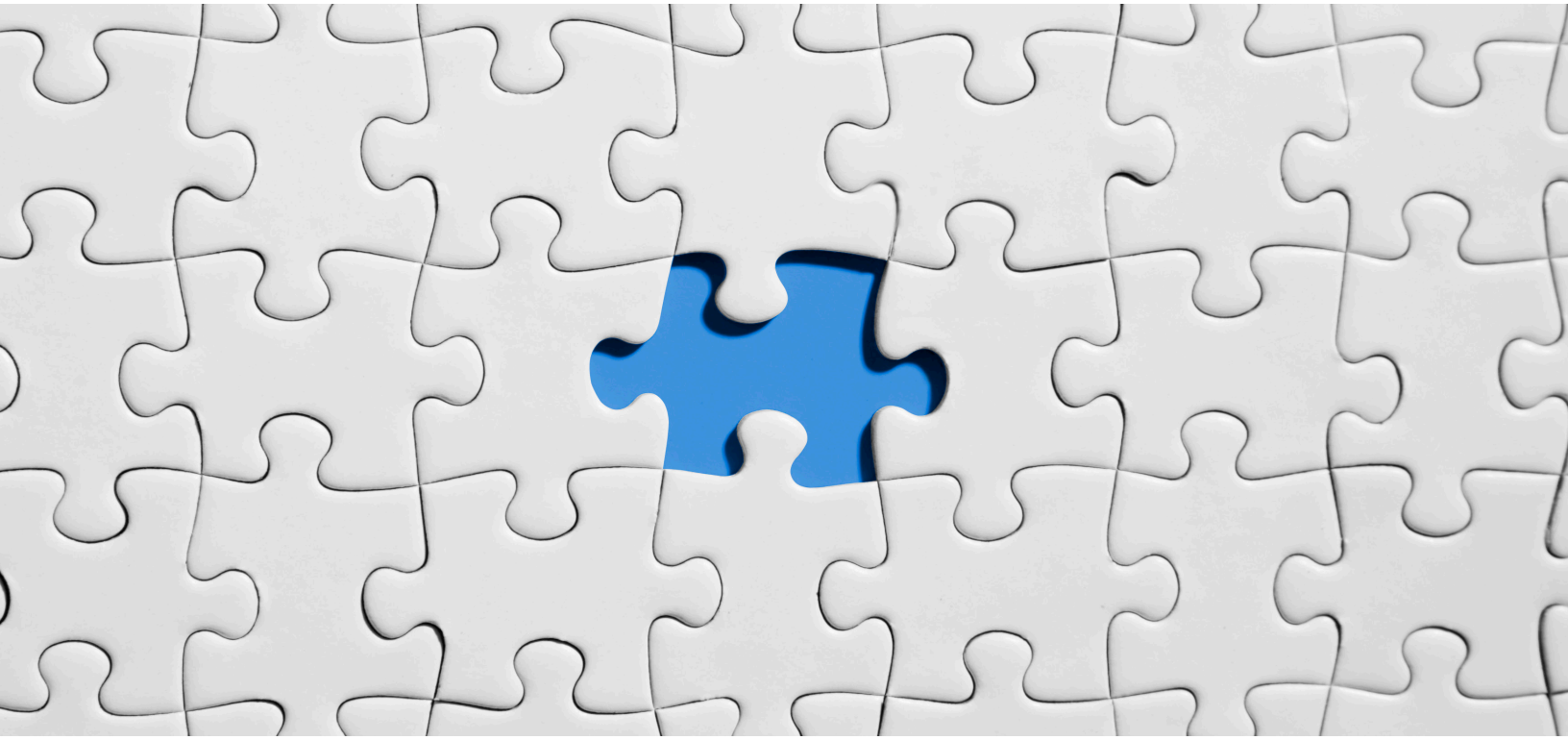
IOT AND BLOCKCHAIN - A WALLET OF SECRETS



Mohamed Sohail

Advisory Solutions Architect

Dell EMC

Mohamed.sohail@dell.com

Waseem Mohammad Fayed

Advisory Consultant

Dell EMC

Waseem.fayed@dell.com

Fidel Kaldas

Advisor, Service Delivery

Dell EMC

Fidel.kaldas@dell.com

Knowledge Sharing Article

Table of Contents

Figures

Preface

In this paper we will provide more information about two trending IT technologies; Internet of Things (IoT) and blockchain. We will explore the implementation models of IoT with blockchain and the challenges of combining the two. This will help the reader that aims to design an IoT solution understand the impact of an implementation leveraging the two technologies.

