a better cryptocurrency for everyone

whitepaper

CONTENTS

INTRODUCTION

INTRODUCTION

Digital currencies have been deliberated over for the last several decades. Alternative ways to create systems which are more innovative, reliable and secure have been on the minds of very knowledgeable people in the field of cryptography. Experts in finance, technology and accounting have tried to design and implement new ideas since the 1980s.

1983

David Chaum and Stefan Brands created the issuer based e-cash protocol [1]

1997

Adam Back developed hashcash, a proof of work scheme for spam control

Wei Dai proposed the distributed digital scarcity based crypto called b-money

1998

Nick Szabo proposed the digital scarcity based crypto called bit gold

Unfortunately, these early attempts to put forward viable alternatives to world fiat currencies did not get off the ground. Governments were vehemently opposed to seeing them succeed and deemed them as a threat to the status quo monetary systems. It was, therefore, difficult for the early contributors in the field to push their ideas to a wider audience. Nevertheless, there was still eagerness to pursue further research.

In October 2008, an individual or group of people known by the alias Satoshi Nakamoto published the Bitcoin whitepaper[2]. It is described as an innovative breakthrough, especially by those who initially read it, for the initiation and implementation of a new type of money called cryptocurrency. Bitcoin learnt from previous failed systems by creating a decentralised network-based transparent ledger. It provides several desirable features including:

- A peer-to-peer decentralised network protocol
- Incentives for users to keep the network robust
- A finite hard cap on supply to prevent inflation

Since the inception of Bitcoin, thousands of cryptocurrencies have been launched. Most ventures into the cryptocurrency sphere have not gone according to plan as their founders would have hoped. Nevertheless, there are currently hundreds of crypto related projects which are succeeding. SnowGem is a new type of cryptocurrency which has objectives to improve upon proven technologies developed so far. There will be similarities between SnowGem and other coins, but the team wish to follow their own philosophy.

After this innovative breakthrough, people have been developing technologies that apply practical use to cryptocurrencies. For example, some cryptocurrencies have focused on providing users with reliable, compatible and user friendly wallet client systems for robust forms of payment.

Most ventures into the cryptocurrency sphere have not gone according to plan as their founders would have hoped. Nevertheless, there are currently hundreds of crypto related projects which are succeeding.

SnowGem is a new type of cryptocurrency that can be developed on verified technology. It is a project that embraces a unique philosophical approach on how cryptocurrency can be used in real life. SnowGem aims to build a better cryptocurrency by incorporating previously proven aspects of blockchain technology including network robustness, feature rich services and end-user friendly support.

WHAT IS SNOWGEM?

WHAT IS SNOWGEM?

WHAT IS SNOWGEM?

SnowGem (XSG) is a cryptocurrency or decentralised currency used via the Internet. It is described as an ecosystem which allows one to transfer value, either transparently or privately, anywhere in the world without the need to trust a central authority such as a bank or other clearing house. SnowGem users are able to send or receive XSG quickly, reliably and securely using a personal computer, laptop or mobile device.

On December 25th 2017 the first Equihash privacy coin implementing zSNARKs code for it's Masternodes was born. Let us show you SnowGem.

Rather than trying to reinvent the wheel from scratch, the founder of SnowGem Tinh Pham (TXID), after studying the codebase of other cryptocurrencies, decided to base SnowGem on Zcash. Zcash is the first cryptocurrency to apply zkSNARKs (Zero Knowledge Succinct Non-Interative Argument of Knowledge) which allow parties to prove a statement without revealing any information other than the validity of the statement. SnowGem began as a fork of the Zcash blockchain[5] and inherited all features of Zcash at that time (23rd December 2017).

SnowGem officially launched its blockchain on the 25th December 2017 after 72 blocks had been timestamped. During the first 72 blocks, no external miners could mine (less than 7 XSG was mined during this period). It was considered necessary to make sure the blockchain launched seamlessly.

On the 15th April 2018, masternode payments were activated. This meant that SnowGem became the first Equihash algorithm oriented cryptocurrency with zkSNARKs[6] to implement active masternode technology.

Like all cryptocurrencies, people have chosen to adopt SnowGem as a medium of exchange/ store of value through personal choice. An innovative feature, affinity towards the brand or high confidence in the community could be reasons for doing so. Key advantages of using SnowGem are:

- SnowGem is permissionless, so anyone is free to use its services.
- It is accessible from anywhere in the world.
- It has no central point of failure.
- It is free from government censorship.
- SnowGem users receive regular block rewards for participation in helping to secure and decentralise the network protocol.

