CrushCrypto

Deep Dive into IOTA (MIOTA)

An Open-Source Distributed Ledger

September 7, 2018

What is IOTA?

- IOTA is a public distributed ledger that utilizes an invention called the Tangle at its core. The tangle is a new type of distributed ledger based on a directed acyclic graph, meaning there are no blocks, no chain, and no miners.
- IOTA was initially funded through a December 2015 crowdsale where approximately $500,000 worth of Bitcoin and other cryptocurrencies was raised. All of the token supply was issued to the crowdsale participants, with no tokens reserved for founders, developers, or advisors.
- Considering the team did not allocate any tokens for themselves, the community decided to support the project's vision by donating roughly 5% of the IOTA supply to the non-profit IOTA Foundation.

The IOTA protocol

- The IOTA protocol aims to enable this machine economy by enabling feeless machine-to-machine payments and provide a scaling solution for the upcoming growth of the Internet of Things (IoT).

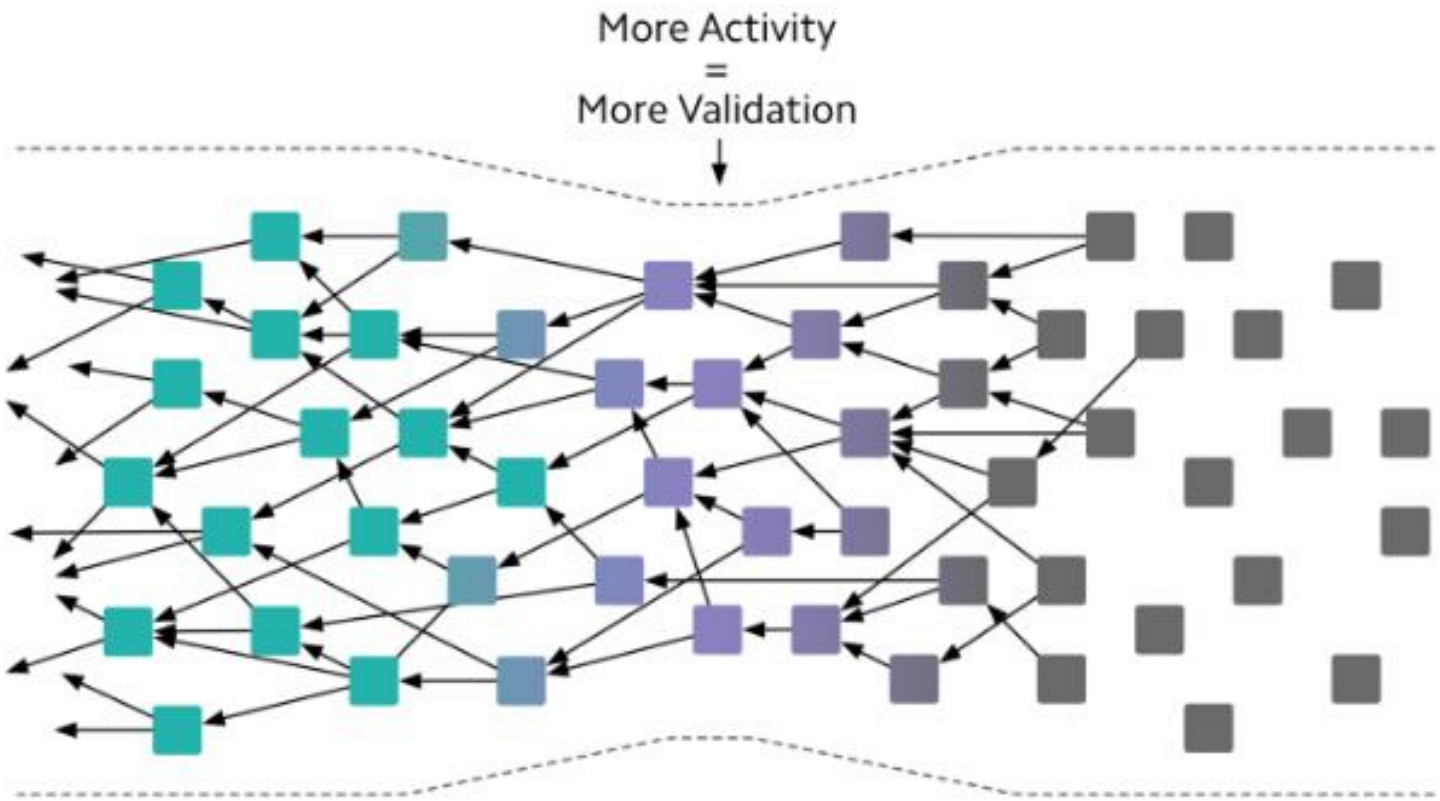
The Tangle

- The Tangle is a new data structure based on a directed acyclic graph (DAG) created specifically for the IOTA protocol.
- A directed acyclic graph is a complex data structure that moves in one direction without looping back onto itself. Here is an explanation that breaks it down further:
- A graph is a structure of nodes that are connected to each other with edges. Directed means the connections between the nodes have a direction, e.g. A → B is not the same as B → A. Acyclic means non-circular, where moving from node to node along the edges means you never encounter the same node twice.

The Tangle (continued)

- The IOTA Tangle is a DAG where the connected nodes are transactional data and consensus is an intrinsic part of the system. Instead of a blockchain, where consensus is decoupled and requires miners, a transaction on the Tangle must confirm two previous transactions – resulting in a decentralized and self-regulating peer-to-peer network.
- This is how IOTA transactions will always remain feeless, regardless of how large the network grows. There are no miners to pay because the person sending a transaction is required to use a small amount of their computing power to confirm two previous transactions.

The Tangle (continued)



Key features

- **The Tangle**
- **Zero transaction costs**: The inner-workings of the Tangle provide the means for transactions that require no fees on either end of the transaction. This gives it an advantage over blockchain, especially for micro-transactions that occur rapidly on the Internet of Things.
