GoldCoin Reverse Fork

(*Bitcoin/Goldcoin Blockchain Merger*)

December 25th, 2018

"The Bitcoin the World Was Promised: Rebranded."

Authors:

Goldcoin Community
Greg 'MicroGuy' Matthews
William Coogan

Developers:

Goldcoin Core Developers
Peter "Bushstar" Bushnell

www.goldcoin.org

GoldCoin Reverse Fork

(*Bitcoin/Goldcoin Blockchain Merger*)

Abstract:

Goldcoin was launched on the Bitcointalk.org forum on May 15th, 2013 by an anonymous developer using the name GLDCOIN. The following month, like Satoshi, he vanished, never to be seen again.

Since those early days, the community has grown exponentially with many developers contributing to the project. There have been several innovative advances added to the currency over those years including a 51% attack defense system, Golden River difficulty algorithm, ACPD (Advanced Checkpointing with Difficulty Detection), along with bigger, faster blocks. Throughout this period, Goldcoin has been dedicated to on-chain scaling and following the principles set forth in the original Bitcoin whitepaper[1].

There have also been many exciting advances in Bitcoin during those last 6 years that provide a method of scaling that is not part of the main blockchain. The overall problem is that the Bitcoin Core blockchain is being artificially throttled, meaning these external systems have become dependencies rather than features.

This whitepaper discusses an experimental merging of two blockchains that will bring the Bitcoin and Goldcoin communities together onto a single united blockchain advocating for and advancing both on-chain and off-chain scaling.

This will allow Goldcoin to grow at a much more rapid pace and will help to unite both ideological camps, supporters of Bitcoin Core, and supporters of Bitcoin Cash and Bitcoin SV.

"Don't be afraid of potential hard forks. They are a key component of Bitcoin's ability to upgrade through rough consensus/game theory." ~ Matt Odell

Introduction:

Goldcoin has followed the ideals set forth in the original Bitcoin whitepaper since 2013. Goldcoin is widely recognized as one of the earliest cryptocurrencies in existence.

As a matter of fact, the community has often times been criticized for openly promoting our mission of completing Satoshi's vision, a mission we embraced years before Bitcoin Cash or Bitcoin SV came into existence. Reverse hard forking Bitcoin and recapturing the Bitcoin genesis block is the next natural step in the evolution of our project.

Given the numerous splits in the Bitcoin brand, it's no wonder there is a tremendous appetite for a return to the original bitcoin protocol under a unified protocol brand. Afterall, financial institutions will remain reluctant to build on an unstable protocol and brand that keeps splintering into pieces. This reverse fork will unify these various camps and unit them under a single undivided brand.

Bitcoin was created for many different reasons and every day, people find new reasons to adopt Bitcoin. One of the historical reasons is that people do not trust states or banks or any such intermediaries to

[1] https://bitcoin.org/bitcoin.pdf

control their money.

However, in order to properly scale, Bitcoin must be allowed the freedom to do so both *on-chain* and *off-chain*. This allows the Lightning network to be a primary 'feature' of the system and not a dependency.

No longer will users be required to "pick a side" between the various camps. Goldcoin combines the best of the Bitcoin forks and unites them again. The new Goldcoin will be a rebranded version of Bitcoin, only with dual scalability, and bigger, faster blocks.

"I personally like hard forks. Sure, they can be a little more chaotic if they're controversial, but that's the price of freedom." ~ Vitalik Buterin

Reverse Fork Methodology:

Bitcoin is a distributed consensus system. All Bitcoin full nodes are running software that enforces the same consensus rules; full nodes that enforce different consensus rules are not part of the Bitcoin network, by definition. If a miner finds a new block that follows the network consensus rules and broadcasts it to the network, all full nodes in the network will accept that block and all of the transactions in it as valid, and miners will build the next block on top of that one. A blockchain hard fork occurs when a block is mined that does not comply with the network consensus rules.

