SnowGem Whitepaper

LAST UPDATED: MAY 27, 2018

SNOWGEM TEAM

Table of Contents

1 Introduction

Digital currencies have long been a topic of much interest for academic researchers. Seeking innovations in a somewhat stagnant field that is finance and accounting, experts, in economy as well as technology, have been putting forward new ideas since the 1980s, with the first being *e-cash* proposed by David Chaum in 1983 [1]. After *e-cash*, several other digital currencies and payment systems were proposed; however, due to problems in both design and implementation, none of these systems has seen widespread adoption. But it was clear that the traditional fiat currencies and payment systems no longer satisfied the needs of users.

In 2008, Satoshi Nakamoto published the Bitcoin Whitepaper [2]. Bitcoin appears to have learned from previous systems and provides several desirable features: peer-to-peer network, decentralized consensus, incentives for users to keep the network robust, and finite lifetime supply to prevent inflation. Bitcoin is the first implementation of a digital currency that has gained a significant adoption and has led the way for many other new ideas to improve on our currency system. Having said that, Bitcoin is certainly not perfect, and thus, our team is doing our own take on cryptocurrency with SnowGem.

SnowGem (XSG) is a new cryptocurrency based on Zcash. We believe that there are already many great ideas and teams in the field, and therefore, we should try to "improve upon great ideas of other cryptocurrencies", rather than try to reinvent the wheel and start from scratch. There will be similarities between SnowGem and other cryptocurrencies where we find that the existing solutions are sufficient, but there will also be differences in philosophy, direction as well as execution where we believe we can improve upon those existing solutions.

2 SnowGem

We are excited to share with you the features included with SnowGem.

2.1 Decentralized and Trustless Protocol

Probably the most significant breakthrough monetarily Bitcoin has brought is the removal of a central authority over the currency. Traditionally, fiat currencies are heavily influenced by some central authority, namely the governments which issue said currencies. Any governmental currency is susceptible to manipulation as well as fluctuation due to external factors that its users have no control over.

Moreover, this traditional currency system requires transactions to be performed via a trusted third party – banks. Any trusted third party is a security hole. While disasters rarely happen, your bank can be hacked, your bank can be robbed, or simply due to unwise business decisions, your bank can be insolvent. In any of those scenarios, you may lose your money.

Therefore, it is important for a currency to remove the central authority – decentralize – and to remove the need for trusted third party – do not trust, verify. SnowGem is a decentralized cryptocurrency where everything will be decided by network consensus, and there is no need to trust anybody to perform transactions as they are always verified by rules of the blockchain.

2.2 Enhanced Privacy

One of the major complains with Bitcoin is that the level of anonymity provided by Bitcoin is simply insufficient for many users. By design, every transaction on the Bitcoin blockchain is recorded in a public ledger, thus, at any point in time, the full transaction history as well as the balance of any given address is open for everyone to see. Although a Bitcoin address does not contain any personally identifiable information, it is definitely possible to deanonymize users using various methods, such as network analysis [3] or web purchases tracking [4]. This is obviously not ideal for users who would like to preserve their privacy.

Fortunately, recent breakthroughs in cryptography present us with solutions to this privacy problem. "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge" (zkSNARKs) provides us with a protocol that allows parties to prove a statement without revealing any information other than the validity of the statement. Zcash is the first cryptocurrency to apply zkSNARKs and is one of the most prominent privacy-focused cryptocurrencies [5]. SnowGem starts as a fork from Zcash codebase and inherits all features implemented in Zcash at the time of the fork, including the ability to perform shielded transactions, enabled by zkSNARKs.

Similar to Zcash, SnowGem provides two types of address: t-address and z-address. T-addresses are used to perform transparent transactions with all information public like Bitcoin transactions. On the other hand, users can use z-addresses to perform shielded transactions, which hide the identity of both the sender and the receiver, as well as the amount of money included in the transaction. Despite not revealing any information, the protocol is safe against double-spend attacks. For more details on how zkSNARKs works, please refer to their whitepaper [6].

2.3 Masternodes

Nodes are computers that host a full copy of the blockchain and help verify the validity of transactions on the blockchain. Nodes are integral components of any blockchain network, the more nodes are running, the more robust the network will be. Ideally, we want as many nodes as possible to stay online and remain connected. Anybody can run a full node if they want to. However, keeping a node running at all time has an associated cost, in storage and bandwidth, that increases over time. It is understandable that not many users are comfortable with paying for those always connected full nodes.

