Pluto: A Lightweight, Hybrid Network Cryptocurrency

GitHub repository

Overview

Pluto, a hybrid cryptocurrency designed for the purpose of bartering to eliminate the problem of double spending which had to be rectified by other cryptocurrency projects.

1. **The Pluto Blockchain**

The Pluto blockchain is a simplistic Python program which is a part of all Pluto clients. It is a modified version of an *existing blockchain demonstration* created by howCode for the purpose of educating people around the subject of blockchain technology and Bitcoin. The blockchain has its own preset rules such as the mining difficulty (dependent on which version you download) and block limit/supply (1000000000).

2. **Proof of Work**

Pluto uses a simplified version of the PoW system from other cryptocurrencies such as Bitcoin. Each Pluto node is instructed to automatically accept the longest available chain as the correct one. This is also assuming that the blockchain has the correct required pieces of data. No other PoW systems are in place in order to keep the simplicity of Pluto.

3. **Who Gets The Reward?**

Each block is worth a coin, this simplifies the system a lot. Since the longest chain is automatically accepted as the correct one and adopted, the person who submitted that longest blockchain gets that reward of 1 coin.

4. The Network

The Pluto network is a unique hybrid TCP (Transmission Control Protocol) P2P (Peer-to-Peer) connection of centralized and decentralized technology. It uses a computer's TCP ports to connect to other devices remotely without going directly through the internet or a server/middleman, specifically ports 8080 (server) and 8081 (client). The network relies on one node to become the server, when this node is deactivated the next node becomes the server to replace the previous one. Essentially, this protocol has 1 central point of failure, making it centralized, but at the same time every node is treated equally and is also treated as a client. On top of this despite having one central server, this server is also a client as it can be removed from the network without causing any issues, because of it's replacement making sure the system stays afloat. Making it also be decentralized. Like I said, it's unique. I'm going to be honest though, the network is the most ridiculous thing to program in the whole protocol. The network is basically just a modernized version of the ARPANET, so it's in a way like trying to set up a system from the 70s-90s on technology from 2020. Horrible year by the way. Back on topic though, the network is the most complicated part of the whole Pluto protocol, probably the only complicated part of the whole thing considering the simplicity of the rest of the program. That's why it gets a whole damn page in this thing.

The first person to join the network will become a node, specifically the "server" of the network and have TCP port 8080 used to connect to the next user in the network, whoever that may be. This next person has TCP port 8081 open for the next user and so on, so forth. If the server node is disconnected from the network then the next user in line becomes the new server node. The server node and client node are treated the same and have the same abilities, however they use different ports in order for other nodes to be able to identify what each node is quickly. It uses this "hybrid" system because Python is not compatible with other forms of P2P connectivity, which was obviously super helpful. If everyone suddenly stopped mining then the system wouldn't actually shut down, it would instead go into a sort of cold storage or self preservation mode which allows the Pluto users to keep their balance by downloading a copy of the blockchain for use when mining resumes.

5. **Blocks**

Every block in the chain has a specific set of data that is shared throughout all blocks, although it will be different. To be specific a block contains: Block hash, previous block hash, current owner (identified as the user's account key which is used to identify them and to receive Pluto, in a way a username), block number, hash number (How many hashes did the computer perform to mine the block). When printed in the full network blockchain's output, it looks something like this:

```
Block Hash: blockhashblockhashblockhash
BlockNo: 2
Hashes: 1000000
Previous Hash: prevhashprevhashprevhash
Owner: myplutocoinkey
----------
```

Here you can see all of the block's data. We can see it is the second block in the chain and has the hash of "blockhashblockhashblockhash" while the previous block has the hash of "prevhashprevhashprevhash". Don't worry, your key can't be used to steal your account. It can be shared publicly safely and can only be used to transfer Pluto into the account or to identify which user owns a block.