HISTORY

Since the inception of SnowGem back in December 2017, the project has grown from strength to strength.

By laying the brickworks of our foundation the SnowGem team and the community have worked non-stop in a diligent manner to ensure the rapid success of SnowGem.

Both the SnowGem team and community have contributed to the ongoing success of the project.

HISTORY

Key events which have occurred during SnowGem's relatively short history include:

- On the 22nd December 2017, the SnowGem blockchain was announced to the wider cryptocurrency community via an online forum called Bitcointalk.

- On the 25th December 2017, the SnowGem blockchain officially launched at 00:32:41 UTC at block number 73.

- On the 12th January 2018, the first cryptocurrency exchange to initiate live real-time XSG trading was Stocks.exchange (now known as STEX).

- On the 13th February 2018, the initial testing phase of masternode technology was announced by Tinh Pham. Beta specifications were made available.

- On the 5th March 2018, an updated simple wallet client (version 2.0.0) was released for users to install. It became possible for users to create SnowGem masternodes.

- On the 15th April 2018, the first masternode payments were received by operators at block number 159,428.

- On the 4th May 2018, the first SnowGem mobile application was released on the Android operating system. It became possible for users to store XSG on their phones.

- On the 20th May 2018, the SnowMine mining application tool was released.
- On the 28th June 2018, the SnowGem blockchain successfully hard forked to an improved variant of the Equihash hashing algorithm (from <200,9> to <144,5>).
- On the 6th September 2018, the SnowGem Modern wallet was released. It is a client which includes way more features than the simple wallet client. Presented with a more professional and seamless GUI, users can manage and monitor their SnowGem portfolio as well as other coins which are being added.

Members of the SnowGem team are dedicated to build upon the progress made in the last year or so. There is enthusiasm that, with the help from the community, SnowGem will become a highly adopted and used method of payment.

SPECIFICATION

SPECIFICATION

SnowGem officially launched on the 25th December 2017. Before the launch, Tinh Pham (TXID) unveiled the initial coin specification which outlines the structural parameters of the SnowGem blockchain.

SnowGem is a Proof-of-Work coin using the Equihash Algorithm that started without an ICO or a pre-mine environment and has a limited supply of 84,096,000 XSG.

These being:

Genesis Block:	23rd December 2017 at 13:08:01 UTC
Official Launch:	25th December 2017 at 00:32:41 UTC
Timestamping Algorithm:	Proof of Work
Hashing Algorithm:	Equihash <200, 9> (currently <144,5>)
Block Time:	60 seconds
Block Reward:	20 XSG*
Block Halving:	Every 2,102,400 blocks
Difficulty Re-targeting:	Every block
Total Coin Supply:	84,096,000 XSG
Pre-mine:	0 XSG
ICO:	None
Founders' Reward:	5% block rewards for the first four years**

*The founder coded block generation to incrementally increase by 0.0025 XSG each block beginning with a 0.0025 XSG block reward at block number one. It attained the 20 XSG block reward at approximately block number 8,000. This gave users ample time to join the network and prevented high hashrate miners from accumulating a large number of XSG early on.

**A Founders' Reward was decided upon as the best method by which to raise the necessary funds for code development, marketing and other operational activities. While acknowledging that an ICO (initial coin offering) is a great way for blockchain projects to raise initial funds, it was considered as a risky approach. SnowGem know the importance that, for a project to succeed in the competitive crypto sphere, funds are required to attract talent and pay for services. In the future, the team are seeking outside investors. SnowGem knows the importance of this, for a project to succeed in the competitive crypto sphere, funds are required to attract talent and pay for services. In the future, the team will seek outside investors.

BLOCKCHAIN

Every cryptocurrency has a corresponding blockchain within its decentralised network protocol. A blockchain is simply described as a general public ledger of all transactions recorded in blocks ever executed since the very first block. Additionally, it continuously updates in real-time when a new block is successfully mined.

Our blockchain is strong and made for the GPU miner in mind. Hashing the Equihash Algorithm with the <144,5> parameter setting makes for an ASIC resistant mining environment.

Blocks enter the blockchain in such a manner that each block contains the hash of the previous one. It is therefore utterly resistant to modification along the chain since each block is related to the prior one. Consequently, the problem of double-spending is solved.