This will be accomplished in the next sections.

Defining IoT & Blockchain

- You will learn the meaning of IoT and blockchain.
- The correlation between the two and why people want to implement blockchain everywhere.

Challenges of current IT consumption

- IoT with blockchain enabled.
- Our vision for a successful blockchain implementation.

Emerging security paradigms for IoT and use cases

- Benefits of deploying blockchain with IoT.
- Successful use cases of using new blockchain security paradigms.

This paper will provide a straightforward understanding for moving forward in adopting the right model of blockchain security with your IoT environment.

Introduction

"I'd say that any device on the Internet with an open inbound port will be attacked. It's a matter of when, not if."

Gartner predicted that more than 20% of businesses will have deployed security solutions for protecting their IoT devices and services by 2017. IoT devices and services will expand the surface area for cyber-attacks on businesses by turning physical objects that used to be offline into online assets communicating with enterprise networks. Businesses will have to respond by broadening the scope of their security strategy to include these new online devices.

Figure 1 : IoT & blockchain view

The crux concept for IoT manufacturers is this: hardening devices against intrusion is a good first step, but it is nowhere near a complete security model. The concept that we propose in this Knowledge Sharing article is to illustrate a wallet of secrets between the IoT and blockchain technology to provide a holistic concept of how the two technologies can integrate together.

Internet of Things promises to bring online everything from the lightbulb in our living rooms to entire shipping fleets, enabling the industry to leverage this enormous amount of new data to provide innovative new solutions and technologies to all aspects of our lives. As 50 billion new devices are estimated to come online in the next 5 years, Gartner Research lists security as the #1 challenge to making the Internet of Things a reality.

Why?

Well, in order to be useful, IoT devices must be able to make real time bi-directional connections to a network, one that allows the device to send the data it has collected and also receive instructions, new configuration or even new software and updates. Naturally, with the sheer number of devices, their geographical disparity, and sometimes the inability to secure them physically, this need for being connected becomes a very big security concern. Whereas security protocols and best practices for servers, personal computers, and smartphones are well-understood and broadly adopted, security for IoT devices is nascent and rarely sufficient. We have seen many examples of security breaches that have utilized IoT devices such as the 2016 botnet attack.

It's a hacker's dream come true.

Figure 2: Example of a DDos

To combat this impending security crisis, we need a robust security model that works across the many different paradigms of device communication. Additionally, the security model should enable devices to be plug-and-play for the end user. Blockchain emerged for many technology professionals as a life boat for the booming number of IoT devices and resultant security gaps.

Figure 3 depicts how it works.

