The Road to

ECONOMY OF THINGS

BY SUSHEAT TEAM - TECHNION INSTITUTE

Motivation - IoT

Internet of Things

18 years have passed since ***Kevin Ashton*** coined the term, ‘The Internet of Things’. Speed on to 2017 to a time where IoT is giving rise to a new phenomenon called the Economy of Things. Since IoT gives way to EoT, one must first understand IoT.

http://www.rfidjournal.com/articles/view?4986
That 'Internet of Things' Thing
In the real world, things matter more than ideas.
By Kevin Ashton

Motivation - IoT

Internet of Things

In a nutshell, IoT refers to all Smart Devices connected through the internet. These Smart Devices will include all mundane objects like consumer goods as well as industrial products and manufacturing processes. This means that IoT's affects range from objects like coffee makers to crop harvesting equipment to cars according to ***elavon***.

" There's a fairly basic formula here: contextually aware devices streaming rich data via ubiquitous connectivity = The Internet of Things."
— elavon

https://www.elavon.co.uk/content/dam/elavon/en_GB/documents/Economy-of-Things-white-paper-released-October-16.pdf
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03678USEN

Motivation - IoT

Internet of Things

Gartner predicts that by 2020, 20.8 billion IoT devices will be connected. These devices will produce IoT data with a value of up to $7.1 trillion. ***(According to IDC)***

The Internet of Things will be seamlessly integrated into our lives, however, how IoT data is commercialised has not yet be fully determined. Questions regarding IoT data security and monetisation are of peak interest, as consumers and businesses alike realise the value of IoT data.

But what exactly is your IoT data and how does it fit into the Economy of Things?

https://www.gartner.com/newsroom/id/3598917
http://www.zdnet.com/article/internet-of-things-market-to-hit-7-1-trillion-by-2020-idc/

IoT

IoT Data and Artificial Intelligence (AI)

IoT data is produced by all kinds of Smart Devices, ***e.g. Roomba vacuum robot*** recreating floor plans from its movement while vacuuming.

You can imagine that by 2020 Smart Devices and machines will be using Artificial Intelligence (AI) to ‘learn’ user preferences. Ultimately making the life for the user easier and more efficient. These user preferences, made up of IoT data, will form valuable Digital Assets that can be monetised.

http://uk.pcmag.com/news/90449/roomba-is-mapping-your-house-to-make-iot-gadgets-smarter

EoT

Economy of Things

If IoT is “digitizing the physical world,” then the Economy of Things represents the “ liquefaction of the physical world.”

— IBM

https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03678USEN

EoT

Economy of Things

- IoT describes the digitization of things
-
-
- IoT Data is information and measurements produced by IoT Devices (Smart Objects) that can be traded in IoT marketplaces
-
-
- EoT describes the monetizations of things, where IoT Devices are able to share their Digital Assets autonomously via IoT marketplaces leading to a new Economy (Economy of Things)

EoT

Economy of Things

The Economy of Things is created when new value is extracted from the Internet of Things.

This means that **physical assets** are turning into **Digital Assets** that are able to participate in new disruptive digital markets, liquefying the ***physical world***.

The *'liquefaction'* of the physical world refers to assets around us to become ***"indexed, searched and traded as any online commodity"***.

This does not only refer to a Smart Home where the lights come on when you open the door or a Thermostat that uses AI to 'learn' your temperature preferences, but this also refers to a world where a **web of connected IoT Devices are in communication with each other**, searching for what they need and **trading autonomously** in **new digital marketplaces** forming the Economy of Things.

https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03678USEN

Digital Assets

Digital Assets

How can we asssign modeling to digital assets?

How can we trade digital assets securely?

In the next chapter, we will review a new technology that implements a solution to such needs

Digital Assets - Motivation

Bitcoin, Ethereuum, and The Blockchain in general

First, we will review and respect the first solution ever made to such needs - The Blockchain

Blockchain In a Nutshell

What is blockchain?

Internet of Value

Internet of Information

TCP/IP = communication protocol
Revolutionized the way we exchange information
aka *'Information Data Highway'*

First use case - Email

Internaet of Value

Blockchain = value exchange protocol
can fundamentally transform business, economy & politics by *'Decentralizing Trust'*

First use case - Bitcoin

Trust Machine

Blockchain lets people who have no particular confidence in each other collaborate, without having to go through a

neutral central authority

aka

trusted 3rd party

Blockchain replaces the trusted 3rd party!

Secure, decentralized peer to peer transactions
insted of central authorities

How to get rid

of the trusted 3rd party?

- **Shared**
- **Trusted**
- **Public ledger of transaction**
- **That everyone can inspect**
- **But with no single user controls**

Blockchain

Combination of technologies that we have had for a while

Peer to Peer Networks
Every node of the network is client as well as server, holding identical copies of the application state

Cryptography
Distributed hash trees for security & privacy

Proof of Work
Distributing Transaction Validation:
Validating transactions in a distributed network to find consensus about what transaction is true or false

How?

