A Comparative Analysis of DAG-Based Blockchain Architectures

Conference Paper · December 2018

DOI: 10.1109/ICOSST.2018.8632193

4 authors, including:

Muhammad Muneeb
Khalifa University
1 PUBLICATION **4** CITATIONS
SEE PROFILE

Irfan Ul Haq
Pakistan Institute of Engineering and Applied Sciences
39 PUBLICATIONS **275** CITATIONS
SEE PROFILE

A Comparative Analysis of DAG-based Blockchain Architectures

Huma Pervez , Muhammad Muneeb, Muhammad Usama Irfan and Irfan Ul Haq

Department of Computer and Information Sciences, Pakistan Inst. of Engineering and Applied Sciences (PIEAS)

***Abstract*— Blockchain is a shared distributed ledger that promises tamper-proof secure transactions over the highly available and resilient network involving multiple participants. Directed Acyclic Graph (DAG) has revolutionized the blockchain technology. Owing to its optimized validation mechanism, high scalability, efficient provenance, support for IoT and multi-party involvement, DAG is rapidly over-shadowing traditional blockchain architecture. In this paper, we present a comparative analysis of most popular DAG based blockchain architectures including Nxt, IOTA, Orumesh, DagCoin,Byteball, Nano and XDAG. The comparison is based on the functional data structures for maintaining the ledger, consensus algorithms, transaction validation, ledger size, scalability and popularity. Extracting the best features various DAG based blockchains, we move on to outline the best of all worlds DAG-based blockchain architecture.**

I. INTRODUCTION

Blockchain is one of the most discussed technologies today owing to recent international adaptations such as Dubai's 10x program [1], Chinas Blockchain Industry [2] and Maersk and IBM collaborating TradeLens Blockchain Shipping Solution [3]).

Blockchain is planned to be adopted by UAE government at wide scale with the aim of 10x smart Dubai. The vision of 10X smart Dubai is to reduce/eliminate the human intervention in jobs and develop autonomous organizations [1].

Chinese government is enthusiastically motivating the development and adoption of blockchain technology within the nation. It has made a distinction between crypto-currencies and blockchain, and the Chinese government taking the initiative role in supporting the technology is paying off. The campaigning of blockchain technology in China is addressed at three levels: the government, the provinces, and the enterprises [2].

In January 2018, Maersk and IBM declared the plan to institute a new blockchain platform to deliver more efficient and secure techniques for conducting global trade using blockchain technology [4].

Blockchain is a digital ledger of transactions that comprises of either public or private network where a set of transactions are continuously packed in blocks[5]. Blockchain was formerly designed as a crypto-currency and has been deliberated as an innovative method of the ledger or distributed database , where irrational data can also be kept in the metadata of the transactions [6]. A blockchain database or ledger contains two levels of records: Transactions and Blocks. Block contain list or batches of transactions in it. Blocks are time-stamped and linked to a previous block [5]. Time-stamped blockchain data is hashed and stored in encrypted form to make it secure. Each block contain previous block's hash. Thus, each block will link with previous one to make a linked-list like data structure. First block has no previously linked block so its previous hash value is set to NULL and is referred as the genesis block [7]. Blockchain technology has certain limitations in terms of scalability, cost and efficiency which is hampering its utilization in those applications where efficient micro transactions are required. This shortcoming has a major impact on its adaptation in emerging Internet of Things (IoT) applications. Directed Acyclic Graph (DAG) has revolutionized the blockchain technology due to its specific implications in Internet of Things. Owing to its optimized validation, high scalability, efficient provenance, IoT support and multi-party involvement. DAG is rapidly overshadowing the traditional blockchain architecture.

Scientific contribution of this paper includes:

- a comparative analysis of DAG based blockchain architecture.
- identification of the best features from various DAG based blockchains.
- an outline the best possible DAG based blockchain architecture based on the on-going best practices.

The remaining paper has been structured as follows. Section II elaborates how blockchain works. In section III, we discus shortcomings in existing blockchains, Section IV highlights the architecture on Next generation of Blockchain.In section VI, best practices of DAG based Blockchain architecture are discusses.Finally, section VII concludes the paper.