- **Scalability**: Unlike blockchain-based networks, the Tangle becomes more efficient as more users and transactions enter the network. Bitcoin, Ethereum, and other blockchain networks are facing major scaling challenges that IOTA will not have to deal with in the future.

Key features (continued)

- **Fixed token supply**: There is no inflation within the IOTA protocol, meaning no new tokens will ever be created. The IOTA supply is forever fixed at 2,779,530,283,277,761.
- **Quantum resistant**: Although quantum computers have only been theorized and not actually built, they will likely have a large impact on systems that rely on cryptography (specifically hash-based signatures) in the future. However, IOTA uses the Winternitz one-time signature scheme (W-OTS) which has been researched as existentially unforgeable.

Historical milestones

2016

First IOTA Foundation grant of $5,000 for API libraries is announced.

The IOTA JavaScript Library is released as the first IOTA library.

IOTA Testnet is announced for community experimentation with the protocol.

IOTA GUI is released.

2017

Community made IOTA mobile wallet, IOTA Learn is released.

IOTA Ecosystem Fund is announced, worth around $10 million and designed for fostering the growth of IOTA.

The first exchanges began to list IOTA.

IOTA is selected by the Tokyo Metropolitan Government to participate in their accelerator program.

2018

Collaborations announced with InnoEnergy, UNOPS, Audi Think Tank.

IOTA joined the Mobility Open Blockchain Initiative (MOBI).

Trinity mobile and desktop wallet beta is released.

EU Commission gave approval for IOTA and the European Smart City Consortium to work together on creating smart positive energy cities.

Future development

- On the R&D side, the IOTA Foundation is working on advancing the IOTA infrastructure, network decentralization, Dapps, cryptography, and adoption/usage of IOTA.
- There are 18 projects being worked on by the IOTA Foundation (see table to the right).

Coordicide	Analysis, modeling, and simulations for coo-less IOTA.
Crypto Spec	A detailed spec of cryptography in IOTA, intended for peer review.
Consensus Spec	A detailed spec of the IOTA consensus mechanism, building on the outline in the whitepaper.
Attack Analysis	Simulation and analysis of known network attack vectors.
Qubic	Enabling oracles, outsourced computations, and smart contracts on the Tangle.
Local Snapshots and Permanodes	Enabling node operators to maintain or dispose of the Tangle history as they see fit.

