Fantasy Gold

Fantasy Gold Whitepaper v1.3.1

May 2018

Fantasy Gold Core Team:
Nicolas Hernandez (Lead DFSCoin and Fantasy Gold Dev)
Jason Liberto (Sr Vice President Business Operations)
Alok Kumar Saxena (CTO and Lead DraftDaily.com Dev)
Tim Baker (Fantasy Gold Coin Dev)
Mark Petrozzella (Director of Business Development)
Steven Spooner (Communications Director)
Craig Williams (Community Director)
Kevin Browne (EU Business Development)

https://FantasyGold.io

Acknowledgements

Fantasy Gold would not have been possible without the prior works of the respective Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash, PIVX, and Bulwark teams. We would like to thank these teams for continuing to improve upon open-source Blockchain technology which has been a springboard for new innovations and a new digital revolution.

Our most important thanks is to the original DFSCoin community who HODL'ed through it all. They supported our project and believed in us. They say that Blockchain empowers the people, but without a community it's just bits of data in cyberspace.

"Creativity comes from applying things you learn in other fields to the field you work in."
—Aaron Swartz

DISCLOSURE STATEMENT

THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR INFORMATIONAL AND EDUCATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS INVESTMENT ADVICE. FANTASY GOLD IS AN IN-GAME DIGITAL CURRENCY. FANTASY GOLD IS NOT A SECURITY AND SHALL NOT REPRESENT FRACTIONAL OWNERSHIP OF THE OPEN-SOURCE FANTASY GOLD PROJECT, BUT RATHER AS ACCESS RIGHTS, USE RIGHTS AND PAYMENT MEANS WITHIN THE PROJECT'S ECOSYSTEM. CERTAIN FUNCTIONS OF THE FANTASY GOLD BLOCKCHAIN SUCH AS MASTERNODES, STAKING, AND BLOCK REWARDS ARE IN NO WAY TO BE CONSTRUED AS A DIVIDEND, INTEREST PAYMENT OR PROFIT SHARING.

FANTASY GOLD IS A DIGITAL CURRENCY, AND AS SUCH, READERS SHOULD BE AWARE THAT THE MARKET FOR DIGITAL CURRENCY IS STILL NEW AND UNCERTAIN. NO- ONE SHOULD HAVE FUNDS INVESTED IN DIGITAL CURRENCY OR SPECULATE IN DIGITAL CURRENCY THAT HE OR SHE IS NOT PREPARED TO LOSE ENTIRELY. WHETHER THE MARKET FOR FANTASY GOLD WILL MOVE UP OR DOWN, OR WHETHER FANTASY GOLD WILL LOSE ALL OR SUBSTANTIALLY ALL OF ITS VALUE, IS UNKNOWN.

Introduction

Built by the developers of DFSCoin, the Fantasy Gold Blockchain replaced DFS on April 30th, 2018 through a 1:10 swap as a means of capitalizing on the latest advancements in masternode technology and decentralized community governance. Fantasy Gold is a peer-to-peer cryptocurrency serving the growing fantasy sports and eSports industries in both the B2B and B2C spaces. Functioning as both in-game and prize payout currency for contest entry, Fantasy Gold also acts as a secure currency payment processing network. This payment processing network is able to process transactions quickly at only a fraction of the cost compared to traditional options. By using Fantasy Gold Coin, and it's open ledger, players can be confident their deposited funds are safe and used only to pay-out prize pools.

Fantasy and eSports players can secure Fantasy Gold Coins in their own downloadable private digital wallet. They can then send Fantasy Gold Coins from their unique wallet to their personal account on fantasy sports sites in order to enter contests. The Fantasy Gold wallet can be encrypted, backed up, and saved off-line to a USB or other air-gapped device. The wallet only needs an internet connection to sync with the Fantasy Gold Blockchain, send transactions, or when used as a staking wallet once the cryptocurrency enters its proof-of-stake phase.

The Fantasy Gold Blockchain is an encrypted structure of data that represents an open financial ledger and as such, Fantasy Gold deposit addresses can be easily and publicly verified. This allows site owners to publicly display the total amount of deposited funds being held to cover prize pools or the total available Fantasy Gold Coins available to cover guaranteed prize pools and tournament events. Using an open financial ledger, players can be assured that deposited player funds are properly segregated from company expense accounts.