II. HOW A CLASSICAL BLOCKCHAIN WORKS

A typical blockchain architecture exhibits following characteristics

1) **Distributed Database / Ledger** :Blockchain is a reliable and tamper-proof database, ledger or asset management register [8].Every single node /user on a blockchain has full database/ledger access with its complete history. Whenever new node or participants will enter into blockchain network it will load the data of blockchain for that participant since inception. There is no central authority to regulate the information / data of blockchain network. Every participant can verify the records of its transaction partners directly, without an

intermediary. Thus, blockchain eliminates the concept of third-party involvement in any business transaction [9].

2) **Peer-To-Peer (P2P) Communication** : Correspondence happens straightforwardly between peers/ participants rather than through a central node / intermediary party. Every node has copy of information and they can share Information with each others without involvement of third party [9].
3) **Transparency with Anonymity** Each transaction and its interlinked value are transparent to every participant of the blockchain network. Each user / node on a blockchain has unique encrypted address with encryption performed via hashing. Participants can decide whether to keep on stranger or share proof of their self to peers by sharing public key with other peer. Transactions occur between blockchain participants through encrypted addresses [9].
4) **Immutable Data** : Once a new transaction is made by a participant and recorded in the database by updation or addition operation then it will become an irreversible entry. Each transaction is linked to every transaction record that came before them thus making a chain of transactions. To ensure the immutability of blockchain data, various approaches already exist and related algorithms are focus of continuous research. These algorithms will make sure that the transaction entry on the database is immutable, chronologically ordered, and accessible to everyone on the blockchain network [9].
5) **Smart Contract / Computational Logic**: Blockchain data can be tangled with computational logic to result in business rules. Participants / nodes can configure algorithms and self-executable rules that automatically triggered transactions between nodes. The set of these self-executable clauses make a smart contract [9].
6) **Consensus** : The method to agree the consistent state of the ledger is known as consensus in Blockchain network [10]. Some examples of consensues algorithms includes Proof of work , Proof of stake, Solo, Kafka/Zookeeper, Proof of Elapsed Time and PBFT-based [11]. In Table 1 we have shown strengths and weaknesses of different Consensus algorithms.

III. Limitations of Blockchain

Several issues have arised in the classical architecture and algorithms of the blockchain technology. These issues and limitations of the blockchain technology led researchers to think of blockchain variants. Directed Acyclic Graphs (DAG) that will be discussed in detail in the subsequent sections is one of the utmost vital variant of the blockchain technology. In this section we explore the limitations of the classical blockchain architectures.

A. Scalability

Blockchains allow one to track down any record stored in a ledgers history, but their sequential structure is also what hinders significantly their transaction throughput; the flat list nature of blockchains is the biggest bottleneck for their ability to scale. As blockchain is a distributed network maintaining a a shared ledger where nodes / participants keep record of copies of blocks. As the network size grows, more computational and storage will be available that new nodes / participants will bring them but the communication overhead will also increase. This is a major scalability issue in blockchain which explains why bitcoin developersare moving away from the fully decentralized blockchain method to having disbursements cleared by mediators off the blockchain. Even though there is a trade-off among scale and decentralization[8]. Moreover, other blockchains encounter more critical scalability issues. The Ethereum blockchain has been the center of attention several times, for scalability. A new ICO CryptoKitties, selling virtual cats that can be bred and collected, congested the Ethereum network on December 10, 2017. CryptoKitties overwhelming Ethereums network means slower transaction times for all applications running on the decentralized architecture. As the underlying issue is an ineffective consensus algorithm, the cost and time needed to conduct those transfers grew and became out of control.[23] DAGs can impove scalability by coupling network usage and transaction verification, meaning that a user must handle his/hers own transactions in order to use the network.

B. Transaction Fee

Another important shortcoming is the concept of a transaction fee for transactions of any value. Transaction fees are usually calculated on the basis of (the concept of) gas consumed for that transaction. This makes it inefficient for the scenarios where micro-transactions are involved. Transactions which consist of a small payment can also take up to a number of days before they come to be authorized [23]. DAG is providing a Free-less architecture. Detail of free-less or zero fee will be discussed later in this paper.

