STEEM / BLUEPAPER

A protocol for enabling smart, social currency for publishers and content businesses across the internet

Introduction

Steem provides a scalable blockchain protocol[1] for publicly accessible and immutable content, along with a fast and fee-less digital token (called STEEM)[2] which enables people to earn the currency by using their brain (what can be called "Proof-of-Brain"). The two building blocks of this protocol, both blockchain and token, depend on each other for security, immutability and longevity, and are therefore integral to each others' existence. Steem has been successfully operating for over a year, and has now exceeded both Bitcoin and Ethereum in number of transactions processed.[3]

Compared to other blockchains, Steem stands out as the first publicly accessible database for immutably stored content in the form of plain text, along with an in-built incentivization mechanism. This makes Steem a public publishing platform from which any Internet application may pull and share data while rewarding those who contribute the most valuable content.

In the field of crypto-currencies, the unique properties of STEEM make it both "smart" and "social"compared to others, such as bitcoin and ether. This stems from two new token features. The first is a pool of tokens dedicated to incentivizing content creation and curation (called the "rewards pool"). The second is a voting system that leverages the wisdom of the crowd to assess the value of content and distribute tokens to it. These two unique properties when combined are referred to as Proof-of-Brain, which is an entendre based on Proof-of-Work[4], meant to emphasize the human work required to distribute tokens to community participants. Proof-of-Brain positions STEEM as a tool for building perpetually growing communities, which encourage their members to add value to the community through the built in rewards structure.

In addition to these advancements in blockchain and token technology, Steem as a system provides additional advanced features to enhance the user experience, such as Stolen Account Recovery[5], escrow services, user promoted content, a reputation system, and savings accounts. This is all done while providing users with three second confirmation times and zero fees on all transactions. All of this allows it to support the mission of bringing smart and social currency to publishers and community builders across the Internet.

Proof of Brain: Smart and Social Tokens

Token systems that reward users as they contribute to a token-based community system require mechanisms for establishing and evaluating content's social value: we call this "Proof-of-Brain."

[1] Delegated Proof of Stake Position Paper. Grigg, 2017.
https://steemit.com/eos/@iang/seeking-consensus-on-consensus-dpos-or-delegated-proof-of-stake-and-the-two-generals-problem

[2] To differentiate it from the term for its blockchain, the correct spelling of Steem's native digital token is STEEM.

[3] Transaction Volumes: Transactions Per Second Report. Steem Witness and user "@roadscape".
https://steemit.com/blockchain/@roadscape/tps-report-2-the-flippening

[4] Proof-of-Work. Wikipedia.
https://en.wikipedia.org/wiki/Proof-of-work_system

[5] Stolen Account Recovery initiation for Steemit.com users: 07-13-2017
https://steemit.com/recover_account_step_1

The Rewards Pool (“Where do the tokens come from?”)

One of the most innovative (and most misunderstood) aspects of the Steem blockchain is the “Rewards Pool” from which tokens are distributed to valuable content creators. In order to understand what the Rewards Pool is, one first needs to understand that tokens are produced differently in DPoS blockchains than they are in PoW blockchains. In traditional PoW blockchains, tokens are produced regularly but randomly distributed to the people whose machines are performing work (“miners”).

Different from PoW-only cryptocurrencies, tokens in Steem are generated at a fixed rate of one block every three seconds. These tokens get distributed to various actors in the system based on the defined rules of the blockchain. These actors, such as content creators, witnesses, and curators, compete in specialized ways for the tokens. Unlike the traditional PoW means of distribution, where miners are competing over raw computing power, the actors in the Steem network are incentivized to compete in ways that add value to the network.

The rate that new tokens are generated was set to 9.5% per year starting in December 2016, and decreases at a rate of 0.01% every 250,000 blocks, or about 0.5% per year. The inflation will continue decreasing at this rate until it reaches 0.95%, after a period of approximately 20.5 years.

Of the supply of new tokens created by the Steem blockchain every year, 75% of those tokens compose the “rewards pool” which are distributed to content creators and content curators. 15% are distributed to vested token holders, and 10% are distributed to Witnesses, the block producers cooperating inside Steem’s DPoS consensus protocol.

Rewards for Content Creators and Curators

The users who produce content are adding value to the network by creating material that will drive new users to the platform, as well as keep the existing users engaged and entertained. This aids in distributing the currency to a wider set of users and increases the network effect. The users that take time to evaluate and vote on content are playing an important role in distributing the currency to the users who are adding the most value. The blockchain rewards both of these activities relative to their value based on the collective wisdom of the crowd collected through the stake-weighted voting system.

Voting with Staked-Tokens to Determine Allocation of Rewards

Steem operates on the basis of one-STEEM, one-vote. Under this model, individuals who have contributed the most to the platform, as measured by their account balance, have the most influence over how contributions are scored. Stake can be bought or earned. Users can not gain additional influence by owning multiple accounts, since one single account with an amount of stake will have the same influence as two different accounts sharing the same amount of stake. The only way for users to increase their influence in the platform is to increase their stake.