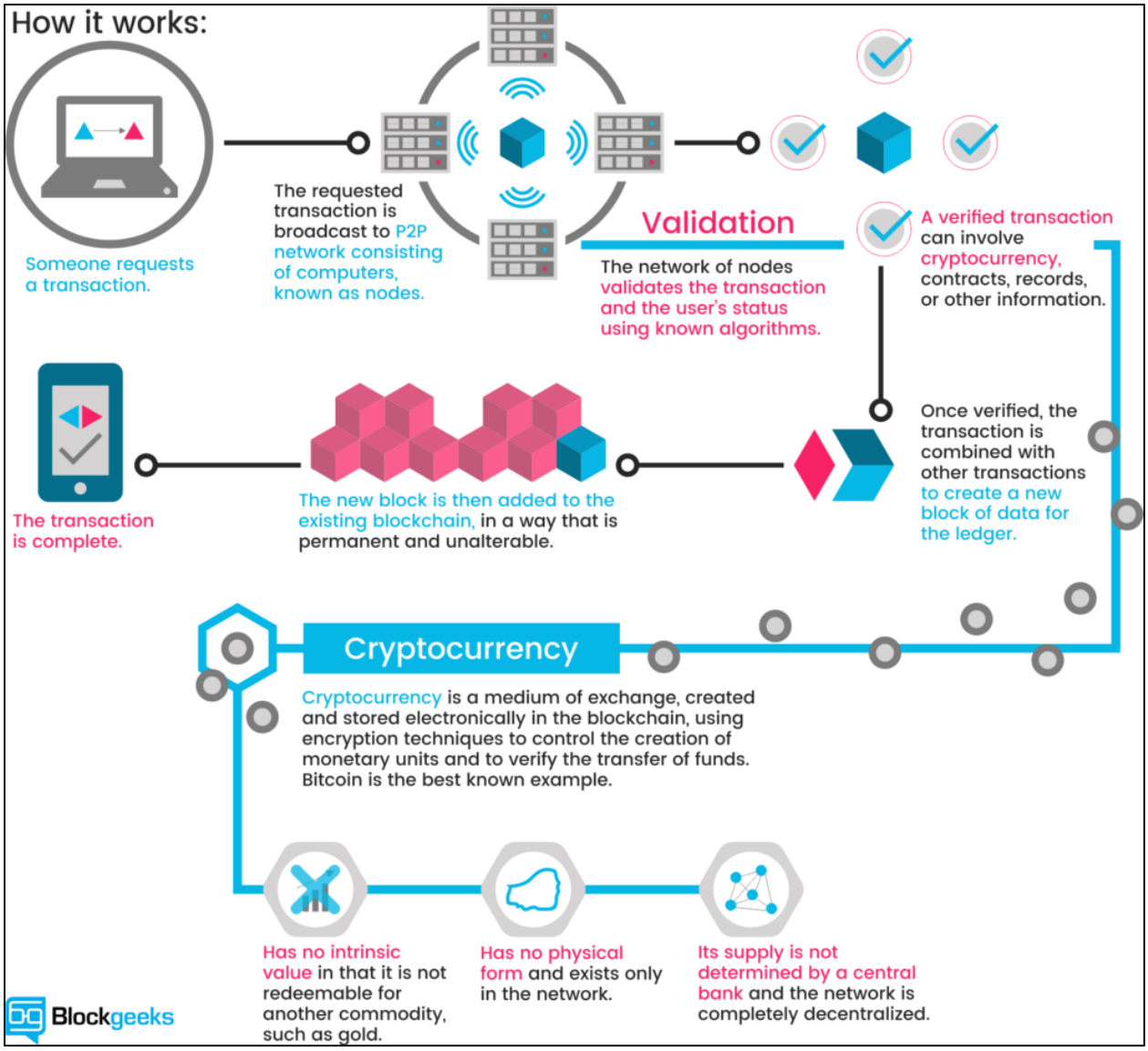


Figure 3 : Blockchain - how it works

Peer-to-peer messaging bypasses inefficient central database hops and allows efficient autonomous communication between peer devices. It is more reliable as central dependency disappears. Failure of one peer doesn't affect the functioning of other peers. In comparison, in the case of central cloud networks, if the central servers or databases become unavailable (e.g. go down), all connected devices get affected, an effect that could disable a city full of devices or hundreds of thousands of homes. Peer device communication will quickly become the new normal for large device deployments.

Everybody Wants to Work Blockchain

“Blockchain is the shift inception of a Database of everything”

The blockchain industry is complex and growing in size and capabilities daily. When you understand the three core types of blockchain and their limitations, you'll know what's possible with this new technology.

This section examines how to assess the three different types of blockchain platforms, what's being built on each type, and why. I give you a few tools that help you outline your project, predict obstacles, and overcome challenges.

There's a lot of buzz surrounding blockchain and the cryptocurrencies that run them. Some of this buzz just stems from the fluctuation in the value of cryptocurrencies and the fear that blockchain technology will disrupt many industry and government functions. A lot of money has been poured into research and development because stakeholders don't want to be made obsolete and entrepreneurs want to explore new business models.

Here we need to ask ourselves this question:

"Where does blockchain add value and how is it different from existing technologies?"

A blockchain is a special type of database. It can be technically utilized anywhere you would use a normal database — but it may not make sense to go through the trouble and expense of using a blockchain when a normal database can do the job.

While brainstorming this question we need to keep in mind the following points.

- Scale and volume
- Speed and latency
- Security and immutability
- Storage capacity and structural needs

In an IoT world we will need to choose the most suitable blockchain technology that will add value of deploying it. There are three core types of blockchain network implementations: public networks like the one used by Bitcoin, permissioned networks like the one used by the Ripple, and private ones like the ones used by the Hijro system.

Blockchain do a few straightforward things:

- They move value and trade value quickly and at a very low cost.
- They create nearly permanent data histories.

Blockchain technology also allow for a few less-straightforward solutions such as the ability to prove that you have a "thing" without revealing it to the other parties. It is also possible to "prove the negative," or prove what is missing within a dataset or system.

