Directed Acyclic Graph-based Distributed Ledgers –An Evolutionary Perspective

Article · May 2020

DOI: 10.35940/ijeat.A1970.109119

2 authors:

Kiran Kumar Kondru
Central University of Tamil Nadu
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Saranya Rajiakodi
Central University of Tamil Nadu
7 PUBLICATIONS **6** CITATIONS
SEE PROFILE

Directed Acyclic Graph-based Distributed Ledgers – An Evolutionary Perspective

Kiran Kumar Kondru, R Saranya

Abstract: ***Blockchain platforms like Bitcoin and Ethereum have introduced a distributed and decentralized cryptocurrency system with no third-party intermediation required. These peer to peer network systems allows Internet users to directly transact with each other. However due to the heavy emphasis on decentralization, scalability has taken a back seat. It has also become a key issue in the wider adoption of these technologies. The change to the underlying data organizing structure to Direct Acyclic Graphs (DAG) of the distributed ledger, has significantly increased transaction scalability. In this paper, we analyse some of the Distributed Ledger Technologies that use DAGs and have shown marked improved in transaction performance without weakening security.***

Keywords: Blockchain, Direct Acyclic Graph, Distributed Ledger, Consensus, Bitcoin

I. INTRODUCTION

A blockchain can be defined as a data structure which contains blocks of transactions linked together linearly. And it's append-only, meaning, new blocks can be added to it, but no block can be removed, or the contents of a block can be changed how so ever. A Blockchain is a distributed and decentralized network with the data being replicated all over the network. In a distributed environment, to have the same replicated data structure, and in a leaderless (no centralized server) network, there should be a mechanism to maintain the same exact structure in all the nodes in the network[1]. A Blockchain can be thought of as being made of 2 components. One is the data structure that is going to store transaction data along with cryptographic information. The other is the distributed network which maintains the transaction ledger.

Traditionally a ledger is a record of monetary transactions from one entity(person) to another entity(bank/person). Since there is a lack of trust in direct transfers, a trusted third party is required to execute and maintain transactions. These trusted third parties are banks (most often) and for providing the services of maintaining ledgers and credibility, they charge a fee.

As can be seen from the above description, that is highly centralized system and though there are significant technological changes like the invention of computers and the Internet, the characteristic of this centralized ledger is not significantly changed. Though there are attempts to make use of rapid changes in information technology, they were not able to create a purely electronic currency to be used in the age of the Internet. This is mainly due to what is called as a double-spend problem. Double spending is a potential flaw in digital cash scheme in which the same digital token can be spent more than once. Unlike physical cash, a digital token consists of a digital file that can be duplicated or falsified[2]

In this paper, we try to analyze the evolution of data organization structure of Blockchains/Distributed Ledgers from serial linked list type to Direct Acyclic Graph-based structures using popular DAG based platforms. In Section II, we discuss how a traditional blockchain like Bitcoin works and in Section III, we discuss its limitations. Sections 4 and 5 discuss Platforms that came up with DAGs with Blocks known as BlockDAG. Sections 6, 7 and 8 we discuss Platforms which completely discarded the concept of blocks, using what is known as Transaction DAG. In Section 9, we illustrate the similarities and differences between Blockchain, BlockDAG and Transaction DAG using a tabular format. And finally, in Section 10, we conclude.

II. HOW BLOCKCHAIN WORKS

Bitcoin can be considered the first blockchain. It's basically a distributed ledger on a public network (the Internet). Its blocks consist of transactions made from one user in the Bitcoin network to another. And this transaction can be verified by all the nodes in the network. This ledger is available with all the nodes in the network and is being continuously synchronized when the whole network comes to a consensus on the validity of the transaction. But there are chances of misuse or malicious use by some nodes in the network. Since transactions are verifiable, the Bitcoin cryptocurrency has an ingenious solution to the problem of double-spend. The consensus mechanism called Proof-of-work is used to verify that there is no double-spend problem, through a computation intensive puzzle solving (used before in Hashcash[3]). Proof-of-work involves the computation-intensive task of finding a hash value of the combined transactions in the block with a specified number of zeros starting in the hash value. The lucky nodes which can come up quickly with this unique hash value are considered the winner and its a block of transactions are broadcasted and after verification by the nodes are added to their own local blockchain (transaction ledger)

But this Proof-of-work consensus mechanism is extremely computationally intensive and excessively wasteful. Also, since the blocks of transactions are linearly added to the blockchain in addition to the slow and time-consuming PoW (Proof-of-work) consensus mechanism, it creates a bottleneck, since many blocks are ready to be added to the blockchain (replicated by all the nodes in the network).

