IOTA Research Report

Table of contents

Table of figures

Introduction

IOTA is a communication protocol based on the distributed-ledger-technology with the goal to provide a secure data and value exchange in the world of IoT (internet of things). Through the waiver of transactions costs the protocol should be established for micro transactions and an automated information transfer (IOTA (2021e).

In contrast to Ethereum or Bitcoin IOTA works with Tangles instead of connected blocks containing the information. This system has neither blocks nor miners. When a transaction is sent it validates two other transactions, this allows to overcome the cost and scalability limitations of the blockchain. The Tangle, IOTA's network, immutably records the exchange of data and value. It ensures that the information is trustworthy and cannot be tampered with nor destroyed. The protocol uses a DAG data structure allowing transactions to be added in parallel, unlike blockchain alternatives (IOTA (2022e)).

Blockchain vs. Tangle

In a blockchain new transactions can only be attached to a single new block. This block follows a previously produced one and is directly cryptographically linked to it. Transactions in a blockchain can only become part of the ledger, if they are included in a newly issued block. In nearly all blockchains, the block producers can decide which new transactions they prefer to include and confirm in the blocks they produce. This leads to competition between the freshly issued transactions to become part of a new block. The fee-based structure (proof of work) of those blockchains favours the user's willingness to pay a higher fee for transactions as these are more likely to be included in the new block than those offering a lower fee.
The Tangle does not have any block producers, and therefore every user is free to issue new transactions and attach them on different parts without an entity that acts as middlemen. The Tangle is not a single chain of blocks that follow each other but rather a network of parallel processed transactions. These transactions offer many different points for new issued ones to be attached, which dramatically speeds up the processing of transactions. Every node in the network is free to attach new data points to the network at any time. Simplified, no entity is needed to decide when and whether those transactions get included if they follow the basic rules of the protocol (valid signatures / no double spending of funds). Those transactions will become part of the ledger by just issuing them to a node.
Opposite to that, a blockchain transactions must be included in a block by a block producer. These are entities that collect new issued transactions, validate them and include them in the next block. A Blockchain must always select a "winner" as a block producer to attach a new block to the blockchain. Only this single block producer will earn all the fees of the transactions that are part of the issued block and earn the reward in the form of newly created tokens for producing the block. This is also seen as a form of centralization in blockchains, as you need middlemen that process your transactions. Regular users are not allowed to write directly to the ledger, which leads to the well-known "miner race", where only the miner with the highest computational processing power has a reasonable chance of becoming a block producer and is allowed to attach a new block including their processed transactions to the ledger. All the electricity used by the other miners in this race of solving the cryptographic puzzle needed to

fulfil the proof of work requirements while producing the current block has been wasted, as their attempted blocks are never becoming part of the blockchain (IOTA (2022b)).

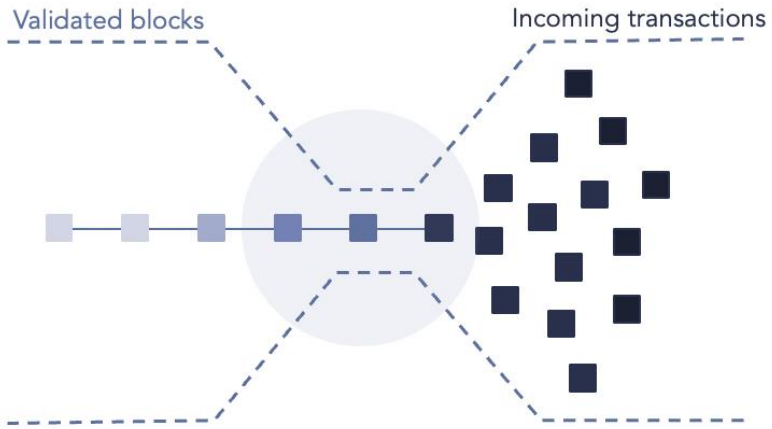

Figure 1: Bottleneck in the Blockchain (own illustration)

IOTA, in contrast, is generally a leaderless protocol. It does not require any middlemen to include transactions into the Tangle. Everyone is free to attach transactions if they are following the basic layout design of the protocol. There is no need to elect a leader as the Tangle can implement new transactions in parallel processing. IOTA is therefore a multi - threaded ledger. This is one of the reasons why IOTA can reach a very high transaction throughput and remains feeless.

