Node Based Blockchains

Most modern blockchains contain wallets. This paper proposes an alternative structure for wallets, where instead of having a single public key, wallets have a potentially infinite number of public keys. These public keys have weights, and in order for these nodes to perform an action on the blockchain, a certain weight must be achieved.

This list of public keys, weights, and required weight for action is called the 'reputation breakdown'. All of these values are decided by the node, and can be changed at any time by the node if the requirements for the previous reputation breakdown are met.

Take for example a node with a required total weight of 1, and 4 public keys that each have weight 0.25. In order for this node to make a transaction, all 4 listed nodes must approve of the transaction. If a 5^{th} key is added at weight 0.25, then any 4 out of the 5 nodes must sign a transaction for it to be accepted on the blockchain.

This allows for committees to make decisions, allows for a sort of democracy to be set up between nodes. But there is even more power involved. The node in question could potentially be an entire different cryptocurrency which has some logic for converting POW into reputation weight on the sister blockchain.

Take for example two theoretical currencies, 'ReputationCoin' and 'BitcoinBridge.' ReputationCoin is a cryptocurrency with a node based blockchain. BitcoinBridge is a cryptocurrency that counts up all of the blocks each wallet has found on the bitcoin blockchain in the past 30 days and converts them to reputation on a node on ReputationCoin. Each bitcoin wallet that has found a block has a public key listed in the reputation breakdown of the BitcoinBridge node on ReputationCoin. Explained:

Bitcoin wallet 'A' has mined 15 blocks in the past 30 days
Bitcoin wallet 'B' has mined 18 blocks in the past 30 days
Bitcoin wallet 'C' has mined 25 blocks in the past 30 days
Bitcoin wallet 'D' has mined 12 blocks in the past 30 days
Bitcoin wallet 'E' has mined 20 blocks in the past 30 days

These 5 wallets are the only wallets that have registered on BitcoinBridge, so they are the only 5 wallets that are given consideration (if wallets were given consideration that did not recognize BitcoinBridge, and most wallets in bitcoin did not recognize BitcoinBridge, then BitcoinBridge would never receive enough signatures to complete a transaction). Each of the public keys of these wallets, 'A', 'B', 'C', 'D', 'E' are given the weights '15', '18', '25', '12', and '20' respectively on the BitcoinBridge node in the ReputationCoin blockchain. The required weight is set to 51% of the sum of these wallets, or in this case, 45.9.

Any spending done from the BitcoinBridge node over ReputationCoin will require enough signatures to add up to a 45.9 weight. For the given weights, a minimum of 3 nodes will need to sign a transaction, but additionally either wallet C or wallet D will need to be one of the signatures (merely having A, B, and D will not yield enough weight).

Let us presume an additional feature in ReputationCoin: every transaction has a message field.

Using transaction messages, BitcoinBridge can associate incoming funds to the various wallets participating in BitcoinBridge. An incoming transaction for N coins could have a message

reading 'Coins for wallet C' that is automatically parseable by the BitcoinBridge blockchain.

To recap, we now have a blockchain that is separate from ReputationCoin, yet has a bunch of nodes each with a recognized balance in ReputationCoins.

Let's add three features to BitcoinBridge. The first feature is an awareness of the bitcoin blockchain. A requirement for participants of BitcoinBridge is that they also have the entire up-to-date bitcoin blockchain. The second feature is a conditional spending protocol that has an api to the spends on the bitcoin blockchain. Finally, BitcoinBridge can have wallets on it that are not part of bitcoin, and are not mentioned in the reputation breakdown.

All by itself, ReputationCoin does not support awareness of the bitcoin blockchain. However, the bitcoin blockchain is included in the BitcoinBridge blockchain, meaning that nodes participating in BitcoinBridge are aware of every spend that happens on bitcoin. Additionally, these nodes have a balance in ReputationCoins.