Prior to BTC block 478558, Bitcoin nodes and Bitcoin Cash nodes were still enforcing the same consensus rules and accepting the same blockchain as valid. But from that block onward, Bitcoin Cash's new consensus rules came into effect, which caused Bitcoin nodes to reject blocks that were mined by miners using Bitcoin Cash software, and Bitcoin Cash nodes to reject blocks that were mined by miners who continued to mine with Bitcoin software. Thus, the network bifurcated.[2]

The Bitcoin blockchain continued to add a new block every 10 minutes on average, but Bitcoin Cash began building a new blockchain that branched away from Bitcoin. This had the effect of creating a new cryptocurrency that shares the same transaction history and ownership distribution up until the fork block, but then diverges from it.

Goldcoin changes different consensus rules than Bitcoin Cash did, but it will fork from Bitcoin in the same manner - by enforcing new consensus rules as of a predetermined BTC block height. The new rules will come into effect on June 17th, 2019. At this time, exchanges will be asked to pause trading to allow them time to upgrade.

The first 10 blocks will be mined by the core developers as we import the existing Goldcoin UTXO set into the newly forked blockchain. From that moment onward, Goldcoin miners will begin building a new branch of the rebranded Bitcoin blockchain and exchanges will be asked to reopen trading.

This new branch is a cryptocurrency with the same transaction history and ownership distribution as Bitcoin at the fork block; if you hold BTC, you will automatically receive a 1:1 amount of GLD. And all

[2] https://bitcoingold.org/wp-content/uploads/2017/10/BitcoinGold-Roadmap.pdf

current Goldcoin owners will maintain a 1:1 amount of GLD on the newly merged chain. This new Bitcoin blockchain will be branded 'GoldCoin.'

"A new fork of bitcoin with a larger block size would probably be valued higher than Bitcoin Cash." ~ Matt Odell

Block Capacity Increase:

Satoshi Nakamoto intended for Bitcoin to scale on-chain. To our knowledge, there is no trusted expert in the field disputing this fact.

While we feel that a scaling solution such as Lightning is a perfectly acceptable feature to add to Bitcoin, it should not be a forced system due to a throttled blockchain. So this new chain will have a maximum block size of 32 MB which will allow 'economic forces to decide' which scaling method to favor, not some human in charge of the system.

The majority of Bitcoin users have long requested faster block times. The new Goldcoin blockchain will have 2 minute blocks. Combined with the increased block size above, this means block size will be 150 MB (effective) and 300 MB to 600 MB (weighted).

"The current system where every user is a network node is not the intended configuration for large scale. That would be like every Usenet user runs their own NNTP server." ~ Satoshi Nakamoto

Proof-of-Work Algorithm:

Bitcoin mining is a proof-of-work system that implements "a distributed timestamp server on a peer-to-peer basis." This is how Bitcoin manages to maintain consensus across a vast, globally-distributed, permissionless network of nodes. In order to remain backward compatible with miners after the fork, Goldcoin will preserve its Scrypt mining algorithm.

Historical Explorer:

Since we are keeping the Bitcoin blockchain and retiring the previous Goldcoin blockchain, it will be necessary to maintain a special block explorer for retrieving pre-fork Goldcoin transactions.

These historical explorers will operate using a snapshot of the Goldcoin blockchain and will be maintained by the team and community. The source code will be made available on the Goldcoin github.

After the fork, regular Goldcoin explorers will provide transaction history for all-post fork transactions and all Bitcoin transactions to date.

Local Node Requirements:

The new Goldcoin clients will support blockchain pruning and SPV techniques like Electrum in order to reduce the burden of the blockchain on user devices.

In addition to an Electrum wallet, the Core client will be distributed in both a default version and a special bare-mode version set to *pruning on* that will only require approximately 5 GB of local disk space and 256 MB RAM memory.[3]

Difficulty Adjustment Algorithm:

In Bitcoin, the difficulty of mining adjusts every 2016 blocks (approximately two weeks) in order to maintain an average interval of 10 minutes between blocks. If the average time between blocks was less than 10 minutes, the difficulty will increase; if the average time was more than 10 minutes, the difficulty will decrease.

