Fantasy Gold Whitepaper v2.19.1

March 2020

https://FantasyGold.io

Fantasy Gold Core Team:

Nicolas Hernandez (Lead Developer)

Djoël van der Leeuw (Business Director)

Eugene Saksonov (PokerVR Lead)

Chris Hanus (Fantasy Sports Liaison)

Alok Kumar Saxena (Developer)

Tim Baker (Fantasy Gold Coin Dev)

Craig Williams (Community Director)

Acknowledgements

Fantasy Gold would not have been possible without the prior works of the respective Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash, PIVX, Bulwark and Qtum 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 A UTILITY BLOCKCHAIN. FANTASY GOLD IS NOT A SECURITY AND SHALL NOT REPRESENT FRACTIONAL OWNERSHIP OF THE OPENSOURCE 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 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.

WHAT IS FANTASY GOLD COIN?

Built by the developers of DFSCoin, the Fantasy Gold Blockchain replaced DFS on April 30th, 2018 as a means of capitalizing on the latest advancements in Proof of Stake and smart contract technology.

Fantasy Gold is a peer to peer cryptocurrency and blockchain that started out to serve the $7 Billion fantasy sports industry in both the B2B and B2C spaces as well as the $1.5 billion competitive eSports industry in 2017. Since then it has expanded its horizon to become a multi-purpose platform offering Ethereum Virtual Machine based smart contracts and lightning fast transactions. It achieves this through the revolutionary Account Abstraction Layer which allows the EVM to communicate with FantasyGold's Bitcoin-like UTXO blockchain for compatibility with most existing Solidity based smart contracts.

Unlike using traditional centralized payment processing, the Fantasy Gold project does not charge any addition transaction or service fees to use the payment network. Senders pay a very small transaction fee that is awarded to stakers who process the transactions and by that keep the chain running.

Using smart contracts, it is possible for anyone to make use of the FGC blockchain, which significantly simplifies creating your own project with your own token. Other than this Fantasy Gold is constantly looking to expand by itself, adding new features to its chain, site and infrastructure.

In the near future the new team will primarily focus on growth and diversification of the Fantasy Gold platforms and eco system. Starting off with our own exchange -which should be ready at the prementioned launch- and moving on to develop an online sportsbook and further down the line an online poker platform. All of this will be in our roadmap 2020, published at https://FantasyGold.io

Usability

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 one of our supported 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 to help support the network and getting some stake rewards in return.

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.

Developer's Tools

- Smart contract deployment tool
    - https://github.com/fantasygold/solar
- DApp JavaScript Library
    - https://github.com/fantasygold/fantasygoldjs
- A toolkit for building fantasygold light wallets
    - https://github.com/fantasygold/fantasygoldjs
- CORS fantasygoldd RPC proxy for DApp
    - https://github.com/fantasygold/fantasygoldportal
- Docker images for running fantasygold services
    - https://github.com/fantasygold/fantasygold-docker
- FantasyGold Insight API
    - https://github.com/FantasyGold/insight-api#insight-api

Blockchain-enabled smart contracts

A **smart contract** is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.

Using proof-of-stake for transaction validation gives FantasyGold a significant performance advantage compared to proof-of-work blockchains.

The FantasyGold smart-contract framework uses smart-contract template libraries for rapid best-practice industry deployment. Full Node operators are rewarded for validating transactions.

- Ticker: FGC
- Transaction model: UTXO (Unspent Transaction Output) from bitcoin
- Smart contract architecture: EVM (Ethereum Virtual Machine)
- Block size: 2 million bytes, scalable up to 32 million bytes
- Average block spacing: 128 seconds
- Smart contract token protocol: FGC20, based on Ethereum ERC20; FGC721 non-fungible tokens in development
- Consensus algorithm: Proof of Stake, version 3.0, upgraded from Blackcoin
- TPS (Transactions Per Second): 70 to 100.
- Block reward: 5.0 FGC (halved every 4 years), plus tx fees and gas
- Mined/Minted Maturity: 500 Blocks
- Maximum supply: 210 million

Account Abstraction Layer

FantasyGold smart contracts use the Ethereum Virtual Machine (EVM) which was designed to work with an account that holds the wallet's balance. However, FantasyGold transactions are based on the bitcoin UTXO model which manages the balance of a wallet as any number of individual transactions. The Account Abstraction Layer interface abstracts all these individual transactions to present a single account balance that allows easier smart contract operation and code reuse from Ethereum smart contracts.

The resulting EVM account model is simple for smart contract programmers to use. Operations exist to check the balance of a contract and other contracts on the blockchain. There are operations for sending FGC to other contracts. Although these operations seem simple, the AAL is fairly complex and enables the addition of new virtual machines, such as the x86 VM.

The x86 VM

Intel's x86 CPU architecture is the dominant CPU platform for servers and desktop computers. The FantasyGold team is developing a virtual machine using the x86 machine language. A "virtual machine" is an isolated software execution environment that can run on many different hardware platforms (Macs, PCs, servers, virtual private servers in the cloud, etc.). FantasyGold's current virtual machine uses EVM and Solidity.

Ethereum's Solidity language was created for smart contract programming. As a brand-new programming language Solidity has some problems. With the x86 VM, a huge population of developers will be able to use familiar languages and tools to write Qtum smart contracts in popular and mature languages like C, C++, Rust, and Python.