Consensus instead of trusted 3rd party

Each transaction on the blockchain is verified by all nodes in the network (true or false?)
If the majority of the network agrees that a certain transaction is true, it is validated and a new Block is created and added on *'top'* of the chain
To verify a transaction, each coin miner (node) has to solve a cryptographic equation, which takes up to 10 minutes by average with today's computing power
Today, Bitcoin miners are commonly using FPGAs/ASICs/GPUs as a computing power to verify transactions. (mine bitcoins)

Why are they called Bitcoin Miners?
The blockchain protocol as implemented for Bitcoin, ensures that the **first** node in the network that verifies the transaction block (solves the cryptographic equation) is acquitted with Blockchain's currency - Bitcoins, as a prize for their hard work.
when the blockchain protocol has just launched, each prize for block verification was 50 bitcoins. Meaning that actually, approximately on every 10 minutes, 50 bitcoins were made out of thin air, causing inflation of the currency.
The protocol stands that every 4 years, the prize is reduced by half. Today we stand on 12.5 bitcoins prize per verificartion

Fun fact - Bitcoin has a maximum value - 21 million coins. Meaning that in 2140 approximately we will reach that maximum, and miners will get their fee for professional services just from transaction fees.

Which Blockchains

exist today?

Bitcoin
first case use of blockchain

Altcoins
Forks of Bitcoin

Ethereum
Universal World Computer

Ethereum - Smart Contracts

Crypto Economy, Crypto Law

Most ambitious crypto-Ledger project

Beyond transferring value

Can verify if a party to a contract has fulfilled its side of the bargain

Smart Contracts - computer software can verify or auto-enforce any type of business transaction/legal agreement

Use Cases

We can build all kinds of Apps on top of the Blockchain

Tamper-proof public databases -
land registries

Registers of the ownership
of luxury goods or works of art

Get rid of the Notary!
Documents can be notarised by embedding information about them into a public blockchain

Fintech
Using blockchains as a record of who owns what instead of having a series of internal ledgers