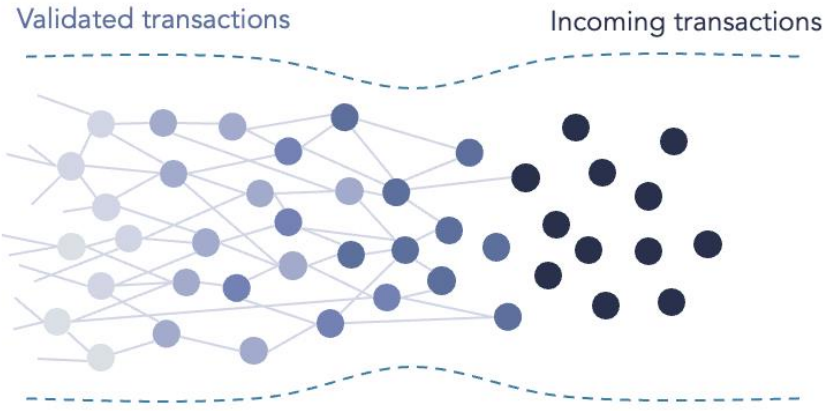

Figure 2: Tangle structure of IOTA (own illustration)

The Tangle data structure is a directed acyclic graph (DAG), where each message is attached to 2-8 previous ones. Rather than being limited to a single place, for attaching new messages, these get attached to different places in front of the tangle. The protocol can process these various attachments in parallel and the messages that will be connected are requested from a node. The node selects these messages by using an algorithm called Uniform Random Tip Selection (URTS). This algorithm selects between one and eight valid tip messages that lead to a valid ledger state. After this, the tip selection Proof of Work (solving a puzzle) needs to be

done to discourage spam messages. These attached messages must contain this proof of work (PoW) validation to prevent clients sending spam messages and putting too much work on the nodes. The PoW can be done remotely trough a random node, the local device that sends the message, or through a device that is neither a node nor the clients device.
Thereafter, the message will be sent to a node that will attach it to the tangle. For a node to issue a massage, it must at least verify two other messages, thereby maintaining the feeless feature and speed of the service (IOTA (2022b)).
All IOTA nodes validate messages and use different functions to reach consensus. Currently, messages will only be considered valid if they reference a milestone. Milestones are issued by a special central IOTA network node (the Coordinator) and these are collectively recognized and accepted by users as a signal for a secure and final transaction. Although network participants generally accept it, the Coordinator is not able to stop transactions in the network, which is why it is a potential single point of failure (IOTA (2021e)).
But the Coordinator is just a temporary solution. In the Coordicide project IOTA will design a new protocol which will eliminate the coordinator and then be released in the upcoming IOTA 2.0 Network (IOTA (2022d)).

IOTA Mainnet

The current IOTA network (IOTA 1.5 Chrysalis) is used by companies, organizations and other actors that explore or rely on business cases that require feeless (micro) transactions, originally designed for the internet of things. Currently, the IOTA mainnet allows roundabout 1,000 feeless data and value transactions per second (tps). The IOTA Token is the current native currency with a non-inflationary supply of 2'779'530'283'277'761 IOTA Tokens, that are traded in millions (MIOTA) at major exchanges. The node software in the mainnet, Hornet and Bee are available through the programming languages Rust and Go. The IOTA foundation, which is currently with the coordinator, focuses on the development of a fully decentralized, permissionless and leaderless consensus algorithm, which is already being tested in the IOTA 2.0 DevNet (IOTA (2021e)).

The next major milestone for the IOTA mainnet will be the integration of new output types for the base layer, included in the recently introduced Tokenization framework, that allow the IOTA ledger to become a multi-asset ledger managing several native tokens in the same ledger as the IOTA token (IOTA (2021e)). Following that will be the integration of IOTA Smart Contracts in the mainnet which are currently only running as a beta version on the DevNet 2.0. The long-term goal is the removal of the Coordinator as Coordicide protocol that is currently pending proper validation in IOTA's staging network, Shimmer (IOTA (2021c)).