FGC20 Tokens

FGC20 tokens are derived from the protocol of Ethereum ERC20 tokens. FGC20 tokens are created by FantasyGold smart contracts as a digital asset for use with DApps. Transactions with FGC20 tokens are made using contract calls and require FGC for gas fees. Some FantasyGold wallets have built-in smart contracts templates to easily create FGC20 tokens by simply filling in a form and publishing that contract. See more details in the FGC20 token documentation.

FantasyGold Core is our primary mainnet wallet. It implements a full node and is capable of storing, validating, and distributing all history of the FantasyGold network.

Fantasy Gold Core is currently implementing the following:

- Sending/Receiving FantasyGold
- Sending/Receiving FGC20 tokens on the FantasyGold network
- Staking and creating blocks for the FantasyGold network
- Creating and interacting with smart contracts
- Running a full node for distributing the blockchain to other users
- Prune+ACI- mode, which minimizes disk usage
- Regtest mode, which enables developers to very quickly build their own private FantasyGold network for Dapp testing
- Compatibility with the Bitcoin Core set of RPC commands and APIs

Note: FantasyGold Core is considered beta software. We make no warranties or guarantees of its security or stability.

FantasyGold v2.19.1 integrates the latest features from the Ethereum Virtual Machine, introducing a comprehensive set of improvements that modernizes the virtual machine within the FantasyGold ecosystem. This update includes a wide range of improvements: cheaper cryptography built-ins, new mathematical operators, gas cost optimizations for storage, as well as new ways to deploy and interact with smart contracts.

As a result of these updates, we expect that smart contract developers on the FantasyGold platform will be able to create new types of applications that enable better privacy, trust, security, and usability within our decentralized ecosystem.

Virtual Machine Improvements

In v2.19.1, several new instructions were added to the virtual machine to improve functionality and decrease gas costs. This includes the smart contract-relevant upgrades from Ethereum's Byzantium and Constantinople updates, including the following EIPs: Byzantium: 140, 196, 197, 198, 211, 214, 658, and Constantinople: 145, 1014, 1052, 1283.

- The bitwise shift operators SHL (shift left), SHR (logical shift right) and SAR (arithmetic shift right) are added for faster, more efficient low-level mathematical operations.
- extcodehash is added to make it cheaper to verify whether an address has the expected smart contract code.
- The revert instruction is added, to report error messages to users, and refund any unused gas.
- Static-call instruction is added, to make it possible to call another contract in "read-only" mode.
- Provide a way for smart contract methods to return multiple values.
- Create2 is added, so it's possible to deploy a smart contract to a pre-determined address.

In particular, the addition of the Create2 instruction opens up the fascinating possibilities of creating "counterfactual contract." Previously, the address of a smart contract was partially determined by the nonce of its creator, therefore it is unpredictable. With Create2, a developer can predetermine the address of a smart contract, without actually deploying the code. This is useful, because the details of some smart contract logic may now be hidden from the public until they are needed by the parties involved. It is like a fair arbitrator who will follow the instructions in a sealed envelope should disputes arise.

Counterfactual smart contracts enable generalized state channel to be implemented on FantasyGold, which could empower off-chain privacy solutions.

Cryptography Improvements

The Virtual Machine within FantasyGold is a general computation platform. While developers can implement any cryptographic algorithms directly in a smart contract, doing so is often too expensive for practical use. Cryptographic algorithms often require special optimizations to run efficiently.

This update introduces highly-optimized implementations of mathematical functions to drastically lower the gas costs for some interesting algorithms, making them practical for actual use cases.

Big Integer Arithmetic

The virtual machine is optimized for 256-bit integers, which are suitable for implementing modern elliptical curve cryptography algorithms. However, older cryptographic algorithms like RSA rely on different mathematical entities, which in turn require a much higher number of bits to achieve equivalent security. Modern guidelines for using RSA recommends 4028-bit public keys to be as safe as 256-bit ECC public keys.

To support these algorithms, this update introduces efficient and cheaper ways to do the math on numbers larger than 256 bits. This is accomplished by adding precompiled contracts that support the following operations (as well as their associated gas costs):

```
GADDSUBBASE: 15
GMULDIVBASE: 30
GMODEXPBASE: 45
GARITHWORD: 6
GQUADDIVISOR: 32
```

ZK-SNARKs Support

Zero-Knowledge proof systems open up exciting new possibilities for enabling privacy applications on the FantasyGold blockchain. However, these systems depend on a different type of elliptical curve than the native elliptical curve used by FantasyGold.

This update adds support for the alt_bn128 curve, which many zk-SNARKs systems rely on. In particular, this is the same curve chosen by the ZCash cryptocurrency.

Storage Gas Cost Optimization

Storing data on the blockchain is expensive since each stored item is stored by every node of the network, and forever! However, the way the storage instruction sstore is implemented is actually optimized to make some cases cheaper, but the system charges the same amount of gas anyway. This update decreases the gas cost for special cases where sstore could be optimized.

Consider the following series of instructions in a smart contract call, setting the position 0x0 to different numbers:

```
sstore 0x00 0x1
sstore 0x00 0x2
sstore 0x00 0x3
```

In this sequence, only the final sstore matters in terms of cost, because that's the number being written onto the blockchain. Previously all these are expensive in gas costs. With the new update, only the last one is expensive, and preceding instructions made as cheap as possible.

Conclusion

Fantasy Gold offers the 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. And this is just a starting point. The FGC team is ever on the look-out for new oppurtunities to add yet another usecase to the Fantasy Gold platform.

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/wpcontent/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.