The Gold Standard of Digital Currency

GoldCoin is a peer-to-peer cryptocurrency that finally delivers on the promises of decentralization. It's completely built and maintained by a team of dedicated volunteers who firmly believe in promoting economic freedom. Thanks to these principles and a focus on game-changing usability features, like two-minute confirmation speeds and instant 0-Conf transactions, GoldCoin is fundamentally changing how cryptocurrency and economies operate.

Table of Contents

Legal Disclaimer

This white paper does not constitute investment or legal advice. By downloading or reading it, you agree that if you use any of the information contained within, you are solely responsible for any and all outcomes, gains or losses that you might experience.

Abstract

Improving on extant peer-to-peer electronic currencies would heighten their viability as value stores for users and investors with diverse motivations. By building on the proven concepts demonstrated in systems such as Bitcoin, the GoldCoin team proposes a cryptocurrency that addresses critical vulnerabilities, including 51 percent attacks, scaling bottlenecks, transaction fees and ASIC attacks. By using difficulty algorithms, block enhancements, and other programmatic tools to maintain more stable network trends and block generation events, this network tries to compensate for inflationary tendencies and malicious intervention by bad actors. By steering the software implementation forward in the spirit of the philosophies first put forth by Satoshi Nakamoto, GoldCoin sets out to become an invaluable tool for self-guided wealth redistribution in the developing world and wealthier nations alike.

Staying True to the Original Vision

GoldCoin is a pure open-source proof-of-work (PoW) cryptocurrency based on the original Bitcoin protocol and first released on the bitcointalk.org public forum on May 15th, 2013, making it one of the earliest cryptocurrencies to come into existence.

What sets GoldCoin apart is the fact that its development intimately follows the ideals propounded by Satoshi Nakamoto, the anonymous creator of Bitcoin, who strongly advocated for on-chain-scaling. On-chain scaling ensures that “the security of the network increases as the size of the network and the amount of value that needs to be protected grows."

Nakamoto used the word “gold” multiple times in his original whitepaper to describe the inner workings of his historic protocol. Gold is also a term that means value to every English speaking person on earth.

Therefore, no better brand could exist for a project wholly dedicated to developing the most secure and valuable currency ever known.

No longer is humanity willing to be enslaved to the whims of banks and central authorities. Once the people of this world discover the secrets unlocked on the following pages, they won’t want US dollars, Euros, or Yen. The people of the world will demand GoldCoin.

No Need for Third Parties

Bitcoin, created in 2009, was the world’s first cryptocurrency. It was designed to be a decentralized cash payment system with no central authority or go-betweens. In addition, its inflation rate and maximum supply were both guaranteed by a consensus mechanism. Nakamoto’s whitepaper drew a clear line in the sand because it “proposed a system for electronic transactions without relying on trust.”

Unlike the fiat currencies of ages past, Bitcoin was indeed a currency of egalitarian intent. It was geared towards empowering users and using free and open-source, or FOSS, coding standards to create automated processes that would oversee transactions in a transparent, accessible, and more predictable fashion. In other words, free choice was baked into the fundamental mechanism of its trustless design.

Classical financial systems remain enslaved to the whims of those who have the greatest wealth. The fates of their investors hurtle along strapped to the tides of fickle markets. Bitcoin promised to level the playing field by substituting unadulterated mathematics for corruptible human decision making.

GoldCoin: Improving on Good Ideas

While its invention was historic, Bitcoin had one weakness. Over time, the project drifted away from its roots, suffered from the proliferation of manipulatory investments by traditional financial institutions, and found itself compromised; its original protocol contaminated and weakened.

Bitcoin failed to keep pace with usage and adoption as its new corporate handlers throttled the blockchain and publicly ridiculed the vision of its creator. They insisted that Bitcoin become a settlement layer and that separate external networks be created to handle everyday transactions.

GoldCoin rejects the distortions and deviations that have caused endless rifts in the crypto community. By building on the ideals that Satoshi Nakamoto originally promoted and improving them as per our core philosophy, GoldCoin has built the world's most secure payment system.

GoldCoin's Unique Vision

Those who want to change the world should be granted the freedom of choice to do so. Although every human must decide for themselves how to enact such changes, granting them access to novel tools gives them better options to pick from.