IOTA 2.0 DevNet

The IOTA 2.0 DevNet features the new consensus mechanism (Coordicide), designed to fully decentralize the IOTA network. The DevNet, released in June 2021, is built as a public testing ground that allows developers and their community to test different scenarios and improve features continuously to optimize the upcoming, fully decentralized version of the IOTA mainnet (IOTA 2.0). Currently, the network is also limited to 1,000 tps (IOTA (2021e)).

The IOTA 2.0 DevNet offers smart contract capabilities in the form of the beta version, allowing for permissionless deployment of different virtual machines like EVM and Solidity and it can also be written with programming languages like Rust, TinyGo or Typescript. The Tangle serves as a layer 1 for the IOTA Smart Contract DevNet that ledgers on top as layer 2 and runs currently by Wasp nodes. The IOTA 2.0 DevNet also contains the first version of the Tokenization framework (IOTA (2021d))
Without further detail, the IOTA foundation developed various components and functionalities to ensure that the network remains decentralized and runs without a central node. Major features are listed below:

- The Fast Probabilistic Consensus (FPC) for permissionless and decentralized voting
- Fast finality using MANA based approval weight
- Using MANA as low energy Sybil protection system
- Fair access through leaderless IOTA Congestion Control Algorithm
- Save network connections through a secure Autopeering system
- Efficient algorithms using a parallel ledger state

IOTA is also providing a visualizer to see the current DevNet 2.0 in action and understand the Tangle's structural behavior. (IOTA (2021b))
While there is no Coordinator in the IOTA DevNet, the system uses a Nakamoto-style consensus on the directed acyclic graph (DAG) to ensure that only valid messages are attached, without outsourcing security to the miners, nor spending huge amounts on energy for security through PoW. The system works in a cycle to determine which branches of the system will survive to maintain a consistent ledger state. The cycle is explained below:

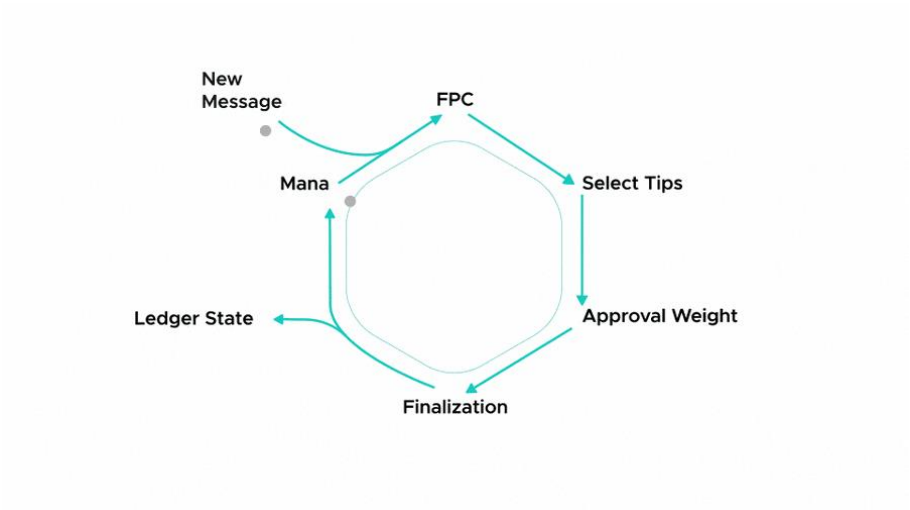

Figure 3: congestion control algorithm of IOTA (IOTA (2021b))

If a conflict occurs, nodes vote on it through the voting protocol (FPC), which branch should be rejected. This protocol is protected from attackers through MANA ("virtual good behavior points"), a reputation system which fairly limits the nodes that are allowed to vote. After the bad branches have been rejected, tips are selected for new messages on the correct branch. As the correct branches are gaining more messages their approval weight grows. And as soon

as one branch gets enough approval weight the transactions are finalized and added to the new ledger state. MANA is updated determining the next FPC voters (IOTA (2020)).