Goldcoin adopts an innovative difficulty algorithm designed by our Chief Scientist Amir Eslampanah. Golden River outperforms many self-adjusting difficulty algorithms, including Kimoto Gravity Well, or KGW. Golden River, which adjusts the difficulty each block, is a vast improvement over the original Bitcoin algorithm, which makes adjustments every 2016 blocks. This more responsive difficulty adjustment algorithm is extremely useful in protecting against big swings in the total amount of hash power.

Golden River recalculates the difficulty at each block by examining recent blocks and determining average and median block times. It differs in that it can make more accurate adjustments by reducing the network difficulty by as much as 50 percent in one block to respond to a hypothetical 90 percent drop in hash power.

Advanced Checkpointing (ACPD):

To protect the network against 51% attacks during the first few years after the fork, Goldcoin will deploy Advanced Check Pointing with Difficulty Detection, a system developed in-house that adds checkpoints to the blockchain while also monitoring difficulty.[4]

Once the difficulty reaches the preset threshold, a level where the network hashrate is deemed safe from 51% attacks, the checkpointing system drops out like training wheels from a bicycle.

Block Rewards and Retargets:

Goldcoin will preserve its current block reward of 4 and existing halving formula. To achieve stability and low latency, the GoldCoin network tries to produce one block every two minutes. In order to maintain consistent block intervals, the difficulty must adapt, or retarget.

Since the introduction of Golden River, these retargets occur with each block. Below is a list of historical

[3] https://bitcoin.org/en/bitcoin-core/features/requirements
[4] https://github.com/goldcoin/goldcoin/commit/7a76ae6933c7e5d96d3b0ce1d66a6133076dde00

retarget times and block times, as well as historical block reward information.

Block Targets:

2.5-minute block targets up till block 44,

2 - minute block targets thereafter

504 blocks per difficulty retarget up to block 44,999

60 blocks per difficulty retarget up to block 248,000

Difficulty retargets each block thereafter

Block Rewards:

Blocks 1 – 200 = 10,000 GLD

Blocks 201 – 2,200 = 1,000 GLD

Blocks 2,201 – 44,999 = 500 GLD

Block 45,000 reward drops to 45 GLD

Block 372,000 reward drops to 4 GLD

The reward is then reduced each year using the following formula:

50 divided by (1.1 + 0.49*every year thereafter)

Total Blocks: 21,441,000

Total Premine: Zero (not premined)

Total Coins: 89,245,700 (post bitcoin fork)

The block reward ends in the year 2100, approximately. The transaction fees will support miners thereafter.[5]

Free Transactions:

GoldCoin isn't only being made into a high-value platform and lasting foundation for the world's financial systems. It's also the ideal cash payment system. To keep it affordable, 5 percent of every 32 MB block is reserved for free transactions. This allows for approximately 10 million free transactions per day.

[5] https://github.com/goldcoin/wiki/wiki/GoldCoin-Whitepaper#block-retargets-and-rewards

This means that users in developing worlds will have the ability to opt-out of paying a transaction fee, while others can include a fee to prioritize transaction speed.

0-Conf Transactions:

The rebranded blockchain will once again support near-instant transactions using 0-Conf. This feature was abandoned in Bitcoin Core and is no longer possible due to network congestion and replace-by-fee, or RBF. Goldcoin will retain 0-Conf capability.

For most merchant transactions, 0-Conf is a perfectly safe method of processing a transaction. For big-ticket items, such as automobiles, the merchant could simply wait the two minutes for the first confirmation before delivering the item. In either case, the risk will be much less than the rate of chargebacks on verified credit card transactions or that of returned checks.