The first block of the SnowGem blockchain timestamped at 13:08:01 UTC on the 23rd December 2017. It was not until block number 73, the time at which the blockchain officially launched, that external miners were permitted to mine blocks. Since this time, there has been one notable update to the underlying codebase which required a hard fork for protocol parameters to change. On the 22nd June 2018, an important update (version 2.0.3) was released for users to install before block number 266,000. Primarily, it changed the parameter setting of the Equihash hashing algorithm from <200,9> to <144,5>, after which the SnowGem blockchain became low-memory GPU and ASIC resistant.

For members of the general public to view the blockchain, web developers create block explorers. They are online websites which present certain aspects of the blockchain including wallet addresses and transaction identifications. SnowGem officially recognises https://insight.snowgem.org as its most reliable block explorer.

BLOCKCHAIN

As time goes by, the number of XSG mined per block will decrease. This means there is a hard cap on the number of XSG to be mined, which is 84,096,00 XSG. What follows is the SnowGem block distribution table which covers a timeframe for the next 23 years.

First Block	Last Block	# Blocks	Reward	Total Coins
1	7,999	7,999		79,990
8,000	2,102,399	2,094,400	20	41,967,990
2,102,400	4,204,799	2,102,400	10	62,991,990
4,204,800	6,307,199	2,102,400	5	73,503,990
6,307,200	8,409,599	2,102,400	2.5	78,759,990
8,409,600	10,511,999	2,102,400	1.25	81,387,990
10,512,000	12,614,399	2,102,400	0.625	82,701,990

EQUIHASH HASHING ALGORITHM

One of the major breakthroughs which Bitcoin brought to the table is the removal of a central authority. Fiat currencies, such as the US Dollar issued by a central bank, are highly susceptible to inflation, manipulation and theft.

Equihash is a memory-hard Proof-of-Work algorithm with ASIC resistance in mind to maintain a decentralized network protocol.

For cryptocurrencies, no central authority or third party is required to verify the validity of transactions on the blockchain. Instead, miners are collectively responsible for validating each and every transaction in a proof of work timestamping process. This competitive task secures and decentralises the network protocol.

SnowGem adopted the Equihash hashing algorithm and implemented its code on the 23rd December 2017. Miners compete to find hashes, then are subsequently rewarded a certain number of XSG as an incentive. These coins are issued by the software in a transparent and predictable way outside the control of its developers. The Equihash hashing algorithm is defined as[7]:

It is a memory-hard Proof-of-Work introduced by the University of Luxembourg's Interdisciplinary Centre for Security, Reliability and Trust (SnT) at the 2016 Network and Distributed System Security Symposium. The algorithm is based on a generalization of the Birthday problem which finds colliding hash values. It has severe time-space trade-offs but concedes vulnerability to unforeseen parallel optimizations. It was designed such that parallel implementations are bottle-necked by memory bandwidth in an attempt to worsen the cost-performance trade-offs of designing custom ASIC implementations. ASIC resistance in Equihash is based on the assumption that commercially-sold hardware already has quite high memory bandwidth, so improvements made by custom hardware may not be worth the development cost.

Therefore, SnowGem is a currency which has no central authority to issue its coins. Its users are not required to trust anyone to perform transactions, but rely entirely on the distributed network consensus of the blockchain.

ENHANCED PRIVACY

Being able to seclude information about oneself from authority is appealing to some people, especially when it involves sending money online. Many central authorities collect, and even distribute, spending habits to find out what people engage in.

SnowGem provides enhanced privacy using zSNARKs, a technologically proven protocol allowing the user to have both private and transparent addresses.

Bitcoin offers a certain level for anonymity for its users, but falls short. By design, every transaction on the Bitcoin blockchain is recorded in a public ledger, thus, at any point in time, the full transaction history is accessible. It is possible to use various methods, such as network analysis[3] or web purchases tracking[4], to track who spends what and where. This is obviously not ideal for users who like to preserve their privacy.

SnowGem utilises a technologically proven protocol called zkSNARKs (Zero Knowledge Succinct Non-Interative Argument of Knowledge) which allow parties to prove a statement without revealing any information other than the validity of the statement. Zcash is the first cryptocurrency to apply zkSNARKs.

Similar to Zcash, SnowGem provides two types of address:

- **t-address**
  used to perform transparent transactions, which are publicly recorded on the blockchain
- **z-address**
  used to perform shielded transactions, which hide the identity of both the sender and the receiver. The amount of XSG transacted is also hidden

Therefore, SnowGem offers its users a choice whether they transact transparently or privately. There are some situations where parties prefer to stay transparent.