The table below shows use case examples of where blockchain may be used and the type of blockchain network that would fit that use case.

Primary Purpose	Type of Blockchain
Move value between untrusted parties	Public
Move value between trusted parties	Private
Trade value between unlike things	Permissioned
Trade value of the same thing	Public
Create decentralized organization	Public or permissioned
Create decentralized contract	Public or permissioned
Trade securitized assets	Public or permissioned
Build identity for people or things	Public
Publish for public recordkeeping	Public
Publish for private recordkeeping	Public or permissioned
Preform auditing of records or systems	Public or permissioned
Publish land title data	Public
Trade digital money or assets	Public or permissioned
Create systems for Internet of Things (IoT) security	Public
Build systems security	Public

As here we are concentrating on the IoT networks, let's look at the main types of networks to know to be able to differentiate between them.

- **Public networks** are large and decentralized, anyone can participate within them at any level — this includes things like running a full node, mining cryptocurrency, trading tokens, or publishing entries. They tend to be more secure and immutable than private or permissioned networks.

They're often slower and more expensive to use. They are secured with a cryptocurrency and have limited storage capacity.

- **Permissioned networks** are viewable to the public, but participation is controlled. Many of them utilize a cryptocurrency, but they can have a lower cost for applications that are built on top of them. This feature makes it easier to scale project and increase transaction volume. Permissioned networks can be very fast with low latency and have higher storage capacity over public networks.
- **Private networks** are shared between trusted parties and may not be viewable to the public. They're very fast and may have no latency. They also have a low cost to run and can be built in an industrious weekend. Most private networks do not utilize a cryptocurrency and do not have the same immutability and security of decentralized networks. Storage capacity may be unlimited.

There are also hybrids between these three core types of Blockchain networks that seek to find the right balance of security, auditability, scalability, and data storage for applications built on top of them.

Now let's discuss the question *why all want to work with Blockchain?* I can confirm that blockchain could also enable smart devices to become independent agents, autonomously conducting a variety of transactions. Imagine a vending machine that can not only monitor and report its own stock, but can solicit bids from distributors and pay for the delivery of new items automatically – based, of course, on the purchase history of its customers. Or a suite of smart home appliances that can bid with one another for priority so that the laundry machine, dishwasher and Robo-vacuum all run at an appropriate time while minimizing the cost of electricity against current grid prices. Or a vehicle that can diagnose, schedule and pay for its own maintenance.

At a more abstract level, blockchain networks themselves also have the potential to become independent agents, what some have referred to as "Distributed Autonomous Corporations." These would supplant systems like banking and arbitration, which have traditionally relied on trusted and centralized human authorities, with trustless and decentralized networks. Examples include electronic couriers to securely transfer sensitive information, escrow services to transfer ownership rights, or even auto-installation services to verify and push updates to the software governing other DACs.

