BITCOINGOLD

Bitcoin Gold (BTG)

www.btcgpu.org
press@btcgpu.org
support@btcgpu.org

Abstract. Bitcoin Gold is a community-led project to create an experimental hard fork of Bitcoin to a new proof-of-work algorithm. The purpose for doing this is to make Bitcoin mining decentralized again. Satoshi Nakamoto's idealistic vision of "one CPU one vote" has been superseded by a reality where the manufacture and distribution of mining equipment has become dominated by a very small number of entities, some of whom have engaged in abusive practices against individual miners and the Bitcoin network as a whole. Bitcoin Gold will provide an opportunity for countless new people around the world to participate in the mining process with widely-available consumer hardware that is manufactured and distributed by reputable mainstream corporations. A more decentralized, democratic mining infrastructure is more resilient and more in line with Satoshi's original vision. Perhaps, if the Bitcoin Gold experiment is judged by the community to be a success, it may one day help build consensus for a proof-of-work hard fork on Bitcoin itself.

Introduction

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

One of the central component of the Bitcoin architecture is mining. Simply put miners verify every transaction and compete with each other to get rewards. To get the reward, a miner has to solve a math problem before anyone else in the network.

Back in the days, a miner would be any geek with a computer, willing to trade electricity for Bitcoins. Today, a miner is usually a huge warehouse full of very advanced computers, constantly running to solve the math problems as fast as possible.

As it becomes more and more difficult to mine Bitcoin, more capital is required to operate profitable mining operations. They often are located in a country where the electricity is very cheap. Today, a great majority of the miners are located in China because they have access to cheap electricity.

In Satoshi Nakamoto's white paper, one of the main idea was that every CPU was going to be an equally important part of the network. We want Bitcoin to be a shared and independent currency. We don't want any fat cat to drive our monetary architecture.

The importance of miners in the network is constantly growing. To preserve the independence of the Bitcoin ecosystem from miners' influence, some people thought that it would be a good idea to change the bitcoin protocol in such a way that more people can have access to Bitcoin mining.

That's why Bitcoin Gold was born, in order to bring Bitcoin mining back to the "people".

Origins of Bitcoin Gold

In July 2017, Jack Liao, CEO of LightingAsic and BitExchange, made an announcement that he was working on a hard fork of Bitcoin to change the proof-of-work algorithm from the SHA256 algorithm originally selected by Satoshi Nakamoto to Equihash. The effect of this change will be to enable a whole new class of individuals and businesses to participate in mining this new branch of the Bitcoin blockchain without being required to purchase specialized equipment that is primarily manufactured by one firm that competes against its own customers with newer, more efficient versions of the old equipment that it sells at a high markup.

Given the dysfunctional current reality of the Bitcoin mining sector, it is no wonder that there is a tremendous appetite for a proof-of-work change hard fork. Since the Bitcoin Gold project was announced, it has grown rapidly, attracting developers, miners, and supporters from across the globe.