Trinity wallet

- The team is currently working on desktop, mobile, and cross-platform updates for Trinity wallet such as node quorum, encrypted QR, multi-language support, and more.
- The Trinity roadmap provides more details on what is being built and what has been completed.

The IOTA Foundation

- Founded in June 2016, this 2017 by Dominik Schiener and David Sonstebo. The foundation never received an initial allocation of IOTA tokens, instead receiving roughly 5% of the total supply as donations. This supply of tokens acts as an endowment fund for the IOTA Foundation.
- The primary goals of the IOTA Foundation are research, development, education, and standardization of the economy of things. The foundation is governed by a formal charter including a governing board, supervisory board, and advisory board.

Team and advisors

David Sonstebo

Co-Chairman of the Board & Founder

A serial entrepreneur who previously founded a stealth hardware IP start-up that developed a low power processor for the internet of things. He co-founded the IOTA Foundation in 2017.

Dominik Schiener

Co-Chairman of the Board & Founder

An entrepreneur from Italy who founded companies including Fileyy, Bithaus GmbH, and Finhaus Ltd before co-founding the IOTA Foundation.

Lewis Freiberg

Head of Ecosystem

Has been in the commercial software industry for 8 years and has been in the distributed ledger technology (DLT) industry since 2013. His current role is to promote innovation and understanding of IOTA and its technologies.

Edward Greve

Head of Engineering

Previously worked as a software engineer at Glossika and WillowTree inc. He connects math, computer science, and business needs together with the engineers who will push IOTA forward.

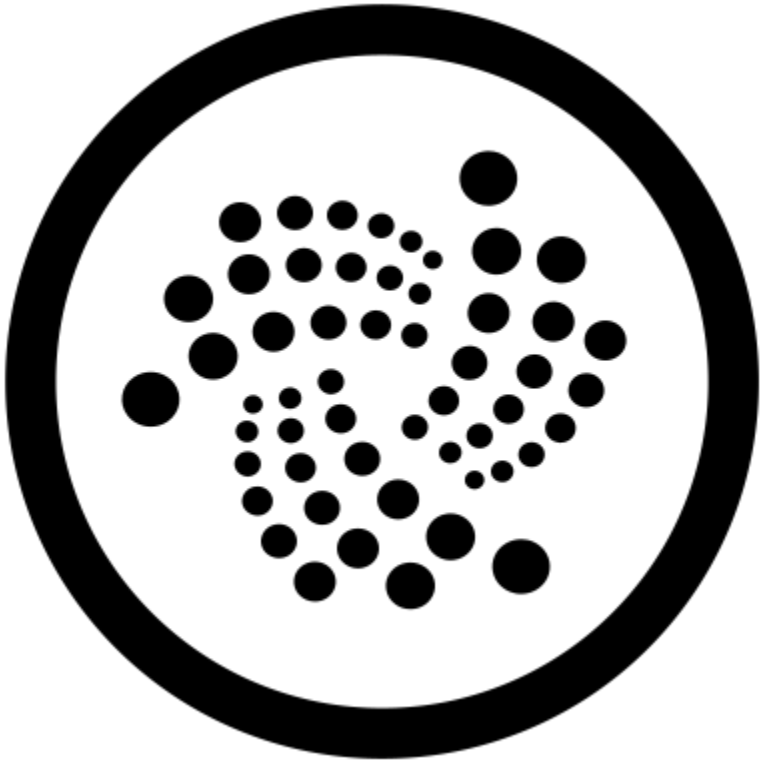
Holger Kother

Head of Partnerships

Worked at multinational corporations for the last 15 years, driving projects and IT services. At the IOTA Foundation he manages the interfaces between the foundation, partners and integrators.

Token economics

- IOTA is the native token of the IOTA protocol and has a fixed supply of 2,779,530,283,277,761.
- Considering the high supply, the protocol uses denominations such as Megalota (MIOTA) valued at 10^6 IOTA, and Gigalota (GIOTA) valued at 10^9 IOTA.
- Sending IOTA will never require a transaction fee, and the token is designed for use as a payment network between machines on the Internet of Things. The Tangle provides the means for IOTA to act as a better micro-payment currency than blockchain based assets such as Bitcoin.