Furthermore, Steem only allows members to vote with STEEM when it is committed to a 13 week vesting schedule called Steem Power. Under this model, members have a financial incentive to vote in a way that maximises the long term value of their STEEM.

Speed and Scale on the Steem Blockchain

The Steem blockchain is designed to be one of the fastest and most efficient blockchains in existence, which is necessary to be able to support the amount of traffic expected on a social media platform larger than the size of Reddit. Steem has already surpassed Bitcoin in number of transactions, and is able to scale to support 10,000 or more transactions per second.

Delegated Proof of Stake (DPoS)

Often bottlenecked by Proof-of-Work (PoW)[6], many blockchains can't scale beyond three transactions per second, which is a fraction of the world's financial traffic. Steem needed far more scale and speed than that offered by PoW, and so a lesser known algorithm called Delegated Proof of Stake (DPoS)[7] was leveraged to lay the foundation for a blockchain suited for billions of users.

Because of DPoS, the Steem blockchain is able to generate a new block every 3 seconds with minimal computational load. This means that the blockchain can process more transactions and hold more information, including content.

By defining the rules for when a Hardfork occurs, the witnesses elected within the DPoS framework can quickly and efficiently decide on whether or not to move forward with a proposed hardfork, allowing the Steem blockchain protocol to evolve more rapidly than most others. The Steem blockchain has already successfully forked 18 times[8], and each time a Hardfork has occurred, only a single chain has persisted after the fork.

ChainBase

ChainBase[9] is the database portion of the blockchain stack and replaced Graphene[10] in 2016. ChainBase has faster load and exit times, supports parallel access to the database and is more robust against crashes than its predecessor. It also has less frequent database corruption, allows instant "snapshotting" of entire database state, and can serve more RPC requests from the same memory.

AppBase

AppBase is the first step in creating a multi-chain FABRIC. AppBase enables many components of the Steem blockchain to become modular by creating additional non-consensus blockchains as dedicated plugins. These plugins can be updated much more rapidly because they do not require

[6] Bitcoin Scalability Problem
https://en.wikipedia.org/wiki/Bitcoin_scalability_problem

[7] DPoS Whitepaper
https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

[8] https://steemit.com/steemit/@steemitblog/proposing-hardfork-0-20-0-velocity

[9] ChainBase Release
https://steemit.com/steem/@steemitblog/announcing-steem-0-14-4-shared-db-preview-release

[10] Graphene Documentation
http://docs.bitshares.org/

replaying the entire blockchain. This makes steemd[11] far more efficient and easier to maintain and scale.

Practically speaking, AppBase enables different cores, or even different computers, to maintain different parts of the Steem blockchain. This is significantly more efficient than requiring every core, and every computer in the network maintain the entire blockchain. Modularizing the blockchain enables it to take full advantage of the modular nature of computers. This is one necessary step in the long process of creating a fully parallel, fully optimized blockchain.

Steem's Platform Features

The Steem blockchain serves a dual purpose of being a digital token processing system, as well as a mainstream social media platform. The features offered by the blockchain need to support both purposes, and provide users with a world class experience when using both aspects of the platform.

Primitives Designed for Content Applications

Steem offers users the unique ability to publish and store different types of content directly and permanently into the immutable ledger of the blockchain as plain text. Once stored in the blockchain, data becomes available publically for developers to build from. Developers are able to interact with the content directly in the blockchain using the available APIs. Several of the blockchain primitives developers can build from include Account Names, Posts, Comments, Votes and Account Balance.

Native Name System

Wallet addresses used by many blockchain technologies, such as Bitcoin and Ethereum, have historically consisted of long strings of random letters and numbers, however, these wallet addresses can make it difficult to transact with other users in a typical online-social-media context because users are unable to recall the long-string addresses from memory. The Steem blockchain uses each participant's user name as their wallet address, which bolsters the user experience for participants who attempt to send tokens because they can verify the addresses from their own memory.

Steem Blockchain Dollars (SBD)

Many users who are introduced to cryptocurrency struggle to comprehend how "magic internet tokens" awarded by the platform can actually have real world value. In order to help bridge the gap between more traditional fiat money systems which mainstream users are used to, and the cryptocurrency tokens which they are awarded through the platform, a new currency called Steem Blockchain Dollars (SBD) was created.

[11] The component of the Steem blockchain framework responsible for processing transactions and the distribution of rewards.

SBD tokens are designed to be pegged closely to one USD, so that users who receive them can know approximately how much they are worth in "real dollar" terms. SBD tokens also offer a relatively stable currency for users to hold if they are looking to preserve their account value relative to USD. A more detailed technical explanation can be found in the Steem technical whitepaper.[12]

Decentralized Exchange

The Steem blockchain offers a decentralized token exchange, similar to the Bitshares exchange.[13] The exchange allows users to trade their STEEM and SBD tokens through a public decentralized peer-to-peer market. Users are able to place buy and sell orders, and order matching is performed automatically by the blockchain. There is also a publicly accessible order book and order history which users can use to analyze the market. Users can interact with the exchange directly using the blockchain API, or use a GUI such as the one on Steemit.com.[14]

Payments Through Escrow

The irreversible nature of blockchain transactions is an important security feature, although there are many cases where users may not be comfortable sending their tokens to another individual without a way to get them back if the other user does not hold up their end of the agreement. The Steem blockchain provides a way for users to send coins to each other with a third party designated as an escrow service. The user acting as the escrow service is able to determine if the terms of the agreement have been met, and either allow the funds to be released to the receiver or returned to the sender.