C. Redundancy and Cost

Having a copy of every transaction with every peer of the network is very expensive as well as redundant. One of the major advantages of blockchain was the elimination of the intermediates and introduction of the self-governance model involving only the participants. Ironically this elimination of the intermediaries has resulted in the introduction of a highly redundant network. In addition to that the role of third parties whether financial, legal or regulatory still exist due to legislative requirement. This redundancy includes extra costs for no comparable benefit [8]. DAG will overcome this issue by providing introducing knot

TABLE I: Comparison B/w Classical and DAG based Blockchain

Aspect	Classical Blockchain	DAG Based Blockchain
Consensus	Proof of Work, Proof of Stake	No need for a leader election since users are obligated to order their own transactions. Proof of Work is still being used, however not for the sake of leader election
Block Creation	Block creation speed is on of the bottleneck of Bitcoin and Ethereum. Time to create new Block on Bitcoin is 10 minutes.	DAG (Nano, IOTA, and Byteball) are the blockless projects
Fast Transaction	No fast transaction due to PoW, PoS	Fast transaction
Mining	Miners involved	No Miners
Quantum Resistance	Can be comprised by large scale Quantum Computer brute force attack	Uses exclusively quantum resistant cryptographic algorithms which are immune to this brute force attack
Scalability	Not Scalable	Are Scalable
Improving Scalability	Blockchain solutions propose the following approaches: increased block size, support of off-chain channels, hierarchical chains and ultimately sharding	DAGs can impove scalability by coupling network usage and transaction verification, meaning that a user must handle his/hers own transactions in order to use the network
Transaction Fee	Yes	No

concept in it. Detail of knot will be discussed later in this paper.

D. Unwanted Decentralization

As we have seen from numerous cryptographic money networks, few minors get together to formulate large group and lessen the variety of the mining reward. This prompts a centralization of intensity that can be seen diplomatically and computationally. These groups can mishandle their capacity to put off transactions, mine their transactions first, or channel for specific transactions. This isn't the main type of undesirable centralization. As the blockchain, or supposed record, keeps on developing, littler hubs won't have the capacity to store a full duplicate of the record leaving just large mining ranches who have the ability to store the full record. On the off chance that just the bigger nodes work a blockchain, this is additionally a type of centralization [23].

IV. Blockchain : From Linked-list to Directed Acyclic Graph (DAG)

Researchers have proposed several distributed ledger protocols over DAG-based blockchains to solve the shortcomings available in existing Blockchain. In this section we will see the next generation of Blockchain i-e DAG based blockchain in detail. The concept of Directed Acyclic Graph (DAG) is similar to that of the blockchain. DAG is composed of a network with a number of different nodes approving transactions. Every new transaction that is performed necessitates the validation of at least two earlier transactions before it is successfully recorded onto the blockchain network. As new transactions are entered, more transactions are authorized / validated and entered, resulting in a distributed network of doubly-checked transactions. Unlike the blockchain concept, however, DAG requires no miners to authorize each transaction as being authentic. By having two parent transactions endorse the validity of a later transaction, human involvement becomes replaceable causing in a enormously faster development: not requiring miners authorization revenues transactions go through almost directly. DAG represented in Figure 1 Furthermore, if there are no miners, there are no miners fees, helping to retain authentic transaction fees to a lowest. It is also worth noting that this low-fee structure opens itself to another important feature; DAGs ability to process micro transactions [7].

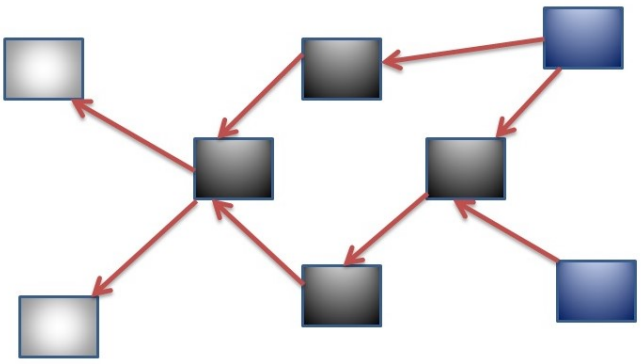

Fig. 1: Directed Acyclic Graph (DAG)

V. Existing DAG Based Blockchain Technologies

In this section some existing DAG based blockchain technologies will be discussed in detail.

A. NXT DECENTRALIZING THE FUTURE

NXT was the first crypto-currency that gave the idea to switch to DAG based on Blocks instead of Linked-list structure of BlockChain. The time of mining remains constant while the storage could be extended by W times with W blocks on the network simultaneously [14].