MASTERNODES

Simply put, a masternode is a server on a decentralised network which can be utilised to carry out bespoke tasks including instant and private transactions. They are specialised nodes (computers) that host a full copy of the blockchain. Like all other nodes, they help to verify the validity of transactions sent from one peer to another.

SnowGem is a Masternode coin that encourages owners with a large percentage of the block reward.

SnowGem fully implemented masternodes on the 15th April 2018. Anyone is free to create a masternode, but must raise the necessary collateral in order to operate one. This associated cost (entry barrier) to become a masternode operator is necessary because it disincentivises one to cheat the system. SnowGem masternode operators must hold a total of 10,000 XSG (cannot be spent and is described as not being part of the overall coin circulation) in a designated wallet address in order to keep the node running.

As an incentive for masternode operators to keep their nodes running, they collectively receive a percentage of overall block rewards. What follows is a table which shows how many XSG have been, and are, rewarded to masternode holders as a whole:

First Block	Last Block	Block reward %	Block Reward XSG
159,428	236,399	35	7
236,400	279,599	40	8
279,600	322,799	45	9
322,800	–	50	10

Date	Number Masternodes	Annual RIO %	Yearly Income US$
31st Aug 18	402	130.02	941.96
30th Sept 18	438	119.92	1,005.09
31st Oct 18	529	98.81	582.84

SnowGem considered the ramp up in masternode reward percentages as allowing users the time to accumulate XSG more easily at the beginning via mining. It is therefore the case that masternode operators earn a passive income on the investment they have locked up. What they receive in terms of the number of rewarded XSG depends on the total number of active masternodes at any given time (see table immediately above).

KEY FEATURES

SNOWGEM MODERN WALLET

Designed to be more professional, comfortable and simple, the SnowGem Modern Wallet was released on the 6th September 2018. It brings together the most important aspects of the SnowGem ecosystem into one place. Transferring XSG units of account is an easier process. Unlike the SnowGem simple wallet, it allows users to monitor and manage their masternodes. SnowMine is also accessible from this wallet.

We had ease in mind when creating our wallets, mining tools and Masternode Map. All have been designed with user friendly features.

SNOWMINE APPLICATION TOOL

SnowMine is the ultimate mining application based on SnowGem. It makes the process of configuring one's mining equipment easier. If mining issues arise, the application promptly sends a notification (either via e-mail or pop-up) to make the miner aware. Users are able to receive statistics and control their mining equipment via a mobile device, Discord or Telegram. No account is required.

SNOWGEM WEB WALLET

Built especially for novice users, the SnowGem Web Wallet does not require users to download, and then install, any software. It is a secure, reliable and robust on-line medium to send, receive and store XSG units of account.

SNOWGEM ANDROID WALLET

Released on the 4th May 2018, the SnowGem Android wallet is a secure, open--source and easy method by which to send or receive XSG units of account via a mobile device. All private keys remain in the control of the user at all times. Like other wallets, multiple wallet addresses can be created and customised.

LIVE MASTERNODE MAP

On the official SnowGem website, visitors are able to check a live world map on which all active SnowGem masternodes are located. Jakub Korbel designed and developed it. He released the completed version in April 2018.

HOW TO ACQUIRE SNOWGEM

HOW TO ACQUIRE SNOWGEM

SnowGem are initially acquired (as an incentive) by miners who direct processing power to successfully finding blocks. Each block has an associated reward that either goes to a lone miner or is split between miners via a mining pool service. Miners are then free to store these XSG units of account, create SnowGem masternodes or place sell orders on the open cryptocurrency exchange markets.

SnowGem can be acquired via GPU mining or by purchasing XSG on one of many exchanges.

Over time, cryptocurrency exchanges have initiated XSG trading on their platforms. They allow people to buy or sell XSG units of account at the going market price. What follows is a table of all exchanges on which SnowGem has been added:

Cryptocurrency Exchange	Date Trading Initiated	BTC Trading Market URL
STEX	12th January 2018	https://app.stex.com/en/basic-trade/pair/BTC/XSG/1D
Graviex	9th February 2018	https://graviex.net/markets/xsgbtc
Southxchange	11th February 2018	https://www.southxchange.com/Market/Book/XSG/BTC
Safe.trade	12th June 2018	https://www.safe.trade/
Mercatox	19th June 2018	https://mercatox.com/exchange/XSG/BTC
Cratex	11th October 2018	https://cratex.io/index.php?pair=XSG/BTC
Bitker	31st October 2018	https://www.bitker.com/#/bbTrades/xsg_btc

Instead of acquiring XSG units of account via mining or exchanges, there are other ways to become a SnowGem holder or investor. These include:

- By being a SnowGem masternode operator. It is then possible to receive a percent-age rate of interest on the 10,000 XSG locked as collateral.
- Receiving coins for contributing to the project. This can be done by either participating in code development, marketing, graphics designing and so forth.
- Receiving coins from someone as a donation or gift.
- Taking part in a face-to-face transaction where XSG units of account are bought/sold with both parties agreeing the terms.