Shimmer Network

The Shimmer network is going to be the younger brother of the IOTA 2.0 DevNet, based on the consensus mechanism currently tested in the IOTA 2.0 DevNet. The current node software they use is Hornet and later probably also Bee. Shimmer will act as a validation network for any IOTA features before they are integrated into the mainnet. Therefore, upgrades can be tested, audited and reviewed by the community making faster releases on the mainnet possible. Like the current IOTA mainnet, Shimmer offers feeless microtransactions but access to the network will be regulated through Mana (Shimmer (2021)).
Also, a big difference to the IOTA 2.0 DevNet is Shimmer's fixed ledger. The Shimmer network is designed as a real decentralized staging network and not as a controlled environment test net. That is why the ledger state will not be reset as soon as new upgrades are made available. Due to that, it allows for the validation of new modules in a real-life scenario and the token to be listed on cryptocurrency exchanges.

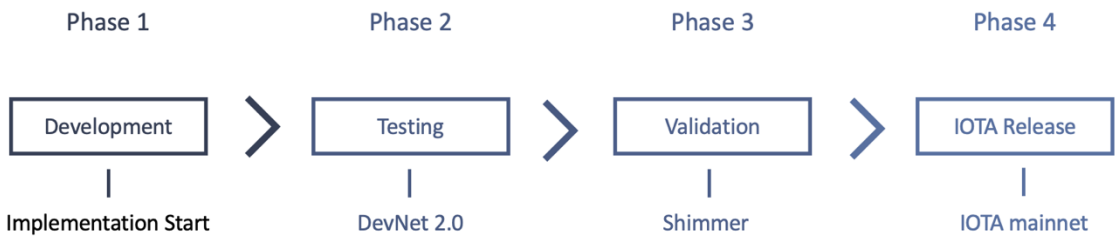

Figure 4: Development to market of new features (own illustration)

Every new development will go through four phases: new features are developed in phase one, the implementation start. In the second phase the upgrades will be tested in the controlled test net environment, the DevNet. Then these are going to be validated in the real-life public environment, the shimmer network, before they are going to be released in phase four to the IOTA mainnet (Shimmer (2021)).
In the beginning the Shimmer network will start out with the current features of the IOTA Chrysalis mainnet and will gradually be upgraded with modules of the IOTA 2.0 DevNet after they have been tested. Due to the absence of miners a feeless and energy efficient system of less than a billionth of a kWh for an IOTA transaction will be build (compared to approximately 2,000 kwH / one ton of CO2 for a single BTC transaction). That means that one bitcoin transaction will be able to power around 600 million to 1 billion IOTA transactions (IOTA (2021a)).

Assembly Network

Assembly is a permissionless multi-chain network for smart contracts that adds fully decentralized and scalable smart contract capabilities to the IOTA ecosystem. It is anchored to the feeless base layer of IOTA, that serves as layer one and therefore allows smart contract chains to write their blocks in parallel to the tangle on layer two ("off-Tangle"). The unique architecture fully parallelizes the execution of smart contracts, enabling the entire network to scale horizontally. The more smart contract chains there are, the more transaction throughput on Assembly is possible. Anyone can create their sharded smart contact chain, while defining their own parameters, virtual machine (VM) and validation requirements as well as their own customized fee and incentive structures. That is why smart contracts on Assembly can run theoretically feeless, due to their own governance functions and configuration parameters. As the novel architecture is built on IOTA smart contracts, the protocol currently runs on Wasp nodes (and not like IOTA Smart Contracts on GoShimmer Nodes). Assembly will have full EVM (Ethereum Virtual Machine) compatibility and will thereby be able to transfer Solidity smart contracts to the new network. WASM (WebAssembly) will be supported as well using multiple source languages such as Typescript, Rust and TinyGo (Assembly (2021a)).
The network has its own native ASMB token with an initial supply on 100 billion and an inflation of 8%. Thereof 70% will be distributed to the community, currently through staking IOTA tokens (IOTA (2022a)). Because Assembly relies on proof of stake, the ASMB token plays an essential role in the Sybil protection and security. Token holders can stake their ASMB and become validators themselves or delegate their stake to a validator. Stakers and validators are in general compensated with staking rewards, transaction fees, or other token incentives defined by the smart contract chains (Assembly (2021a)). But when a validators misbehavior is detected, their stake gets slashed (burned), the protocol rotates the validators, and their trust score drops (Assembly (2021b)). Becoming a validator requires only running an operational node and a small amount of the native ASMB token at stake (Assembly (2021a)). In the following infographic the context of the Assembly network architecture is explained:

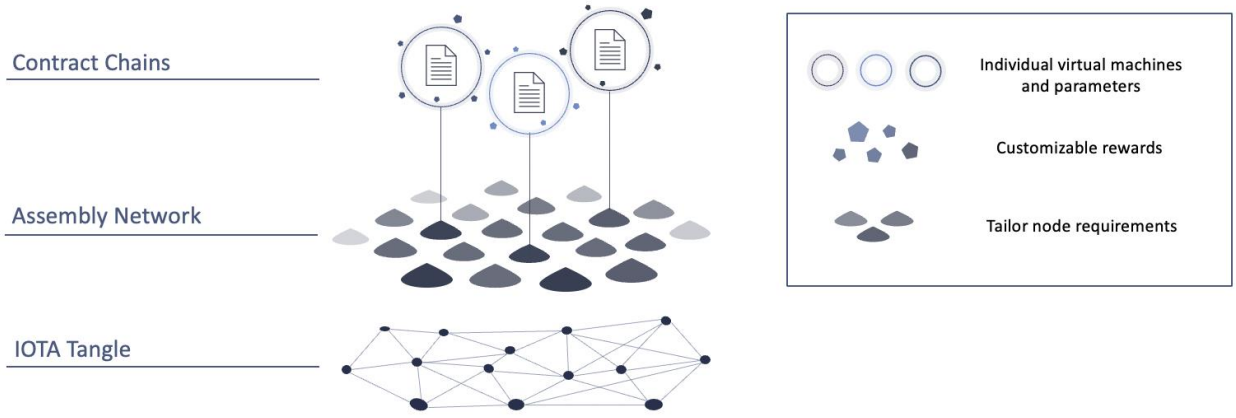

Figure 5: Layer structure of Assembly on IOTA (own illustration)

In other words, IOTA's base layer is the anchor for Assembly. This is the is the governance layer for the permissionless ecosystem/market of IOTA Smart Contract chains and their validators, who execute smart contracts (IOTA (2021e)).

Current Status

Currently IOTA has a circulating supple of 2'779'530'283 MIOTA token with a current value of around 0.769 USD, that results in a market cap of 2'137'420'189 USD. In comparison to other platforms the market cap dominance is around 0.11% and therefore the network is located in 59th place of the market cap rank (Coingecko (2022)). Currently 76.6% of the Chrysalis network tokens are at stake (Chrysalis (2022)).
The Network Chrysalis 1.5 is currently running, but by now still with the coordinator in place. Several steps like the On-Tangle-Voting feature or the improved congestion control were released on the DevNet 2.0, but even more will need to follow, like the Local Snapshots, Timestamp Voting and many more, to let the upcoming IOTA 2.0 network run decentralized. Programmable smart contracts are currently available on IOTA 2.0 DevNet with basic support for EVM and Solidity. Upcoming goals are the Extended EVM & Solidity Support with Native asset support and cross chain communication that should be released soon and the support for Chrysalis, which includes the anchoring of smart contracts in the Shimmer mainnet. Later goals like the Tokenization Framework Integration should follow soon according to the roadmap of IOTA (IOTA (2022c)).
Currently there are four more days left to stake IOTA token and receive therefore free ASMB tokens of Assembly and free Shimmer tokens in the first 90 day staking phase. In the Assembly network will be an initial total supply of 100 billion ASMB tokens of which 70% will be distributed to the community (20% to IOTA stakers over next two years and 50% to community governed DAOs (decentralized autonomous organizations), developer, governance incentives and in the form of grants). Assembly's development is largely connected to the IOTA smart contract framework. There is no timeline yet to the launch of the Assembly mainnet. The project is currently in Phase one, the ASMB token generation, which will be followed by the launch of the network with one main open chain that runs on EVM and is secured by an open, permissionless committee (Main Assembly). Currently, tokens can be staked by validators, but smart contracts cannot be deployed easily yet. The final phase will be the creation of a multi-chain environment with further optimization (Assembly (2022)).
Same as Assembly, the Shimmer network has no official release date. As soon as the staging network is released, it is going to be used to speed up the development and implementation process for upgrades, that will eventually lead to the upcoming fully decentralized IOTA 2.0 (Shimmer (2022)).