Using the conditional spends, BitcoinBridge can actually act as a decentralized exchange between ReputationCoin and bitcoin. To sell bitcoins over this exchange, a wallet on BitcoinBridge would announce an intention to buy ReputationCoins. The announcement would look something like 'I am willing to buy up to N ReputationCoins for M bitcoins each from bitcoin wallet A. The ReputationCoins are to be sent to BitcoinBridge wallet Z.'

To sell ReputationCoins over this exchange, a wallet would send ReputationCoins to the BitcoinBridge node with a message placing the coins in a wallet they control. They now have ReputationCoins which can be traded for bitcoins. They wait until a bitcoin seller announces a sale at a satisfactory price. They then post a response using a conditional spend that says: 'If bitcoin wallet A sends N bitcoins to bitcoin wallet B, then BitcoinBridge wallet Y will send M ReputationCoins to BitcoinBridge wallet Z.' Because this is a conditional spend, the BitcoinBridge blockchain will enforce this statement; the M ReputationCoins are withdrawn immediately from the wallet and kept until either the bitcoin spend completes or until the conditional expires (BitcoinBridge automatically expires all conditionals after 1 day).

Because BitcoinBridge is aware of the bitcoin blockchain, it can verify that bitcoin wallet A has sent N bitcoins to bitcoin wallet B. As soon as that happens, the conditional will be fulfilled and BitcoinBridge will send the ReputationCoins to their final destination.

Even though bitcoin has no awareness of ReputationCoin (and isn't even node based!), and even though ReputationCoin has no awareness of bitcoin, BitcoinBridge is able to use the node system on ReputationCoin to form a *decentralized, trustworthy, and low-fee* exchange between bitcoin and ReputationCoin. Because ReputationCoin is node based, it supports decentralized, trustworthy, and low-fee exchanges between itself and any other POW or reputation-based cryptocurrency. All that is needed is some bridge blockchain to act as a communicator between the two. For some currencies, this may be non-trivial, but for most cases I believe that a strong solution can be established. In our bitcoin example, the BitcoinBridge blockchain can be protected by the same exact POW mining that occurs over bitcoin. If all bitcoin miners are participating in BitcoinBridge, then BitcoinBridge is just as safe from attack as bitcoin, and bitcoin miners do not even have to sacrifice mining power on the bitcoin network.

Currently, the only way to trade between different cryptcurrencies is to use a centralized exchange that likely takes a large fee of some sort, either a .1 - 1% fee or a flat rate that is nontrivial for high-frequency traders. This does not need to be the case, and is a problem that can be solved using node-based cryptocurrencies instead of wallet-based cryptocurrencies.

This is only a single example of the power of node based cryptocurrencies. A node-based cryptocurrency is extensible, just like an object in Object-Oriented programming. Nodes can be used to add features to a cryptocurrency that were not in the original design. Nodes allow for cryptocurrencies to communicate with each other.

There is one concern with node based cryptocurrencies: the reputation breakdowns of nodes could potentially become very large. Imagine if a government like the US government (I request your suspension of disbelief) decided to add a node to the node-based cryptocurrency where each citizen got a public key and had an equally weighted vote on how money got spent from this node. At 300 million citizens, each with a different public key of 512 bytes, the reputation breakdown for this single node is going to be 150mb. Assuming that at least ½ of the citizens must agree in order for a transaction to be successful, each transaction would have a minimum of 150 million signatures, meaning 75mb per transaction. This single node has added an enormous amount of bloat to the blockchain. If there are many such bloated nodes, the node-based currency could be overwhelemed. In short, this system is not scalable when used with a traditional blockchain structure. Some solution would need to be devised to safeguard scalability. (one example might be a transaction fee based on size in bytes, and a separate fee-per-block on nodes over a certain size, fee based on the size of the node.)

An addition to the node based protocol could be to allow correlation between multiple keys. For example, you could add a limitation that A and B have a correlation of 3. If A had a weight of 20, and B had a weight of 10, and they had a correlation of 3, then the combined weight of A + B would be '20 + 10 – 3' = 27. This could be useful in a number of ways, though I have no concrete examples at this time.