Plenteum Whitepaper

Plenteum is a cryptocurrency with a primary objective of replacing enforced transaction fees with a "DustFund" to sustain the long-term viability of the blockchain by creating a sustainable mining reward fund. Through this we provide more control over the future viability of the network to our community members.

What is Plenteum?

Plenteum is a Cryptonote based cryptocurrency and blockchain network that was launched in mid-2018. Crytonote based coins are established in the cryptocurrency space with many successful implementations, such as Monero, Electroneum, Aeon.

Cryptonote based coins are CPU and GPU minable coins and can be implemented with a number of "proof of work" algorithms, some of which are ASIC resistant.

This (ASIC Resistance) was an important part of why we chose Cryptonote as our basis for Plenteum, as this allows every day users to participate in our network on several levels, without having to buy specialist equipment, or hold large amounts of our coin.

Since we are a community focus project aiming to provide more influence over the future viability of the network to our community, we believe that everyday users should be able to participate in all aspects of the network.

Why do we need miners?

Put simply, miners keep transactions moving through the network by adding them to blocks to confirm them.

Without miners, we would not be able to add blocks to the blockchain, and your transactions would be stuck in limbo.

What is an ASIC?

ASIC stands for "Application Specific Integrated Circuit". These are machines, or processors built specifically to solve the "proof of work" algorithm for a specific coin or blockchain. ASIC's produce a significantly higher hash rate than CPU's and GPU's which would negate the viability for everyday users to participate in mining and receive rewards from the blockchain.

Ultimately, allowing ASICs on a network results in a limited few getting most of the base rewards emitted, which is problematic from a distribution perspective.

ASIC's can also cause mining centralization of a network. This is potentially dangerous for cryptocurrency networks as it opens the door to the possibility of a 51% attack.

Why did we create Plenteum?

Before we get into the details of why we created Plenteum, it's important to first understand a few fundamentals of "proof of work" based cryptocurrency networks as they stand today.

- Current implementations rely on charging the end user a fee to process transactions on the network.

- The reason fees exist in the first instance is to be able to provide rewards to miners for mining on that network.

- Once a coin has emitted its total supply (the maximum amount of coins that can be in circulation), the sustainability of the network becomes heavily dependent on these fees being enough to keep miners incentivized to continue mining on that network.

- Fees are based on the "physical" or byte size of a transaction, not the actual monetary amount.

Due to the way transactions work behind the scenes, dust gets created in the blockchain and users' wallets.

We created Plenteum to introduce a new concept that aims to solve two fundamental problems:

1. **Dust clogging up wallets and the blockchain**
2. **Fees being too expensive for users, or not enough for miner's incentive to sustain the blockchain into the future.**

This is done by implementing a new feature called the "**DustFund**".

The DustFund will then supply mining rewards, instead of fees when the coin enters its tail emission phase (when it's nearing its total supply in circulation, and base rewards are lower).

How do cryptocurrency wallets work?

First, there is no physical "balance" stored in a crypto wallet or in the blockchain for any address. When a wallet is first created there are no transactions and thus, the available balance of the wallet is 0.

Then someone sends you some coins. This is stored in your wallet as incoming transaction(s), all of which are grouped together to make up your available balance. When you then send some of that coin to another address, the "unspent" amounts (i.e.: the amounts left over from the sum of your incoming transaction that have not been sent to another address) from the transaction(s) are returned to your wallet as "unspent transaction outputs", or UTXOs. The combination of your incoming transactions and unspent transaction outputs is what makes up your balance. This is calculated by your wallet by scanning the entire blockchain to find these transactions that might exist in any of the blocks on the chain to date.

What is Dust?

Dust is basically the tiny amounts that are left over on each transaction (less than 0.01) that are "un-spendable" because they are less than the minimum fee required to send a transaction on a network, or less than the enforced minimum amount.
Dust is problematic for blockchains as those UTXOs accumulate and cause "bulk" in the chain and the wallet they belong to.
It's also problematic for users as it causes their transactions to be too big (in bytes) and therefore pushes up the fees they require to consolidate those dust UTXOs together into spendable amounts.

Users may also need multiple wallets to be able to group and send UTXOs to themselves to consolidate those amounts into one.

So how does it work?

How this works is that fees will not be mandatory on our network, any transactions can be sent completely free of charge (although users may opt to pay a fee in order to increase their transaction priority).

