifying that record is another big goal for IoT. Such auditability improves analytics, network performance, legal compliance, and safety. The blockchain's immutable record is ideal

for creating reliable networks histories.

Smart Contracts: Smart contracts are an amazing asset in IoT networks allowing for a high degree of coordination and authority. Particularly when it comes to managing transactions and interactions, smart contracts ensure proper cohesion. IoT is always built on the idea of being able to take the right amount of action at the right time. Put another way: Suppose you want your house to be able to order a new lightbulb when one burns out. You wouldn't want your house indiscriminately ordering crates of lightbulbs. Smart contracts are a great way to protect against this.

Transactions: The original blockchain killer app, transactions (particularly micro-transactions) are also useful for IoT. Especially for machine-to-machine interactions, micro-transactions are a key part to ensuring economic feasibility and optimality.

Device Integration: Adding devices to an IoT network in a secure manner can be a tricky thing. A lot of proposed IoT security revolves around effective encryption/handshake protocols. For devices to trust one another and establish communication, they verify initial communications against known device registrations. The problem is that these registries are an ideal target for hacks. Blockchain is great alternative for tracking these registrations and updating the system.

These benefits are more fully elaborated in a whitepaper by Filament, a IoT company with a strong emphasis on security:

"Unlike centralized technologies such as the Domain Name System (DNS) in which addresses are assigned in a hierarchical context (device@host, with the host obtaining its identity through registration of a DNS domain name), a blockchain-based approach is more agile because it enables devices to register directly. This obviates the need for accounts at centralized host servers, which are often subject to external cracking (e.g. dictionary attacks) and internal leaks (e.g. theft of password databases). In addition, the decentralized nature of these technologies reduces the threat of denial of service (DoS) attacks of the kind that have been launched against the DNS." (Source: Filament)

By maintaining a trustless and immutable record of access and integration, an IoT

network can significantly increase its security.

Problems with Blockchain in IoT

There are two big issues with integrating blockchain into IoT: speed and computational complexity.

At its current state, the bitcoin blockchain can manage 7 transactions per second. At its max, Ethereum can handle 25 transactions per second. These speeds are far too slow to be useful for IoT networks with hundreds or even thousands of connected devices all functioning and transacting simultaneously. There is no firm number of transactions per second that a blockchain must be able to handle for it to be useful for IoT, but the faster it gets the more useful it becomes and the tipping point for adoption is probably somewhere in the realm of thousands per second.

IoT devices are frequently built with connectivity, not computation in mind, and average processing power reflects this; IoT networks cannot handle computationally complex consensus algorithms. Proof of Work, the workhorse of crypto, demands far too much for it to be effectively used in IoT. Proof of Stake, variants upon it, or entirely different protocols are more likely to be implemented, but none of these have yet seen standard adoption for IoT.

Implementation

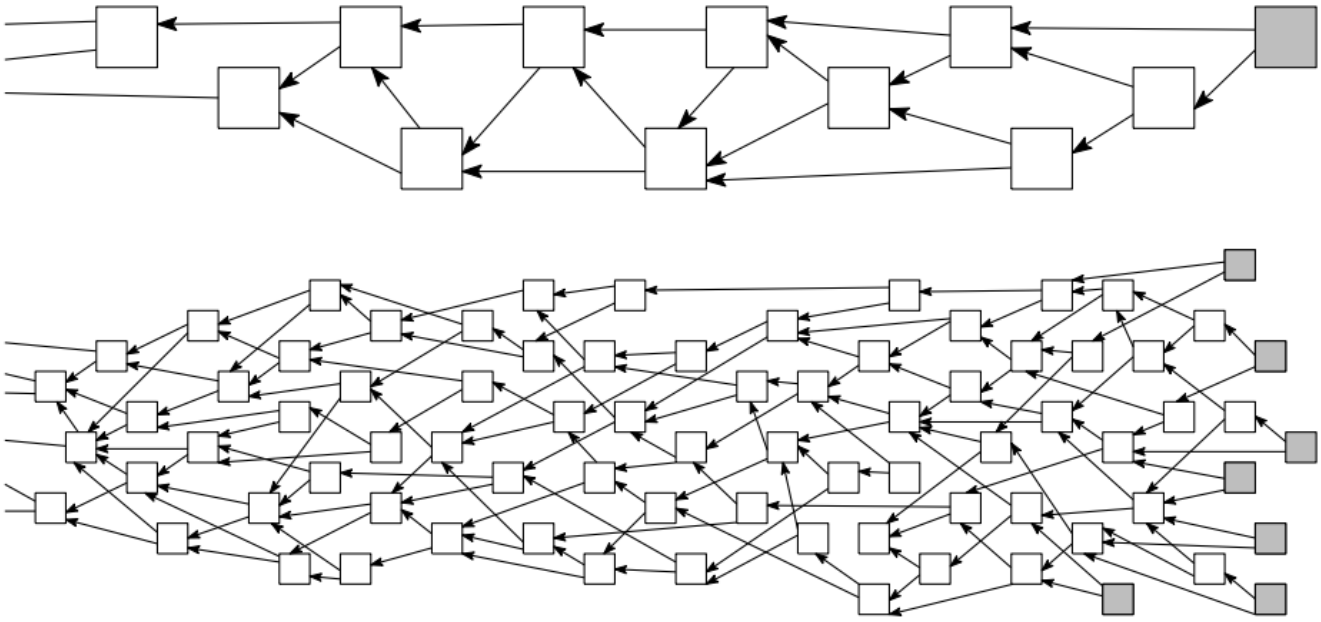
Blockchain in IoT is new territory for both emerging technologies and there aren't many initiatives focused on this sector, but it is quickly gaining attention. Here are the handful leading the way:

IOTA

IOTA was one of the first startups focused on IoT. Early on, the company built a grand vision for what affect distributed ledgers could have in IoT and pursued that vision with passion. Incredibly, the IOTA platform claims to have zero transaction costs. Besides convenience, this is an incredible feature for IoT. Micro-transactions are an important

part of sustaining an IoT network and transaction fees make micro-transactions meaningless (what's the point of spending $0.0006 when there's a transaction cost of $0.3?).

In terms of its architecture, IOTA isn't actually a blockchain. It operates on a data structure called a directed acyclic graph, referred to by IOTA as "the tangle." The tangle is roughly similar to a blockchain and still falls under the category of distributed ledger technology, but it features a different consensus structure. Notably, the tangle's structure makes the platform blazing fast. Blocks are added to the ledger by referencing an array of interconnected prior transactions (hence the tangle), rather than the single stream of a normal blockchain. There's a bit more magic to be done when actually verifying transactions, but the process as a whole has a much higher confirmation speed. Recent network performance has clocked the tangle at nearly 1,000 transactions per second, which is an enormous improvement over standard blockchain rates.



Source

Despite its impressive performance speed, several security concerns have been raised over its inherent nature and exact implementation of the tangle. As of yet, none of these issues have resulted in a network breach, but more work and research should be conducted before adoption of the network.

The exact details of how the tangle operates, IOTA's platform structure, and security concerns are fascinating, but far too much to be covered in this single post. More information about them can be found here.

HDAC

The Hyundai Digital Asset Company (HDAC) is pursuing IoT through a more traditional blockchain route. By tweaking a proof-of-stake protocol and utilizing an intriguing mix of private and public blockchains, HDAC has bumped the transaction speed considerably.

HDAC's platform is focused on three shrewd goals:

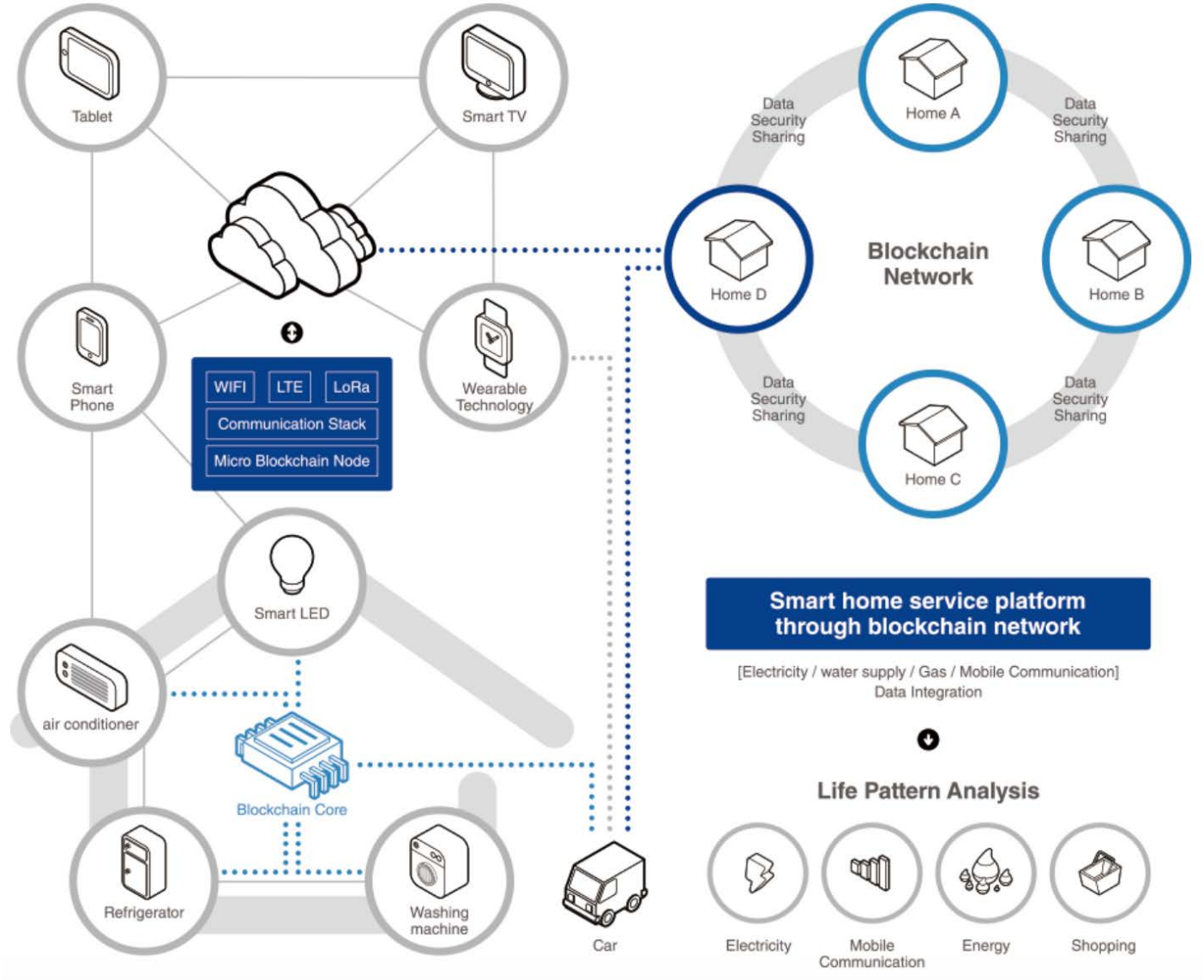
1. Authentication between devices

2. Mapping — once authenticated, the devices can connect easily

3. Machine to machine transactions

These are the basics for ensuring that blockchain covers the gaps in IoT infrastructure.

HDAC employs a permissioned blockchain to connect devices within a specific ecosystem (e.g. house, factory, etc.) and connects that ecosystem to a public blockchain. This relationship can be seen in the diagram below.



Source

Although somewhat vague, HDAC seems to argue that it uses the permissioned blockchain as a means to increase security by reducing access and increase network throughput and speed. Although it obviously increases the number of transactions per second, it remains to be seen that it improves the overall security of the system. The permissioned system would make it more difficult to add more devices to the network.