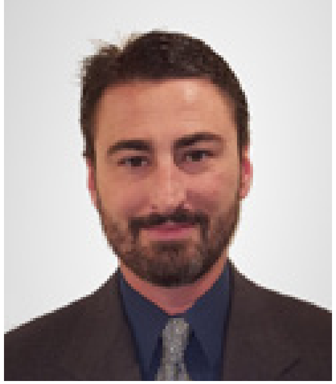
TEAM

Tinh Pham
@Txid
Founder, CEO

Jakub Korbel
@DaX
Project manager

Ingvar Örn Þórarinsson
@IggiPop
Backend developer

Bartlomiej Sztefko
@Abakus
Backend developer



Michael Munson
@BlockMinerMike
Content manager

William McLaren
@mclaren86
Content manager

Hugo Zupan
@Bet-Well
Marketing manager

Jason Harp
@nUm
Applications developer

FUTURE VISION

In a similar way how other cryptocurrency teams operate, SnowGem believes that blockchain technology will have a revolutionary impact on society. SnowGem acknowledges that there is still a lot of work to do before that time.

The future of SnowGem will be filled with many technological advances in cryptocurrency to be desired by other projects.

Looking forward, SnowGem will investigate and develop ways to improve upon their blockchain. What follows are the most exciting things being worked on:

Overwinter and Sapling Upgrades

SnowGem are working hard to implement two network protocol parameter changes. In particular, the Sapling upgrade will integrate improvements to the efficiency at which shielded transactions are processed and lower CPU memory to optimise performance on mobile devices. Both upgrades will be integrated into SnowGem via a single hard fork of the blockchain.

Masternode Reference

Masternode operators will be able to invite friendly masternode servers. By being a reference, the masternode operator will receive an extra 2.5% XSG bonus reward when the friendly invited masternode has received their masternode payment. If no reference is applied, the block reward is sent to proof of work miners instead.

Lottery Systems

SnowGem users will be able to participate in regular lotteries via the SnowGem Modern Wallet.

Payment Solutions

An objective to make it easier for everyday users to purchase goods and services. SnowGem wants to create a fast, unique and secure payment processing system, directly on top of their blockchain. It will be built into any software which supports API calls including ecommerce, e-shops and Point of Sale (PoS) systems.

Decentralised Exchange

It is well known in the cryptocurrency space how frustrating online centralised exchanges can be. Users regularly complain about lost, manipulated and stolen coins. SnowGem wishes to create their very own decentralised exchange (DEX) that will help improve the trading experience without downtime and maintenance periods.

Content Masternodes

SnowGem plans to improve the code to make it possible for all types of data to be stored on their blockchain. Documents, media files and contracts will be publicly or privately stored. They will also be necessary for running the SnowGem DEX and provide file storage for data required for decentralised applications (dApps) (based on IPFS protocol).

Blockchain Technology Company

In order to take great strides forward, legally and compliantly, SnowGem wants to establish an official foundation. It will help SnowGem become more professional and attract much needed investment.

Ultimately, the goal is for SnowGem to be used instead of fiat currencies. At the moment, the main purpose of SnowGem is a store of value for performing transparent or private transactions. After further development, there is confidence that SnowGem can gradually expand its reach to become a trusted, reliable and secure worldwide payment solution .

ROADMAP

Paymentsolution

Purchasing of products and services directly via the SnowGem network; accessible to everyday users.

DEXsolution

Provide a fast, reliable and secure trading platform solution for all holders using crypto or fiat currencies.

Cryptocompany

Register SnowGem as a first Equihash „Blockchain Technology“ company.

Contentmasternodes

Publicly accessible media and data; directly integrated in our secured and anonymous network.

BIBLIOGRAPHY

BIBLIOGRAPHY

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-bensasson.pdf.

[7] Wikipedia article [Online]. Available: https://en.wikipedia.org/wiki/Equihash"

snowgem

a better cryptocurrency for everyone

www.snowgem.org

Ver. 11/2018