Nxt is a 100% proof-of-stake crypto-currency, developed in open-source Java since inception[15]. Nxt developed an independent exceptional proof-of-stake algorithm that does not require any application dependency on the coin age concept used by other proof-of-stake crypto-currencies, and is resilient to rare nothing at risk attacks. Aggregate numbers of one billion in-hand tokens were divided in the genesis

TABLE II: Comparison of Existing DAG Technology

Feature / Technology	IOTA	DagCoin	ByteBall	Nano	XDAG	NXT	Orumesh
Distribution Method	ICO	DAG IS BASICALLY BASED ON BYTE BALL. REFERENCE	Aidrop rounds to BTC holders	Official faucet	-	-	-
Average Confirmation Time	1-60 seconds	around 30 seconds	Minutes	1-10 seconds	-	minutes	3 sec Best
Wallets Available	Windows (Full/Light), Mac (Full/Light), Linux (Full/Light)	At the moment, the app is available for Mac, Android, Windows, and Linux. WEB WALLET is also available	IOS (Light), Android (Light), Mac (Full/Light) , Windows (Full/Light) Linux (Full/Light)	Windows (Full), Mac (Full), Linux (Full), IOS (Light), Android (Light)	For window PC,Android,Mac and ALSO GPU Miners are also available	NXT client (Linux, windows, mac, android)	OruWallets
Spam Protection	PoW when attaching a transaction	It has method against spam protection but not reviled	Fees	PoW when attaching or receiving a block	ECDSA algorithm with a 256-bit private key. The session key to it is transmitted using the 8192-bit key RSA algorithm. These are security algorithms not Spam Proection	-	-
Open Source / Decentralized	Partially - Checkpointing coordinators are closed source	decentralized	Fully	Fully	Decentralized	Decentralized	Decentralized
State of the Network	WIP	NA	Advanced	Advanced	N/A		
Fees	Zero fees	almost zero transaction fees	Low fees	Zero fees	-	Minimum fee	Zero fees
Additional Features or Main Selling Point	Micro-transactions, Data transfer, Voting, Masked Messaging, IoT, Machine to Machine transaction	chatbot, conditional payments, decentralised exchange, P2P payments	Anonymity, Spending conditions, Multisig, Private messaging	Micro-transactions - Value transfer, Person to Person transaction	XDAG is both CPU and GPU mineable. Making it the first mineable DAG project. XDAG is working on incorporating privacy features	Monetary System, Asset Exchange and Assets ,Messaging, ,Marketplace ,Coin Shuffling ,Voting, Account Control , Alias System, Data Cloud	-
Market Cap	5.25 bln	-	279 mln	2 bln	-	64,681,006 USD (9,963 BTC)	-
Coin Count	2.779 bln	1 000 000 000 Dags which means 10*15 microDags.	Circulating: 645k Total: 1 mln	133 mln	-	NXT 20.78 M (206.45)	-

block. Cryptography Curve25519 and SHA256 are used for security.

1) Forging in Nxt: Blocks are created after every 60 seconds, by and large, through transactions which are not locked on the nodes. Due to supply of available tokens, Nxt is redistributed by charging some transaction fees which are deposited to an account responsible to create blocks. This is called forging, and it is quite similar to the process of mining proposed by other crypto-currencies. After 10 block authorizations transactions become secure. Nxt allows 367,200 transactions per day and block size cap. Nxt transactions are created without involving script handling or transaction I/O computation on the the nodes of the network. This allows basic support for: asset exchange encrypted messages alias registration monetary system digital goods store phased transactions voting system shuffling account control cloud data account properties By using these primitive transaction types, Nxts core can be seen as an fast, base-layer protocol upon which a huge collection of services, applications, and other crypto-currencies can be created.

2) Proof of Stake: Nxt proof of stake model uses network security that is administered by peers having stake in the blockchain network. In contrast to Proof of Work algorithms, the incentives provided by proof of stake algorithm do not promote domination of miners. Data on Nxt network is highly decentralized since inception. In NxT network, large volume of individual blocks participates which is evident from the fact that the top five accounts have created 42% of the total number of blocks[16] [17].