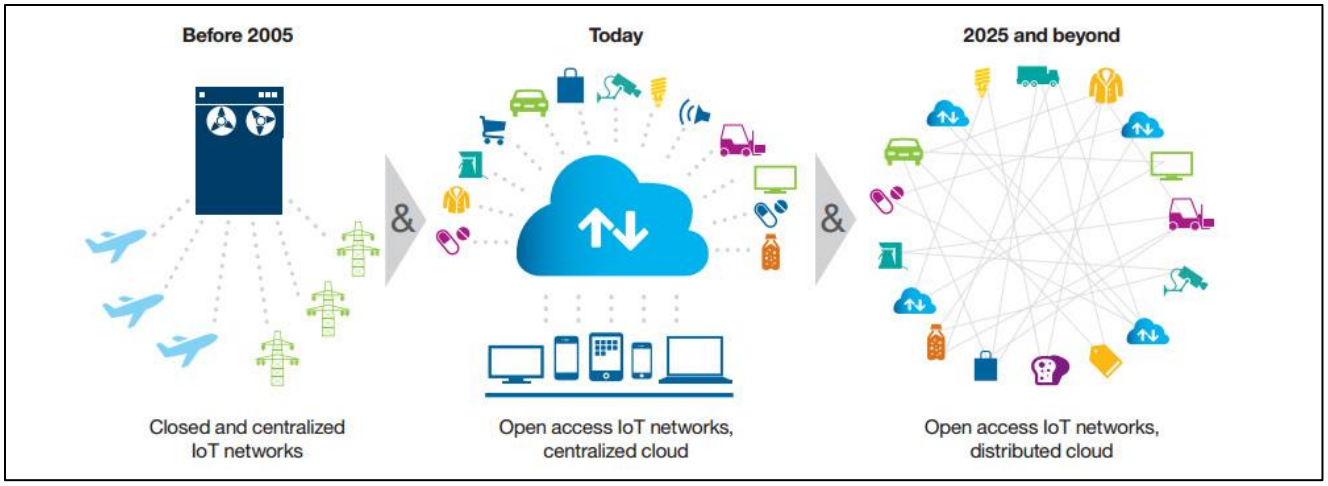


Figure 4 : IoT and Blockchain Evolution

Challenges using Blockchain with IoT

Although Blockchain technology provides a great solution for IoT, it has some disadvantages that would make it not a perfect match for IoT.

Transaction Latency

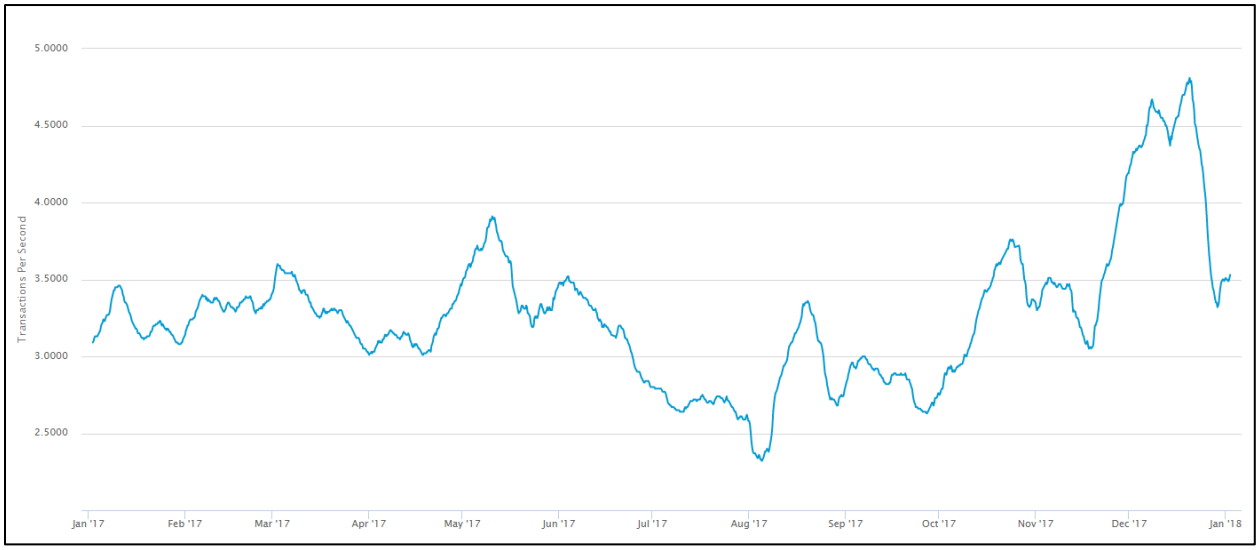


Figure 5: The number of Bitcoin transactions added to the mempool per second[1]

According to the blockchain.info website, the average transaction rate for bitcoins throughout the past year is around 3.5 transaction/second. We are talking about "the" largest blockchain network that ever existed. In comparison with other traditional payment platforms like Visa, it provides 24,000

[1] Source: https://blockchain.info/charts/transactions-per-second?timespan=1year&daysAverageString=7

transaction/second[2]. The values are incomparable and such transaction rate is inapplicable for most modern IoT applications.

One other aspect is the time needed for new transactions to be validated. For example, on the current Bitcoin network, new transactions require a 10 minute window to be validated. Such large latency values make Blockchain networks unusable for IoT mission-critical applications.

Limited Scalability

If you think that the growth of the blockchain network would increase the transaction rate, you are wrong. The complete opposite happens because, by definition, more than 51% of the blockchain network must validate any new transaction. This concludes that the blockchain solution is not scalable. Adding more nodes to the network definitely makes it more secure to any attack, but it makes it slower with validating new transactions. In an IoT environment, this scalability constraint is crucial, as the number of connected IoT devices is growing exponentially.

Blockchain Bloat

The current size for the bitcoin blockchain is around 145 GB[3] with an average of 400,000 transactions per day. This gives us an indication of the storage requirements of the nodes in the network. Hypothetically, this means that you will hook up a large drive along every sensor you use. What can we do with 400,000 transactions per day in the IoT world?