Revised Manuscript Received on October 30, 2019.

Kiran Kumar Kondru, Ph.D. Research Scholar, Department of Computer Science, Central University of Tamil Nadu, Thiruvarur, India. Email: kirankondru.tech@gmail.com

Dr R Saranya, Assistant Professor, Department of Computer Science, Central University of Tamil Nadu, Thiruvarur, India. Email: saranya@cutn.ac.in

This creates a problem as Bitcoin runs on a public network (The Internet) and allows nodes to join and leave as they wish. The problem is as more and more nodes join the network and start transacting, there will be more blocks to be added to the blockchain and hence slowing down the entire network. To overcome this problem of scalability, the alternative consensus mechanism has come up, trying to solve some or all of the issues in the PoW or the Bitcoin platform

III. LIMITATIONS OF BLOCKCHAIN

As it's well known that the main problem with the Bitcoin network is its scalability. Block size is limited (and fixed) and Block creation rate is slow. The security and strength of the Bitcoin network stem from these limitations. Either increasing the Block size or increasing the block creation rate, it would be easy for malicious users to take control of the whole Bitcoin network. The strength of the Bitcoin network is that a malicious user must take control of 51% of the Network Computation power, in order to misuse the cryptocurrency network, like double-spending[2]. A double-spend problem is one when a malicious user sends some amount of currency to another user and before that amount being debited in his account and replicated throughout the network, he makes another transaction with that already spent currency.

Banks and Financial services solve this double spent problem in a centralized way to leave no ambiguity. But since bitcoin is a distributed ledger and there's no central authority to prevent double spent, it uses Proof-Of-work consensus to dissuade those who want to double spent[2] and rewards the good users(miners) who verify the transactions (and authenticate them) with bitcoins.

Since Bitcoin is a chain of Blocks, still malicious users can create their own blocks and add them to their blockchain and ask others in the network to replicate their ledgers too. Then this creates a kind of a side chain in blockchain, with other nodes adding more blocks to that side chain too. But the side chains[1], after a certain number of blocks being added will be discarded. And all the transactions in the blocks added to the side chains are not included in the ledger. This is enforced in the Nakamoto Consensus[1] which is also known as the Longest chain rule. This is done to prevent double spending[2] by malicious users

In an attempt to increase the throughput of the existing blockchain architecture, there has been a focus on the design of the data organization in the blockchain itself. Instead of putting blocks sequentially like a linked list kind of structure, there have been attempts to make use of a different data structure – Directed Acyclic Graph[4]. This change in the underlying data organization also required a change of the consensus mechanism for transaction validation.

IV. SPECTRE PROTOCOL

SPECTRE protocol[4] is one of the earliest to come up with a DAG-based design structure along with the required consensus mechanism. Even before DAG as a data structure is being used, other data structures like trees are also used[5] to address the scalability issues in the Bitcoin[1] like networks. For example, The protocol Greedy Heaviest-Observed Sub-Tree (GHOST)[5] uses trees instead of a chain of blocks. The nodes in the GHOST based network store all the observed and valid blocks and maintain a tree of their forks. A fork is a situation in which more than one node wins the PoW based puzzle[1] and tries to attach its own created block to the chain. So, instead of a chain of blocks, we get a tree as shown in the Fig.1 below

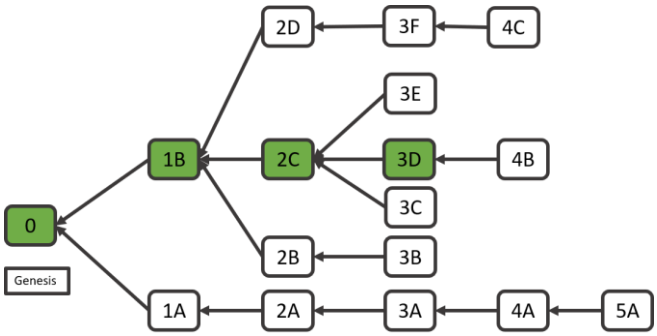

Fig.1: A tree of Blocks. Block 1A through 5A makes the longest chain. But it's not chosen in GHOST. Instead, Block 1B is selected with a weight of 11 to be part of the main chain. Blocks 2c(weight of 5) and Block 3D(with a weight of 2) are selected into the main chain[6]

To calculate the cumulative weight of a subtree, we add all the weights of its children. If the child nodes are leaf nodes, then their weights are 1 and if they themselves form a subtree, then it's the cumulative weights of its children and so on. As we see from the above figure, though blocks 1A through 5A forms the longest chains, it's not taken as the main chain but the subtree 1B with its other subtrees, namely 2C and 3D are taken to be part of the main chain. By doing this, subtrees of nodes with heaviest weights are added to the main chain. As such, instead of having only one block added linearly at a time, more than one block can be added to the blockchain in the form of trees. As such, GHOST relaxes the block-generation constraint. but retains the same level of security as in a Bitcoin network. Which is, it still requires a 51% total hashing power[1] of the network to cause a security vulnerability.