Hierarchical Private Key Structure

Steem employs a first of its kind hierarchical private key system to facilitate low-security and high-security transactions. Low-security transactions tend to be social, such as posting or commenting. High-security transactions tend to be transfers and key changes. This allows users to implement different levels of security for their keys, depending on the access that the keys allow.

These private keys are the Posting, Active and Owner. The posting key allows accounts to post, comment, edit, vote, resteem[15], and follow/mute other accounts. The active key is meant for more sensitive tasks such as transferring funds, power up/down transactions, converting Steem Dollars, voting for witnesses, placing market orders, and resetting the posting key. The owner key is only meant for use when necessary. It is the most powerful key because it can change any key of an account, including the owner key, and to prove ownership during an Account Recovery. Ideally it is meant to be stored offline, and only used when the account's keys need to be changed or to recover a compromised account.

[12] Steem Whitepaper
https://steem.io/SteemWhitePaper.pdf

[13] Bitshares Decentralized Exchange
http://docs.bitshares.org/_downloads/bitshares-general.pdf

[14] Steemit.com Currency Market
https://steemit.com/market

[15] "Resteem" is the term used in the Steem blockchain for when a user shares the content with their followers.

Steem also facilitates the use of a Master Password that encrypts all three keys. Webservices can use a Master Password that decrypts and signs with the necessary private key. Master Passwords may allow users to trust certain services to keep improper keys from being transferred across any servers, thus increasing user experience while maintaining a secure client-side signing environment.

Multi Sig Authorities

The Steem blockchain allows an authority to be split across multiple entities, so that multiple users may share the same authority, or multiple entities are required to authorize a transaction in order for it to be valid. This is done in the same way as Bitshares[16] where each public/private key pair is assigned a weight, and a threshold is defined for the authority. In order for a transaction to be valid, enough entities must sign so that the sum of their weights meets or exceeds the threshold.

Multiple Reward Beneficiaries

For any given post there may be a number of different people who have a financial interest in the reward. This includes the author, possible co-authors, referrers, hosting providers, blogs that embedded blockchain comments, and tool developers. Whatever website or tool that is used to construct a post or comment will have the ability to set how rewards from that comment are divided among various parties. This allows for various forms of collaboration, as well as a way for platforms that are built on top of the Steem blockchain to collect a portion of the rewards from their users.

Smart Media Tokens (SMT)

This protocol layer is under development. Its whitepaper will be posted here.

Stolen Account Recovery

If a user's account is compromised, they may change their keys using their private owner key. In the event that the attacker is able to compromise the private owner key and change the password on the account, the user has 30 days to submit a previously functional private key through Steem's industry-first stolen account recovery process, and regain control over their account. This may be offered by a person or company who provides registration services to Steem. It is not mandatory for the registrar to provide this service to its users, but it is available to increase the value of a registrar's users' experience.

Security Through Time-Locks

If a user's active or owner key is compromised, the attacker would have full access to all of the funds in their account. Because blockchain transactions are irreversible, users have no way to

[16] Bitshares Flexible Identity Management
http://docs.bitshares.org/_downloads/bitshares-general.pdf

get their funds back after they have been stolen.

The Steem blockchain allows users to store their STEEM and SBD tokens in a savings account, so that the funds may not be withdrawn until after a three day waiting period. In addition, STEEM that is held in the 13 week vesting schedule may only be withdrawn at a rate of 1/13 per week, after an initial waiting period of seven days. These time-locks prevent an attacker from being able to access the full portion of the user's funds immediately, so that the rightful owner has time to regain control over their account before all of their funds can be withdrawn.

Bandwidth Rate Limiting for Fee-less Operations

Because the witnesses are paid entirely through the generation of new tokens, there is no need to charge users a fee for powering the blockchain. The only reason to charge a fee would be as a deterrent to prevent users from completing an unreasonable amount of transactions, which could potentially impact the performance of the blockchain.

In order to place reasonable limits on the system use, each user is given a limited bandwidth. Whenever users perform blockchain operations such as token transfers, posting content, and voting, it uses up a portion of their bandwidth. If a user exceeds their bandwidth allowance, they must wait to perform additional actions until their bandwidth recharges.

Bandwidth limits adjust based on network use, so users have a higher bandwidth allowance when the network usage is low. The amount of bandwidth that an account is allowed is directly proportional to the amount of Steem Power a user has, so users can always increase their bandwidth allowance by getting additional Steem Power.

Conclusion

The unique rewards and incentive program offered by the Steem blockchain and token are designed to make Steem the ultimate on-ramp into cryptocurrency for mainstream users. The performance of the blockchain is designed with widespread mass adoption of the currency and platform in mind. When combined with the lightning fast processing times and fee-less transactions, Steem is positioned to become one of the leading blockchain technologies used by people around the world.