GoldCoin is about empowering freedom of choice for those whom society traditionally relegated to the role of the voiceless. Many projects pursue similar goals through methods like charity, STEM education funding, political action and job creation. GoldCoin recognizes that in contemporary society, all of these processes remain trapped by an economic system that doesn't give them the asset management power they need.

GoldCoin offers access to cryptocurrency tools that promote the cultivation of personal wealth and the concepts that gave rise to Bitcoin. By learning from the digital money mistakes of the past and millennia of economic experimentation, this crypto asset works to give people control over their own wealth.

GoldCoin is hard money - a super secure value store and cash payment system for the new digital world

Demystifying GoldCoin and Cryptocurrency

GoldCoin is a uniquely independent form of digital money that adheres to the values and philosophies of cryptocurrency's leading innovators. Unlike traditional currency, it isn't controlled by a central government or authority figure, including the GoldCoin development team. Instead, each GoldCoin is the sole property of its owner, or the last person who received it in a transaction.

How does GoldCoin differ from something like the U.S. dollar, Japanese yen or Swiss franc? These currencies are what's known as fiat currencies. According to Merriam-Webster, fiat is a term for "an authoritative or arbitrary order."^4

In other words, the main thing that gives traditional money its value is the fact that a government or some other legal authority decided to declare that it was

worth something. Sure, the people have to go along with the pretense for it to work, but fiat limits their say in the matter.

The Trouble With Traditional Money

Fiat currency can cause a host of problems that commonly overshadow its benefits. For instance, governments, corporations and financial institutions can easily manipulate the price and availability of currencies like dollars to enrich themselves at the cost of entire economies.

As governments attempt to manage their money supplies, fiat policies can result in deflationary and inflationary trends that induce social upheavals on massive scales.

From the early 20th century hyperinflation of the German mark and the resulting political and military turmoil to the unchecked devaluation of the Zimbabwean dollar and its eventual abandonment in 2009, fiat currency has a well-established potential for instability.^56

GoldCoin's Cryptocurrency Inspirations

What makes GoldCoin such a superior option? After all, nothing is perfectly stable. The key difference is that GoldCoin implements a variety of essential features specifically designed to sidestep the pitfalls of antiquated fiat currency systems. GoldCoin is a unique combination of digital cash and digital gold secured by a trustless, permissionless blockchain.

(^4) https://www.merriam-webster.com/dictionary/fiat

(^5) https://en.wikipedia.org/wiki/Hyperinflation_in_the_Weimar_Republic

(^6) https://en.wikipedia.org/wiki/Zimbabwean_dollar

The Blockchain: A Distributed Public Ledger

As the word "cryptocurrency" attracted growing interest in the early 21st century, so did another phrase: "blockchain." This makes perfect sense because the two ideas are closely related, but to those who've never dealt with either, the links can seem confusing.

If the Blockchain Is the Account Record

Cryptocurrencies work by keeping all transaction records in a shared public document called the blockchain. Every validating node has a copy of the blockchain.

Every time you successfully receive or send cryptocurrency funds, evidence of the exchange gets stored in a specially formatted digital record known as a block. When you pay those funds to someone else in the future, another block record gets added to the old record, forming a chain of records: the blockchain.

Blockchains have a few game-changing advantages

They're distributed among large groups of networked users so that all of the records can reach a consensus about who has how much cryptocurrency. This eliminates the need to trust the bank.

Cryptography (which is where the "crypto" part of the term "cryptocurrency" originates) makes it possible to verify the connections between different blocks and catch certain types of fraud automatically.

Not having to store the records in one place means that you don't need to invest in a secure storage setup, such as when you place an heirloom in a bank vault.

The Cryptocurrency Wallet App Is the Account

Blockchains are a kind of shared ledger technology. Each software-based wallet application uses secure authentication keys to access the records for a given wallet address, which is a long string of 26 to 35 random-looking numbers and letters, such as:

EFEPWnXpj3JgfzmAMZgRooSd9NQuzA2Sr

This is a GoldCoin (GLD) address and the QR code that goes with it. If someone wants to send you money using GoldCoin, all they need is your QR code or address.