Fantasy Gold transactions cannot be reversed which eliminates the increasing risks and fees associated with chargeback fraud. Because the Fantasy Gold Blockchain and network is decentralized there is no central authority that can freeze funds unlike with traditional centralized payment processors and banks. In effect merchants, players or even casual holders of Fantasy Gold Coins are acting as their own bank and payment processor. When end-users make deposits or purchases using Fantasy Gold Coins, merchants can store funds in cold-storage offline, in a private encrypted desktop wallet, or stowed away on a paper wallet. Transactions sent offline can still be monitored and confirmed by simply viewing the Fantasy Gold block explorer.

An open source and free to use Fantasy Gold API will be published on the projects block explorer. Also free, is the source code for the explorer in the Fantasy Gold public software repository which is hosted on GitHub along with the full Fantasy Gold source code for public inspection.

Instead of using traditional centralized payment processing, the Fantasy Gold project does not charge any additional transaction or service fees to use the payment network. Senders pay a small transaction fee that is awarded to miners who process the transactions and Masternodes who verify the transactions. Anyone with access to standard desktop graphics cards can act as a miner and anyone who holds 10,000 Fantasy Gold Coins can run a Masternode on a basic VPS, a server or even a raspberry pi with a static IP address.

What is a Blockchain?

A blockchain is the structure of data that represents a financial ledger entry, or a record of a transaction. Each transaction is digitally signed to ensure its authenticity and that no one tampers with it, so the ledger itself and the existing transactions within it are assumed to be of high integrity.

This ledger of past transactions is called the blockchain as it is a chain of blocks. The blockchain serves to confirm transactions to the rest of the network as having taken place. The transactions are collected in blocks, which are found approximately every ninety seconds in a random process called Mining.

As transactions transfer ownership of Fantasy Gold Coins, each of these blocks represents an update of the user's balances on the network. By following the blockchain from the Genesis Block and applying all transactions that were validated in each block in the correct order, you arrive at the current status quo.

These digital ledger entries are distributed among a decentralized network infrastructure of masternodes. These additional masternodes and layers in the infrastructure serve the purpose of providing a consensus about the state of a transaction at any given second; they all have copies of the existing authenticated ledger distributed amongst them. Masternodes are authoritative in the sense that they check the work provided by miners.

When a new transaction or an edit to an existing transaction comes in, generally a majority of the masternodes within a blockchain implementation must execute some algorithms. This process evaluates and verifies the history of the individual blockchain block that is proposed by coming to a consensus that the history and signature is valid. Once this stage is complete, then the new transaction is accepted into the ledger and a new block is added to the chain of transactions.

Conversely, if a majority of masternodes do not concede to the addition or modification of the ledger entry, then it is denied and not added to the chain. This distributed consensus model is what allows blockchain to run as a distributed ledger without the need for some central, unifying authority dictating what transactions are valid and (perhaps more importantly) which ones are not.

What is Mining? (Proof- of- Work)

Mining serves two purposes:

1. To verify the legitimacy of a transaction, thereby avoiding “double- spending”.
2. To create new Fantasy Gold Coins by rewarding miners for performing the previous task.

When sending a transaction this is what happens behind the scenes:

- Transactions are bundled together into what we call a block.
- Miners verify that transactions within each block are legitimate.
- To do so, miners should solve a mathematical puzzle known as a Proof -of--Work problem. A reward is given to the first miner who solves each block’s problem.
- Verified transactions are stored in the public blockchain.

This “mathematical puzzle” has a key feature: asymmetry. The work, in fact, must be moderately difficult for the requester side, yet easy to check for the network. This idea is also known as a CPU Cost Function, a Client Puzzle, a Computational Puzzle or a CPU Pricing Function.

All network miners compete to be the first to find a solution for the mathematical problem that concerns the candidate block. This problem is a problem that cannot be solved in other methods such as through brute force. Essentially, the problem requires a large number of attempts to solve.

When a miner finally finds the right solution, they announce it to the network and at the same time receive a cryptocurrency prize (the reward). In the Fantasy Gold Blockchain’s case a reward of Fantasy Gold Coins is provided by the protocol.

From a technical point of view, the mining process is an operation of inverse hashing: it determines a number (nonce), so the cryptographic hash algorithm of block data results in less than a given threshold.