To incentivize users to run full nodes, SnowGem implements a masternode system. Masternodes support the network by staying connected to help other nodes easily find peers and propagate messages over the network. As a reward for hosting a reliable and powerful node, masternodes will earn part of SnowGem's block reward. Following is the detailed reward share for masternodes:

Block	193200	236400	279600	322800
Masternode block reward share	35%	40%	45%	50%

Reward for masternodes will start on block 160000, and block reward percentage for masternodes will ramp up beginning at 35%, finally reaching 50% at block 322800 and afterwards, this would allow our users time to accumulate the amount of SnowGem required as collateral for masternodes, which is 10000 SnowGem per masternode. This collateral will be locked up and not spendable as long as the masternode is running. Once a user acquires 10000 SnowGem, either via mining or trading, they can immediately decide to start running a masternode. Instructions for setting up a masternode will be provided in a separate document.

Since masternodes require a collateral, they can be considered a form of investment. A masternode reward will be shared among all active masternodes, therefore, each masternode's earning will vary depending on the number of active masternodes on the network. The annual return on investment for each masternode can be calculated using the following formula:

$$Annual\ ROI\ per\ masternode = \frac{R \times P \times B \times 365}{MN} \times 100\%$$

where R = block reward = 20

P = percentage of block reward awarded to masternodes

B = number of new blocks in a day = 1440

MN = number of active masternodes

For reference, we have calculated earnings for some given number of active masternodes below:

Masternode block reward share	Annual ROI 100 active masternodes	Annual ROI 200 active masternodes	Annual ROI 500 active masternodes	Annual ROI 1000 active masternodes	Annual ROI 2000 active masternodes
35%	367.92%	183.96%	73.58%	36.79%	18.40%
40%	420.48%	210.24%	84.10%	42.05%	21.02%
45%	473.04%	236.52%	94.61%	47.30%	23.65%
50%	525.60%	262.80%	105.12%	52.56%	26.28%

In the future, it is intended that masternodes will be utilized to provide additional powerful features.

3 Specifications at Launch

SnowGem is officially launched on December 25, 2017 with the following specifications:

- Algorithm: Equihash.
- Block time: 1 minute.
- Block reward: 20 XSG. *
- Reward halving: every 2,102,400 blocks (approximately 4 years).
- Difficulty adjustment: every block.
- Total coin supply: 84,096,000 XSG.
- Pre-mine: 0.
- Founders' reward: 5% per block until first halving (block 2102400). **

* The block reward will slowly ramp up to a full reward at block 8000. This allows users time to join the network and prevents anyone from exploiting the lack of miners at the start to accumulate a significant amount of coins.

**While an initial coin offering (ICO) can be a great way for development teams to raise funding at the start of a project, it also has been a huge risk for investors, since they can lose the whole investment if they encounter scammers that abuse an ICO, or teams that promise more than they can deliver. Considering that fact, we have decided to stay away from ICO and to not pre-mine any of the coins. On the other hand, funding is necessary for the project to run smoothly, thus, we have set the founders' reward to be 5% of each block until the first block reward halving, which ultimately equals to 2.5% of total supply. In the early stages of the project, all money gained from the founders' reward will be put towards funding activities surrounding the project, such as paying for bounties or paying fees to list SnowGem on exchanges and informational websites.

4 Upcoming Developments

Here we would like to share what can be expected to be upcoming for SnowGem. As with all development plans, these are only for reference and there will likely be changes at some point, our team will try our best to keep it updated.

4.1 Improving User Experience

No matter how good a product can be, there will be no users if the user experience is terrible. At the heart of the SnowGem user experience is SnowGem wallet. At the moment, we provide our user with a GUI Simple Wallet. Aside from the core functionality that allows users to easily send/receive coin, and keeping track of their balance and transaction history, an important feature of the Simple Wallet is providing an easy way to set up and monitor masternodes.

We have a plan for the next version of SnowGem to have more refined features, ensuring a smooth experience for our users, and we will make it available on all popular platforms/operating systems (PC, mobile, and web). At the same time, we are working on bringing SnowGem to existing multi-coin wallets and hardware wallets to reduce the amount of migrating our users need to do.

4.2 Upgrading Core Protocol

It is important to keep in mind that we are still in the early days of cryptocurrencies and there is a lot of work to be done to the underlying technology. Our team is always researching what we can improve as well as keeping a close watch on new ideas and innovation from other projects in the field.

Since Zcash is where we originally forked from, we are very curious about the Overwinter update as well as the upcoming Sapling network upgrade from the Zcash team. These updates are said to provide several improvements including replay protection for future upgrades, better performance for transactions, and other new features. We will look at these updates and integrate them into SnowGem if appropriate.

4.3 Building an Ecosystem

Currently, cryptocurrencies are viewed by many people as a speculative investment, that they are a way to make profit while not producing any practical value to society. We disagree with this view and want to showcase the usefulness of a new kind of currency by building an ecosystem surrounding SnowGem. There are multiple steps to achieving this goal.