3) Nxts Proof of Stake algorithm Principles: Nxt uses a structure where each coin in an account can be assumed of as a mini mining rig. More the token are held in the account, the greater the chance that account will receive the authority to create a block. The aggregate incentive received as an outcome of block creation is the sum of the transaction fees set within the block. Nxt does not create any new tokens as a result of block generation. Restructuring of Nxt takes place as a result of block creators getting transaction fees, so the term forging is used instead of mining. Later blocks are created based on validated, irreplaceable, and almost-not able to guess the information from the previous blocks. Blocks are connected by virtue of these links, creating a chain of blocks. To generate a block, targeted time is 60 seconds. Proof of Stake system assures the blockchain network security. Following are the basic principle of Nxt's Proof of Stake algorithm:

- Each block stores the cumulative difficulty value as a parameter, and each later block originates its own difficulty from the preceding blocks value. In case of uncertainty, the network automatically do consensus by choosing the chain fragment or block with the utmost cumulative difficulty.
- To eliminate the block generation probability through the movement of one account information to another for getting of operating revenues, tokens must be constant within an account for 1,440 blocks before they can participate to the block generation process. Tokens that come across this norm participate to an account having balance, and use balance to decide probability of forging .
- To keep an attacker from creating a new chain all the way from the genesis block, peers allow chain restructuring of no more than 720 blocks after the current block height. A block reaching at a height inferior than this threshold is declined.
- Due to the exceptionally low possibility of any account getting authority of the blockchain by creating its own chain of blocks, transactions are considered secure once they are encrypted into a block that is 10 blocks after the existing block height.[16]

4) Assets, Tokens currencies : The Nxt blockchain offers a comprehensive, established, protected and trustworthy data of transactions inside the Nxt eco-system. Empowered by its innovative blockchain architecture, Nxt can be used to build, to issue and practise two types of user-defined tokens, furthermore as providing the native NXT crypto-currency. With a specific end-goal to do this, Nxt offers a collection of great tools to established customized tokens on the blockchain, either as assets or the other complex Monetary System coins. These tokens can be used by projects to form an association from the virtual world of digital currency to the real world: a token can represent factually anything: property, stocks/bonds, commodities, or even concepts [18]. NxT supplies overall 1 billion tokens, divisible to eight decimal places. NxT tokens were supplied with the construction of the genesis block, leaving the genesis account with an opening -ve balance of 1 billion Nxt. anti-tokens existence in the account of genesis block has following remarkable drawbacks: Any kind of transaction can not be issued by the genesis account , until its balance is -ve and unable to pay transaction fees. As a consequence,every one is free to use the private pass-phrase for the genesis account. Tokens sent to the genesis account are efficiently misused, since that accounts -ve balance will terminate them out. By this way, Several thousand Nxt tokens have been burned. The choice of the word tokens is intentional due to Nxts intention to be used as a base protocol that gives various other features. Nxts core feature is traditional system for payment , but it was aimed to do far more [16]. In fact, Nxt network can be used to trade anything. We can use token in many ways other than trading,for example it could give voting rights in an organization. Nxt provides a great toolkit to project developers and individuals that also include an easy to use API system, thus letting individuals to integrate and use Nxt blockchain technology in their applications and projects [18].

B. IOTA

IOTA is designed especially for the IoT industry; a permission-less distributed ledger for a new economy. They claim it to be the pioneer open-source distributed ledger that is made to command the future of the IoT with fee-less micro-transactions and data integrity for machines and upcoming technologies [19]. By solving the issues observed in the Blockchain (Figure 2), IOTA, established on the revolutionary distributed ledger technology, the Tangle. The core feature of this innovative crypto-currency is the tangle

(Figure 3), a directed acyclic graph (DAG) for storing transactions [19].

1) Tangle: IOTAs distributed ledger, by contrast, does not comprise of transactions assembled into blocks (Figure 4) and stored in sequence of chains rather as a stream of individual transactions tangled together (Figure 5) [19].

Fig. 2: Blockchain

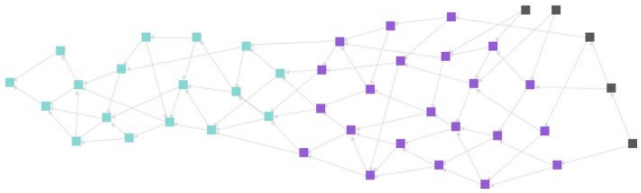

Fig. 3: Tangle [19]

Generally, a tangle-based crypto-currency works as follows: In lieu of universal blockchain, there is a DAG that IOTA calls the tangle. The transactions supplied by users set up the site set of the tangle graph, which is the ledger for keeping transactions. The advantage of the tangle is attained in the following way: when a new transaction enters, it must authorize two earlier transactions. These authorizations are denoted by directed edges(Figure 6). If there is not a directed edge in the middle of transaction U and transaction V, but there is a directed path of size minimum two from U to V, we say that U indirectly authorized V. It too has genesis transaction, which may be authorized directly or indirectly by all other transactions (Figure 7). The genesis is defined in the following way. In the creation of the tangle, there was an address with a balance that holds all of the tokens. The genesis transaction led these tokens to numerous other founder addresses. No tokens is generated hereafter, and there is no mining through which miners get financial incentive out of thin air.