This threshold, called “difficulty”, is what determines the competitive nature of mining: the more computing power added to the network, the higher this parameter increases, thereby increasing the average number of calculations needed to create a new block. This method also increases the cost of the block creation, pushing miners to improve the efficiency of their mining systems to maintain a positive economic balance.

What are Masternodes?

Masternodes help secure the Fantasy Gold network by making it more decentralized and providing a consensus for every transaction.

Masternodes are nodes (servers) that run the Fantasy Gold wallet software that provide additional services to the network, including instant and private transactions. For providing these important services, Masternode owners are rewarded a portion of each block. Block rewards will be split between POS and masternodes. Please see the block rewards and circulation table below for a breakdown.

These changes in the block reward split and the switch from Proof--of -Work to Proof--of--Stake happen automatically and are hard -coded into the Fantasy Gold Blockchain and cannot be changed any one-person, central authority or bad actor. We are able to give the times at which changes will occur because these events are programmed to take place when the blockchain reaches a certain height or number of blocks. The Genesis Block, or first block to be created, is block zero (0) and a new block is created every 90 seconds. The 90 second block spacing means that 960 blocks will be created every 24 hours.

What is Proof -of- Stake? (PoS)

Unlike the Proof--of -Work (PoW), where the algorithm unfairly rewards mass-miners solving resource-exhausting mathematical problems with the goal of validating transactions and creating new blocks at an unevenly distributed rate, Proof-of-Stake (PoS) rewards all holders of the coin by creating new blocks in a deterministic way, depending on wealth, also defined as “Stake”.

Once Fantasy Gold switches to a PoS network, wallets holding Fantasy Gold will “Mint” coins by letting them mature. The minting process involves first holding coins in a wallet, then unlocking that wallet, and simply staking those coins. Wallets that stake will earn 20% percent of the block reward, this will begin at block 43201. This algorithm, known as Proof--of-Stake allows users to generate more coins without the need for any specialized mining hardware or with the expense of higher electricity costs.

Because of its advantages, PoS is a better protocol than Proof-of-Work to validate transactions and achieve the same distributed consensus. It is still an algorithm, and the purpose is the same as Proof-of-Work, but the process to reach the goal is more efficient.

Specifications

Dark Gravity Wave 3.0

Dark Gravity Wave is employed by Fantasy Gold from the start as a method of retargeting PoW difficulty. It uses a simple moving average that can respond to large nethash increases or drop-offs in just a few blocks. This alleviates the “stuck block effect” often caused by multipools and prevents one person adding a substantial amount of computing power from instantly solving more than a few blocks.

Specification	Descriptor
Ticker	FGC
Algorithm	NIST5
RPC Port	57814
P2P Port	57810
Block Spacing	90 Seconds
Difficulty Algorithm	Dark Gravity Wave v3.0
Block Size	1MB
Mined/Minted Maturity	67 Blocks (~100 Minutes)
Confirmation	6 Blocks (~9 Minutes)
Circulation (1 Year)	17,138,612 FGC
Circulation (5 Years)	21,000,000 FGC
Block Rewards	20% PoS / 80% MN
Protocol Support	IPV4, IPV6, TOR
PoS	Blackcoin v3.0 PoS

Block Rewards and Circulation

POW will be in effect until block 43,200 - The block reward is 90% to masternodes and 10% to miners. At Block 43,201 Fantasy Gold will start its POS phase where block rewards will be 80% to masternodes and 20% to staking wallets.

Block 1 (4,750,000 FGC) was used to swap team and community’s held DFSCoin to Fantasy Gold Coins at a rate of 10 DFS to 1 FGC.

Subsidy	Blocks	POS	MN	Circulation
4750000	1	NA	NA	4750000
47	2 - 43200	NA	90	6780353
47	43201-86400	20	80	8810800
35.25	86401 - 172800	20	80	11856400
26.4375	172801 - 259200	20	80	14140600
19.8281	259201 - 345600	20	80	15853750
14.8711	345601 - 432000	20	80	17138612
11.1533	432001 - 518400	20	80	18102258
8.36499	518401 - 604800	20	80	18824993
6.27374	604801 - 691200	20	80	19367044
4.70531	691201 - 777600	20	80	19773582
3.52898	777601 - 864000	20	80	20078485
2.64674	864001 - 950400	20	80	20307162
1.98505	950401 - 1036800	20	80	20478670
1.48879	1036801 - 1123200	20	80	20607301
1.11659	1123201 - 1209600	20	80	20703774
0.837444	1209601 - 1296000	20	80	20776129
0.628083	1296001 - 1382400	20	80	20830395
0.471062	1382401 - 1468800	20	80	20871094
0.353297	1468801 - 1555200	20	80	20901618
0.264972	1555201 - 1641600	20	80	20924511
0.198729	1641601 - 1728000	20	80	20941681
0.149047	1728001 - 1814400	20	80	20954558