Mechanics of a Hard Fork

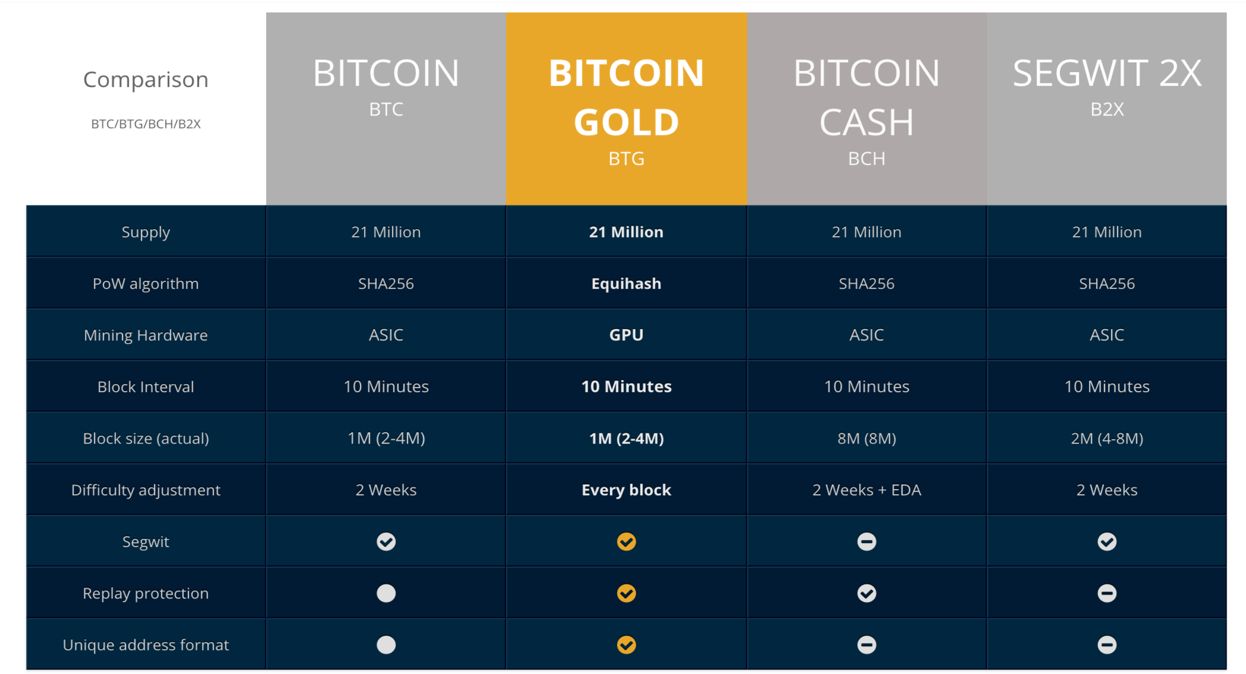
Bitcoin is a distributed consensus system. All Bitcoin full nodes are running software that enforces the same consensus rules; full nodes that enforce different consensus rules are not part of the Bitcoin network, by definition. If a miner finds a new block that follows the network consensus rules and 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.

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.

Bitcoin Gold 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 at block 491407. From this block onward, Bitcoin Gold miners will begin building a new branch of the Bitcoin blockchain. This new branch is a cryptocurrency with same transaction history and ownership distribution as Bitcoin at the fork block; if you hold BTC, you will automatically receive an equal amount of BTG.

Here are some of the differences between Bitcoin Gold and other forks of Bitcoin:



Comparison BTC/BTG/BCH/B2X	BITCOIN BTC	**BITCOIN GOLD** BTG	BITCOIN CASH BCH	SEGWIT 2X B2X
Supply	21 Million	**21 Million**	21 Million	21 Million
PoW algorithm	SHA256	**Equihash**	SHA256	SHA256
Mining Hardware	ASIC	**GPU**	ASIC	ASIC
Block Interval	10 Minutes	**10 Minutes**	10 Minutes	10 Minutes
Block size (actual)	1M (2-4M)	**1M (2-4M)**	8M (8M)	2M (4-8M)
Difficulty adjustment	2 Weeks	**Every block**	2 Weeks + EDA	2 Weeks
Segwit	✓	✓	⊖	✓
Replay protection	●	✓	✓	⊖
Unique address format	●	✓	⊖	⊖

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 the Bitcoin manages to maintain consensus across a vast, globally-distributed, permissionless network of nodes.

Satoshi Nakamoto chose SHA256 as the algorithm to use in the original design of Bitcoin’s PoW system. SHA256 served Bitcoin well during the early years of its existence, but as Bitcoin became more popular and more valuable, competition in mining became more fierce. Skilled engineers from a small number of companies developed Application Specific Integrated Circuits (ASICs) that could perform SHA256 calculations millions of times faster and more efficiently than any other computer. This made non-specialized computer hardware obsolete for mining Bitcoin. Satoshi’s vision of “one-CPU-one-vote” was replaced by one-ASIC-one-vote.

Now, the only way to participate in Bitcoin mining is to buy hardware from one of those manufactures - the biggest of which is believed to manufacture over 70% of the global supply of SHA256 ASICs. This has led to a situation where one entity can hold the entire network hostage, and this is exactly what happened when the backwards compatible Segregated Witness upgrade was blocked by a faction of miners, despite there being universal consensus from Bitcoin experts that it should be activated.

