DECINT WHITE PAPER

Christopher Rae
email: raecd123@gmail.com

Contents

1 Introduction

2 Blocks

2.1 Transactions

Transaction on the DECINT blockchain use the SECP112r2 ecdsa encryption curve to sign transactions transaction are signed slightly differently depending on the transaction type. Currently there 3 different types of transaction the first being the normal token transfer transaction it looks like this:

{time: 1671020930.9900985, sender: "...", receiver: "...", amount: 657.0, sig: "..."}

These types of transactions are made up of 5 parts. The time in Unix Time, the senders public key which consists of a 56 character string generated from the SECP112r2 curve, followed by the receivers public key, then the amount sent and finally the transaction signature the transaction signature is generate from a string of all the information in the transaction separated by a blank space " " and signed using the senders private key. All token transfer transactions have a 1% transaction fee, 0.5% of the transaction goes to the validator of the block which the transaction is in, the other 0.5% is put towards the AI training nodes.

The next 2 types are are pretty similar these are the stake and unstake transactions. Both have the same structure:

{time: 1671020930.9900985, pub_key: "...", stake_amount: 657.0, sig: "..."}

In the case of unstaking stake_amount becomes unstake_amount. the process of signing is the same as with token transfer transaction. There are no transaction fees associated with staking and unstaking.

2.2 Temp Blocks

Blocks are created based on time. As of writing, every transaction that happens within 2 minutes from the first transaction in a block is added to that block, the next transaction after that 2 minutes, acts as the first transaction in the next block and the process repeats.

Temp blocks are made up of 3 parts the head, main body and tail. The head is a list of values the first being the hash of the previous temp block followed by the block index and the time of the first transaction in the block:

["6db4f412053b48a7f2579ed59d28a7d623ef6ebc9d5023b17cb331b8b92d5be8", 2, 1802.9900985]

The main body is made up of all the transactions that occur within the time allocated for that block:

[[HEAD], {"time": 1802.9900985, "pub_key": "...", "stake_amount": 1.0, "sig": "..."},
{time: 1850.23739823, pub_key: "...", stake_amount: 657.0, sig: "..."}]

The tail is added when the next block is created, it is made up of 3 parts.The first holds the blocks hash and the time of the first transaction of the next block. The hash is calculated by concatenating all the signatures and the hash of the previous block into one long string. The second part is the total transaction fees rewarded for validating that block and the final part has 2 values a False

boolean value to indicate that the block has not been validated and the time of the first transaction of the next block

[[HEAD], TRANS,
["0a5d31b6e2c57dc6c81bf916006bd2c412eb79b3cedad7d90ec7a50ab2eeb78b", 1950.23791313],
[6.57], [false, 1950.23791313]]

2.3 Chain Block

The chain block is the most important block when a block is validated it get added to the chain block. Much like the temp block the chain block also is made up of a head a main body and a tail, the head is the same as the temp block the main body however is made up of a json object where the keys are wallets. All transaction recorded in the temp block effect the values stored in the wallet(If the transaction is valid), so if Bob has 100 DCNT and send 20 to Alice, Bobs wallet value would go down by 20 and Alice's wallet would go up by 19.8 and the other 0.2 would be split between the validator and the AI nodes. If Bob staked 20 of his DCNT, his wallet would go down by 20. Instead of storing every transaction the nodes only store the current wallet values.

The Tail is once again made up of 3 parts the first 2 not changing from the temp block but the 3rd part now contains 3 values the first being a True boolean value, the second being the time of validation and the third being the validators public key. The wallet value of the validator increase by the validation reward of the block within the main body of the block.

3 Validation

3.1 Validator

The Validator of a temp block is determined by the hash of the previous block (which is stored in the head of the block). Validation can only occur when the previous block has been validated in order for all nodes to share the same block hashes. The hexadecimal hash is converted into base-10 and used as the seed for the random algorithm. If a validator fails to validate within 20 seconds of the blocks tail being added, the next validator is chosen. This is done by generating the next node in the sequence based of the seed (the previous blocks hash), If that node then doesn't validate within the next 20 seconds the process repeats until the block is validated. If a node fails to validate within the allocated 20 seconds it will lose all the DCNT which it has staked and the node and any future node with the node's wallet will not be allowed to validate.

Each node has a weighted value associated with it dependent on how much has been stake it is scaled linearly. There is a minimum stake amount this is in place to discourage malicious nodes but there are plans to add built in staking pools for users who want to stake without the large upfront cost and running the risk of sending their DCNT to someone else's wallet.

3.2 Validating Blocks

When a transaction is received its time and signature are verified and it is added to the temp block. When validating a validator checks if every transaction to make sure it has the balance to make the requested transaction, if the transaction is true it adds it to a list of true transactions. The list of true transactions gets sent to every node, each node then checks every transaction if it agrees with all the transactions the main body of the chain block is updated with the new balances from, the transaction that occurred in the list of true transactions. If any of the transactions received in

list of true transactions is false the validator will lose all the DCNT which it has staked and the node and any future node with the node's wallet will not be allowed to validate.

If a transaction is not received by the validator it will not be added to the chain block even if another node receives it. Once a block has been deemed valid its temp block is removed from the chain and the chain block is updated. All staking and unstaking transaction are saved with the block index in which they occurred in separate file.

4 Communication

4.1 Structure

TCP is used to communicate messages, which are encoded in UTF-8. All messages are communicated as a string. Each message starts with the protocol and is followed by the information for that protocol. Different Protocols contain different information for example a transacrion message contains the time, sender, reciever, amount sent and the signature. Each segment of the message is seperate with with a space (" "):

TRANS 1802.9900985 ... ... 679.0 ...

It is important to make sure spaces a removed if sending a json object(when updating the blockchain):

"["a":12,"b":34,"c":-3,12]" $\neq$ "["a":12, "b":34, "c":-3, 12]"

4.2 Protocols

5 AI

5.1 Problems