6. Determining Value

An important part of any cryptocurrency is the value of 1 coin, without this the currency would have no value whatsoever meaning that nobody would use it for anything at all. The value of each block is actually 1 coin, and the 1 coin is deposited exclusively to the person that contributed most to its creation, generally the person to submit the longest chain. A coin's value is determined by the general community demand for coins. If the demand rises then the price rises accordingly, if it falls then the price falls accordingly. Simple.

7. Users

To be able to mine or be in any way involved in Pluto you will need an account. Luckily, Pluto comes with its own built in account and wallet system in order to make setup easier and let you directly store your coins. Signing up will create a new account for you, username being the same as your account key. Your account key is used to identify you and to send coins to you. The account key is generated at random and has no correlation to your password or email. Now that you've got this account you can begin to mine, send, receive and generally use Pluto. (God, I feel like I'm writing a tutorial on how to set it up..)

8. Every Feature Was Once a Flaw

You've heard the saying, "Every feature was once a flaw". Guess what? It's exactly right. Most of what makes Pluto unique was initially only there to keep the program simple and lightweight. They then became features of the program (or more accurately I came up with an excuse to keep them that way). Rather than attempting to fully tackle the double spending problem, for example, the system just doesn't save any data on past owners which prevents them from spending the same block/coin multiple times. Another example is the "hybrid" part of Pluto. It's not like it was ever intended to be a frankenstein hybrid of centralization and decentralization. It just turned out that way due to the Python programming language's limitations/me not being good enough to work around it to deliver the standard network system.

9. Why the hell did I even make it?

Yeah, I asked myself that a lot while trying to get the thing to work. I mean, I was too stubborn to use ERC20 to create it and too dumb to program the thing properly, plus I'm not a literal math wiz so that's how we ended up with this. I initially began to develop this in order to better understand cryptocurrency and how it works. Essentially it was a self education thing. Then I guess at some point I said "You know if this turns out decently I could probably launch this thing onto the web somehow." Now we're here. Hooray, now I can stop going to sleep every night with early 2000s computer jargon stuck in my head. Thank god for that. To summarize that, I'm just some random guy who wanted to understand some weird thing that makes people rich.

10. Math, I always hated math.

Anyone experienced with cryptography or cryptocurrencies is probably asking themself right now, "Where's all the mathematical calculation doohickeys, man?". To that I answer with great sadness, right here. Although no we aren't doing some pythagoras theorem thingamabob or calculating Pi. All we are going to do in this segment is some basic calculations on the testing blockchain, although of course being cranked up to the release hash difficulty for study purposes.

On midrange hardware using the midrange version of Pluto it took 125515862 hashes and 22 minutes to mine a block. This is while the computer is under stress, I'd estimate the hashrate was about 120 compared to its potential of 400h/s.
Using this data we can determine that the amount of hashes required to mine a block at maximum power would be a minimum of 3765475 hashes. This is a 97% decrease from the initial required hashes, using that data you can then determine that it would take roughly 20 minutes at maximum power and efficiency for the computer to mine a block. This is double the amount of time it takes for one Bitcoin to be mined, however the power requirements are lower. Every +1 on difficulty (If I am not mistaken) is actually equivalent to 432 times the previous difficulty. To conclude, each computer can mine a block every 20 minutes. And with the limited supply of blocks this means mining could continue for a total of 95 years constantly on a computer of equal specs.

11. Conclusion

We now have a cryptocurrency protocol that can act as a store of value (Like cash notes or Bitcoin). The currencies network operates in the same way as any other cryptocurrency, although at its core it is a hybrid P2P network (combination of centralized and decentralized P2P network). It has several versions that help it operate on anything between low grade and high grade computers which can all interlink equally via TCP ports. It is unknown how long before the program can be released. Thank you for reading this proposal.

Links

Original Bitcoin White Paper
howCode Blockchain
Official Pluto GitHub Repository
Cryptocurrency Explanation
TCP Ports
ARPANET
Donate to the project (Bitcoin): bc1qzeyteav30ehj8w26pdah4hq8lu488rakjawk2x

White Paper 1 (Can and likely will be replaced by new white paper in future)