Challenges and Cons

of the blockchain

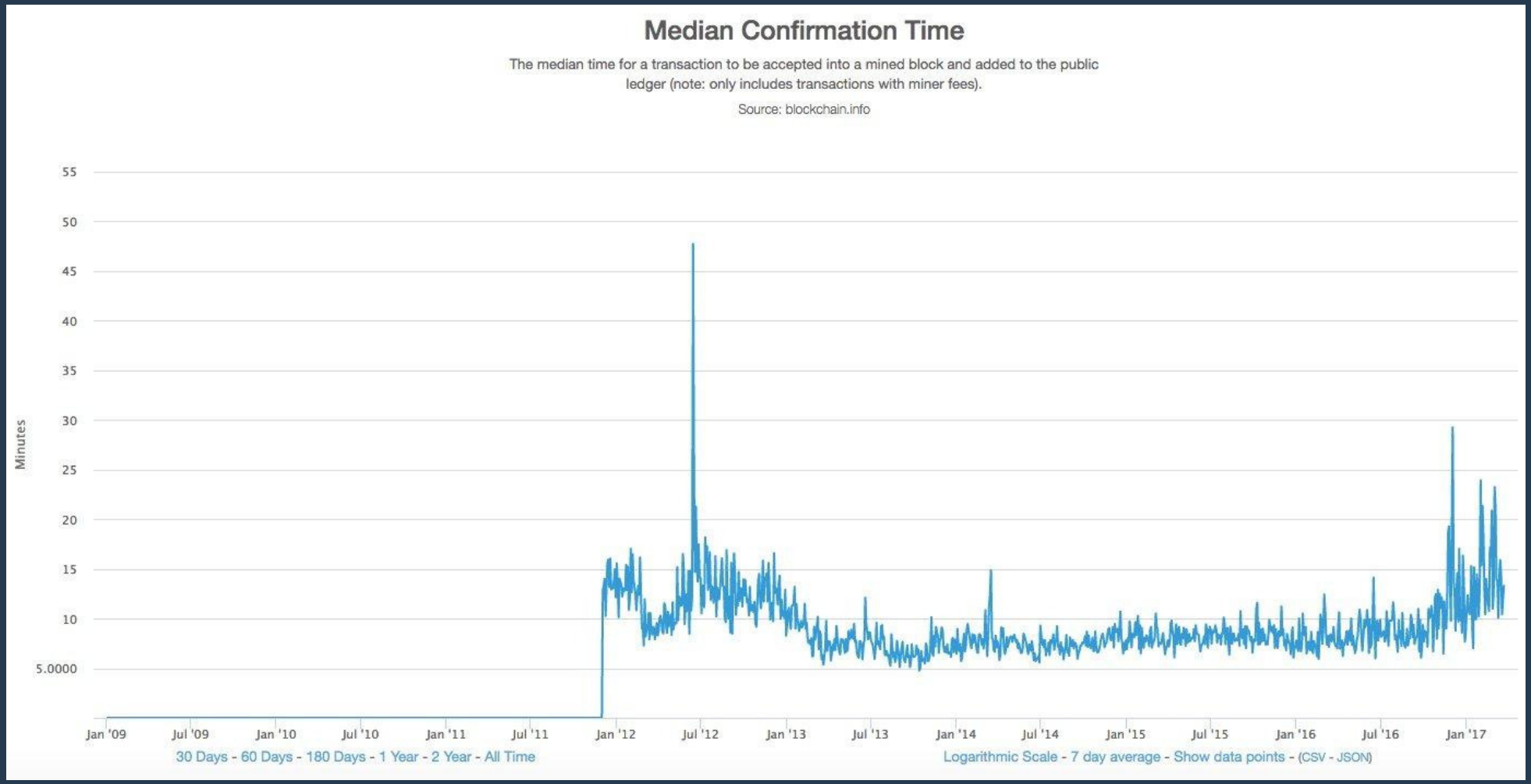
Scalability

of the blockchain

For bitcoin and ethereum to compete with more mainstream systems like visa and paypal, they need to seriously step up their game when it comes to transaction times. While paypal manages 193 transactions per second and visa manages 1667 transactions per second, Ethereum does only 20 transactions per second while bitcoin manages a whopping 7 transactions per second!
If we were to categorize the main scalability problems in the cryptocurrencies, they would be:
The time is taken to put a transaction in the block.
The time is taken to reach a consensus.

Scalability

of the blockchain



High transaction Fees

of the blockchain

(Opinion) - Blockchain as implented today, is not suitable for micropayments, as transaction fees are too high.

Since Bitcoin is implemented as a fixed-size block chain, each block can only contain a fixed amount of transactions, which means that during times of high network congestion (lots of transactions happening), fees will rise as the miners can only fit X amount of transactions per block.

