

WhaleCoin

Rhett Creighton, Amber Hancock

Austin, TX, USA

rhett@heyrrhett.com, amberrayh@gmail.com,

Chain Starter, Inc.

August 27, 2017 WORKING DRAFT

Abstract. We describe a simple mined cryptographic blockchain which is designed to power a unique decentralized social network. The social network supports several types of roles and notably the “Whale” role which is given to any user who holds at least 1,000 tokens. The total number of Whales on this network will always be limited and Whales will have the power to influence how blockchain rewards are distributed. An incentive structure will be designed so that “Followers” will attempt to gain approval from Whales who will then influence the blockchain to send them rewards.

1 Designing an Exclusive Club on a Blockchain

The founding principle of WhaleCoin is a simple idea: if you have 1,000 WhaleCoins or more, you are a “Whale”. Whales have the power to send upvotes to other users.

Unlike other social networks where upvotes or “karma” have no inherent value, in WhaleCoin, the blockchain will pay users a portion of the mined block reward based on how many upvotes a user received from the Whales.

Like other cryptocurrency, WhaleCoin is mined, limited in supply, and impossible to counterfeit[1].

2 Decentralization and Participation in WhaleCoin

There are only two ways to obtain most cryptocurrencies:

- Mine them using special hardware, electricity, and technical knowledge of the process.
- Buy them using cash if local, or more likely using other cryptocurrency on some kind of internet exchange.

Unfortunately, the vast majority of people on the planet still do not have easy access to the two processes described above as they can be expensive and technologically difficult to get started. In order to spread awareness and use of cryptocurrencies, it is important to provide people with cheap and easy ways to become invested in a crypto-community.

For example, Blocki and Zhou described a process where humans could mine a cryptocurrency by solving CAPTCHAs in “Designing Proof of Human-work Puzzles for Cryptocurrency and Beyond”[2]. However, a key piece of technology known as a cryptographic obfuscator[3] requires further development for this process to work.

Giving away currency has proven to be a successful way to attract new users in the past. Noted early Bitcoin investor Roger Ver received his first Bitcoin from an online “faucet” set up by Gavin Andresen[4]. Stellar claims over 6 million Facebook auths due to their giveaway[5]. But these giveaways do not ensure long-term interaction of the new users with the coin.

In contrast to simply giving away coins, or to the difficulty of creating CAPTCHAs for humans to solve, WhaleCoin taps into the natural behavior that people already exhibit of continually following other people on a social feed.

3 Steem / Steemit.com Case Study

Since launching in 2016:

- Steem is currently the 22nd most valuable cryptocurrency on <https://coinmarketcap.com> with a market cap of \$347,163,415.
- Alexa.com ranks steemit.com as the 1,370 most popular U.S. website and 2,428 most popular website globally.

Steemit is a social network site similar to Reddit where users can post links or longer form articles. Everyone is able to upvote posts or comments, and the blockchain pays a portion of the block rewards to users based on upvotes received. In order to prevent people from spamming by creating many accounts to send upvotes with, upvotes are weighted with the amount of Steem currency which a user holds.

This has the effect of users being paid much more if they receive an upvote from a “Steem Whale”. A full list of Steem Whales can be found at <https://steemwhales.com/> . The algorithm has gone through several changes to determine vote weight after many users complained that the Whales had too much influence.

The authors of this paper believe that, while Steemit is a novel and groundbreaking project, a flaw in the user experience is that it solicits everyone to post whatever they want, but mostly rewards people only if Whales happen to send an upvote. This leaves many users frustrated when they put effort into high quality posts which may not fit the tastes of Whales, or perhaps happens to get overlooked by Whales on that particular day. In Steemit, the top 20 Whales may be so powerful that it actually hinders the value of the community. It feels impossible to catch up to the Whales that already have millions of coins. By contrast in WhaleCoin, each Whale with over 1,000 coins has equal power. The mined blockchain can support a maximum of 864 new Whales every 30 days at a 5 coin reward rate every 15 seconds.

4 WhaleCoin User Experience Design

On the WhaleCoin platform, Whales are the star of the show intentionally. Whales can share news stories that they've read or videos that they've watched, or a Whale might ask followers for advice or research. To send an upvote to a Follower, it only costs a Whale a blockchain transaction fee, but is otherwise free. This is similar to tipping, but at no cost to the Whale.

Followers, on the other hand, are humans (or possibly bots) that are rewarded for doing a task that Billions of people already do every day: follow a social network feed and interact through comments.

Because WhaleCoin is decentralized, an unlimited number of portals could be built on top of it, which could include chat, SMS, email, or other integrations. It may be possible, for example, to build a decentralized personal assistant application on top of WhaleCoin.

5 Technology Overview

WhaleCoin is a fork of Ethereum and shares many things in common with Ethereum. However, in Whalecoin, consensus rules state that miners must pay a fraction of their mining reward to a smart contract.

The smart contract will split the rewards several ways including:

- A Developer's Fund for development and maintenance of the WhaleCoin code and surrounding applications such as a social network Dapp that connects to Whalecoin.
- Rewards paid out to followers of whales based on upvotes from whales. The reward algorithm should have anti-spam limit to ensure that a small minority of whales don't control a large fraction of the reward. Also, upvote rewards should decay over time to incentivize followers to participate in the social network and block chain.

It is possible that the rewards will also be split to include a moderator role to help ensure that the network runs optimally and to prevent anti-spam attacks. The contract rules will likely be updated after launch to promote decentralization and participation in the network.

6 Mining Schedule

Whale coin will use the same mining schedule as Ethereum, which is currently 5 coins every block. Blocks are mined through proof of work approximately once every 15 seconds.

For the first 200,000 blocks (approximately 35 days), rewards will not be paid out to Whale followers. The reason for this is to allow the initial set of coins to be mined in a fair and decentralized manner.

After block 200,000, anyone that holds at least 1,000 Whale Coins has the option to be a “Whale”. Being a whale allows a user to send upvotes to other users in the reward distribution smart contract.

Ethereum has an experimental plan to switch consensus algorithms in the future to Proof of Stake. It is currently unknown whether WhaleCoin would upgrade along with Ethereum, or if it would keep using the same consensus algorithm. Most likely, WhaleCoin would wait and see how software changes affect other blockchains first before making any major changes.

7 Risks

There are many risks involved with launching and deploying any new decentralized mined currency. Some of the risks that would be involved in this process include:

- Designing properly tuned economic smart contract rules. It is possible that someone will find a way to game or cheat a contract that handles the logic for a reward unlocking mechanism.
- There could be bugs or vulnerabilities in an unlocking smart contract that gives an attacker access to the funds.
- Some social networks have more or less success than others. It can be difficult to predict this success or failure ahead of time.

This list is not exhaustive. Whalecoin is an experimental idea and the authors of this paper are not able to predict all of the problems which might occur once it is put into practice.

References

1. Satoshi Nakamoto. Bitcoin: A Peer-to-peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>, Oct 2008.
2. Jeremiah Blocki, Hong-Sheng Zhou. Designing Proof of Human-work Puzzles for Cryptocurrency and Beyond. <https://eprint.iacr.org/2016/145.pdf>, August 24, 2016.
3. Garg, Miles, Mukherjee, Sahai, Srinivasan and Zhandry. Secure Obfuscation in a Weak Multilinear Map Model. <https://eprint.iacr.org/2016/817.pdf>, 2016
4. 20 questions with Roger Ver (Exclusive Interview) <https://steemit.com/life/@wadepaterson/20-questions-with-roger-ver-exclusive-interview>
5. Stats - Stellar <https://www.stellar.org/stats/>