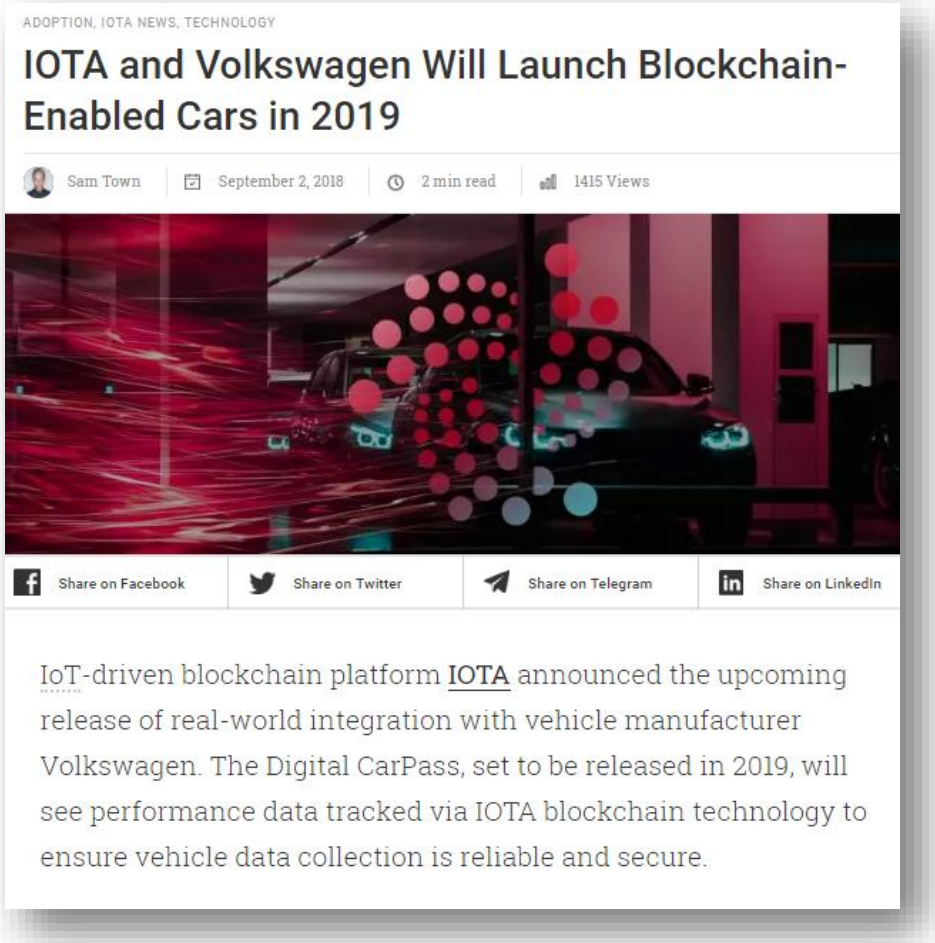


Strengths

- The Tangle is an innovative new technology that allows for global feeless payments, meaning IOTA is well-equipped for micropayments and machine-to-machine value transfers on the Internet of Things.
- IOTA has no inflation and will have a fixed supply forever. This is beneficial for long term token holders from a token value perspective.
- The IOTA protocol is designed such that scalability increases as more transactions occur on the network. In addition, the time between placing a transaction and validating approaches zero as the network reaches a large enough size.

Strengths (continued)

- The biggest partnership IOTA has is with Volkswagen. Volkswagen's Head of Blockchain has stated that the Digital Carpass program is scheduled to launch in 2019. This is a validation to IOTA's technology and can bring real-world adoption to the cryptocurrency.
- IOTA's crowdsale raised a reasonable amount of money at $500,000, much less than many other recent ICOs have been raising. They did not have large pre-sale bonuses and did not allocate any tokens for the team. The crowdsale was performed in a fair manner that incentivized community building over profit.


