www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 7 Issue 4 April 2018, Page No. 23823-23826
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i4.05

IOTA-Next Generation Block chain

Divya M [1], Nagaveni B. Biradar [2]

1. B.E 4th Year, Dept. of CSE, RYMEC, Bellary, Karnataka (India)
2. Associate Professor, Dept. of CSE, RYMEC, Bellary, Karnataka (India)

Abstract-

IOTA is a revolutionary new, next generation public distributed ledger that utilizes a novel invention, called a “Tangle”, at its core. The Tangle is a new data structure based on a Directed Acyclic Graph (DAG). As such it has no Blocks, no Chain and also no Miners. Because of this radical new architecture, things in IOTA work quite differently compared to other Blockchains.

I. Introduction

IOTA was first conceptualized in 2014 and later founded in 2015 by David Sønstebø, Sergey Ivancheglo, Dominik _Schiener, and Dr. Serguei Popov. Several of the founders were working on a hardware startup with an IOT focus when they began to see the limitations of current options for IOT payments. They created IOTA as a solution to these problems.

II. Releated Work

The way a blockchain works is that a pair of addresses that want to transmit a message to each other must connect to a node. The node validates the transaction and forwards it to the miners so they can permanently record it on the blockchain. While this is a very powerful and reliable type of network, it doesn’t scale particularly well as transactions have to be processed sequentially and are therefore bottlenecked by the speed that the blockchain can be written.

There are a number of solutions being developed, including off chain payment channels like the Lightning Network, increasing block sizes such as what Bitcoin Cash does, or how Dash uses Master nodes to instantly validate transactions.

While these solutions may work, they don’t change the fact that blockchains don’t natively scale well. The tangle on the other hand was designed from the ground up to not only scale, but to actually get faster as demand on the network increases.

The way it does this is that instead of nodes and miners validating and recording transactions, each device attempting a new transaction in the tangle must first validate two prior transactions. Because of this set up, the more new transactions attaching themselves to the tangle, the more transactions get validated, thus increasing the speed of the network as demand increases.

As in all things, this system is not perfect. For a device to interact with the IOTA network, IOTA technology must be hard coded into the device’s CPU, which prevents existing devices to join the tangle. This change in the CPU structure, however, is not hard to implement nor is it expensive, and there are several global companies already committed to implementing IOTA technology.

The major difference that is worth mentioning (apart from the DAG vs. Blockchain) is how IOTA achieves consensus and how transactions are made. As mentioned previously, there are no miners. What this means is that each participant in the network that wants to make a transaction has to actively participate in the consensus of the network by approving 2 past transactions. This attestation on the validity of two past transactions ensures that the whole network achieves consensus on the current state of approved transactions, and it enables a variety of unique features that are only seen in IOTA.

IOTA is the missing puzzle piece for the Machine Economy to fully emerge and reach its desired potential. We envision IOTA to be the public, permission-less backbone for the Internet of Things that enables true interoperability between all devices.

IOTA as a platform is both a protocol and a currency. It’s a way for connected devices to talk to each other in a common language and to convey and transmit value.

III. Literature Survey

1. [KIMCHAI YEOW] This paper is motivated by the shortage of comprehensive reviews on decentralized consensus systems for edge-centric Internet of Things that elucidates myriad of consensus facets, such as data structure, scalable consensus ledgers, and transaction models. Decentralized consensus systems adopt either blockchain or block chainless directed acyclic graph technologies, which serve as immutable public ledgers for transactions. This paper scrutinizes the pros and cons of state-of-the-art decentralized consensus systems. With an extensive literature review and categorization based on existing decentralized consensus systems, we propose a thematic taxonomy.

2. [Serguei Popov] In this paper we analyze the mathematical foundations of IOTA, a cryptocurrency for the Internet-of-Things (IoT) industry. The main feature of this novel cryptocurrency is the tangle, a directed acyclic graph (DAG) for storing transactions. The tangle naturally succeeds the blockchain as its next evolutionary step, and offers features that are required to establish a machine-to-machine micropayment system.

IV. Working

The tangle is what is known as a directed acyclic graph (DAG): a data structure that moves in one direction without looping back onto itself. Like the Blockchain, the tangle is a distributed ledger, in which a network of independent accounts performs transactions among themselves, reaching consensus about who owns what without depending on a centralized authority.

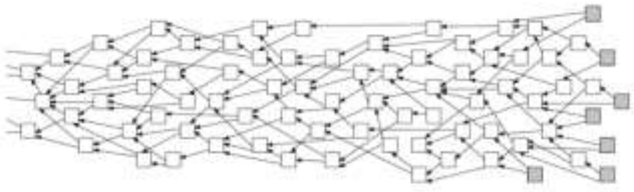

Fig 3.1: Tangle network

Time passes from left to right in this graph. In Fig 3.1 we see, each box represents a transaction issued by a device (or "node") on the network. In proof-of-work blockchains like Bitcoin’s and Ethereum’s, Popov writes, there are "two distinct types of participants in the system, those who issue transactions, and those who approve transactions"; in the tangle, every device works to maintain the ledger. Every node is also a kind of miner.

As a tangle transaction receives approvals, and the transactions approving it receive approvals in turn, the "cumulative weight" of that transaction builds up. Similar to confirmations for a Bitcoin transaction, higher cumulative weights indicate more reliably immutable transactions. The gray boxes at the far right of the diagram, representing recent transactions that have received no validations, are called "tips."

Since transactions are not being shared all at once as blocks, divergences are more prone to happen on the tangle than the blockchain. "It is important to note that the iota network is asynchronous," Popov writes. "In general, nodes do not necessarily see the same set of transactions. It should also be noted that the tangle may contain conflicting transactions."