NIST5 Hashing

What is NIST5?

The National Institute of Standards and Technology **(NIST)** opened a public competition on November 2, 2007, to develop a new cryptographic hash algorithm – SHA-3, which augments

the hash algorithms specified in the Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard (SHS). The competition was NIST's response to advances in the cryptanalysis of hash algorithms. NIST received sixty--four submissions in October 2008, and selected fifty--one first- round candidates on December 10, 2008; fourteen second--round candidates on July 24, 2009; and five third -round candidates – BLAKE, Grøstl, JH, Keccak and Skein, on December 9, 2010, to advance to the final round of the competition. Eighteen months were provided for the public review of the finalists, and on October 2, 2012, NIST announced the winning algorithm of the SHA-3 competition – Keccak.
NIST5 chains together the 5 final-round candidates for SHA-3 hash competition, which were all selected for their performance & security (BLAKE Grøstl JH Keccak Skein). For more information on the NIST competition see here:

http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf

Feature Set

Masternodes

Masternodes are, a decentralized network of servers that serve the Fantasy Gold blockchain. Masternodes perform important network functions and receive part of the block rewards. Masternodes help the Fantasy Gold ecosystem by stabilizing coin supply, processing transactions, and securing the network. Masternodes require 10,000 Fantasy Gold Coins to activate and modest technical knowledge to operate. Any Fantasy Gold wallet holding at least 10,000 Fantasy Gold Coins can set up a masternode.

Obfuscation / Coin Mixing

Fantasy Gold has Obfuscation features, based on CoinJoin, coin mixing is done in a decentralized fashion through masternodes allowing for an additional layer of privacy. While not perfectly anonymous, Obfuscation via node mixing has security advantages over normal bitcoin transaction. For example, all Bitcoin transactions are transparent. For Fantasy Gold, if a bad actor gained control over 50% of the operating masternodes they would still have less than 0.5% chance of de-anonymizing a single transaction that was mixed with 8 rounds of Obfuscation (Kiraly 2017b). This important feature provides a high -level of anonymity and security for Fantasy Gold users that elect to obfuscate their transactions

SwiftTX

Masternodes, like simple nodes, are authoritative in nature, but using SwiftTX provides masternodes with the ability to lock and consensus transactions. When a transaction is submitted to the network, a group of masternodes validate the transaction. If those masternodes reach consensus on the transaction's validity, they are locked for later introduction into the blockchain, greatly increasing transaction speed compared to conventional systems (like

Bitcoin's 10-minute block times with multiple confirmations). SwiftTX makes it possible for multiple transactions to take place before a block on the network is mined with the same inputs. This system is based on Dash's InstantSend. (Kiraly 2017a).

Sporks

The Fantasy Gold network employs the multiphase fork mechanism known as "sporking". This enables the Fantasy Gold network to implement new features while minimizing the chances of an unintended network fork during rollout. Spork changes are deployable via the network and can be turned on and off as necessary without requiring node software updates (strophy 2017). This feature is extremely useful and allows the network to react quickly to security vulnerabilities.

TOR & IPV6 Masternodes

Fantasy Gold users will be able to run their Masternode from either an onion address or an IPV6 address. With TOR Masternode support, masternodes can be run as a TOR hidden service. This allows users to operate masternodes out of their home network without revealing their home IP or location, thereby avoiding dangers of potential cyber-attacks.

Governance System

The Fantasy Gold community is the most important factor behind the long-term success of the project, and their ability to meaningfully influence the future of the coin is paramount. Delaying the activation of this system will give us time to develop the underlying framework necessary for a positive user experience and maximize block rewards available to miners and masternodes.