Extending on this concept, DAG as a data structure was proposed [7]. The Blocks are ordered in a Direct Acyclic Graph and each block can have multiple parents (predecessors). This is in contrast to the GHOST protocol where parent block can have many children, but a child block can only have one parent (predecessor). This DAG based blockchain allows the blocks to be selectively included in the ledger. The blocks waiting to be included in the DAG ledger – so-called off-chain blocks, can still be included in the ledger as long as it's not far from the main chain. In a chain-based network like Bitcoin, there will be forks where a block has more than one descendant. But after a certain number of blocks being added, the longest chain rule is applied, and the forked chain of blocks gets discarded. But in the case of GHOST, these chains of would be discarded blocks are not thrown away. By using the would be discarded blocks this proposed protocol[7] slightly increases the network throughput as more blocks of transactions are included in the ledger at any given time.

The protocol proposed in [7] is later extended to form the protocol SPECTRE[4]. SPECTRE further relaxes the node synchronization and allows blocks to grow on the DAG-based ledger concurrently.

That too without specifying the main branch like GHOST. SPECTRE uses a concept called Virtual Pairwise Voting mechanism to determine the order of any pairwise blocks in the DAG. According to this mechanism, each block votes on the relative order of not only their parent (preceding) blocks but also their descendant blocks according to the topology of the DAG.

SPECTRE is shown to do better with Block Withholding attacks that a Bitcoin network is prone to[8]. A block withholding attack is a form of Double spend attack wherein a miner would generate a valid block but would not broadcast it. Instead, he broadcasts his own transaction in an attempt to double spend. With this new vote based pairwise ordering, attackers creating secret chains cannot win the votes by the existing blocks from honest nodes. There are fewer connections in the DAG in for this secret attacker chain. This can be seen in the below diagram.

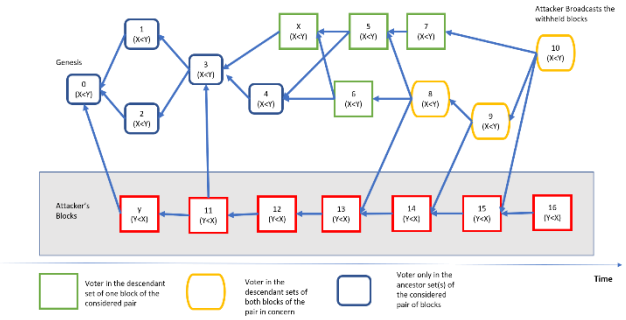

Fig 2. The Figure shows how the honest blocks are created with pairwise voting mechanism[4].

As an example, we consider X and Y blocks and the relative ordering is voted by other blocks. X < Y means X precedes Y. Blocks which are descendants of X will vote X < Y since they see more X < Y since they only see X. Blocks 0-4 will vote X < Y since they see more of X < Y in their descendant blocks. Blocks 8 – 10 which have both X and Y as ancestors run a recursive query to their predecessor sets and use the majority voting results as their own votes. Here the attacker though has the longest chain which says Y < X (Y precedes X), they cannot win the votes from existing honest blocks because of the lack of connection to the existing blocks[6].

In this protocol, the block creation rate is accelerated as more blocks can be added to the network as there are honest miners creating blocks exist. As such, the more nodes in the network the higher the expected block generation rate.

SPECTRE is able to increase transaction throughput as the network size increases. This makes it more scalable compared to chain based Blockchains. However, there are disadvantages to this protocol. Though SPECTRE protocol can be very fast without any conflicts in the network, like no double-spending, but with visibly double-spend transactions the same speed is not guaranteed.

