PANDANITE

Panda TEAM*

Date: February 2023

1 Introduction

Pandanite is a minimalist implementation of a layer-1 crypto-currency similar to Bitcoin. Pandanite is designed with utmost simplicity, performance, and user friendliness in mind and is written from the ground up in C++. Our hope is that Pandanite will be a more portable and lighter weight codebase than Bitcoin, enabling Pandanite nodes to run on a broad range of low-cost devices yielding a democratized network that is both fast-growing and expansive

2 Circulation

Bamboo is minted by miners who earn rewards. Mining payments occur using the following algorithm, which yields a total final circulation of 100M PDN:

- 50 PDN per block until block 666666
- $50 * (2/3)$ PDN per block from blocks 666667 to 2*666666
- $50 * (2/3)^2$ PDN per block from blocks 2*66666+1 to 3*666666 etc.

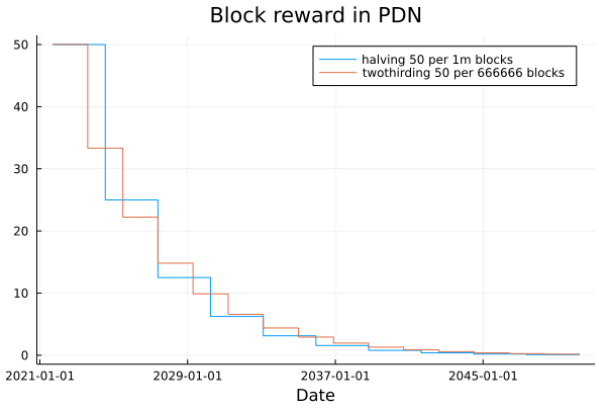

Figure 1: The payout curve is smoother in twothirding compared to halving:

*founder Mr. Panda Bear

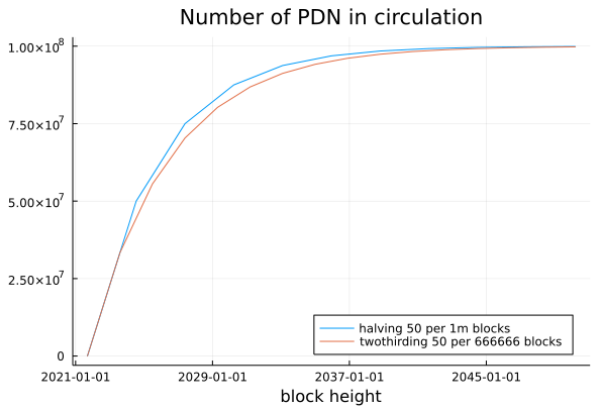

Figure 2: Block reward changes are more often and have less impact compared to halving.

3 Core Objectives

Pandanite coin is intended to do as few things as possible and to do them incredibly well – it is a store of value coin that:

- Maintains account balances for billions of users.
- Provides extremely fast transactions between these accounts.
- Runs on low-cost hardware.

That's it. We don't aim to solve everything. We desire to keep the code simple.

4 Implementation

Pandanite is written in less than 6K lines of code (Bitcoin has ¿100K). There are a few optimizations that we have made to help further our core objectives:

- Switched encryption scheme from secp256k1 (which is used by ETH & BTC) to ED25519 – results in 8x speedup during verification and public keys half the size.
- 25,000 transactions per block
- 90 seconds block time
- SHA-256 based proof of work

Each block can contain between 1 and 25,000 transactions. The single transaction that is required is the block mining fee paid out to the miner wallet.