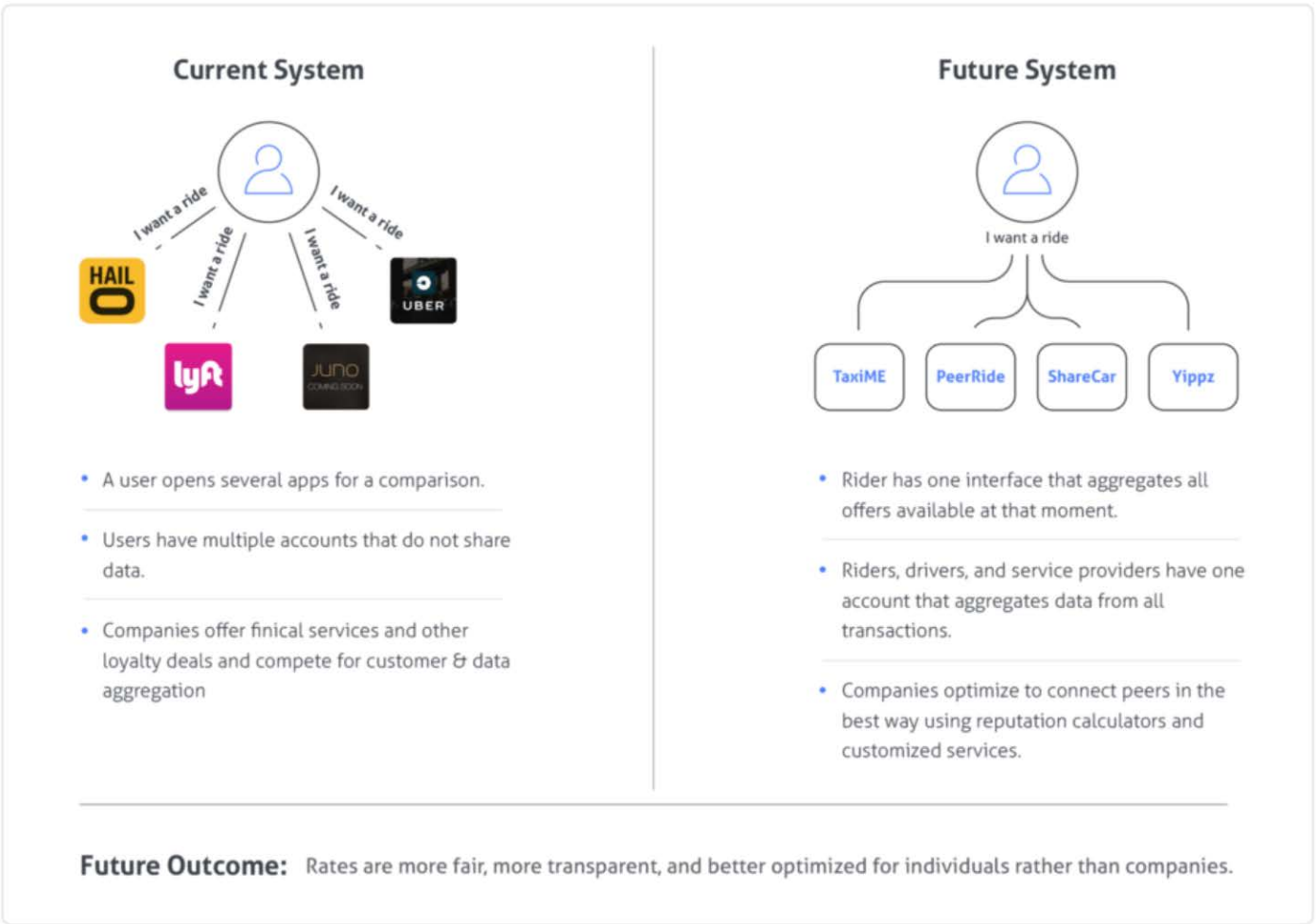
HDAC has now completed their token pre-sale and TGE, and claims to have finished with a war chest of almost $240 million. Backed by Hyundai, the company has stated an impressive list of goals to achieve in the coming year.

More information of HDAC can be found in their technical whitepaper.

The Likely Road Ahead

Besides improving the IoT software infrastructure to make toasters communicate with each other better, blockchain could create an autonomous, decentralized network of things for common use. This would be a groundbreaking step towards a more shared economy.

For example, consider the below comparison between ridesharing services in centralized and decentralized systems:



Source

This is a large jump ahead, but widespread IoT systems run on blockchains could not only decrease costs for taxi rides, but also lead to less wasteful power grids, smarter cities, and more efficient material usage.

Conclusion

The Internet of Things is the stuff of science fiction, but it is also a quickly approaching phenomenon. However, its inherent security flaws make it a tremendous risk for widespread implementation. Blockchain tech could alleviate some of those concerns and, in addition, add a range of other features to IoT networks.

Believing too much in a silver bullet is a good way to miss a shot; blockchains have a long way to go before being technically competent enough to securely handle a bulky IoT network. Nevertheless, blockchain appears to hold great promise for future IoT development and it's extremely exciting to see where that path leads.

Thanks to Swan and Melissa Mokhtari.

Calvin Price
Calvin is a student at UC Berkeley studying Economics, Computer Science, and Chinese.

Blockchain at Berkeley
We are a non-profit organization involved in blockchain tech-consulting, education and research at UC Berkeley. Contact us if you are interested in