Conclusion

Due to the new architectural design the IOTA research foundation released in 2016 with the Tangle, a lot of attention was brought to the network. Especially when they announced that big tech firms like Microsoft and Google invested in their non-profit end of 2017 (CNBC (2017)). Although at that point, the technology they provided was not ready for the end consumer and there were still major problems, like the decentralization and technical implementations to

overcome. The IOTA foundation fell into disrepute for not delivering delayed or what was promised to the community. But since IOTA is a research foundation, they have always had the intention to provide the best final solutions. Even though it might take them longer to research or reinvent their current resolutions, they are not willing to take shortcuts. Nevertheless, the progress in IOTA Smart Contracts and the upcoming release of the Shimmer and Assembly Network seem very promising. IOTA Smart Contracts will probably be released on the mainnet this year, while the decentralization of the main network, IOTA 2.0, has surely to wait until 2023 or 2024. At the moment the network is not ready to run oracles of BCP securely and permanently, but hopefully will in near future.

List of references

Assembly, 2021a, Announcing Assembly and the ASMB Token from the website, https://blog.assembly.sc/announcing-assembly-and-the-asmb-token/, 8.03.2022.

Assembly, 2021b, Introduction: The World's at Scale from the website, https://wiki.assembly.sc/learn/introduction, 12.03.2022.

Assembly, 2022, FAQ – General question; Token distribution & economics from the website, https://assembly.sc/faq, 23.03.2022.

Chrysalis, 2022, Chrysalis network status from the website, https://chrysalis.iota.org/status, 23.03.2022.

CNBC, 2017, A little-known digital currency surges 90% after teaming up with firms like Microsoft from the website, https://www.cnbc.com/2017/12/04/cryptocurrency-iota-rallies-after-launch-of-data-marketplace.html, 22.03.2022.

Coingecko, 2022, MIOTA Price Statistics from the website, https://www.coingecko.com/en/coins/iota, 23.03.2022.

IOTA, 2020, Explaining Mana in IOTA from the website, https://blog.iota.org/explaining-mana-in-iota-6f636690b916/, 15.03.2022.

IOTA, 2021a, An Introduction to the Business Ecosystem of IOTA from the website, https://blog.iota.org/an-intro-to-the-iota-ecosystem/, 15.03.2022.

IOTA, 2021b, Chapter 2: Decentralized IOTA Explainer from the website, https://v2.iota.org/how-it-works/decentralized, 14.03.2022.

IOTA, 2021c, Introduction research report from the website, https://www.iota.org/foundation/research-department, 20.03.2022.

IOTA, 2021d, IOTA 2.0 DevNet (Nectar) - The Era of IOTA's Decentralization Starts Here from the website, https://blog.iota.org/iotav2devnet/, 11.03.2022.

IOTA, 2021e, IOTA x Shimmer x Assembly: A Comprehensive Overview of All Three Networks from the Website, https://blog.iota.org/iota-shimmer-assembly/, 16.03.2022.

IOTA, 2022a, Announcing Assembly and The ASMB Token from the website, https://iota-news.com/assembly/, 14.03.2022.

IOTA, 2022b, An Introduction to IOTA from the website, https://wiki.iota.org/learn/about-iota/an-introduction-to-iota, 18.03.2022.

IOTA, 2022c, interactive Roadmap of IOTA Research and Development from the website, https://roadmap.iota.org/smart-contracts - nextRelease, 23.03.2022.

IOTA, 2022d, IOTA 2.0 DevNet from the Website, https://v2.iota.org/, 17.03.2022.

IOTA, 2022e, Wiki – IOTA Smart Contracts from the website, https://wiki.iota.org/smart-contracts/overview, 23.03.2022.

Shimmer, 2021, Announcing the Shimmer Network and Token from the website, https://blog.shimmer.network/announcing-the-shimmer-network-and-token/, 20.03.2022.

Shimmer, 2022, FAQ – General questions; Token economics from the website, https://shimmer.network/faqs, 23.03.2022.