Also, as SPECTRE uses pairwise ordering it's only suited to support cryptocurrency where strict ordering of transactions is not a necessity

V. CASANOVA

Casanova[9] is a leaderless optimistic consensus protocol, optimized for Blockchain. It was introduced by researchers at Pyrofex Corporation[10]. As with SPECTRE[4] protocol, it also uses BlockDAG data organization style. While it would be appropriate for Proof-of-Stake[11] blockchain, it can also be used in a variety of applications. Casanova can pipeline voting and message-passing rounds by combining block creation with votes.[9]

Since Casanova was designed to use Proof-of-Stake, it uses validators instead of miners (as in the case of PoW based blockchains). And these validators produce blocks of transactions (from clients) on a regular basis. When the validators receive a transaction from a client, they include it in their block and sign the block to show that they have seen it. Validators also exchange blocks with each other, to ensure that everyone sees all the transactions. When a validator is ready to produce a new block, it includes information about blocks that it has seen from everyone else.

Existing blockchains like Bitcoin, take considerable time and consume considerable resources[12][13] getting an entire network to agree on a global ordering of each transaction. Casanova protocol is developed with two key observations. Observations learned from existing blockchains like Bitcoin[1] and Ethereum[14].

Transaction on a Blockchain network does not conflict. Majority of the users do not double spend, as they want their transactions to clear quickly

Transaction does not need to be completely ordered, as most of the transactions are unrelated. A partial order will be enough.

In case of conflicts, a conflict exclusion protocol is used. This protocol is based on a choice consensus protocol and used only when double spends happen. If there is a double spend in the network, then the network must choose exactly one of those transactions. One of Casanova's features is that anyone can spam the network with double spends, which will slow it down, but the network will only slow down for the spammer's account. Everyone else's transactions get processed at the usual speed because you can't force them to conflict with your transactions. According to its researchers, Casanova has a sort of 'line item veto' on spammy transactions that's unique in the industry.

Casanova is designed taking into consideration the FLP Impossibility[15] problem for fully asynchronous Byzantine networks[16][13]. FLP Impossibility states that in a deterministic consensus protocol cannot have (1) Liveness, (2) Safety and (3) Fault Tolerance in a fully asynchronous network. The protocol does impose synchrony upon the network, rather a mild one. Messages get delivered in some bounded time in order for the network to be a live network[13]. But almost all distributed protocols make a trade-off with the above three properties.

However, as every platform and consensus algorithms have some disadvantages, Casanova to has some. (1) If a network partition results in the partitions lacking a fault-tolerant majority[13], no consensus can be found. (2) In situations where network delay grows unboundedly, no consensus can be found. The creators of the protocol insist that the responsibility is on the node operators of the network to provide on an environment where such failures are rare and resolvable in a reasonable amount of time.

VI. IOTA

IOTA platform takes a different direction to solve the problem of scalability using DAG.

But instead of using blocks as in SPECTRE and Casanova platforms, it discarded the concept of blocks completely and allows nodes to directly put transactions into the transaction DAG. The DAG which IOTA uses is called Tangle[17] and has the following properties. (1) Each vertex in the Tangle DAG is a transaction and a (directed) edge is the approval (validation). (2) Every new transaction has to approve at least 2 new transactions in the Tangle DAG which in turn gets validated and approved by the later coming transactions(vertices).

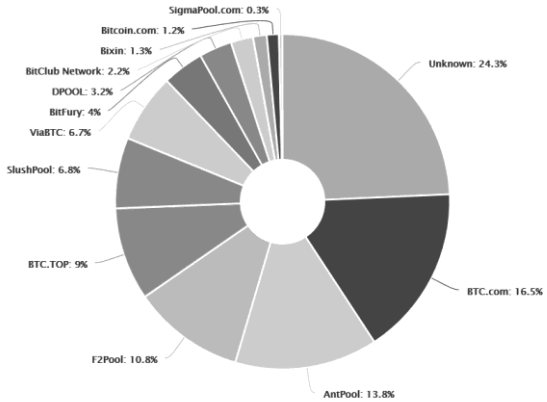

Fig 3. The above graph shows the market share of the most popular bitcoin mining pools[18].

In the case of Bitcoin[1], the miners, having huge hashing power, hold the reigns to either include or not include a transaction in the block they create. The miner usually decides this by choosing the transactions offering higher transaction fees. In the case of Bitcoin mining, a large portion of the hashing power of the network is held by few organizations pooling their hardware resources to gain an upper hand in winning the PoW puzzle. This more or less guarantees the reward of mining to these pools. A side effect of this is that sometimes the transaction fees are higher than the amount transacted.

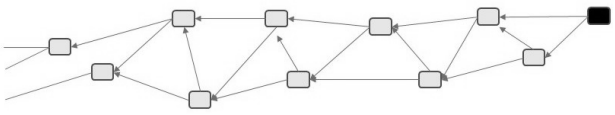

Fig 4. A simple Tangle DAG[17].