First, we want to improve accessibility to SnowGem. As said above, we will provide SnowGem wallet on all popular platforms. Whether you use Windows, Linux or MacOS, whether your phone is Android or iOS, or as long as you have a device with a browser and an internet connection, you will be able to use SnowGem. All SnowGem users, existing and new alike, can choose their favorite device for use with SnowGem with no fear of unavailability.

To further increase accessibility, we will make it easier to acquire SnowGem by listing on more exchanges. Ideally, we would like to eventually reach the level of ubiquity of the top 20 cryptocurrencies, that is to be listed on all popular and major exchanges with multiple trading pair, possibly including a direct trading pair to fiat. This is ambitious, as recently it has been increasingly difficult and expensive to get listed on major exchanges, but it is certainly within our ability.

Next, we want to bring quality of life updates to our miners and long-term coin holders – masternode owners. We will create our own GUI mining tool which supports all miner programs like EWBF, Dstm, Claymore, Bminer, which allow miners to easily switch a coin, mining pool, and also provide monitoring functions for mining rigs. Masternode owners will be provided with services to easily manage and monitor their masternodes. We are also working on a native masternode sharing solution to allow people who have not acquired the required collateral to still be able to gain a proportion of the masternode reward.

Finally, our ultimate goal is to let people use SnowGem as replacement for their current currency. Presently, you can use SnowGem as a store of value and also as a way to send money from person to person. Beyond that, we want SnowGem to be used between merchants and customers, and between service providers and clients. As SnowGem continues to grow, we will get in contact with merchants and services that are interested in using cryptocurrencies to use SnowGem as an alternative method of payment. It is also not outside the realm of possibility that we will build our own service utilizing SnowGem to kickstart the ecosystem. Of course, it is still a long way from this goal, but our growth has been great recently, and our goal may be closer than we imagine.

5 Our Vision

Like many other teams that work on cryptocurrencies, we believe that cryptocurrencies have a purpose in our society. If we keep working hard and improving cryptocurrencies, one day cryptocurrencies will be able to replace fiat currencies. But there is still a lot of work to be done before that day.

We have chosen to prioritize privacy as a feature of SnowGem and we would like to share with you why. We believe that privacy and decentralization go hand in hand. A decentralized system is much more resistant against surveillance and censorship than a centralized system, and thus, is more supportive of individual freedoms and civil liberties, such as privacy and freedom of expression. In return, without privacy, a system is more vulnerable to adversarial forces attacking its individual users and handing control over to a few powerful parties. While there are concerns that privacy would allow more illegal activities, there are also legal and important reasons for desiring financial privacy.

The first reason is real life security. If the information about your wealth is publicly known, you will likely become a target for extortion or theft. And unlike traditional assets where there are certain difficulties in seizing your assets, once an adversarial force gets hold of your private key, your money is lost. The second reason is circumstantially appropriate privacy, such as when you would like to donate to non-profit or charitable organizations. The third reason is preserving your business information from competitors. If you run a business, you certainly do not want your competitors to know about the details of your contracts with other partners. Needless to say, there are other reasons for desiring privacy that we have not listed here, but we hope the above reasons are enough to convince you that privacy is necessary.

We believe that everybody has a right to privacy, and that privacy is about consent. You should be able to choose what, when, and to whom do you reveal your information. Once privacy is secured, then we can move on to focusing on other aspects of the currency.

As stated before, we believe that cryptocurrencies in general, and SnowGem in particular, will one day replace fiat currencies. Although SnowGem's use case is at this time mainly a store of value for performing private transactions, with our development plans described above, we imagine that SnowGem will gradually expands its reach. We have high hopes for the future of SnowGem, and there will be challenges along the way, but we believe that with the support of the community, we will be able to overcome any obstacle.

Bibliography

[1] D. . Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology Proceedings,* vol. 82, no. 3, p. 199–203, .

[2] N. . Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," , . [Online]. Available: http://bitcoin.org/bitcoin.pdf.

[3] F. . Reid and M. . Harrigan, "An Analysis of Anonymity in the Bitcoin System," *arXiv: Physics and Society,* vol. , no. , pp. 1318-1326, 2011.

[4] S. . Goldfeder, H. A. Kalodner, D. . Reisman and A. . Narayanan, "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies.," *arXiv: Cryptography and Security,* vol. , no. , p. , 2017.

[5] E. . Ben-Sasson, A. . Chiesa, C. . Garman, M. . Green, I. . Miers, E. . Tromer and M. . Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," , . [Online]. Available: http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf.

[6] E. . Ben-Sasson, A. . Chiesa, E. . Tromer and M. . Virza, "Succinct non-interactive zero knowledge for a von Neumann architecture," , 2014. [Online]. Available: https://usenix.org/system/files/conference/usenixsecurity14/sec14-paper-ben-sasson.pdf.