Future Blockchain

IOTA

IoT (Internet of Things) has made immense progress from conceptual to deliverable aspect in the last couple of years. We started our digital era with sharing of files only, now it has turned into a stage where we can share anything as a digital product. From wearable gadgets to vehicles to home appliances, the objects that are connected to the internet are increasing exponentially. In the beginning, we were unable to share these physical entities through the internet now we are in the 4th industrial revolution where we can transfer anything in the world through internet.We know IoT is the network of physical devices like gadgets and home appliances, vehicles etc., But what is IOTA?

In simple words, IOTA is blockchain technology which enables the digital trans- action of IoT products across the network. The Blockchain technology is known as the future internet where IOTA (Internet of Things tAngle) is known as future Blockchain. Yes!!! These things are making the real technologi- cal revolution in the industry.

IOTA- a 'Block' less Blockchain IOTA provides a Blockchain for the Internet of Things. But the interesting thing is that there are no blocks in IOTA. Then how Blockchain is created? Then answer lays in another concept known as DAG (Directed Acyclic Graph) which is a directed graph without cycles. In IOTA there is no ledger as in normal block- chains instead they use a DAG called Tangle for the transaction management.

In Tangle, the vertices of the graph represent the nodes/physical devices and the directed edges represent the transaction from one device to another. In short, IOTA network is a lightweight tangle which is scalable to any extent for adding any number of transactions and DAG is the backbone of it.

No Transaction Fees? In most Blockchain networks the transaction cost is often a matter of concern. But IOTA is not charging any fee for the transaction. The IOTA is mainly designed to perform Nano transactions and these Nano transactions will be ex- ecuted without any transaction fee. The IOTA can create both private and permissioned networks of IoT, and can manage the transactions with Tangle.

No miners? In case of a Blockchain mining is a vital element, but IOTA is an exception to it. There is no miners or mining process in IOTA network. So how the trans- actions are verified in IOTA? The tangle just needs a verification only. And the verification is done by the node who generated the transaction, with the help of a validation algorithm. But the node will be able to proceed this trans- action only after verifying two other random transactions in the network using the same validation algorithm.Instead of the Bitcoin protocol, IOTA uses the GHOST(Greedy Heaviest Observed Subtree) protocol, which is a modified ver- sion of bitcoin protocol itself. GHOST just modify the bitcoin protocol by creat- ing a tree instead of a blockchain.

Weighted graphs In IOTA, the priority of the transaction is measured with the help of 'weight' associated with each transaction. DAG is a weighted graph and the weight of each transaction is proportional to the amount of work that the issuing node invested into it. And obviously, the transactions with higher weight will get higher priority than the transactions with lower weight

Developing IOTA The supporting languages for IOTA are Python and JavaScript. The library packages for the languages are available on the IOTA website itself. The developer may use an IOTA sandbox environment or install IOTA core client for developing the IOTA network. In IOTA network, every object is

considered as a service. Or in other words, the physical existence of a 'thing' will be converted as a 'service' in the tangle. This conversion is done with the help of IoT sen- sors. An IoT sensor is nothing but a simple hardware device attached to the physical entity, which will detect and digitize all the movements of that particular entity. The digitized data will be used in our IOTA network for the management of these entities. All machine to machine communication are controlled using this IoT sensors in IOTA network.

Security

IOTA offers a high level of security for both transactions and assets. The data transfer through the tangle will be in encrypted form and fully protected from external attacks. I

OTA uses the masked massaging technique ensure the security of data transfer. In Masked messaging service, the data is encrypted with quantum proof security which makes the data broadcasting also easy. Starting from the weight calculation to restricting an external attack, IOTA employs several mathematical equations which are capable of detecting any small changes in the graph. This highly mathematical approach ensures the protection of data from any kind of external attacks.

The combined advantage of blockchain and IoT has already brought many application areas to IOTA. As the IoT and blockchain is expanding rapidly, more existing services may come under this technology in near future.