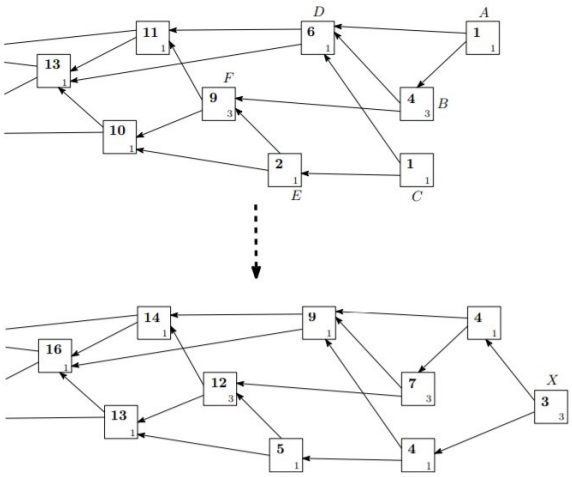

Fig. 4: Weight Assignments IOTA DAG. [20]

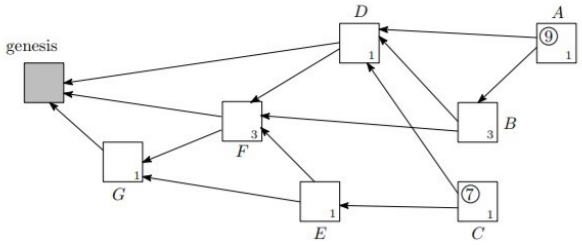

Fig. 5: IOTA DAG [20]

To issue a transaction, users / participants must work to authorize/approve further transactions. Thus, participants who issue a transaction are participating to the networks security. Nodes inspect if the authorized transactions are not contradictory. If node detect a transaction has conflicts with existing tangle record/history, the user will reject the contradictory transaction.

2) Stability of the system: This Tangled/ DAG structure also facilitates high scalability of transactions. The more activity in the Tangle, the quicker transactions can be complete.

C. Orumesh

is open source, prompt, fee-less browser based distributed database /ledger protocol by hybrid eco-system. OruMesh is implemented on DAG struxture. It doesnt use classical bitcoin mining process which makes it fee less. It has 51% resilience for design and quantum attacks.. [21].

1) OruMesh Structure: Tips are the un-approved transactions interconnected to each other so that every tip consists of at least one hash of previous tips, which works both to accept previous transactions and to inaugurate the order of tips. DAG doesnt create blocks. There is no There is no central authority everything is decentralized. The participants will confirm the newly inserted transactions by adding its hash inside their particular block. As new tips are inserted, each previous/earlier tip,which is presently a specific level complete transaction of a specific weight, gets affirmations by later tips, as each new transaction insert its particular weight to the current certain dimension complete transaction

that incorporate its hash, straightforwardly or in a roundabout way.To record a transaction, a user / participant does the following:[22].

- Initially, it selects arbitrary two other unauthorized transactions to authorized.
- It authorizes by incremental size if the 2 transactions arent contradictory and dont allow contradictory transactions.
- For the transaction to get validated, the transactions need to solve a well-defined proof-of-work cryptographic puzzle.

For OruMesh protocol the OruMesh system, attention credit model is used to give transactions an incentive. Every node is supposed to calculate the percentage of latest transactions performed by its neighbour nodes. Orumesh full node is constructed on P2P social media called the OruSocial Wallet. Participant earns Orus while utilizing the application in a consideration credit model. In this application, the OruSocial Wallet perform as both a user application layer and full node for the OruMesh protocol. In the OruMesh system, attention credit model is used to give transactions an incentive. The Orumesh also contains OruSocial Wallet. Attention credit model has been utilized for the users to gain Orus. The OruSocial Wallet has been designed both for user application layer as well as to act as full node for the OruMesh protocol. The transaction speed is faster as more participants are being added to the network. On the off chance that one particular node is under controlled it'll be dropped by its neighbours. In this way, regardless of whether transactions dont issue further transactions despite everything it has incentive to issue transactions. Assets are put away by the clients on remarkable addresses to that require multi-signature to have the capacity to spend. Before a spend happens conditions are assessed by the DAG by searching for particular data presented on the DAG by different clients. Nodes will issue new resources and framework decides that oversee their transactions capacity. The tenets incorporate, spending confinements like an interest for each exchange to be co-signed by the backer Assets which are as yet not distributed to the database can be presented and also issued by a client, and in this way not unmistakable to outsiders. Rather, the data with respect to the move is changed in private among clients, and just a hash of the gathering activity and a spend verification (to avert twofold spends) are distributed to the AMesh. [22].

