Directed Acyclic Graphs as a Second Layer Scaling Solution for Bitcoin

David Nettey

davidnettey@protonmail.com

Abstract

Bitcoin was created as a new type of currency that could improve on the short falls of fiat currencies. It is decentralized, permission-less, immune to hyperinflation, and open source. Despite all these advantages, it does have flaws and limitations. One of the most pressing limitations in Bitcoin is scaling. Bitcoin has a low transaction throughput, less than 7 transactions per second [1]. When the network is congested, transaction fees can skyrocket. Some solutions seek to add a second layer to Bitcoin so that most transactions happen off the blockchain. The Lightning Network is one such project. Other projects built on Nakamoto's vision to create entirely cryptocurrencies. One of these projects is NANO, formerly known as RaiBlocks. NANO uses a directed acyclic graph, or DAG, in lieu of a traditional blockchain to facilitate fee-less, near instant transactions. However, due to the fact that NANO is fee-less, there is no internal incentive from the network to run a node and help it decentralize.

We believe that a marriage of ideas can be used to help solve the scaling issue. A second layer of nodes can be created that uses a DAG to facilitate transactions off the blockchain. Users deposit their Bitcoin into the network to make use of it. Most transactions take place on the network. At any time, a user may withdraw their balance from the network. This solution can reduce congestion on the Bitcoin network, lower fees, and speed up transactions.

Background

Bitcoin

Satoshi Nakamoto's idea of a distributed ledger is the core of Bitcoin [2]. Each node on the bitcoin network has a copy of the ledger. This ledger is composed of blocks that are linked to one another, hence the name blockchain. Each block has a set of transactions, a header, and a block hash. Only 1 MB of transactions can be added to a block. In the block's header's is metadata like the previous block's hash and time. The block's hash is the result of passing all the data in the block's header through a hash function called sha256.

Each person on the bitcoin network has a public and private key. The public key is used to "lock" bitcoin to an address. The private key is used to create signatures. These signatures are intrinsically linked to an address and transaction. A signature can be used to "unlock" the funds at that address. The signature also ensures that only the linked transaction can be performed.

Transactions are composed of inputs and outputs. Outputs are analogous to packages of bitcoin that belong to a someone. Each output is locked by the address using its owner(s)'s public key. Inputs point a set of existing, unspent outputs and uses them to create new outputs locked by new address. When a transaction is put on the blockchain, all outputs that the transaction's inputs point to are considered spent. The new outputs on that transactions are considered unspent. The sum of the spent outputs must be equal to the new, unspent outputs.

Blocks of transactions are confirmed by a mechanism called Proof-of-Work. Nodes called miners listen for new transactions and add them to a candidate block. When 1 MB of transactions have been added, the miners begin mining. There is a special field in the block's header that a miner can change called a nonce. When they change the nonce, the block's hash changes. Mining is a race between miners to change the nonce until the block hash meets certain conditions. The miner who meets the hash conditions first broadcasts the new block onto the network. Baked into the new block is the block reward, newly created bitcoin that goes to the miner. The miner also gets all fees in that block. If there are conflicting blocks, nodes create a fork in their copy of the blockchain. Each fork has one of the conflicting blocks. The nodes continue listening for new blocks. The longest fork is the one that will be trusted.

Proof-of-Work is a tried and true method of updating the blockchain. However, there are drawbacks. Mining uses large amounts of electricity. If this electricity is sourced from fossil fuels, it increases the amount of CO2 in the atmosphere, contributing to climate change. Another drawback is the transaction throughput. The mining process was designed to take approximately 10 minutes. The difficulty of mining automatically adjusts to ensure this timespan. This is already impractical for day to day transactions. If the network is congested, transactions can take far longer. This is due to the fee system. Transactions compete to be included into a candidate block. Transactions can offer high fees to the miner to be prioritized. The higher the fee, the quicker a transaction can be added to a block. This means transactions with low amounts must either offer disproportionately high fees or potentially wait for hours to be confirmed.

NANO

NANO is a cryptocurrency which aims to compete with Bitcoin as a form of digital cash. NANO's main feature is its fee-less, instant transactions [1]. This is possible due to the way the NANO network structures transactions. Instead of using a traditional blockchain, the nodes on NANO use a directed acyclic graph (DAG). A graph is a data structure that links packages of data (nodes) together with edges. In this case, the nodes are transactions and the edges are the references to other transactions. The graph is directed, meaning the references only go one way. Finally, the graph is acyclic, meaning that ending up at the previously visited node while traversing the graph is not possible.

Each participant in the network has one or more public-private key pairs called accounts. Each participant also has a private "blockchain" called an account chain that keeps track of the participant's transaction history. The account chain is made up of blocks that have only one transaction. The head of the chain has the account's most recent balance. The first block of the chain is called the open block. This is where the initial balance and representative is recorded. Each block has a reference to the previous block of the chain. An account may only change the balance and representative on its own account chain. This is enforced through signature checking.