Corda

Corda is a distributed ledger platform specially designed for the financial sector. It is an open source platform that can be used to build apps for financial institutions on top of it. It is a permissioned private network designed to record, manage and synchronize contracts and other shared data between partners. Corda is governed by R3 consortium which is a collaboration of 70+ finance institutions. According to R3, Corda is a distributed ledger technology and isn't a blockchain. In fact, R3 provides a platform for developing and deploying distributed apps for different financial use cases. The distributed apps created with Corda is known as CorDapps. DemoBench is a standalone desk- top application provided by Corda to configure and launch local Corda nodes. It is a useful tool for training sessions and development of CorDapps. Corda has many similarities as well as differences with many existing block- chain/distributed ledger technologies. Corda allows the creation of immutable records for financial events. But unlike other blockchains, the transactions are done privately in Corda. Corda smart contracts can be written in Java or any other JVM language like kotlin (a java derived language).

And most importantly, Corda is not tied to any particular consensus algorithm and it doesn't have its own cryptocurrency. It uses the "Notary" infrastructure for 'sequencing of transactions' and validating the transactions. And it does not broadcast a transaction globally for validation purpose. A Corda network may have multiple 'Notaries' and they validate the transactions using different algo- rithms. The ultimate objective of Corda is to remove costly friction in business transactions by avoiding businesses intermediaries. Since it is only focusing on finance domain, its architecture is simple than that of Ethereum or Fabric. This approach gives performance and security advantage for Corda over other enterprise-level blockchain frameworks. Just like many other distributed technologies, Corda is also in its infant stage and it is hard to make a conclusion on its prospects.

Chain Core

Chain Core is a blockchain management software developed by Chain Inc. in 2014. The software is designed to manage the permissioned blockchain networks. The chain core can manage any number of independent blockchains or it acts as a blockchain client for different permissioned blockchains. Chain core keeps the copy of the ledgers of multiple blockchains and updates these ledgers during the validation of transactions. The validation and consistency in Chain core are ensured by a Federation of block signers. Here any digital assets including digital currencies, securities, bonds etc. are issued in a common format and represented using any units of value guaranteed by the trusted issuer

There are two editions of Chain core available. A Free Open Source Developer edition and an Enterprise Edition. The Developer edition can be used to test and make prototypes. The Enterprise Edition is essential to develop and deploy the original product based on this prototype.

The leading financial service firms like Visa, Citi group etc. are working with Chain core to develop their blockchain infrastructure.

There are basically three operations available in the software.

1. Create a blockchain.

This option is for creating a new blockchain. The chain core act as a block generator as well as a block signer in the created network. The core provides a Url and a blockchain id for the created network. The id and Url are useful when another core is going to join this network.

2. Connect to an existing Blockchain network

This option enables a core to connect to an existing network. A user must have a blockchain url, a blockchain id, and an active access token for manag- ing the transactions and digital assets.

3. Connect to the test blockchain network

This option is basically oriented to beginners. They may join the blockchain network of chain core and test the blockchain network by making basic opera- tions like account creation, transaction, digital asset management etc.

Development & Security

The chain core application can be developed with Java, node.js, or Ruby. The respective packages and APIs are available in respective repositories. Chain core uses HSM (Hardware Security Module) for a production environment. Compared to other platforms this approach provides a better security standard for the digital assets.

Chain core uses private & public key pairs for the locking and unlocking of assets. Assets are always loaded with a control program. The transactions are verified by running these control programs along the data (public key). If it produces a valid result then the transaction is declared as valid. Using multi- ple keys for transactions will improve the level of security.

Ivy and Ivy Playground

Ivy is the high-level programming language developed by Chain for creating smart contracts in Chain core. The Ivy playground is an additional tool to create, compile and load the smart contract that can be run along the core.

As the number of blockchains is being created for different purposes, the importance of a tool like the core is evident. The security features like HSM and simplicity in blockchain management makes core an appropriate option for blockchain management