Instead of then returning dust to users' wallets, dust is grouped and accumulated into the DustFund on the blockchain itself.

Should the user elect to pay a fee, a minimal portion of fees paid will also contribute to the DustFund. The large majority of the fee will be paid to miners to allow for faster throughputs of those transactions.

Plenteum uses a system of 8 decimal places, only 2 of which are usable, or visible in a user's wallet. From a usability perspective this is more in line with what people are used to with fait currency. The remaining 6 decimal places (e.g. 0.00######) is the dust.

The user will never actually see these amounts as they're smaller than the amounts the wallet will display.

Wallet balances are always displayed as floored to the closest 2 decimal places.

However, it's important not to think of this in terms of physical amounts. This system works in that if the block rewards from the DustFund are lower, that will drive the price up, maintaining the incentive (as scarcity becomes more of a factor). If the block rewards are higher and transactions (previous transactions) have been plentiful, the value may reduce, but the circulation increases, so this system allows things to stay "in balance" more naturally.

Ultimately this system leaves the future of the blockchain and the value of the currency entirely in the users / participants hands, as the

A scenario:

Let's say you start out with a new clean wallet, and someone sends you 100.00 PLE (for arguments sake). That comes into your wallet in the form of a transaction, which is stored on the blockchain in the block that the transaction was sent in.
The following day, you decide to send 20.00 PLE to someone else... As we explained earlier, this works by taking in your original transaction of 100 PLE as an "input", the 20.00PLE you are sending out goes in a "Spent" output, and the remainder of 80.00 PLE is returned to your wallet in the form of an "Unspent Transaction Output" (UTXO)
In the above scenario, it's clean and there is no dust.

Now, let's say you send a few different amounts to different people, each of your spends will generate a UTXO, which are all stored in the blockchain as having been returned to you (as UTXO's).

You do this (spend) a few times and dust UTXOs will accumulate in the blockchain and in your wallet. Depending on the amounts you send, and depending on the amounts you receive from others, there will be dust for at least some of the resulting UTXOs.

In current fee based implementations, these can be grouped together and "consolidated", but because fees are based on the "byte size" of your grouped transactions, it's often VERY expensive to consolidate all your dust into one transaction, and you also need a second wallet to send it to.
Finally, you'd have to pay a fee again to send it when you want to spend it.

* remember that the available balance you can spend, comes from the sum of all your UTXOs, so when grouping multiple transactions, and spending portions of this, the likelihood of their being DUST in at least some (not all) of your transactions increases.

implementation decisions of the development team have less of an impact.

Also, block rewards will be more consistent for miners, as they will be based on the available funds in the DustFund and not of the available fees within a single block.

There are no enforced fee levels, lowering entry barriers, transaction size (in terms of bytes) is no longer a consideration for the average user, and does not impact the ability to transact on the network, and the blockchain itself is left lighter and therefore capable of handling more volume in transaction numbers.

How does this help the longevity of the blockchain?

As previously mentioned, current block chains rely on fees (in combination with emission rewards). This is potentially problematic as there's uncertainty whether the fees will be enough to sustain the incentive to mine, or whether they will become too expensive for users. The current "system" requires a fine balancing act and with Bitcoin, a single transaction can already cost in the region of $20 USD!

Plenteum's solution is to accumulate the dust amounts left over from UTXOs and use this to build up a DustFund over time. The more transactions there are on the blockchain, the quicker this fund will grow and sustainability is therefore fundamentally based on usage.

The major difference with fee only based implementations is that the DustFund will pay more consistently per block to miners, as it's emission will be based on averages over time, rather than fees accumulated within the current block being mined. This allows miners to more accurately predict their returns and not mine purely based on the hope that transaction fees will cover the cost of mining and be profitable.

What's in a name?

The name Plenteum refers to being plentiful. This is related to the ultimate longevity and sustainability of the blockchain and has nothing to do with the ultimate capped money supply of 21 billion units of Plenteum.

Where to from here?

The development roadmap for the foreseeable future is available on our website. Beyond that we will be determining future direction based on community feedback and participation. As we've indicated, one of the key outcomes of the solution we are implementing, is that it gives more control over the future of the coin to the community. It's this community driven approach we want to build upon to determine future direction, as we don't presume to know what the community's needs will be years from now.