See more technical information - https://en.bitcoin.it/wiki/Transaction_fees

Back to EoT and IoT

IOTA

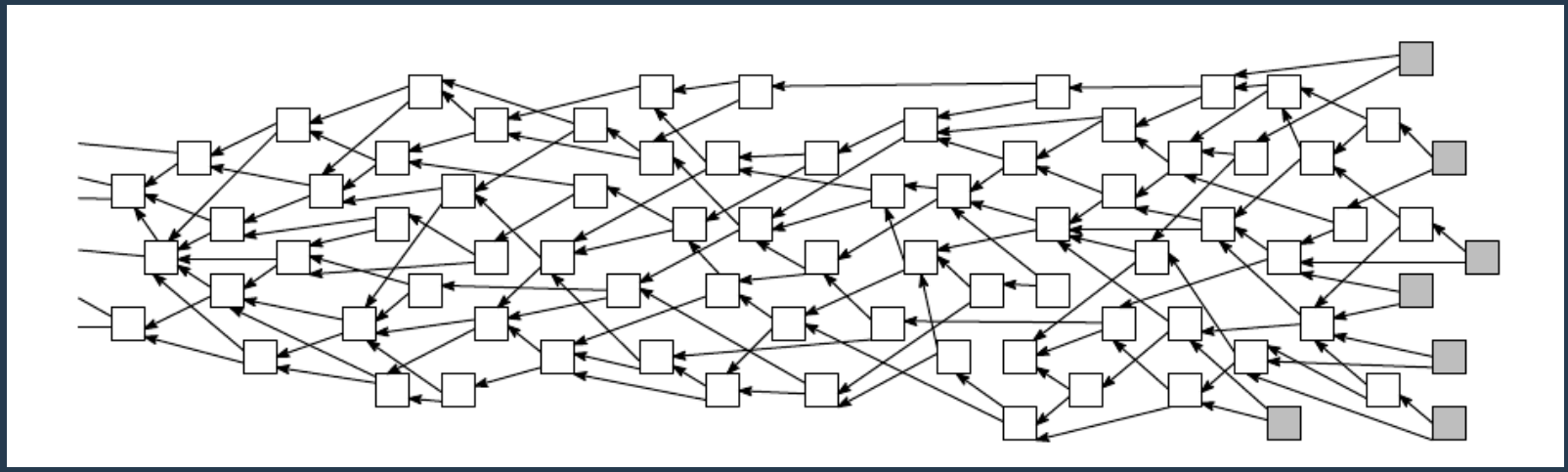
Economy of Internet-of-Things

IOTA

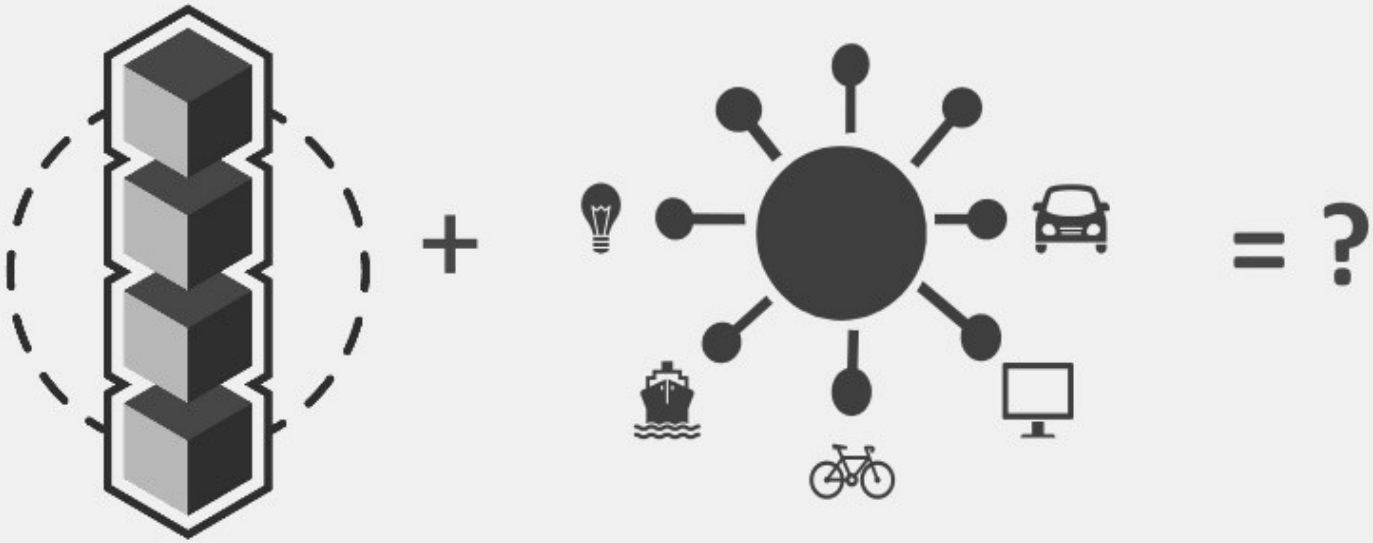
Economy of Internet-of-Things

In a nutshell IOTA is designed to be the backbone of the Internet-of-Things economy. It is an open-source, decentralized cryptocurrency that is meticulously engineered specifically for real-time micro-transactions in an environment that requires scalable flexibility and lightweight hardware. It will solve infrastructural problems for IoT and enable the ‘sharing economy’ of distributed technological resources.
The core innovation of IOTA is the Tangle

The Tangle retain the blockchain features of the distributed ledger and secure transactions, but drops the blocks. Instead it takes the form of a Directed Acyclic Graph (DAG).



Blockchain and IoT



IoT and Blockchain: A relationship that makes sense?

The exploration of Blockchain-related use case has been actively pursued by pretty much everyone in this space (corporates, startups, researchers, individuals) over the last 4 years. One of the areas that most excites us and many others is the Internet of Things. Not only has IoT a tremendous potential since it’s going to be everywhere (after all, it’s an ubiquitous computing and sensor platform), but it also has a whole range of problems where distributed ledgers could be the solution.

Blockchain: We're not quite there yet

- Scalability
- Fees
- High Hardware & Resource Requirements

Blockchain: We're not quite there yet

The simple reality when it comes to Blockchain + IoT (or Blockchain and anything else), is that we're simply not there yet. The technological limitations are apparent to everyone (including consultants) at this point. The two major problems are scalability and transaction fees.

In Bitcoin we're already seeing the consequences of a protocol that is inherently limited, but is (intended to) being used by a wider audience. Over 200.000 transactions were unconfirmed at the time of writing. This is cumbersome for users, and means that the majority of use cases cannot be executed, simply because you will never get your transactions through. If you're a large corporate, you don't want to wait, pay a higher fee, or bear with the uncertainty of not getting your transactions through.

The biggest issue next to scalability is transaction fees (they are largely intertwined). Bitcoin's mean transaction fees have already risen above $1. The question of "Who is going to pay for it?", arises regularly. Especially when it comes to micropayments and enabling a thriving Machine Economy, this question is a prohibitive factor that renders many of the use cases useless.

Blockchain: We're not quite there yet

Having uncertainty about how much money you will end up receiving in a monetary transaction means that you have uncertainty if your business model even works (after all, you want to make a profit..).

How much money will you end up making from selling one resource (e.g. electricity, bandwidth, computation) from one machine to another, when transactions fees are often unpredictable?