2) AMesh (Acyclic Mesh): AMesh is an extremely distributed design amalgamation the models of transactions and blocks which turns transactions into a reward-based computational function. Every transaction has a proof of work and references at least one earlier transactions. The resultant legitimate data structure is a Direct Acyclic Graph of all accepted transactions. Each transaction achieves authorization via a structured and non-cyclic process. A new transaction only enters the DAG after authorization of two or more unverified earlier transactions [21].

3) Knot: Once a transaction turns out to be established Oru creates a new structure based on this transaction, calling it a Knot. Each knot consist of information about all its forefather knots (via parents), the portion of information it rely on develop like knots in AMesh. There is a flag in the knot that expresses us if it completed being void and we have instance to older knots that we'll use later to form proofs for light clients. We can only build a knot when the corresponding transactions turn out to be stable and we know for definite whether it is sequential. As the current AMesh is seen by multiple users are ultimately stable, they will all construct accurately the identical knots based on the same transactions. It must be noted that the concepts about usage of DAGs in the crypto-currency / blockchain context were around for some time. Specifically, the work presents the so-called GHOST protocol, which recommends an alteration of the Bitcoin protocol by making the main ledger a tree instead of the blockchain /list of chains; it is presented that such a variation authorized to minimize the authorization times and enhance the overall security (Figure 8). [21]

```
knot: {
transaction: "hash of transaction",
parent_knots: [array of hashes of knot based on parent knots],
is_nonserial: true, // this field included only if the transaction is Non-serial
skiplist_knots: [array of earlier knots used to build skiplist]
}
```

Fig. 6: knot [22]

D. DagCoin

The objective of DagCoin to offer the most usable cryptocurrency In the world. DAG technology aims to deliver a scalable and fast network with almost zero fees for transactions. While Bitcoin gets slower Dagcoin built upon DAG-chain technology, claims to gets faster and securer with the growth of the usage. DagCoin developers envisage DagCoin to be the fastest and most easy-to-use cryptocurrencies in the universe [27].

E. ByteBall

ByteBall aims to create a commonly accepted smart-payments network that advertises an efficacious use cases,made conceivable with DAG technology incorporated with features such as P2P (Peer-to-Peer) Insurance Prediction Markets, P2P Betting, P2P Payments Via Text Messaging, Bot Stores, Blackbytes for Private Transactions etc. 98% of all bytes and black-bytes are distributed for free so it will be massively adopted. Few Bytes will be distributed as cash-back for purchases at the merchant stores it partners with. Mostly, the offered cash-back is 10% of the purchase amount. Another fragment of the distribution is divided into several rounds and in every round owners of BTC and Bytes are rewarded. The amounts you receive are relational to your confirmed balances in BTC and Bytes on the distribution date, these are the procedures for the November round: For each 16 BTC you acquire 0.1 GB (1 gigabyte= 1 billion bytes), For each 1 GB you acquire extra 0.1 GB [27].

F. Nano

NANO (formerly known as RaiBlocks) are also experimenting with DAG based DLTs [28]. Colin LeMahieu launched RaiBlock (now known as Nano) in 2015, aplatform with low-latency payment that wants minimum resources making Nano ideal for P2P transactions. Nano is a trustless, low-latency cryptocurrency that uses a novelblock-lattice architecture, where each participant has its own blockchain and attains consensus via delegated Proof of Stake voting. Nano Offers feeless, instantaneous transactions,as well as unlimited scalability [29].

1) XDAG: XDAG is new DAG-based cryptocurrency and novel application of Directed Acyclic Graph (DAG) technology that solves the issues currently faced by blockchain technology. It was launched in Jan 2018 with No pre-mine feature [30].

VI. Best of DAG Practices

We have discussed seven different communities working on Directed acyclic Graph (DAG) based blockchain in detail. we discussed major terminologies and working methodologies of these DAG based communities. Table II shows the comparative analysis of DAG based Technologies.

