Aptum Protocol

Lucas Nestler, Chris Mrozek

August 5, 2019

Abstract

We present a decentralized and distributed platform equipped to meet and surpass the capacity currently maintained by centralized payment processors. Through the implementation of an account-based transactional model aided by lossless compression algorithms and an intelligent checkpointing system, our proposal, Aptum [AP], is tailored to handle the heavy demands of real currency (high speed and massive throughput). Supplementary to exceeding the requirements of the financial consumption market, built-in is a methodology to keep inflation in check by rewarding currency savers via interest earnings created directly out of a low and healthy inflationary rate. All is handled via our proposed energy-efficient multi-layer model that maximizes security on the first layer and allows for decentralized applications and smart contracts on the second layer.

I. Introduction

Two of the main problems with current implementations in blockchain technology are scalability and adaptability. Bitcoin and similar cryptocurrencies can process approximately ten transactions per second, while VISA and other centralized payment processors can handle more than one thousand times that much. Furthermore, there are multiple centralized payment processors, which together process more than twenty-one thousand non-cash transactions per second[1]. A proposed cryptocurrency solution, therefore, must be able to handle the baseline minimum established by existing centralized payment processors and process them without the need for an exterior payment processor. Bitcoin and similar systems cannot provide the needed speeds, even with the proposition of removing the limitation of block size[2]. This proposed solution is hotly debated as it will also add new issues[3]. Even if one were to ignore the unique issues that are inherent with the proposed Bitcoin solution, the removal of block size limitations would still not be sufficient. It would provide only up to ten-thousand transactions per second on an average computer. An ordinary computer with a quad-core CPU and a 2MB/s DLS connection (each transaction is made of 200 bytes).

II. Transactions

The "Aptum" protocol proposed the following in order to address and solve the issue of scalability. By using an account-based transaction model, as implemented in Ethereum[4], the memory required for each transaction to be stored in the blockchain can be reduced to 140 bytes that store all relevant data. Those bytes includes not only the input and the destination address but also the transaction amount, a nonce to protect against replay attacks and a signature to prove its origin. Unfortunately, Ethereum still does not meet the target speeds desired to match centralized payment processors. Aptum proposes a solution to enhance the throughput to 24 thousand transactions per second. The input and the output are two addresses that are redundant data stored many times in the blockchain. Therefore these can be replaced with a smaller chunk of data, similar to how lossless compression algorithms

III. Usernames

Since those five bytes do not need any specific property, they can be self-assigned by any user and act as on-chain usernames. On-chain usernames allow anyone to send funds to anyone else, using the username they give themselves. This username-implementation means Alice can send ten units of a shared currency to Bob, without Bob telling her his lengthy and unspeakable address. Instead, Alice enters "Bob," and the blockchain does the rest. A similar everyday example is an email where one can send to an email address instead of a lengthy and unreadable string of characters. Considering that most individual's usernames are reused and not unique[6], it is effortless to donate or move funds based on someone's handle.

IV. Checkpoints

Additionally, there is the issue of a massive ledger everyone must host in existing protocols. With 2MB/s, approximately 64TB are added to the blockchain every year to ensure secure and immutable storage of data. Blockchain bloat has become a significant issue and will only continue to snowball as time goes by. One advantage of cash, making it such an ideal tool for commerce is speed due to the absence of a ledger. Cash purchases of the past do not have to be recorded forever. Cash transactions are not provable after funds have changed hands. The vital part of the transaction in financial exchange is the transfer of funds, not the permanent storage of the transaction. In the Aptum protocol, this property of cash-money has been adapted to the blockchain. By creating a checkpoint which saves the previous state of the blockchain after every block, the old chain can be discarded without concern. When using a checkpointing system like this, the maximum size of the entire blockchain will never be more extensive than one block plus the previous state of the blockchain. In numbers, the capacity of the state with several active users similar to bitcoin[7] and the transaction throughput necessary to process all non-cash transactions is approximately 256MiB. Ensuring that there are no chain splits, a hash of the previous state is appended to the block. The hash of the last state, therefore, is a direct replacement for the hash of the past block.

V. Consensus

To ensure that chain splits will not happen in the first place, a robust consensus algorithm which is as distributed as possible is needed. Achieving this robustness is the reason Pure Proof of Stake (PPoS) is utilized. Pure Proof of Stake ignores the age of the stake entirely and takes nothing but the staked funds in the account, increasing the incentive for all investors to stake. PPoS encourages the most people possible in decision-making by rewarding only the people who actively stake their coins. Non-participants forfeit their potential interest earnings to active participants. Additionally, by staking funds, they are removed from the market. Therefore, this implementation decreases the trading supply while keeping the demand, which in turn drives up the price.

VI. Second Layer

To ensure that trades can be done safely and decentralized, an enforceable contract layer is necessary. Aptum adds a second layer to deploy decentralized applications or contracts. In contrast to Ethereum and similar implementations, Aptum does not use smart contracts[8] to create a new chain or interfere with it. Instead, Aptum creates new independent chains, which all have their separate source code. A second-layer chain, or side-chain, can interact with Aptum, by transferring coins or reading from the original chain. Other than those fixed operations, a side-chain provides complete freedom. Since the side-chain does not come with a language, any programming language can be used to write for it, leaving a Turing-complete basis for developers from every origin.

VII. Emission

A reward for adding security to the first layer is required to have a high-security level consistently. By emitting new coins to the address of the one who creates the new block, there is a reward for participating. The reward diminishes with more people securing the network, which is why Aptum proposes an increased compensation for an increased difficulty[9] as first introduced by MonetaVerde[10]. By increasing the total reward per block if more coins are staked, the average payment per staked coin stays the same, even if an attacker buys a large portion of the stake. Similarly, to MonetaVerde, Aptum proposes the usage of the square of the second logarithm of the difficulty multiplied with the base reward to be the total reward of a block. Instead of reducing the emission over time, a constant base reward of one-thousand coins is used. So, if the bonus should increase from sixteen to twenty-five thousand coins per block, the amount of staked coins would have to double. With an average block time of fifteen seconds, a minimum of 2.19 billion coins will be emitted every year.

VIII. Monetary Policy

A monetary policy of having an (almost) constant emission forces the ecosystem to be conducive to spending coins rather than just holding on to them[11]. Being able to spend a currency is the most crucial part about it, other than being a store of value. Something must be used to be a store of value, implying that a spendable currency with modest inflation is usually worth more (by market cap) than a limited resource. The largest and most used currency, the US Dollar, has a high supply[12], which can be seen as a correlation between abundant supply and usability. Therefore emitting billions of coins per year helps to build a healthy financial system. Unfortunately, with a high amount, a low value per unit comes as well, which is why it is recommended to use a different measurement. There are 2’190’000’000 AP emitted every year and a minimum of one-thousand AP is pushed out every block.

References

[1] https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf

[2] https://medium.com/@sumsun.he/bitcoin-sv-mainnet-stress-test-report-english-translation-35533556c640

[3] https://bitinfocharts.com/comparison/bitcoin%20sv-size.html

[4] https://blockonomi.com/utxo-vs-account-based-transaction-models

[5] https://en.wikipedia.org/wiki/Lossless_compression

[6] https://www.freehaven.net/anonbib/papers/pets2011/p1-perito.pdf

[7] https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

[8] https://en.bitcoin.it/wiki/Contract

[9] https://en.bitcoinwiki.org/wiki/Proof-of-stake#Mining_Process

[10] https://bitcointalk.org/index.php?topic=653141.0

[11] https://github.com/mimblewimble/docs/wiki/Monetary-Policy

[12] https://fred.stlouisfed.org/series/M2