ADOPTION, IOTA NEWS, TECHNOLOGY

IOTA and Volkswagen Will Launch Blockchain-Enabled Cars in 2019

Sam Town | September 2, 2018 | 2 min read | 1415 Views

Share on Facebook | Share on Twitter | Share on Telegram | Share on LinkedIn

IoT-driven blockchain platform IOTA announced the upcoming release of real-world integration with vehicle manufacturer Volkswagen. The Digital CarPass, set to be released in 2019, will see performance data tracked via IOTA blockchain technology to ensure vehicle data collection is reliable and secure.

Weaknesses

- Unlike blockchain-based systems such as Bitcoin and Ethereum, the difficulty of proof o work is not adaptive on the IOTA network. This means the security of the Tangle depen directly on how many transactions are being processed and there is no way to adapt the security level to real-world conditions.
- IOTA co-founder Sergey Ivancheglo claimed that a flaw in their curl hash function was deliberate and designed as "copy protection" to prevent projects from copying them. This was a hostile act towards the open-source community, and implied that IOTA was not willing to make their real codebase freely available for the advancement of the technology.

Weaknesses (continued)

- IOTA's goal to serve as a machine-to-machine payment network means that there will b a high velocity of money on the network. This could hurt the value of IOTA as a long-term investment because the currency will act less as a store of value.
- Leaked transcripts from August 2018 uncovered a fallout between Sergey Ivancheglo, Dominik Schiener, and other IOTA founders. Ivancheglo stated "I don't longer trust Domink Schiener and I think he should quit the IOTA Foundation for the better future of IOTA". The foundation has since released an explanation about the situation, blaming pent-up emotions for the fallout. Dominik did not resign because of this situation, but it may highlight the potential for future issues within the IOTA Foundation.

Weaknesses (continued)

- Side Tangles, also known as parasite chains, have previously impacted the confirmation rate of IOTA transactions. These parasite chains are the result of a spammer using modified software to select tips that only reference themselves, and have brought the IOTA confirmation rate as low as 6%.
- The protocol uses a numeral system called balanced ternary, containing the 3 digits -1, 0, and 1. IOTA is built to run on existing hardware and communication networks, which all use the binary system. This means all its internal ternary notation must be encapsulated in binary, leading to increased storage and computational overhead.

Conclusion

Overall Rating: C

- IOTA is one of the more unique projects in the cryptocurrency space considering their invention of the Tangle and lofty goal to become the main currency for the Internet of Things.
- The Tangle is beneficial because it provides the means for feeless transactions, is theoretically quantum resistant, and extremely scalable.
- Nevertheless, there are some major security concerns with the protocol, such as side Tangles that can disrupt the transaction confirmation process. The IOTA network is still at an experimental stage and rigorous testing will be needed going forward to ensure it can act as a machine-to-machine payment system for the internet of things.

Conclusion (continued)

Overall Rating: C

- Also, as IOTA is used as a currency for machines and machines do not generally store a high balance, IOTA would suffer from a high velocity of money. The high velocity that IOTA is designed for could hurt its token value.
- The team's hostility towards the open source community is a big issue in an ecosystem where open source principles are the driving force behind community building, especially for developers. They will have to get around this or change their attitude toward open source technology to attract developers across the world.

Conclusion (continued)

Overall Rating: C

- The founding team has also shown that there is significant distrust between some members, and they might not be able to continue working well together in the future. This is a big concern considering that team members in a startup work closely together and communication is paramount to the coin's success.
- However, the IOTA Foundation is doing a great job on the business development side, securing partnerships with major corporations and working hard to advance the adoption of the IoT. They have a strong network of support that will greatly benefit them if the Tangle is improved and established as a secure distributed ledger.

Additional resources

- Website: https://www.iota.org
- Whitepaper: http://iotatoken.com/IOTA_Whitepaper.pdf
- Blog: https://blog.iota.org
- GitHub: https://github.com/iotaledger
- Technical documentation: https://iota.readme.io/docs
- Twitter: https://twitter.com/iotatoken
- Facebook: https://www.facebook.com/iotatoken/
- Reddit: https://www.reddit.com/r/Iota/
- IOTA Tangle explorer: https://thetangle.org/

CrushCrypto