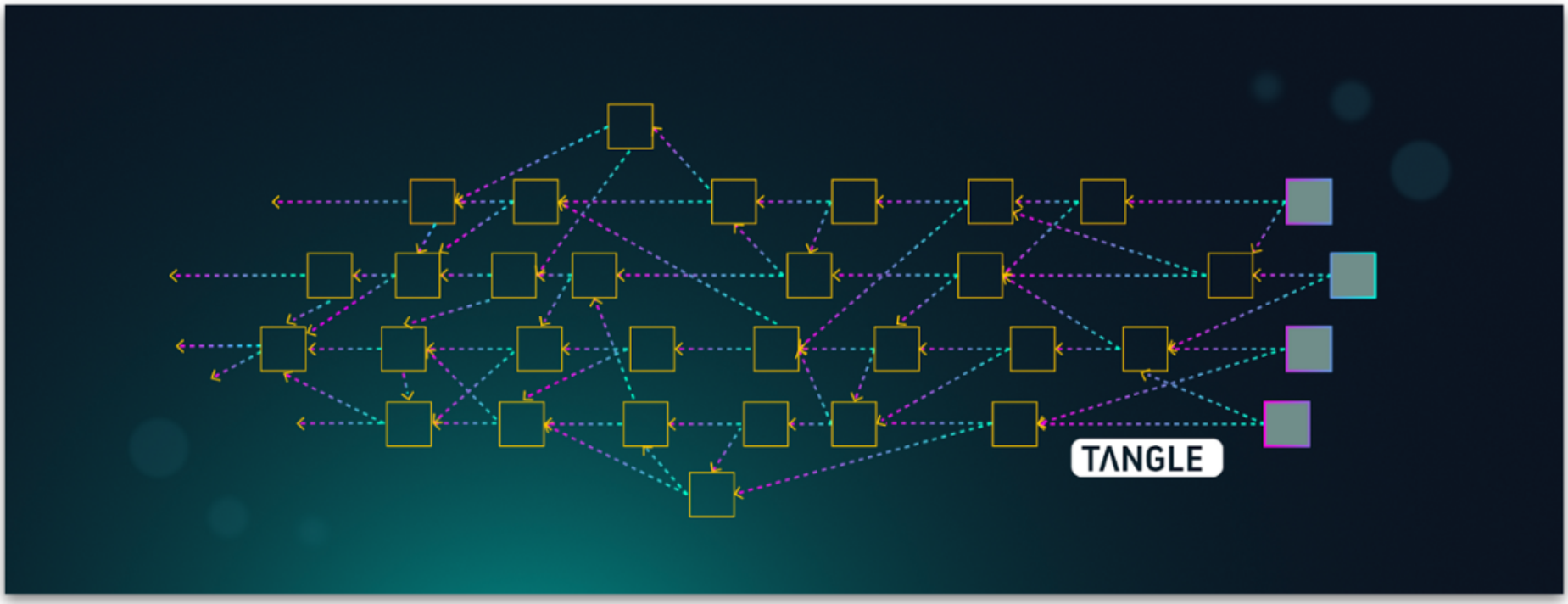
Even though we're seeing a lot of R&D in this area, the overall conclusion is that Blockchain is not production ready, and most of the use cases that are being discussed right now cannot be executed at scale.

Every technology in this space today is a Proof of Concept—even Bitcoin.

The Tangle

A Blockchain **without the Blocks** and the **Chain**

The Tangle



Read IOITA's Whitepaper: https://iota.org/IOTA_Whitepaper.pdf

The Tangle

The main innovation behind IOTA is the Tangle. It's a novel new distributed ledger architecture that is based on a DAG (Directed Acyclic Graph). One might refer to it as a "Blockchain without Blocks and the Chain" (semantically, it's not really a Blockchain).

At its core, the Tangle still has the same underlying principles as a Blockchain: it's still a distributed database, it's still a P2P Network and it still relies on a consensus and validation mechanism.

But, if we are to summarize the main differences between the Tangle and the Blockchain, the two most apparent ones are how the Tangle is structured (a DAG), and how we achieve consensus.

The Tangle

In IOTA there are no “blocks” in the classical sense. Instead, a single transaction references two past transactions. This referencing of transactions is seen as an attestation: with your transaction you attest directly that two transactions, and indirectly that a subsection of the Tangle are valid and conform to the protocols rules

Instead of a smaller subset of the network being responsible for the overall consensus (miners / stakers), the entire network of active participants (i.e. devices making transactions), are directly involved in the approval of transactions. As such, consensus in IOTA is no longer decoupled from the transaction making process: it’s an intrinsic part of it, and it’s what enables IOTA to scale without any transaction fees.

The Tangle

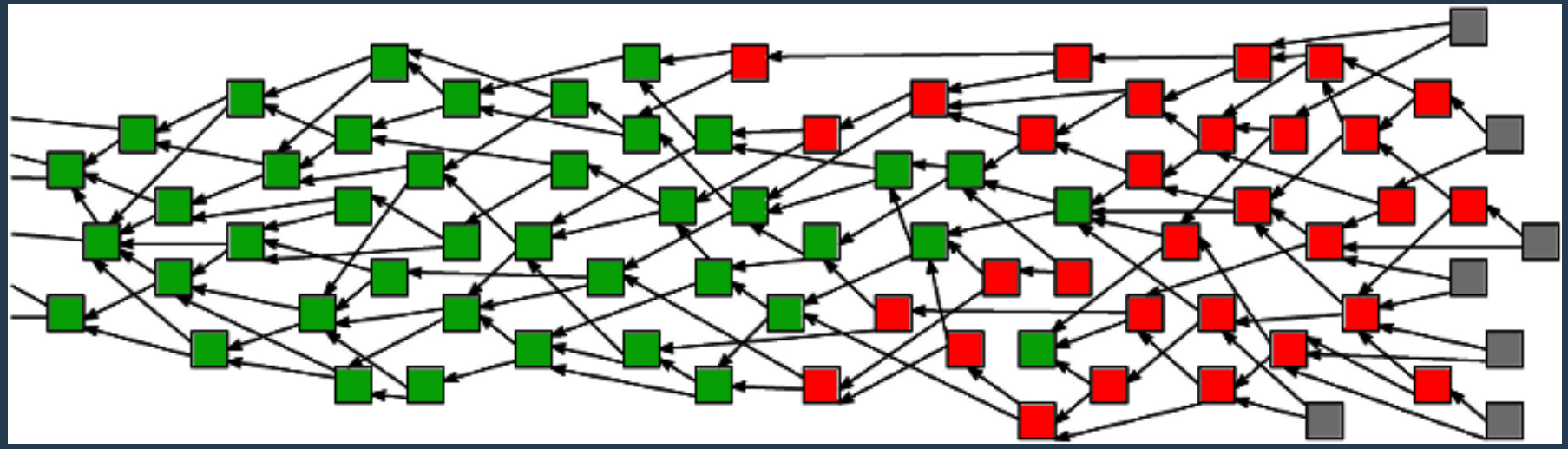
The transaction making process in IOTA is a simple, 3 step process:

1. Signing: You sign the transaction inputs with your private keys
2. Tip Selection: MCMC (Markov chain Monte Carlo) is used to randomly select two tips (i.e. unconfirmed transactions), which will be referenced by your transaction (branchTransaction and trunkTransaction)
3. Proof of Work: In order to have your transaction accepted by the network, you need to do some Proof of Work—similar to Hashcash (spam and sybil-resistance)

Once you've done that, your transaction will be broadcast to the network. Someone else will come along, choose your transaction in the tip selection process and validate it. And just like that, your transaction is confirmed.

Consensus in IOTA

As with any Distributed Ledger the question is: how does the network agree on the current state? With that question, we directly also tap on the “double-spending problem” (which probably confuses most people with IOTA)



Colored Tangle picture from the IOTA Consensus Masterclass: https://forum.iota.org/t/iota-consensus-masterclass/1193

Consensus in IOTA

Lets take a look at the colored Tangle picture above. Green blocks: transactions on which consensus was achieved (i.e. transaction finality with some security guarantees); red blocks: transactions where we are still uncertain on their full acceptance; grey blocks: tips (unconfirmed transactions).

Goal of any transaction is it to be green—you want it to be confirmed and accepted by the entire network. The question is, how do you go from grey, to red, to green? Without going into discussion on the CAP Theorem and the concept of eventual consistency, let us explain.

Consensus in IOTA

When we look at the picture, the main difference of the green and the red blocks, is that the green blocks are indirectly referenced by all the grey blocks. This means that for every confirmed transaction, there is a direct path leading to it from a tip. As such, it is quite easy to determine the confirmation level of your transaction: we execute the MCMC algorithm N times, the probability of your transaction being accepted is therefore M of N (M being the number of times you land on a tip that has a direct path to your transaction).

As a merchant, in IOTA you have complete freedom to decide with what probability you will start accepting transactions. If you are happy with 51% probability, you execute MCMC 100 times, and if 51 times or more there is a path, you accept the transaction and exchange goods. For high value transaction you can increase this threshold to 99 or even 100.

Once you have understood this concept of transaction finality in IOTA, you will start appreciating the simplicity and beauty of this system. It’s completely self-regulating and ensures both scalability and security.

Lets dive into some of the main features of IOTA, so you better understand why IOTA is so awesome.

No Transaction Fees

No transaction fees

Because IOTA achieves consensus on the validity of transactions without the involvement of any miners, we also have no transaction fees to pay.

IOTA is the first transactional settlement protocol that enables you to transact even sub-cent values Peer-to-Peer without any transaction fees for either the sender or the recipient.

As such, we really perceive IOTA to be the backbone of all current and future micropayment and nanopayment use cases.

It Scales!

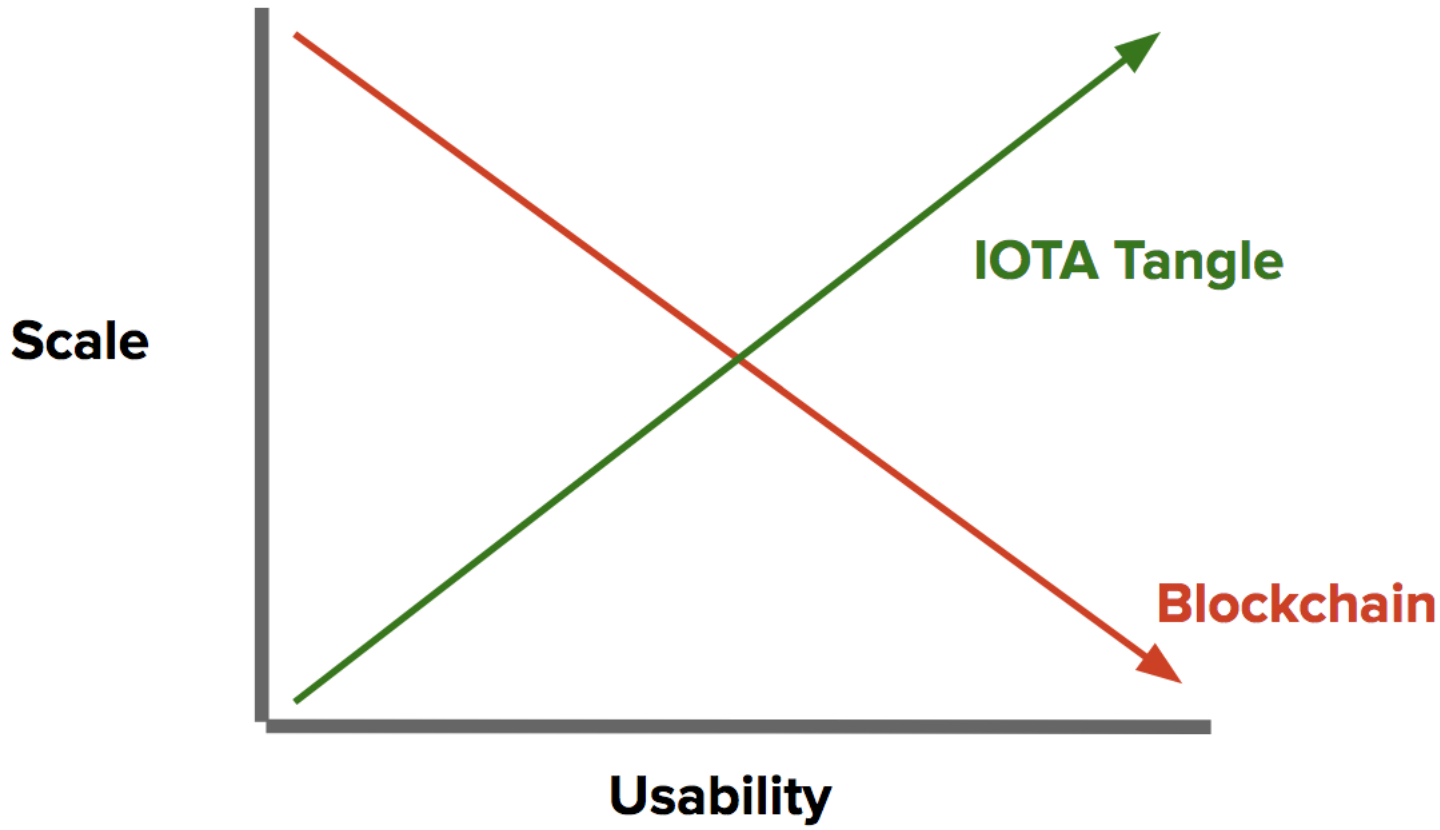
IOTA was designed to enable transactional settlement at scale.
Since consensus is parallelized, and not done in sequential intervals of batches as in Blockchain, the network is able to grow and scale dynamically with the number of transactions.