We will utilize a multi-phase process for creating and submitting proposals. Each step will need to be fully completed. Failure to complete the steps outlined will likely result in a proposal not being activated. A basic outline of these steps are as follows:

• Start in our Discord chat and talk with some of the seasoned users. Gauge interest and if the response is positive, move to the next phase.
• Utilize multiple social media platforms to discuss and get feedback. Remember that Fantasy Gold has a diverse user base and differing levels of governance participation, reaching a portion of the user base will often require some footwork. Take note of these discussions and be able to cite them in the formal pre-proposal. The more citations provided, the better.
• Be open to suggestions from the community and developers. Be flexible and willing to incorporate external ideas and suggestions in your proposal.
• Create a formal pre-proposal on the Governance->Pre-Proposal section of our website. Provide citations for all discussions that occurred from the previous step. Treat your pre-proposal as if it is what will be submitted to the blockchain for voting.
• Upon completion of these steps, you will submit your proposal to the blockchain. Be prepared for two fees, one at the time of submission and a ballot fee paid to the developer that activates

your proposal on the blockchain. The submission fee is non-refundable, and the balloting fee will only be paid upon approval and activation of your proposal.
• Everyone is free to adjust their proposal to include the reimbursement cost of these two fees. Please make sure in your formal proposal you state that you are adding reimbursement to the stipend requested.
• Be sure to get back in touch with everyone you spoke with so your idea will be voted on. For a proposal to be paid out, 10% of the eligible masternodes must vote 'yes' on your proposal.

This process of getting a 10% consensus can be much harder than it sounds, so be diligent, informative, and respectful in procuring the votes necessary for your proposal to be paid.

Conclusion

Fantasy Gold Masternodes offer the Fantasy Sports and eSports Industries a platform where their payment processing gateways will help pay for themselves rather than being an unnecessary additional cost. Ultimately, Fantasy Gold offers a secure means to save the Fantasy Sports Industry and the eSports Industry hundreds of millions of dollars per year in merchant fees. In planned updates its open-source decentralized blockchain allow fantasy sports developers to build and integrate their own applications, distributed content, and more. Fantasy Sports developers can already take advantage of our Daily Fantasy Sports API located at https://api.draftdaily.com

References

Aumasson, L.M., Jean- Phillipe Henzen, 2013. SHA-3 proposal: BLAKE. Available at: https://131002.net/blake/blake.pdf.
Bertoni, G., Daemen, J., Peeters, M. & Van Assche, G., 2012. The keccak sha-3 submission. Available at: https://keccak.team/files/Keccak-submission-3.pdf
Bitcoin Core Team, T., 2017. Bitcoin developer reference. Available at: https://bitcoin.org/en/developer-reference#block-headers
Bulwark Whitepaper: Available at: https://bulwarkcrypto.com/Bulwark_Whitepaper_v1.1.pdf
Chang, S.-J., Perlner, R., Burr, W.E., Turan, M.S., et al., 2012. Third- round report of the sha-3 cryptographic hash algorithm competition. Available at: http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf.
Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Available at: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf
Ferguson, N.L., Schneier, S., Whiting, B., Bellare, D., et al., 2010. The skein hash function family.
Available at: http://www.skein-hash.info/sites/default/files/skein1.3.pdf
Gauravaram1, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., et al., 2012. Grøstl – a sha-3 candidate.
Available at: http://www.groestl.info/Groestl.phttp://www.skein-hash.info/sites/default/files/skein1.3.pdfdf.

jakiman, 2017. PIVX purple paper. Available at: https://pivx.org/wp-content/uploads/2017/03/PIVX-purple-paper-Technincal-Notes.pdf
Kiraly, B., 2017a. InstantSend. Available at: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146928/InstantSend.
Kiraly, B., 2017b. PrivateSend. Available at: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146924/PrivateSend.
Nakamoto, S., 2009. Bitcoin: A peer -to -peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf
Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Available at: https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf.
strophy, 2017. Understanding sporks. Available at: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/128319489/Understanding+Sporks.
Wiecko, R., 2017. Dash instamine issue clarification. Available at: https://dashpay.atlassian.net/wiki/spaces/OC/pages/19759164/Dash+Instamine+Issue+Clarification.
Wu, H., 2012. The hash function jh. Available at: http://www3.ntu.edu.sg/home/wuhj/research/jh/jh_round3.pdf.