Most transactions are represented by send and receive blocks. Send blocks show the destination of the sent funds and the new balance afterwards. Send block can only be made if the chain has an existing open block. Send blocks can no longer be changed once confirmed. A transaction is completed when the recipient creates a receive block. Receive blocks show the source of the the new funds and the new balance. Due to the network being feeless, microtransactions can take place. To prevent the spamming of microtransactions, each block requires a small amount of proof-of-work. The hashing can be done in seconds. This means that spammers require large amounts of computing power to send many transactions.

To confirm new blocks, NANO uses a consensus mechanism called Open Representative Voting. Each participant in the network votes on whether to confirm a block. However not all participants in the network can be active at the same time. To solve this problem, participants can elect representatives to vote on their behalf. Representatives are assigned via open blocks and change representative blocks. A change representative block simply elects a new representative for that account. An account may name itself as its own representative. A representative's votes are weighted by the funds in its account and the funds in the accounts that have named it as their representative. Nodes with at least 0.1% of the total voting weight in the network become principal representative nodes. These nodes have their votes rebroadcasted by other nodes who receive them, accelerating consensus. The ORV consensus mechanism allows for transactions to be confirmed in under a second.

Nodes do not take any fees from transactions as there is no block leader like in Bitcoin or other proof-of-work or proof-of-stake cryptocurrencies. Therefore, there is no incentive provided by the network itself to help it decentralize.

Directed Acyclic Graph as a Second Layer

What we propose is the creation of second layer network for Bitcoin that uses a DAG ledger and ORV to process transactions.

Accounts

To open an account, a user's wallet generates a public-private key pair and must have an open block. An open block can be created in two ways. The first way is for another account to send funds to the new account via the network. The second way is for the user to deposit Bitcoin into a multi-signature address that corresponds with the account and several other random nodes on the network. The sum of all multi-signature addresses on the network is called the communal treasury. A user's deposited bitcoin makes up their share of the communal treasury. A wallet may have multiple accounts and a user may have multiple wallets.

Transactions

There are several types of transactions that can be performed on this network. All blocks that make up a transaction are confirmed by the network through ORV.

Open blocks are special receive blocks that open an account. As described in the Accounts section, an open block may be created through depositing bitcoin into the network or receiving funds from another account.

Transfers are transactions that have a send block and a receive block, just like in the NANO network. Once the send blocks are confirmed through ORV, the recipients of the funds may receive blocks. Send block are irreversible once confirmed.

A special send block called a withdrawal block can be used to send funds to addresses outside the network. Just like a send block, it must be created and and verified. If the account has a share of the communal treasury, funds will be sent from that share. If the required funds is larger than that share, the network queries for a combination of UTXOs of wallets on the network to cover the rest of the withdrawal. These wallets send the appropriate signatures to the withdrawing account. The account then creates the transaction and broadcasts it to the Bitcoin network.

A special receive block called a deposit block can be used by external bitcoin accounts to send funds to accounts within the network. The external account simply sends funds to the multi-signature address associated with the recipient account. This will automatically create a deposit block in that user's account.

Finally, an account may assign a representative using two types of blocks: an open block and a change representative block. The open block assigns the account's first representative for ORV. An account may change their representative at any time by creating a change representative block.

Transaction speed

Due to the similarity of this system to NANO's network, confirmation speeds for each block should be comparable. Overall, transfers on this system will be slower than that of NANO's network due to the fees. Up to six blocks total are created for a transfer compared to NANO's two. For the sender, the speed of creating and sending transfer blocks would up up to three times slower than NANO. However, transactions would be multiples of times faster than sending a transaction on the Bitcoin network.

Fees

Unlike the NANO network, there are two fees associated with a transaction. Both fees consist of automatically generated send receive blocks. The first fee is a network fee, sent semi-randomly to a node on the network. The second fee is a reward fee. This reward fee is sent semi-randomly to accounts that are currently on the network. If the account making the transaction is chosen for the reward, the block is simply not created. Network fees go to nodes participating in ORV on the network. This incentives more nodes to join the network and stay online. This fee ultimately incentives the network to stay decentralized. The reward fee goes to wallets currently online. This fee incentives wallets to stay online to provide liquidity for withdrawals.

The recipients of both fees are chosen semi randomly. The more votes delegated to a node, the more likely that account is to be chosen to receive network fees. The larger a share an account has of the communal treasury, the more likely it is to be chosen for reward fees.

Levying fees on each type of transaction can have different effects on the network. Levying fees on transfers between accounts can increase the frequency of rewards to nodes and accounts. However, this makes micro-transactions impossible. Fees on deposits and withdrawals allow for transactions on the network to be free. However, the amount of rewards is likely to be less than that generated by transfer fees. Fees on deposits also increases the barrier of entry into the network.

Therefore, we propose fees only on withdrawals from the network. Withdrawals are likely to be large amounts, so a small percentage of the withdrawn funds can help support the network. Fee-less transfers between accounts and micro-transactions within the network adds extra incentive for users to join. Having no fees on deposits will keep the barrier of entry to only the fees on the Bitcoin network.

Vulnerabilities and Concerns

This network shares vulnerabilities with the NANO network and has its own unique vulnerabilities [1][3]. This section will address some of these concerns and how they differ from NANO.