Creating Transaction Messages

What happens when someone tries to send cryptocurrency from one wallet to another? Suppose you want to send your friend a payment. First, you'll ask your friend for their address. Then, you'll go to your wallet app and enter their address along with the amount that you want to send. After pressing send, your wallet app will create a message about the transaction that includes three important details^7 :

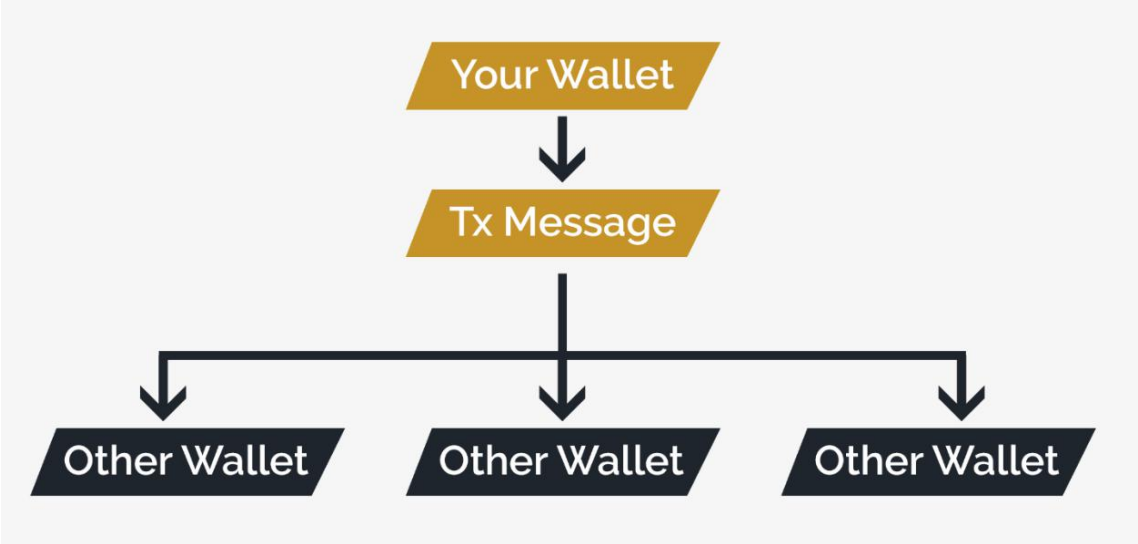
Input: The sender's address.

Amount: The amount of cryptocurrency to be sent.

Output: The recipient's address.

Broadcasting Transaction Messages

After your wallet has created a message about the transfer, the wallet app will broadcast the information to the other wallet apps on the network.



(^7)
https://medium.com/@rilcoin/how-a-bitcoin-transaction-works-edeb3282a

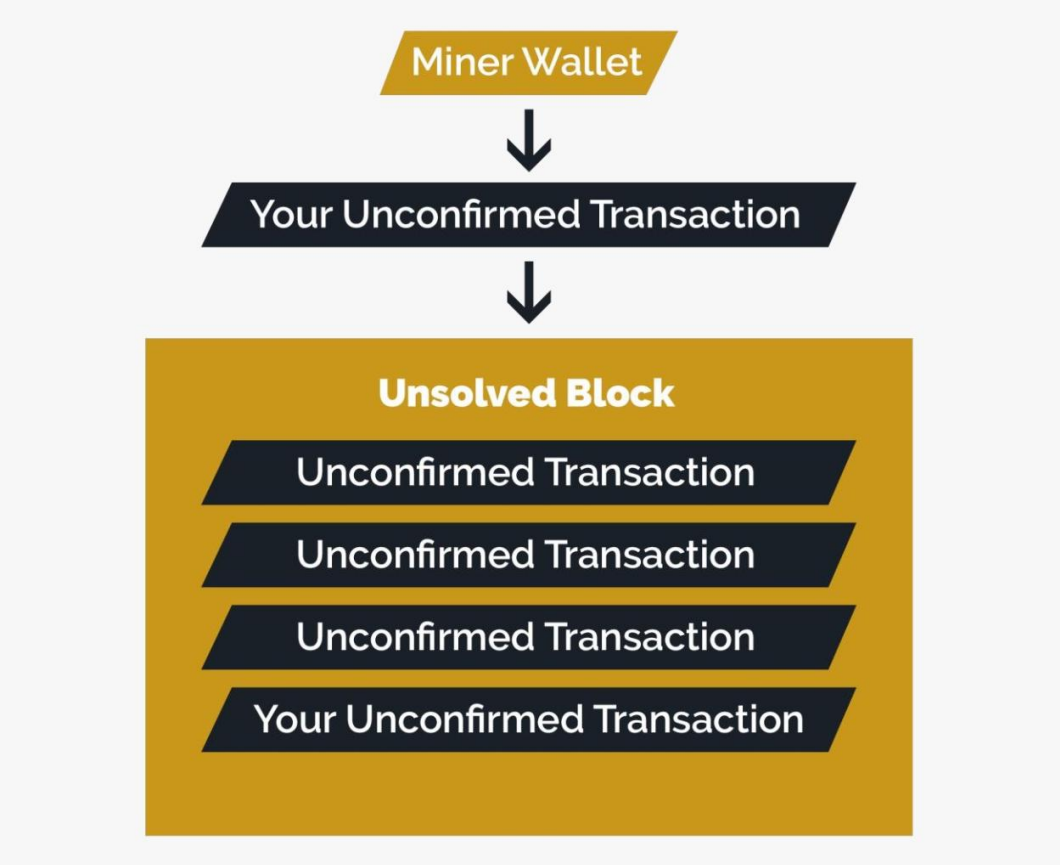
Upon receiving your transaction message, wallet apps across the network use cryptography to:

Verify that the sender's address actually owned the cryptocurrency that it tried to send, and

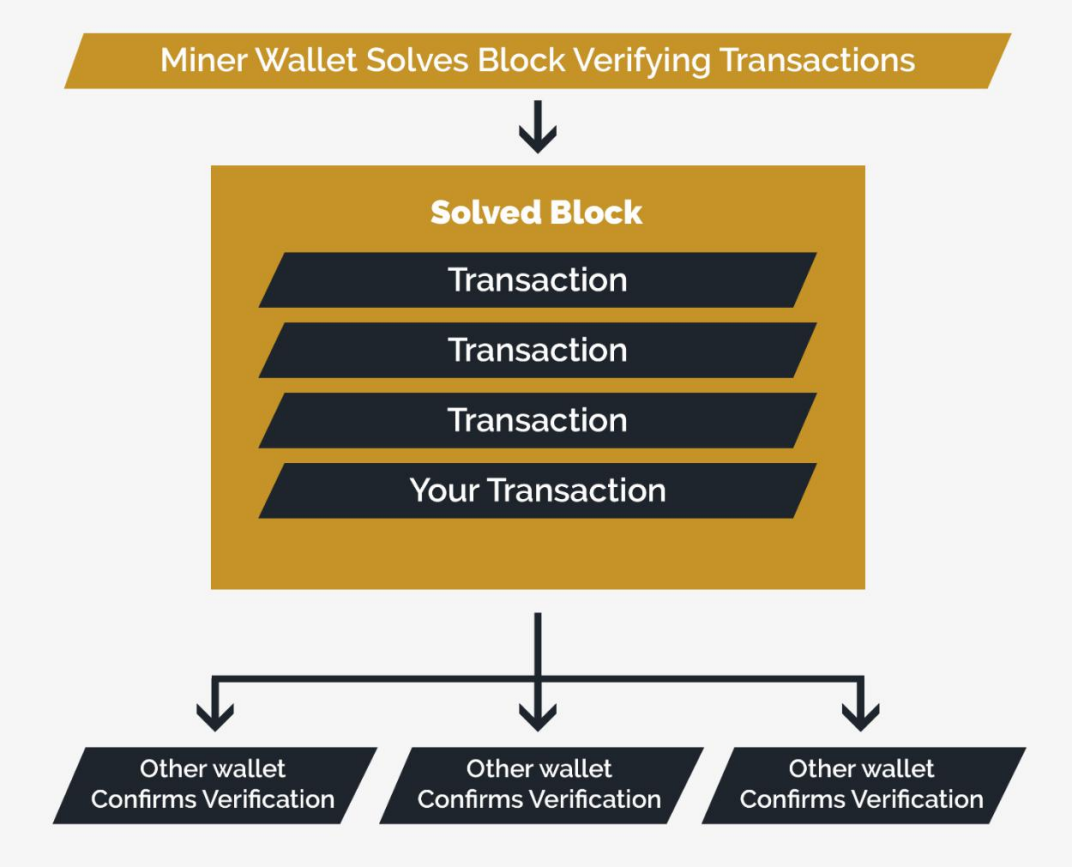
Determine if the transaction follows other network requirements.