Each vertex is a transaction and each pointing edge is the validation of the transaction. The last edge with a dark color is a transaction yet to be validated.

The condition that requires any new coming transactions to validate two existing transactions. By making all the transacting nodes participate in the validation process, the IOTA platform completely removed the need for miners and the associated transaction fees. As such even smaller transaction are now feasible over this network.

The genesis vertex is the starting vertex and contains all the crypto tokens named iotas[17] in it. There is no more creation of iotas or mining like in a bitcoin network. All transactions (vertices) either directly or indirectly approve (validate) the genesis vertex. Once a transaction has been approved by a large number of transactions (indirectly) the transactions become part of the Tangle DAG permanently and are practically impossible to alter.

Newer transactions which already validated and approved two existing transactions (vertices) will still need to get themselves validated by other transactions (vertices). They are called tips (edges). In Fig 5, the grey blocks for the tips. Transactions coming in later have to select tips for validating and approving. This tip selection is an important part of the protocol and is done by performing a random walk from Genesis to the tips (edges) and stops when it reaches a leaf node. This walk is performed twice so that 2 tips can be chosen for that new transaction to validate.

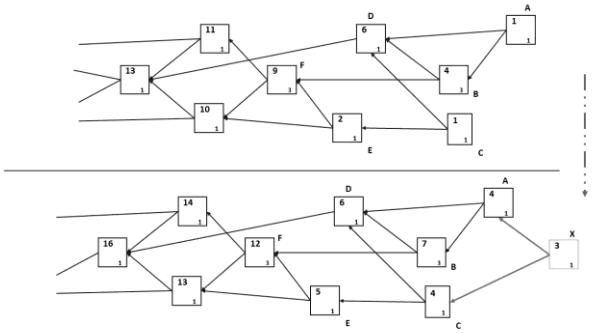

Fig 5. This figure illustrates how adding a new transaction X to the Tangle DAG increases the cumulative weight of the nodes it validates.[17]

This walk is usually done by the Random Walk Monte Carlo (RWMC) algorithm[19]. The goal is to generate fair samples from some difficult distribution. And it's used in two ways. (1) To choose two tips when creating a transaction and (2) to determine if a transaction is confirmed.

This walk is biased towards transactions with more cumulative weights. The cumulative weight of transaction is defined as the own weight of a transaction plus the sum of own weights of all the transactions that directly or indirectly approve this transaction. This concept is illustrated in Fig 6. In the figure, the South East number indicated a transaction's own weight and North West number indicates the cumulative weight. Transactions A, B, C, and D have cumulative weights of 1, 4, 1 and 6 and a new transaction X with its own weight of 3 comes in and approves A and C. Now the cumulative weights of A, B, C and D has increased to 4, 7, 4, 9[17]. Once a cumulative weight has reached a threshold value, the transaction is said to be confirmed. It's similar to the Bitcoin's own confirmation mechanism. In Bitcoin only after 6 blocks are added to a given block, does it the transactions in that given block be counted as confirmed transactions[1].

After a new transaction validates two transactions, it still needs to do some bitcoin like PoW[1]. Here the PoW is not as stringent as in Bitcoin as this is mainly used in preventing spam and also to prevent Sybil attacks[20] in the system. IOTA is also resistant to Quantum computing level attacks. IOTA uses Winternitz One-Time Signature Scheme[21] and this is resistant to Quantum computing level attacks.

Table 1: Comparison of Blockchain Platforms with Tangle DAG resistance to Quantum Computer Attacks[22].

	Blockchain: To issue a block, we need N = 2^68 nonce to find a hash	Tangle DAG: To issue a transaction, need N = 3^8 nonce
Classical Computer	O (N)	O(N)
Quantum Computer	O (√N), √2^68 = 2^34	O (N) = 10(√N)
Quantum Computer Efficiency better by	17 billion times	Only in the order of 3^4 = 81

While for traditional blockchains, it would become 17 billion times easy to hack using a quantum computer, whereas for Tangle DAG it would only be 81 times easy to corrupt. With no need for miners and including the nodes in the network to validate transactions with an incentive of their own transaction being validated subsequently, IOTA offers a model which is truly scalable. As the network grows in size so does the speed of transaction validations and the security along with it.

IOTA uses a new hashing function called Curl based on KECCAK-384/KERL. But vulnerabilities were found[23][24]. And IOTA patched it up by replacing the existing hashing algorithm with KECCAK-384 hash function. This function is used for generating addresses and signing transactions.