Eventually, some conflicting transactions are "orphaned"—not completed—while others stand. The tangle relies on incentives to reach consensus about these transactions' fate. As the white paper points out, "if a node issues a new transaction that approves conflicting transactions, then it risks that other nodes will not approve its new transaction, which will fall into oblivion."

In order to find transactions to approve that are unlikely to lead its own transaction to be orphaned, a node runs a "tip selection algorithm." Iota's tangle doesn't mandate any algorithm in particular, but the white paper makes the case for the Markov Chain Monte Carlo (MCMC) variety.

Popov's MCMC algorithm would place at least two "random walkers" somewhere back on the tangle: not at the beginning (that would take too long), but not too recently (the quality of the selection would suffer). These move chronologically along the paths defined by validations, favoring paths linking transactions of similar cumulative weight. Say that transaction x (cumulative weight = 20) was approved by transaction y (= 19) and transaction z (= 3). The walker has a much higher probability of moving from x to y.

The rationale is that "lazy" nodes—ones that rarely issue transactions and therefore rarely validate others' transactions—will be at a disadvantage. Punishing lazy nodes is useful not just because it cuts down on free riders, but because lazy nodes pose a risk for double-spend attacks: the white paper describes several such attacks and the ways an MCMC could be used to defend against them.

Storage

Storage is an immediate concern for tiny, resource-constrained IoT devices. The white paper doesn't address this issue, but light bulbs and toasters clearly aren't able to store the entire tangle, as full nodes do the entire 153 GB Bitcoin blockchain or 338 GB Ethereum blockchain.

Iota's development roadmap, published in March 2017, describes solutions including automated snapshotting—similar in principle to pruning—and a swarm client, which would allow devices to shard and collectively store the database.

Decentralization

If a party controls more than a third of the tangle's hashing power, the network is insecure. Bitcoin and Ethereum are generally considered secure as long as a single party does not control a majority of the network. In other words, while blockchains are vulnerable to 51% attacks, the tangle is vulnerable to a 34% attack.

Iota's implementation does attempt to mitigate this vulnerability, however, by amassing hash power itself. The IOTA Foundation runs what it calls a "coordinator" node.

V. Advantages

- **Scalability**
  - IOTA's network structure should allow it to increase throughput as more nodes join the network.
- **Zero Fees**
  - Transactions on the IOTA network do not incur fees.
  - 1 MIOTA sent results in exactly 1 MIOTA received.
- **Decentralization**
  - In IOTA, users and validators are one in the same. There is no distinct set of miners or validators separate from users.
  - In theory, this results in more decentralized validation**.**
- **Quantum-Resistance**
  - IOTA is designed from the ground up to be resistant to the threat of quantum computing.
- **Strong community**
  - Something notable for IOTA is its community as well, having a huge slack user base new developers are able to find tons of experienced developers to ask questions to.
  -

VI. Disadvantages

- **Proof Of Work:** The tangle requires proof of work for it is security, this means that transaction generators will be spending money on electricity and chips, money that could be kept within the currency if it had POS security
- **No Smart Contracts:** Contracts that do not require transaction order finality, like a voting contract, could be implemented in the tangle, though there is little incentive for new transactions to confirm these more complex transactions as they require more computation to validate.

VII. Applications

1. **Micro transactions:** real-time micro transactions are enabled, giving IOT developers and web developers a brand new set of tools to reassess business-to-business opportunities.

2. **Data Transfer:** One of the core features of IOTA is the feasibility of transferring data through Tangle in a completely authenticated and tamper-proof way. IOTA gives users several options of transferring data without the

risk of any hacker attack. This seamless data transfer is a great benefit to establish reliable communication channels between devices.

3. **Voting:** The Tangle architecture is ideal for a variety of projects that require secure data transmission, especially in the realm of e-governance. A very important aspect of e-governance is e-voting, and many companies and academics have already started exploring the possibility of using Tangle in this field of use.

4. **Masked Messaging:** Masked authentication messaging (MAM) is the first extensible module of the IOTA core. This feature enables nodes (computers/smart devices) to transfer/exchange fully authenticated and encrypted data through Tangle.

5. **Share-A-Service:** IOTA will be driving this sharing economy into the future, where anything with a chip in it can be leased in real time.

6. **Solar Energy:** The use of IOTA in the solar industry is just one example of how IOTA can be used to power its way into the future. They believe IOTA is ideal for them because of its scalability, speed, robustness, and no fees.

VIII. Conclusion

The IOT aspect of IOTA is also quite interesting. Giving machines the ability to trade information, services, and goods for income is an interesting proposition using a transaction-free network. While IOTA was one of the first major projects to build a DAG instead of a blockchain, we find that the approach taken by the IOTA team presents many reasons to be highly concerned. DAG-based systems may form an important part of the future of the crypto ecosystem

It looks absolutely phenomenal and seems like it could solve many problems that blockchain has today. First coin with a cool new idea isn't always the one that ends up being successful in the end.

REFERENCES

[1] Serguei Popov “The Tangle”, October 1, 2017. Version 1.3 URL:http://iotatoken.com/IOTA_Whitepaper.pdf

[2] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues and K. Ko, "Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues," in *IEEE Access*, vol. 6, pp. 1513-1524, 2018.

[3] Iota Medium Blog Post, URL: https://blog.iota.org/the-tangle-an-illustrated-introduction-4d5eae6fe8d4

[4] Blog Post URL: https://steemit.com/cryptocurrency/@bikash08/what-is-iota-it-s-future-and-working-mechanism