Replay Protection:

The risk of a replay attack is inherent to every cryptocurrency hard fork and has to be taken into consideration to protect users from losing their funds. A hard fork is an exact duplicate of the blockchain, and as such, a transaction that is broadcast publicly to the network can be replayed on both sides of a fork, unless replay protection is implemented.

To safeguard against such attacks, Goldcoin will incorporate replay protection. This is a studied problem, and we are using the industry standard solution called (SIGHASH_FORK_ID). It is an effective replay protection mechanism that adds a new algorithm to calculate the hash of a transaction so that all the new Bitcoin Core transactions will be invalid in the Goldcoin blockchain and vice versa.

Unique Address Format:

By default, both sides of a cryptocurrency hard fork will continue to use the same address format. That means it's possible to send coins to an address on the other blockchain unintentionally, which can cause users to lose funds by mistake. Bitcoin Cash, for example, is a hard fork that did not change the address format; its addresses are indistinguishable from Bitcoin Core addresses. There have been many reports of people accidently sending their BTC to a BCC address and vice versa. In some cases these coins could be permanently lost.

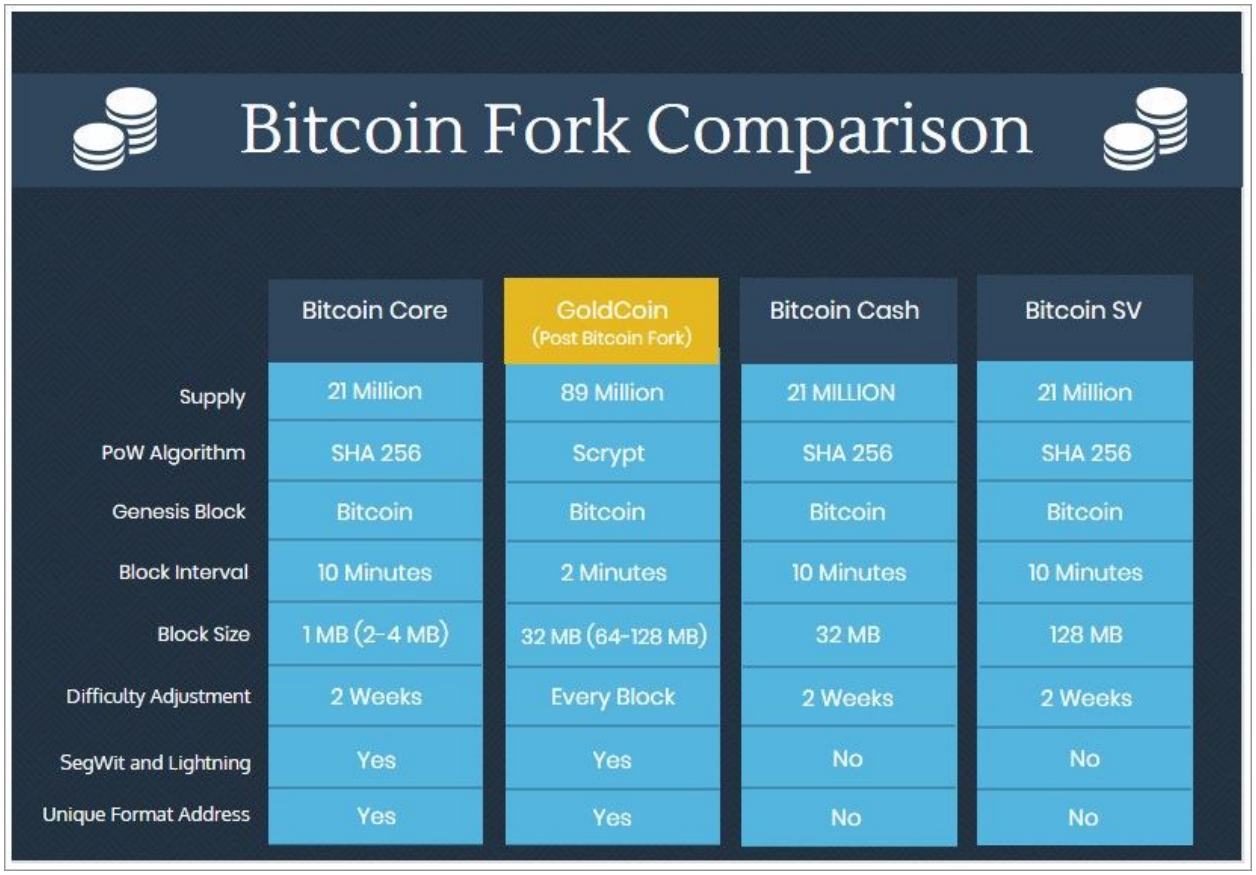
In order to ensure that this potential confusion does not exist in Goldcoin, a unique address format will be implemented. The prefix of PUBKEY_ADDRESS and SCRIPT_ADDRESS from the previous Goldcoin chain will be used which is easily distinguishable from Bitcoin Core or Bitcoin Cash addresses.