In order to counteract this concentration of power in the mining sector, Bitcoin Gold will implement a new proof-of-work algorithm - Equihash. Replacing the SHA256 algorithm means that all of the ASICs designed for Bitcoin will be useless for mining Bitcoin Gold. Equihash is a memory-hard algorithm that can be most efficiently solved by GPUs - a standard type of computer and smartphone hardware that is manufactured by mainstream companies and available around the world. With ASIC manufacturers out of the picture, Bitcoin Gold will provide an opportunity for a whole new class entrepreneurs and investors to get involved with mining. Bitcoin Gold mining will be decentralized again, closer to Satoshi's original vision.

ASIC-resistance is a permanent attribute of Bitcoin Gold. It is much more difficult to create ASICs for a memory hard algorithm like Equihash than SHA256, however it is not impossible. If the day ever comes when Equihash ASICs begin to proliferate and mining begins to centralize again, Bitcoin Gold will have another hard fork to implement a new PoW algorithm.

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.

Bitcoin Gold will adopt a difficulty adjustment algorithm called DigiShield V3. The idea behind it is to look at how much time has elapsed between the most recent block and the median of a set number of preceding blocks, and to adjust the difficulty every block to target a 10 minute block interval. This more responsive difficulty adjustment algorithm is extremely useful in protecting against big swings in the total amount of hash power. Such swings can result in extreme deviation from the normal 10 minute target block interval. Bitcoin Cash attempted to protect against this risk by implementing an "emergency difficulty adjustment" algorithm, but that had the catastrophic effect of causing sometimes 50 blocks to be mined in one hour, and other times more than 12 hours between two blocks.

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.

Bitcoin Gold will implement a solution called *SIGHASH_FORK_ID* replay protection. It is an effective two-way replay protection mechanism that enforces a new algorithm to calculate the hash of a transaction so that all the new Bitcoin transactions will be invalid in Bitcoin Gold blockchain and vice versa. Bitcoin Gold will implement replay protection BEFORE THE LAUNCH.

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 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 Bitcoin Gold, a unique address format will be implemented. The prefix of PUBKEY_ADDRESS and SCRIPT_ADDRESS will be changed to a new prefix (yet to be determined) that can easily be distinguished from Bitcoin addresses.

How to Acquire Bitcoin Gold

The hardfork will occur on block 491407. To acquire free Bitcoin Gold you simply have to hold Bitcoin at the time of the fork. If you hold BTC at that time, you will automatically receive an equal amount of BTG at the same address (new and old address format are convertible), spendable with the same private keys, when the Bitcoin Gold network launches in November. 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 Bitcoin Gold 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.

Timeline

Step 1: The hard fork occurs: a 'snapshot' of the blockchain is taken

Usually a hard fork will happen at the same time when Bitcoin reaches the fork block. However, Bitcoin Gold uses a different way to launch the hard fork: by "taking a snapshot" of the Bitcoin blockchain before the fork block height 491407. Instead of forking immediately, the Bitcoin Gold p2p network will launch a few days later from that snapshot.

When Bitcoin reaches the block 491407, nothing special will happen. Bitcoin block 491407 will be mined with SHA256 as normal. No block will be mined in the Bitcoin Gold p2p network because it is not launched yet.

However, when the full node client of Bitcoin Gold is ready a few days later, instead of mining from the latest Bitcoin block, Bitcoin Gold will start to mine its own 491407th block on top of block 491406. Bitcoin Gold full nodes will only accept a block 491407 that is mined with Equihash, so they will not recognize BTC block 491407 as a valid BTG block.

At the same time, Bitcoin already have a longer blockchain. That's why it's called a "snapshot hard fork". We didn't follow the common realtime hard fork pattern because a PoW change means there will always be a gap between the fork block.

The first Equihash block will be block 491407 of the Bitcoin Gold blockchain, and from that point on GPU miners participating in the Bitcoin Gold network will begin mining more Equihash blocks on top of it. In this way, the Bitcoin blockchain will bifurcate and a new coin - Bitcoin Gold (BTG) - will be created. Everyone who holds BTC at block 491406 will then control an equal amount of coins on the BTG blockchain branch, which can be spent at any time in the future with the corresponding private keys.

Step 2: The BTG blockchain is activated

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 your corresponding BTG at any time in the future. There is no expiration date for your BTG. 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 BTG will still be there decades from now.