The more transactions are made, the more secure and the more efficient the Tangle gets.

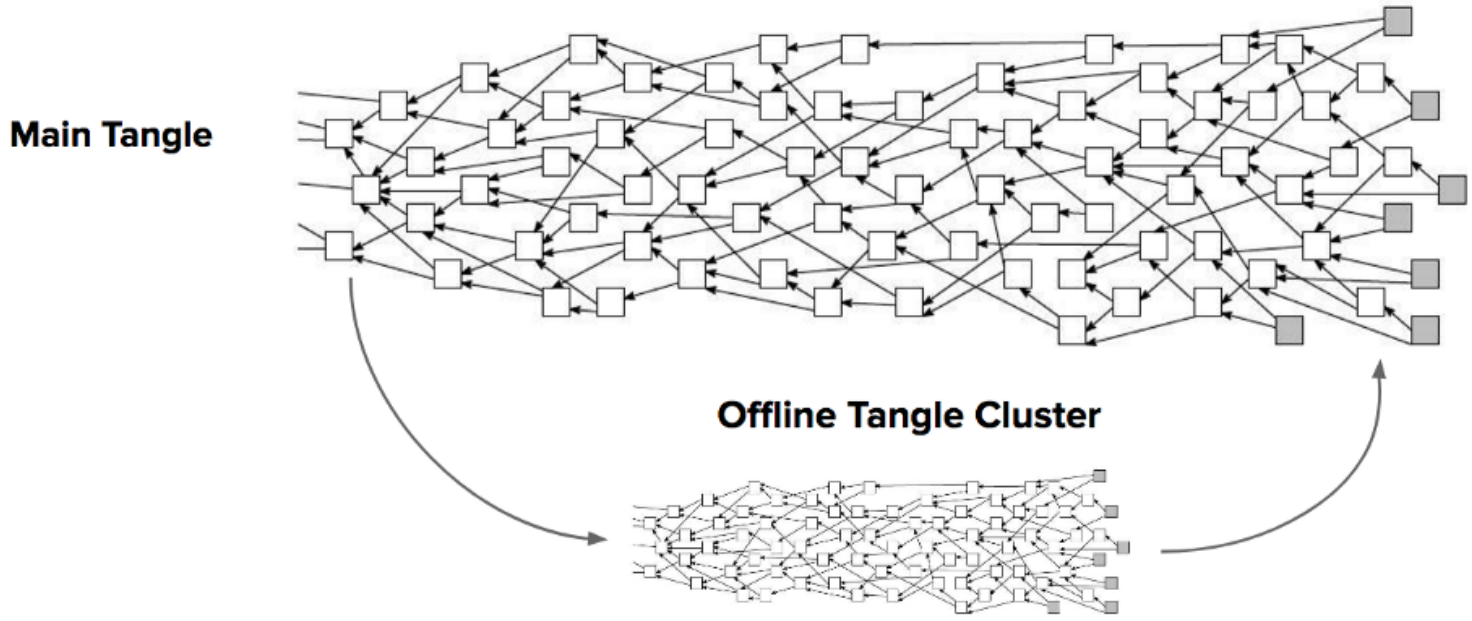
Some of the most recent stresstests have already shown Confirmed Transactions Per Second ***above 100 in smaller networks of less than 250 nodes***, with confirmation times of 10 seconds or less.

https://twitter.com/DomSchiener/status/858379721029111808

It Scales!