With the help of comparative analysis of above discussed DAG based blockchains, an outline best of all world DAG Blockchain architecture skeleton can be formulated. To overcome the short comings of existing blockchain , best of all the world architecture should facilitate to resolve the scalability issue , allow to chose or configure plug and play / configurable) consensus algorithm so that transaction fee and costly blockchain issue will also be addressed through this architecture. The best architectur should have no transaction fees. It should have gradual provenance similar to the concept of Knots in Orumesh. The best architecture should not allow centralized monopoly as Bitcoin is feared to suffer from. The best of all DAG must have low latency and high efficiency such as Nano claims. Another of the best practices is the support of micro transactions and browser based interface to help plugin with IoT devices. Another charactersitic of the best of all architectures should be its high flexibility and generic nature so that it can be utilized in various application domains.

VII. Conclusions and Future Work

Traditional blockchain architectures are very costly for IoT scenarios due to their highly expensive proof-of-work algorithms as well as long chains of provenance. A DAG (Directed Acyclic Graph) based blockchain architecture having properties such as tieing knots of provenance validation on various progressive levels of the trees can be address this problem. Smart Contracts built upon such a DAG based blockchain will help to realize scenarios such as self-driven cars automatically contacting maintenance service providers and then validating the quality of service through built-in sensors and releasing payments. This framework will be useful to any kind of IoT oriented micro transaction scenarios including those related to logistics. There is a need to design and develop smart and cost-effective algorithms for transaction validation, proof of work, provenance, dynamic contract formation, negotiation/renegotiation etc.

References

[1] http://dubai10x.ae/about-dubai-10x/ last accessed on Sept 15, 2018
[2] https://hackernoon.com/the-future-of-chinas-blockchain-industry-7a1c37abcef last accessed on Sept 15, 2018
[3] http://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution last accessed on Sept 15, 2018
[4] https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/ last accessed on Sept 15, 2018
[5] Carlozo, L. (2017). What is blockchain?. Journal of Accountancy, 224(1), 29.
[6] Kuo, T. T., Kim, H. E., and Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.
[7] http://www.gibraltarlaw.com/directed-acyclic-graph-vs-blockchain/ last accessed on Sept 15, 2018
[8] Ammous, S. (2016). Blockchain Technology: What is it good for?.
[9] Iansiti, M., and Lakhani, K. R. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127.
[10] https://blockgeeks.com/guides/blockchain-consensus/ last accessed on Sept 15, 2018
[11] https://mastanbtc.github.io/blockchainnotes/consensustypes/ last accessed on Sept 15, 2018
[12] https://www.newgenapps.com/blog/8-blockchain-consensus-mechanisms-and-benefits last accessed on Sept 15, 2018
[13] https://medium.com/swlh/hyperledger-chapter-6-hyperledger-fabric-components-technical-context-767985f605dd last accessed on Sept 15, 2018
[14] https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/ last accessed on Sept 15, 2018
[15] https://bitbucket.org/JeanLucPicard/nxt/src last accessed on Sept 15, 2018
[16] https://nxtwiki.org/wiki/Whitepaper:Nxt last accessed on Sept 15, 2018
[17] https://nxtportal.org/monitor/ last accessed on Sept 15, 2018
[18] https://nxtplatform.org/what-is-nxt/nxt-tokens/ last accessed on Sept 15, 2018
[19] https://www.iota.org/get-started/what-is-iota last accessed on Sept 15, 2018
[20] https://www.iota.org/research/academic-papers last accessed on Sept 15, 2018
[21] https://orumesh.com/beta/ last accessed on Sept 15, 2018
[22] https://orumesh.com/whitepaper2.0.pdf last accessed on Sept 15, 2018
[23] https://www.cointelligence.com/content/tangle-dag-vs-blockchain/ last accessed on Sept 15, 2018
[24] https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/delegated-proof-of-stake last accessed on Sept 15, 2018
[25] https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256 last accessed on Sept 15, 2018
[26] https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3 last accessed on Sept 15, 2018
[27] https://steemit.com/steem/@khaleelkazi/what-is-dag-technology-an-alternative-ledger-system-for-cryptocurrencies-or-coinpickings-podcast-2 last accessed on Sept 15, 2018
[28] https://medium.com/nakamo-to/dags-the-future-of-dlt-8c61f405df8a last accessed on Sept 15, 2018
[29] https://nano.org/en/about/ last accessed on Sept 15, 2018
[30] https://xdag.io/ last accessed on Sept 15, 2018