IOTA is still in the nascent stage and is prone to vulnerabilities. As in the case of the Curl hashing function[23][24]. Due to this, the IOTA platform included a temporary solution named the Coordinators. These are intermediaries that are scattered across the globe by the IOTA foundation. Due to the smaller initial size of the Tangle Network and a lighter PoW puzzle, Sybil kind of attacks are possible.

The use of untested cryptographic hash functions like Curl and the chance of Sybil kind of attacks in the nascent stage of the network doesn't put IOTA in the same league as Bitcoin[1] or Ethereum[14] as far as security is concerned. As IOTA's Tangle still uses a lighter version of PoW, it is still computationally intensive and since it's specially designed for IoT devices, this might turn out to be a real problem

VII. OBYTE

Obyte[25] (previously Byteball) is a Cryptocurrency platform whose features include different asset classes, conditional payments and is focused on privacy. This platform has transactional DAG as IOTA's tangle. Also eliminates miners and has lower fees.

Platforms like Bitcoin and Ethereum were built such that they operate completely outside of the existing financial world. Obyte, on the other hand, is built to make possible the interaction between the crypto world and the existing financial system. Obyte has multiple asset classes. That includes currencies and other commodities. Obyte's main cryptocurrency is Byte and is publicly traded. It also has what is known as Blackbytes which are not traded publicly, and the transactions are done in near complete anonymity. Obyte can also send payments through chat or via email. Obyte also provides merchant bots which can converse using plain and simple language.

The most popular use case as of now is Betting for Obyte. A special feature called conditional payments makes it possible to make payments in a risk-free approach. This conditional payment feature along with easy-to-use smart contract language seems to be a perfect match for use cases like online betting. Obyte's DAG based technology has eliminated miners like in IOTA's Tangle. But Obyte approaches differently to the problem of double spending. The Platform involves what is known as Witnesses to verify transactions. Witnesses are individuals deemed to be trustworthy and their identities known publicly. Once a transaction is added to the ledger, it must be seen by a majority of the witnesses.

Obyte completely eliminated the fee structure followed by older Blockchains like Bitcoin. Though it didn't completely let go of the concept of fees for transactions. The transaction fees go to the Witnesses who verify the transactions. Here the cost of one Byte of currency for every Byte of data stored. This introduces predictability as this never changes and eliminates volatility seen in other cryptocurrencies like Bitcoin.

Writing Smart Contracts is simpler in Obyte. It uses simple and easy to use language which doesn't require deep coding language. This also eliminates the bugs a developer might introduce while writing these contracts. As contracts once are written cannot be undone once it's on the ledger. All in all, this platform is doing many things at once. It's a crypto platform, has conditional payments, allows Peer to Peer betting, can use text coins (cryptocurrency via email or chat), chatbots, untraceable currency (Blackbytes), and more.

VIII. NANO

Nano(formerly RaiBlocks[26]) is a newer and more popular cryptocurrency platform which promises virtually instantaneous transactions and zero fees. It uses a DAG as its data organizing structure called Block Lattice. But block lattice is a little different from either IOTA's Tangle or Obyte's DAG.

This block lattice structure allows each individual transacting on the network to possess their own blockchains which are controlled by the individual's private keys. One feature of this design is that each user's block lattice tracks their account balance, rather than their whole transactions. This method allows for fewer storage requirements. Additionally, each block lattice that is controlled by a user will also reflect information related to an individual's balance history and can only be updated by the owner. A user's blockchain can be updated asynchronously. As each user has complete control over their own block-lattice, consensus protocols like Proof-of-work are not needed. As such the entire network doesn't need to wait for a consensus on the state of the ledger as a whole. This significantly reduces delay and increases transaction speeds.

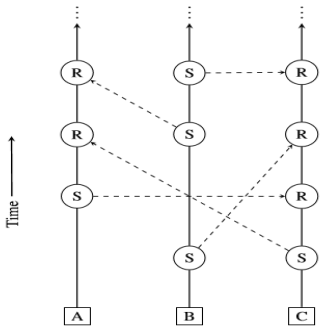

Fig 6: The figure is a Visualization of Block lattice. Every transfer of funds requires to send block(S) and a Receive Block(R), each signed by the account chain's owner.[26]

Transferring funds using Nano's block lattice has 2 separate steps. Through SEND and RECEIVE blocks balance of user's blockchains are transferred. The main features of Nano are (1) complete absence of transaction fees, (2) very fast transaction speeds, (3) highly scalable with transaction lookups scaling with the logarithm of the data size and (4) extremely energy efficient due to the absence of PoW based crypto puzzles and no requirement for consensus.