- 50 Temperature sensors
- Sending a reading each 10 seconds

With only those 50 sensors, you have created your equivalent “Bitcoin” network.

IoT traffic consists of a huge number of messages with small data usually representing the sensor data. Thus, the bloat of the network would be a challenge to be faced for big IoT networks.

Transaction Fee

There are two types of users inside the blockchain network.

1. Miners: Users having high computing power devices to validate new transactions.
2. Transaction generators: These represent normal users making transactions.

[2] Visa Transaction Rate: https://usa.visa.com/run-your-business/small-business-tools/retail.html
[3] Current blockchain size: https://blockchain.info/charts/n-transactions?timespan=30days

A major issue with blockchain is that mining and transaction generation are decoupled. In other words, users making transaction are not required to perform validations. Technically, this allows the possibility of centralization of the consensus. If a pool of miners can acquire more than 51% of the network nodes, this pool will have the power to manipulate the transaction data.

In the IoT world, this constraint will force the network designer to add a good amount of miner nodes in different locations, managed by different people to ensure the integrity of the data.

One other aspect of the transaction price is the hardware needed to validate new transactions. The more complex the “proof of work”, the more the network is secure; but the more one transaction will cost. The cost increase is due to the hardware requirements of the miner nodes. Unfortunately, with the growth of the network, the proof of work algorithm will take more time and require more computing power.

Next generation Blockchain - IOTA

What is IOTA?

IOTA is an open-source distributed ledger. It features the "tangle", a direct acyclic graph (DAG) for storing transactions instead of the typical blockchain approach.

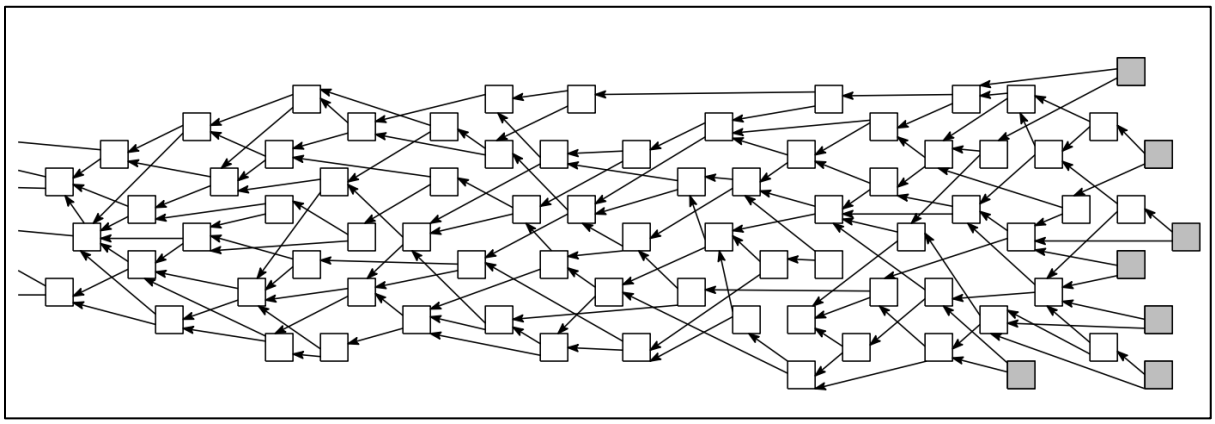


Figure 6: The IOTA Network

Zero Transaction Fee

In the IOTA network, there is no decoupling between miners and transaction generators. Every participant in the network is taking both roles at the same time. Each transaction generator is required to validate two pending transactions. Each network participant is now an active member in the consensus. This element of design prevents the possibility of the centralization of the miners, eliminating the possibility of a biased network.

One smart modification in IOTA is to use Hashcash lite proofing algorithm. This allows IoT devices with low computing power to perform validations; no need for huge expensive graphics processing units (GPUs). The feature opens the door to the IoT network designer to make use of numerous micro-transactions without worrying about fees in terms of money or CPU power.

Indefinite Scalability

Contrary to blockchain, transactions get validated faster as the network scales because there is going to be more people to validate the new transaction. In addition, with more transactions coming in, the tangle gets bigger and bigger and thus the system becomes more secure and harder to manipulate without compromising the fee or speed of transactions. Now, as an IoT network administrator, you are encouraged to add more sensors and gateways, because you know that happily, your network is becoming more

mature. This aspect is going to encourage merging of IoT networks and the sharing of resources. IOTA is a great foundation to build a universal IoT network which opens new opportunities for data monetization and advanced analytics.