Offline Transactions (Partitioning)



Offline Transaction (Partioning)

The beauty of the Tangle is that you can fluidly branch off and back into the network.

This partitioning is key in being adaptive to the rigorous requirements of an asynchronous IoT environment. There is no such thing as always-on connectivity, as such you need to be able to make transactions and secure data even in an offline environment.

IOTA makes it possible for a cluster of devices to branch off and still make transactions in an offline environment; utilizing different communication protocols (ZigBee, Bluetooth LE, etc.) for the P2P communication.

Machine Economy

Machine Economy

The main reason why IOTA was created is to enable and to be the backbone of the Machine Economy.

They envision a future where Machines trade resources (computation, electricity, storage, bandwidth, data etc.) and services with each other without the involvement of any third party—purely Machine-to-Machine.

As the Internet of Things starts unleashing itself, the need for “Smart Decentralization” is apparent.

Towards **Smart Decentralization**

Dumb Decentralization

- "Dumb" devices
- No connectivity / sharing of data
- Human mediators

Smart Centralization

- Smart devices, dumb network
- Cloud as decision maker

Smart Decentralization

- Data Sharing
- Local Real-time Decision Making
- Smart adaptive and intelligent network

Use Cases

IOTA as the economy of IoT

Let’s dive into the sea of possibilities that will be enabled through ubiquitous technological resources and a market driven economy through IOTA.

Technological resource trade

One of the primary effects that IoT’s arrival will have on society is the distribution of resources. As the number of devices grow they will both enable, but also require a lot of technological resources.

Management of said resources is key. For IoT to truly work it needs openness and interoperability, even between competitors.

There is no reason to think that companies will spontaneously adopt an altruistic business model, so a market economy will organically arise. Here we’ll look at some of the use cases where IOTA transactions will be necessary and useful.

Use Cases

Distributed Computing

As our homes, streets and cities become immersed in an endless sea of sensors and actuators there will be an incessant demand for computational power to analyse the perpetual influx of data from these sensors. Sending it back to the cloud for analysis is too costly due to bandwidth limitations and latency. Instead the cloud must include these edge devices.

This means that we'll see a combination of smart sensors where the computational ability is packed into the sensor itself (Mist Computing) in combination with processing stations being spread out (Fog Computing). IOTA micro-transactions enable Party A's sensor data to be processed by Party B's processors in real time. In return Party B can use the iotas it gets compensated with to buy data from Party A or any other technological resource from another party in this symbiotic ecosystem.

Additionally research projects such as BOINC can use iotas to incentivize people with idle processors to participate in research.

Use Cases

Distributed Data

There will be tens of billions of sensors in our world by 2025. There is no reason why this data should only be made useful by one party. However due to physical limitations of bandwidth, storage and energy, as well as upfront hardware cost, it’s unlikely that this real time data will be shared freely unless the owners of these data gathering sensors gets compensated.

As we have seen in the aforementioned distributed computing scenario the owner of one technological resource can trade it in a free market through IOTA to purchase some resource they need.

This also means that companies can pay individuals for sharing direct data that will be of value to the companies either through product development or marketing, removing subjectivity and allowing for accurate analysis of the market.

Use Cases

Distributed Storage

Just like there will be an excess of computational power spread around as a result of the proliferation of devices, so will there be a vast amount of unused storage. This idle storage resource could easily be made useful, again with real time compensation taking place via IOTA.

Use Cases

Distributed Bandwidth

One of the biggest obstacles facing a seamless IoT system is the issue of interference. Everyone has had the annoying experience of a neighbouring internet connection interfering with ones own, which leads to disconnects and lag. For leisure it’s annoying, for industry and societal infrastructure it can be extremely costly.

Through micro-transactions one can compensate and incentivize sharing of the network, bringing down the number of total active nodes in a confined area and thus reducing interference.

Use Cases

Distributed Energy

With the ongoing adoption of residential solar panels and projects such as ***Google's Project Sunroof*** and ***Tesla's Powerwall***, it's possible to glimpse a future where energy is more distributed. Again real-time compensation for sharing of this technological resource will enable new innovations and a fairer existence for all.

In the coming age of wireless energy, it's easy to imagine solar panels selling electricity to sensors in the shade.

https://www.google.com/get/sunroof#p=0
https://www.tesla.com/powerwall

Use Cases

IOTA’s unique feature of feeless transactions enables a plethora of use cases that are not possible on any other platform. Not only do they enable true micropayments (send 1 cent, receive 1 cent), but they also improve existing and enable new data integrity use cases. With the introduction of more IXI modules they will further increase the usability and the use cases enabled by IOTA.

The main industries where thery are running case studies are Mobility, Energy, Smart Cities and Infrastructure (such as smart grids). Even though they mainly focus on the Internet of Things and the Machine Economy, IOTA is well suited for payments between humans as well. Especially if we look at remittances, where they want to be able to transact even a few dollars from Country A to Country B; IOTA has a unique offering.

Thank You For Listening!