In 491407 hard fork is the one and only opportunity to get initial BTG. After that time, your options to acquire it will be to buy it on an exchange like any other cryptocurrency, to mine it with your own computer hardware (GPUs), or to earn it by trading your goods and services for it.

Cryptocurrency exchanges are custodial businesses, which means they control your private keys, not you. When the Bitcoin Gold fork occurs on block height 491407, any exchange that is holding BTC on your behalf will also receive the corresponding BTG. While they should credit your account with the equal amount of BTG, there is no legal authority that can force them to do so. The Bitcoin Gold home page will display the names and logos of exchanges that have promised to credit their users with BTG at the 1:1 ratio. If your exchange is not shown, please consider transferring your BTC to a supporting exchange or withdraw to a personal wallet where you control the private keys.

Financial Strategy

In order to support the current and future development of Bitcoin Gold, the first blocks after the fork will have a reduced difficulty level that will allow the development team to mine these blocks very rapidly, and then the new difficulty adjustment algorithm will kick in and everyone will have the opportunity to mine on equal footing. As a result, the Bitcoin Gold development team will manage 0.476% of the total coin supply, which will be the main source of funding for all future development of this project, including valuable research and testing that may one day help bring about consensus for a proof-of-work change on Bitcoin itself.

- The initial BTG mined by the Bitcoin Gold (0.476%) development team will be held in multi-signature wallets.

- 60% of the funds will be time-locked and released in proportional amounts over the course of three years to cover the development costs.

- All significant expenditures will be made fully transparent according to the best practices of similar open source projects.

- The majority of funds will be allocated as developer bounties, which will be published as issues in the BTCGPU GitHub repository.

- Everyone is able to participate in the Bitcoin Gold developer bounty program; to win the bounty, you must provide the open source code that meets the specific requirements.

The Bitcoin community will be able to support these bounties by buying or holding BTG, as the price of the coin will determine how strong of an incentive these bounties are, and how soon these features can be created. Keep in mind that most of these development bounties are designed to benefit the entire Bitcoin ecosystem, not only the Bitcoin Gold fork. Bitcoin Gold itself was designed to be a feature of Bitcoin, not a rival.

Some of these essential functions will be performed by full-time employees while others will be outsourced to third-party professional services. All of these expenditures will be made as transparent as possible without compromising operational security.

BITCOIN GOLD 40% BTG

Startup expenses

Bounties and app collaboration	7%
Pre-fork costs	5%
Community development	3%
Initial reward for core team	5%
Yearly expenses	20%
Total	**40%**

BITCOIN GOLD 60% BTG

Time-locked funds; 20% released per year

Development	30%
Ecosystem	15%
Community	15%
Total	**60%**

Future development:

- Core protocol
- Lightning network
- Bech32 addresses
- Sidechains
- Cross-chain atomic swaps
- Decentralized exchange

Operational and infrastructure costs:

- Servers:
  - 12+ full nodes on 6 continents
  - 5+ DNS seeds
  - Website
- Domain fee
- System administration
- Security and penetration testing by third-party

Future social action:

- Economic Development Fund:
  - BTG debit card program (Latin America)
  - Decentralized fiat-crypto brokerage network (Global)

- Blockchain Education Fund:
  - Investment in the content creators and influencers who most effectively contribute to rising Bitcoin awareness and adoption.

- GPU Mining Infrastructure Fund:
  - Small/mid-scale individual/business loans for GPU mining hardware operations.
  - Developer bounties for user-friendly mining applications that can bring mining to a non-technical, multi-lingual audience.

Future communication costs:

- Meetups and developer conferences
- Social media
- Design assets
- Press releases

Conclusion

Bitcoin Gold is a free open source project that was created by a small group of Bitcoin enthusiasts from diverse backgrounds. In contrast to the other prominent Bitcoin forks, Bitcoin Gold was specifically designed from the beginning to inspire innovation in the Bitcoin ecosystem and give value to the vision of decentralization. Whereas the others were born from hostility and an ambition to dominate, Bitcoin Gold arises from a desire to protect Bitcoin and ensure that it not only maintains its position as the dominant cryptocurrency but continues to grow until its liberating roots stretch deep into the economic life of all nations.