IX. BRIEF COMPARISION BETWEEN BLOCKCHAIN, BLOCKDAG, AND TRANSACTIONDAG

The following table tries to explain the basic differences of these different data organization structures, though individual platforms differ in their implementation. It's categorized according to the underlying data organization structure. A BlockDAG is a DAG where Blocks are formed into a DAG. A Transaction DAG loses completely the concept of Blocks and puts transactions directly into the vertices of DAG

Table 2: Table comparing the difference between traditional Blockchain, BlockDAG and TransactionDAG

	Blockchain	BlockDAG	Transaction DAG
Description	Chain of Blocks, each block with encrypted transactions that have been verified and validated	Blocks are created but they form a Directed Acyclic Graph, instead of a single chain of blocks	No blocks are created. Transactions are written into vertices directly. And each transaction has to validate 2 existing unvalidated transactions
Consensus Mechanism (Leader Election)	Leader election is through miners competing to win a cryptographic puzzle like PoW. The winner gets to create a block which gets replicated throughout the network	More than one winner is possible in an asynchronous network and the network can accommodate more of the winner's blocks in the DAG structure	No need for a leader and no leader election. Users are obligated to order their own transactions. PoW is still used but for spam protection.
Order of Transaction	Transactions are strictly ordered	Maybe partially ordered or fully ordered	Partially or Fully ordered depending on the Platform
Speed of Transactions	Speed of transactions is very slow as the whole network has to agree on the validity of the block created to come to a consensus	Better transaction speeds as more blocks created are allowed into the data structure	Very fast as there is no concept of separate miner/validator.
Transaction Finality (and Double-Spending Problem)	Transactions are probabilistic. As more and more blocks are added to the chain, the probability increases for a transaction to be non-reversible and become unchangeable.	Same case as in Blockchains. Except for cases which are conflicting in nature, like double-spending. In which case, it varies according to the platform being implemented	Transactions are finalized once the cumulative weights (CW) of the transactions reach a particular threshold. CW denotes the no. of incoming transactions that directly/indirectly validating the current transaction.
Node Scalability	Nodes can join or leave the network whenever and the network accommodates it (at the cost of speed and volume of the transactions)	Nodes can join and leave the network whenever	Nodes can join/leave the network and the network accommodates

Transaction Scalability	Transactions can't be scaled up due to the basic design of the Blockchain based on PoW mining	Can scale up well but the process of block creation and acceptance still is a CPU intensive process	Can scale up or down very well without CPU intensive crypto puzzle solving
Transaction Fees	As a reward for miners who validate and create blocks of transactions, users have to pay up for a transaction.	Same as in Blockchain.	Usually, since there are no miners or CPU intensive mining process, there is no transaction fee unless it's implemented by the Platform
Security	Most secure (Bitcoin has not been tampered with since its creation) - Due to heavy use of cryptographic techniques (like encryption and Puzzle solving – PoW) used	Retains the same level of security as a Blockchain as it retains the same block structure and the same battle-tested algorithms/mechanisms of Blockchain	Security is contributed by each and every node where each node in order to get its transaction validated, it must first validate 2 unvalidated transactions.
Computation Power needed to alter the ledger	51%	51%	33%

X. CONCLUSION

The DAG based DLTs that were discussed in this paper tried to solve some of the existing problems faced by the current Blockchains which are based on a Linked list like a chain of Blocks. Some of them like SPECTRE and Casanova tried the DAG structure on top of Blocks (Bitcoin kind of Blocks) and made them into BlockDAG. They built upon existing and battle-tested block design and PoW based consensus improves throughput and transaction speed of the network.
Others like IOTA, Obyte, and Nano have completely let go of the Block kind of design and instead have come up with a completely novel solution. They made use of the vertices of the DAG for transactions and edges for approving the transactions. For that, they came up with unique consensus algorithms some of which also use some kind of proof-based puzzles like PoW, more as a spam prevention mechanism. By using DAG as their underlying Data organization structure, these Distributed Ledger Platforms not only showed that they improved transaction scalability but also greatly reduced or eliminated the use of CPU intensive cryptographic puzzles like Proof-of-Work. These platforms also removed the separation between miners and transacting users by making every user participate in the validation process and contribute to the overall security of the platform. This also greatly reduced or eliminated transaction fees and paved the way for micro-payments on the network. It can be said that the DAG structure with associated consensus algorithms has made possible the above-mentioned breakthroughs improvements. However, there are still hurdles to cross for these platforms to achieve wider adoption. They are still not battle-tested in the real world like Bitcoin or Ethereum networks.