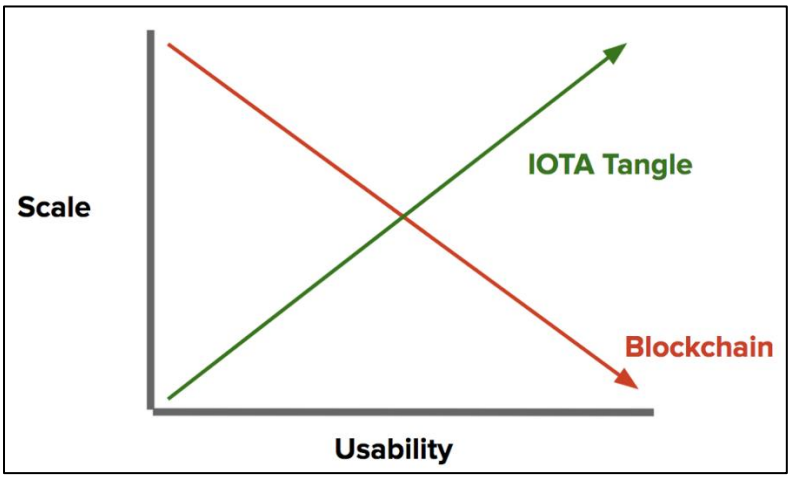


Figure 7: Blockchain vs IOTA Usability

Quantum Resistant

If you want to be ready for the future quantum computers, this is going to be your best bet. Quantum computers are estimated to be 17 billion times more efficient at hashing than current traditional computers.

Tangle security is better than blockchain because it requires the attacker to have 3 times the network's hashing power to be able to manipulate the data blocks. If an attacker acquires 10% of IOTA network computing power, he will have a 0.00001135% chance to breach the network. Thus, hackers with quantum computers would target blockchain networks first before heading to the IOTA networks.

Adoption

According to the press release on December 19th 2017, Robert Bosch Venture Capital (RBVC) is one of the early adopters of IOTA. The company has bought a large quantity of IOTA tokens in support of the technology. "Distributed ledger technology will play an important role in the industry of tomorrow" said Dr. Ingo Ramesohl, Managing Director at RBVC.[4] This investment was just after the launch of IOTA's data marketplace, where more than 30 major companies participated.

[4] Bosch press-release for IOTA http://www.bosch-presse.de/pressportal/de/en/robert-bosch-venture-capital-makes-first-investment-in-distributed-ledger-technology-137411.html

IOTA already enabled the motion of more than 10 billion dollar, secure over-the-air (OTA) updates and electric cars parking and charging payments.

Till we meet

Let me confirm that in today's world, security is imperative for maintaining control of your belongings whether physical or virtual. Cyber security is vital to keeping you protected, safeguarding your integrity, and avoiding unwanted data disclosure. IOTA provides robust cyber security measures around data integrity and confidentiality suitable for IoT, and even future proofs against quantum attacks. While these technological security features are a major benefit to using public/private key encryption, the keys themselves rely on more "human" security measures. It is this latter type of security that is most frequently the weak link.

It is clear that IoT is growing fast and the need for a reference architecture and a security framework will become a necessity to enable the secure and reliable growth of IoT deployments. Some tech giants have already released reference architectures but security remains a concern. Blockchain on the other hand has been around for several years now and has proven its ability – in cases such as bitcoin – to be a reliable and secure model of decentralizing transaction and authentication capabilities but has the shortcomings we discussed in this article. We are certainly going to see IoT solutions being developed and deployed in the future making use of some form of blockchain, we expect those to use IOTA for their needs which best fit the requirements of an IoT deployment.

References

- IOTA Whitepaper : https://iota.org/IOTA_Whitepaper.pdf
- http://blockgeeks.com/blockchain-and-iot-a-perfect-match/
- Blockchain for Dummies By: Tiana Laurence
- https://www.postscapes.com/blockchains-and-the-internet-of-things/
- https://www.pubnub.com/static/papers/IoT_Security_Whitepaper_Final.pdf
- https://www.slideshare.net/dinisguarda/blockchain-in-iot-and-other-considerations-by-dinis-guarda