To acquire free Goldcoin you simply have to hold BTC at the time of the fork. If you hold BTC at that time, you will automatically receive an equal amount of GLD at the same address (new and old address format are convertible), spendable with the same private keys, after the fork in June 2019.

If you own Goldcoin, you will simply need to download and install the latest client software when it is

released. This will be necessary to ensure that you are following the proper chain after the fork. It is also very important to make a backup of your Private key and/or keep the mnemonic phrase required to recover your wallet. However, if you have your BTC on an exchange or custodial service without access to the private key, then you have to make sure that the service will support Goldcoin after the fork. If you have any doubts about that, then you would be advised to transfer your BTC to one of the many reputable services that will support it. If your exchange does not support gld and the reverse hard fork, we suggest you alert your exchange to the need for this support.

Comparison Chart:



If you have BTC in a paper wallet, hardware wallet, multi-signature address, or any other form of secure private key storage, you will be able to spend it on the new chain at any time in the future. There is no expiration date. If you have BTC in cold storage that you did not plan to touch for many years, do not change your plans because of this fork. Your BTC will still be convertible to GLD decades from now.

GoldCoin Reverse Fork

(*Bitcoin/Goldcoin Blockchain Merger*)

Exchanges:

Cryptocurrency exchanges are custodial businesses, which means they control your private keys, not you. When the Goldcoin fork occurs, any exchange that is holding BTC on your behalf will also receive the corresponding GLD. While they should credit your account with the equal amount of GLD, there is no legal authority that can force them to do so. The Goldcoin home page will display the names and logos of exchanges that have promised to credit BTC users with GLD at the 1:1 ratio.

If your exchange is not shown, please consider transferring your BTC to a supporting exchange or, better yet, withdraw to a personal wallet where you control the private keys.

Conclusion:

GoldCoin is a free open source project that's been maintained by a small group of cryptocurrency enthusiasts since 2013. Since the beginning, the team has been dedicated to completing the mission outlined in the original Bitcoin whitepaper. As it was not forked from Bitcoin, it lacks ties to the genesis block. Merging with Bitcoin and recapturing the genesis block is the next logical step in our evolution.

In contrast to the other prominent Bitcoin forks, this reverse fork (or merger) was specifically designed from the beginning to inspire innovation in the ecosystem and to give value to the vision of decentralization, with a strong emphasis on survival.

When Satoshi created Bitcoin, it was the product of an idea. A vision. Unfortunately, instead of a united continuation of his vision, the crypto world got chaos. Whereas the other forks were born from hostility and division, Goldcoin arises from a desire to "unite" the various factions into a single rebranded "Satoshi" chain. The way it ought to be.

Acknowledgments:

We would like to acknowledge the Goldcoin community for their continued support over these many years and also Bitcoin Gold and Bitcoin Private for their contributions to this industry. We'd also like to thank Satoshi Nakamoto and all of the amazing developers who have contributed to these various projects over the years, without them none of this would have been possible.