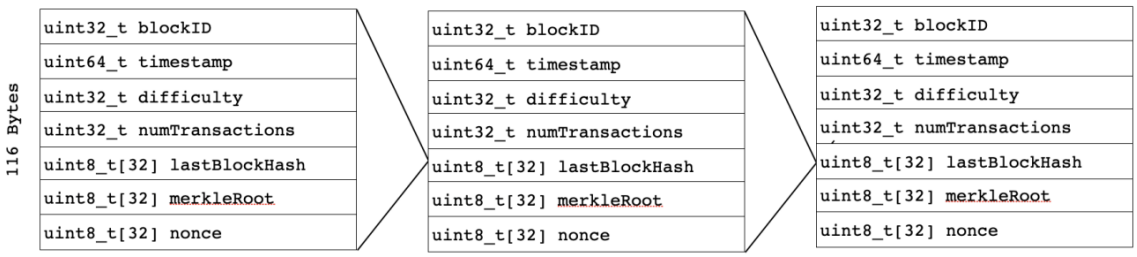

Figure 3: The basic structure of the blockchain is almost identical to Bitcoin

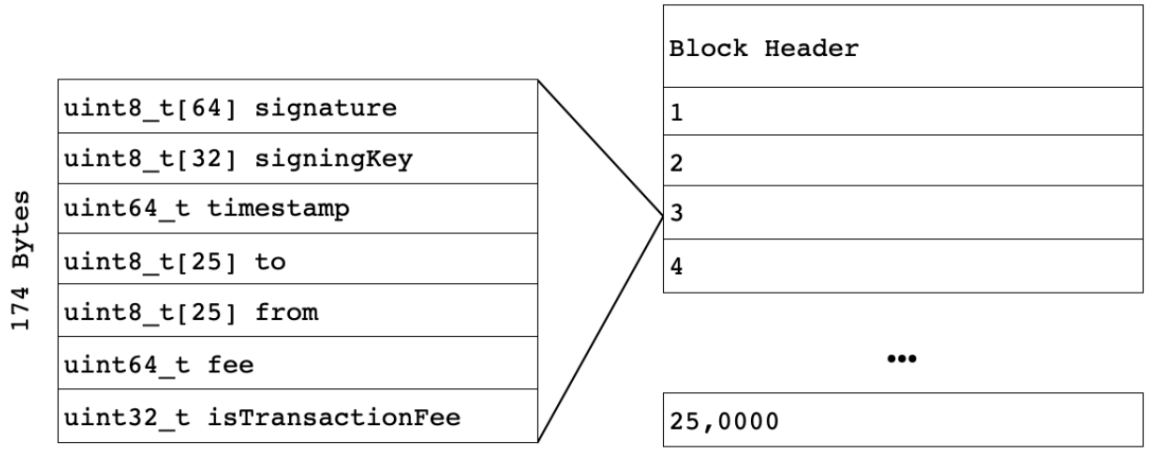

Figure 4: There are up to 25,000 transactions in a single block

5 Account Representation

Each node stores a ledger containing a mapping between the wallet address (25 bytes) and the total balance (8 bytes). This means each gigabyte of diskspace supports roughly 30 million users. Furthermore the nodes store a list of all previously seen transaction hashes (32 bytes each) in order to verify that submitted transactions have not executed in the past. For 1 million blocks at full capacity this represents roughly 800 GB of disk space.

6 Digital Signitures

A key design objective of Pandanite is low compute usage while maintaining a high number of transactions per second. To reach these performance goals Pandanite uses an alternative digital signature system known as ED25519 as a replacement for Bitcoin and Ethereum's secp256k1. ED25519 has several attractive properties for crypto-currency use cases:

- Fast signiture verification
- Batch signiture verification
- Fast signing
- Small public keys
- Performant on low-cost IoT devices

The first iteration of Pandanite utilizes the ref10 implementation of ED25519, which will be replaced with a higher performance custom implementation supporting features like batch verification as the network scales. To provide insight into the performance characteristics we provide comparisons between Rust implementations of ED25519 against a Rust wrapper of Bitcoin's native libsecp256k1.

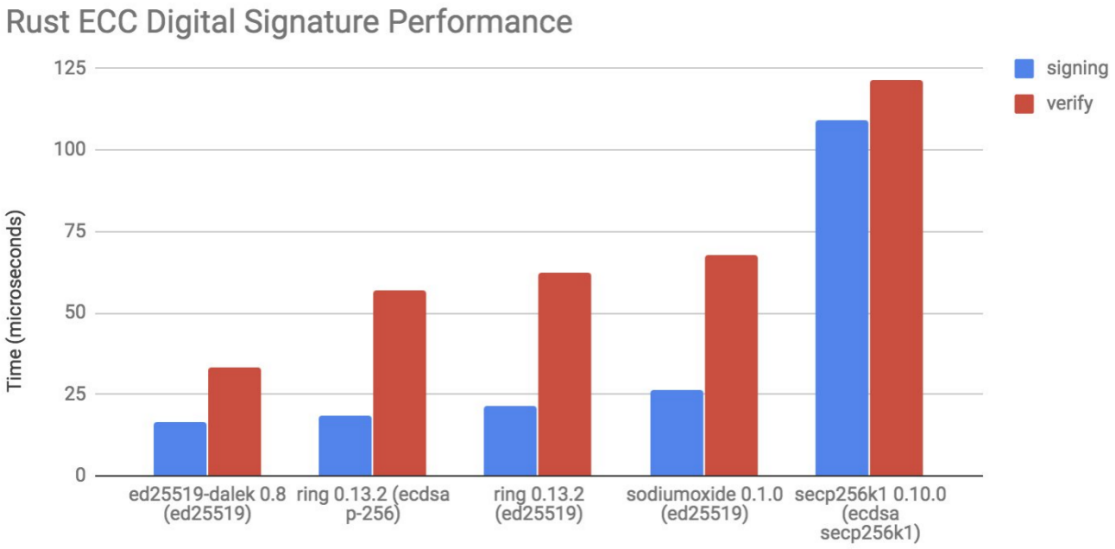

Figure 5: Performance comparison of digital signature algorithm implementations

7 Proof Of Work

Pandanite uses a simple proof of work scheme based on SHA256 and Pufferfish 2 (P). Given a block header B and it's hash $H = \text{SHA 256}(B)$ the miner must provide a 256-bit nonce N such that SHA 256$(P(H||N))$ has a minimum of k leading zero bits, where k is a difficulty parameter.

$$\gamma(\text{SHA 256}(P(H||N))) > k \tag{1}$$

Difficulty is then measured in bits and the number of hashes expected prior to finding a valid nonce at difficulty k is simply 2^k. Difficulties adjust every 100 blocks based on the ratio of elapsed to expected time. Pufferfish 2 is an ASIC resistant memory hard hash function developed for the password hashing competition by Jeremi M. Gosney.

8 Performance

Pandanite coin is designed to support a peak rate of 250 transactions per second (tps), significantly greater than Bitcoin (7 tps) or Ethereum (15 tps). This is due to a larger block size than Bitcoin's (4.35 MB vs 1MB) and shorter block mint time (90 sec vs. 600 sec). We believe that faster internet connections in 2021 than 2010 will enable us to push these fixed limits without yielding an excess number of forks in the network.

9 Roadmap

The Pandanite project timeline:

- February 2022: Pandanite launch
- Soon

10 Conclusion

We have presented our vision for Pandanite: a minimal and elegant layer-1 crypto-currency codebase that can do basic transactions quickly and efficiently for billions of users across a broad number of devices. It is our hope that Pandanite code will always be compact and clear enough that even novice programmers will be able to modify and improve Pandanite. For more information please visit us on:

- Github
- Bitcointalk
- Discord