Sybil Attack

A sybil attack, or 51% attack in other networks, is when an attacker or group of attackers gains a large share of a network in order to gain control over the ledger. A direct sybil attack on the network would be an attempt to gain a disproportionate amount of votes. There is low risk of a direct sybil attack in this network. Each vote is weighted on the account's balance. Simply creating many accounts with a zero balance will not generate the votes needed. In order for an attacker to gain a disproportionate amount of votes, the attacker must have a large amount of funds. The required funds increases with the size of the network.

An indirect sybil attack would be a sybil attack on the Bitcoin network in order to influence this network. There is low risk of this as well. The attacker must gain 51% of the hashing power of the Bitcoin network in order to begin at attack on this network. If a sybil attack is successful and discovered, the value of Bitcoin would drop precipitously due to market forces. The public nature of the bitcoin blockchain makes the keeping the attack secret a monumental and expensive task. As such, there is little financial incentive to perform a sybil attack on Bitcoin.

The only incentive to performing a sybil attack on the Bitcoin network is if the attacker desires the destruction of the network. As more miners unaffiliated with the attacker join the Bitcoin network, the attacker must also commit more computing power and capital. The likelihood of an attacker with the motive and resources to perform a sybil attack decreases as the Bitcoin network grows.

Double Spend

There are two types of double spends. One is forking an account's chain in order to spend the same block twice. We will refer to this attack as a fork double spend. The other is successfully withdrawing the account's share of communal treasury after spending their balance. This will be referred to as a treasury double spend.

In order to perform a fork double spend, an attacker must make a fork in their account's chain. The first block created will propagate through the network and gain votes as usual. If it has gained enough votes, it will be confirmed and the second fork is discarded. If the second block is sent before the voting threshold is reached, the block will propagate through the network. Upon detection of a second block, a node will add up votes for each block from the representatives. Each representative votes for the block that it sees first and deems valid. Once one of the blocks achieves the threshold, it is confirmed and the other block is discarded.

To perform a treasury double spend, the attacker must have the account's private key and the private keys of each node on the communal treasury share's address. To reduce the chances of this happening, each address in the communal treasury will be secured by 11 signatures, one from the account and 10 from randomly chosen nodes on the network. All 11 signatures must be present to spend the treasury share. As long as the account or one of the nodes represented in the address is honest, double spending of this type is impossible. The likely hood of at least 1 of the node signatures being honest, $P(x \geq 1)$, can be estimated with a hypergeometric distribution [4].

$$P(x \geq 1) = \sum_{i=1}^{G} h(i; 100, 10, G)$$

G is the percentage of honest nodes. The network is most vulnerable to a treasury double spend when the network is at its smallest. The minimum number of nodes required for the network is 10. If there is at least one honest node when the network size is 10 nodes, a treasury double spend is impossible. To have a less than 0.1% chance of a treasury double spend, at least 48% of the nodes must be honest. An attacker must control over 93% of the nodes on the network to have more than a 50% chance of compromising a share.

Run on the Treasury

If for any reason the users of the network loses faith in it, a run on the communal treasury is possible. Many users simultaneously withdrawing funds on the network has the chance of overloading it. Some user may not be able to retrieve their funds due to network delays and accounts being offline. A run on the treasury may be due to a successful malicious attack, but is not an attack itself. Runs can also be caused by bugs and flaws in the network that is perceived as compromising to the network. Runs on the treasury can only be prevented via securing the network from malicious actors and sound engineering.

There are likely to be many more avenues of attack or flaws in this network. These vulnerabilities can be tackled by making the software for wallets and the nodes open source. Through careful engineering and collaborative effort vulnerabilities can be remedied and minimized.

Possible Effects on the Bitcoin Network

Making transactions within the network is much cheaper than sending funds outside the network. As a result, users may encourage others to create accounts within the network to receive funds. The incentive of reward fees can be a potential draw to new users as well. As more accounts join the network, the load on the bitcoin network will be reduced. Reducing the load can reduce fees for the Bitcoin network. It is quite possible that a network similar to this will be primarily used for day to day transactions, while the bitcoin network is used for large transactions that don't need to be confirmed right away.

Conclusion

The advent of Bitcoin established that it is possible to have a permission-less and decentralized currency. However, Bitcoin is not perfect and can be improved upon. Nano was an attempt at taking Satoshi Nakamoto's idea and making it scalable. By combining Nano's directed acyclic graph technology with the concept of second layer solutions, it may be possible to scale Bitcoin. The increased transaction speeds and lack of fees within the proposed network would make it feasible to perform day to day transactions using Bitcoin.

References

[1]"Protocol Design Introduction", Nano Docs, 2021. [Online]. Available: https://docs.nano.org/protocol-design/introduction/. [Accessed: 07- Mar- 2021].

[2]S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. 2021.

[3]"georgehara/nano", GitHub, 2021. [Online]. Available: https://github.com/georgehara/nano/wiki/unofficial. [Accessed: 07- Mar- 2021].

[4]"Hypergeometric Distribution", Stattrek.com, 2021. [Online]. Available: https://stattrek.com/probability-distributions/hypergeometric.aspx. [Accessed: 07- Mar- 2021].