REFERENCES

1. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *White Pap.*, pp. 1–9, 2008.
2. U. W. Chohan, "The Double Spending Problem and Cryptocurrencies," *N otes 21 st Century*, vol. Discussion, p. 8, 2017.
3. A. Back, "Hashcash," pp. 1–5, 2006.
4. Y. Sompolinsky, Y. Lewenberg, and A. Zohar, "SPECTRE : Serialization of Proof-of-work Events: Confirming Transactions via Recursive Elections."
5. A. Z. Yonatan Sompolinsky, "Secure High-Rate Transaction Processing in Bitcoin," in *International Conference on Financial Cryptography and Data Security*, 2015, vol. 125, no. 6, pp. 507–527.
6. W. Wang *et al.*, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, p. 40, 2019.
7. Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8975, pp. 528–547, 2015.
8. L. Luu, R. Saha, I. Parameshwaran, P. Saxena, and A. Hobor, "On Power Splitting Games in Distributed Computation : The Case of Bitcoin Pooled Mining," *2015 IEEE 28th Comput. Secur. Found. Symp.*, 2015.
9. K. Butt, D. Sorensen, and M. Stay, "Casanova," pp. 1–16, 2018.
10. "Pyrofex." .
11. S. King and S. Nadal, "PPCoin: peer-to-peer crypto-currency with proof-of-stake (2012)," *URL https//peercoin. net/assets/paper/peercoin-paper. pdf.[Online]*, p. 6, 2012.
12. E. V. MATTHEW HANCOCK, "Distributed Ledger Technology: beyond block chain," 2018.
13. C. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," *Leibniz Int. Proc. Informatics, LIPIcs*, vol. 91, 2017.
14. G. Wood, "Ethereum: a secure decentralized generalized distributed ledger," *Gavwood.com*, 2018.
15. A. Kapinos-Gorczyca, P. Gorczyca, M. Kapinos, and R. T. Hese, "Impossibility of Distributed Consensus with One Faulty Process," *J. Assoc. Comput. Mach.*, vol. 32, no. 2, pp. 374–382, 1985.
16. L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 2002.
17. S. Popov, "The Tangle," pp. 1–28, 2018.
18. "Hashrate Distribution - An estimation of hashrate distribution amongst the largest mining pools." .
19. S. Popov, O. Saa, and P. Finardi, "Equilibria in the Tangle," pp. 1–30, 2017.
20. J. R. Douceur, "The sybil attack," vol. Proceeding, p. 6, 2002.
21. J. Buchmann, E. Dahmen, S. Ereth, A. Hülsing, and M. Rückert, "On the security of the Winternitz one-time signature scheme," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6737 LNCS, pp. 363–378, 2011.
22. 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," *IEEE Access*, vol. 6, pp. 1513–1524, 2017.
23. E. Neha Narula, Thaddeus Dryja, Madars Virza Heilman, "IOTA Vulnerability Report: Cryptanalysis of the Curl Hash Function Enabling Practical Signature Forgery Attacks on the IOTA Cryptocurrency." .
24. E. Heilman *et al.*, "Cryptanalysis

of Curl-P and Other Attacks on the IOTA Cryptocurrency," pp. 1–30, 2019.
25. A. Churyumov, "Byteball : A Decentralized System for Storage and Transfer of Value," pp. 1–49, 2017.
26. C. Lemahieu, "RaiBlocks : A Feeless Distributed Cryptocurrency Network," pp. 1–8, 2016.

AUTHORS PROFILE

Kiran Kumar Kondru is a Ph.D. research scholar in the Department of Computer Science at Central University of Tamil Nadu, India, since 2017. He has a Masters in Computer Applications. He worked as a Software Developer before. His research area includes Distributed Systems, Blockchain, and Consensus algorithms.

Dr. R Saranya is an Assistant Professor currently working in the Department of Computer Science at Central University of Tamil Nadu, India since 2016. She has more than 7 years of teaching experience in Postgraduate and undergraduate courses. Her research areas are in Computer Networks, Cybersecurity, Software Engineering and Internet of Things. Her current research is in DDOS with C-Worm detection. She is also a member of academic bodies like CSI, IEEE, and IE. She has presented more than 15 research papers in International (IEEE) and National Conferences. She has also published more than 10 research articles in peer-reviewed journals