The wallet app that owns the receiving address of your friend will show the transaction as unconfirmed.

Specialized nodes called "miners" will then add the transaction to a block of other unconfirmed transactions. Next, these miners will attempt to solve a difficult mathematical cryptography problem. This process proves that the miner has verified that every transaction in the block meets all of the rules that the network requires.



Once the answer has been produced by a miner, the completed block is broadcast across thenetwork.



Each wallet app easily checks the work and confirms that everything matches up. Then, the transaction gets added to the blockchain in a new block. All wallets will then show that this transaction has one confirmation. Once all of the wallets receive this new block, they are all in agreement that the transaction was sent and confirmed. From there, the process repeats with new transactions, ensuring a continuous, unbroken record that stretches back all the way to the beginning of the currency's lifetime.

No Private Blockchains: Keeping the Record Accessible

Some cryptocurrency organizations dilute their currency's independence by implementing private blockchain technologies. Although many of these groups would claim that their actions serve the greater good by keeping the ledger in the hands of a trusted authority, such activities raise two glaring problems:

Depending on so-called trusted authorities flies directly in the face of Nakamoto's reason for creating Bitcoin.

It's impossible to know whether a third-party is trustworthy.

These aren't the only problems with private blockchains. When one party controls the ledger, all network participants are at the mercy of that party.

If a government official or legislator suddenly decides that it's politically expedient to prohibit the general use of cryptocurrency so that they can acquire a massive market share before profiting from currency speculation, all they have to do is target the central "trusted" authority that houses the ledger. If this seems like science fiction, one only needs to look at existing civil enforcement lawsuits brought by U.S. authorities against cryptocurrency companies.^8

True, most people would agree that government intervention is great when it prevents fraudsters and con artists from scamming unwitting users. Unfortunately, most governments eschew the laissez-faire attitudes that might help many currency markets thrive.^91011 Not all regulations help, and as many corrupt governments have shown, central authorities with too much power can't always be trusted to implement laws fairly or justly.

As cryptocurrency continues transforming the workings of monetary systems, governments will undoubtedly take part in determining how things develop. Regardless where one stands on whether these roles will help or hinder, the idea of private blockchains clearly introduces a major vulnerability that could exacerbate regulatory impacts for better or worse.^12

"The heart of any cryptocurrency can be found in the spirit of its community."

Good intentions aside, private blockchains carry the threat of conflicts of interest. By isolating the ledger from the community, they sacrifice critical public oversight.

(^8) https://bgr.com/2018/01/19/bitcoin-fraud-ponzi-scheme-us-government-investigation/

(^9) https://themerkle.com/the-us-government-wants-bitcoin-exchanges-to-apply-for-bank-status/

(^10) http://www.telegraph.co.uk/business/2018/01/25/bitcoin-draws-calls-regulation-davos/

(^11) https://news.bitcoin.com/russia-finalizes-federal-law-cryptocurrency-regulation/

(^12)
http://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-regulation-value-

GoldCoin Mining: Digging Deeper Into the Concept

Mining is what keeps cryptocurrency going. Whereas a bank makes money by charging its clients interest, overdraft fees and a host of other burdensome assessments, cryptocurrency gives miners an economic incentive to maintain the accuracy of the public record: The software pays out a reward to the mining wallets that solve the latest block's cryptography math problems before their peers do. To ensure that the cryptocurrency retains its worth instead of being devalued by inflation, the software varies key settings like:

The amount of the cryptocurrency that miners receive as a reward,

The difficulty of the cryptocurrency problem, and

The confirmation speed or amount of time needed to solve each problem and confirm a transaction.

Along with other settings, these simple tweaks mean that:

Only a certain amount of coins will ever get generated, limiting inflation,

Forging the blockchain record to give yourself a lot of cash requires more effort and computer power than it's worth, and

People keep mining to sustain the record and process user transactions because they know that they stand to make profits in newly generated cryptocurrency coins.

Each time a transaction is confirmed, it's referred to as having been "mined." Every cryptocurrency coin has a preset target interval for a block to be confirmed.

Block Retargets and Rewards

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.^13

Since the introduction of Golden River, these retargets occur with each block. Below is a list of historical retarget times and block times, as well as historical block reward information.^14

Block Targets:

2.5-minute block targets up till block 44,

2 - minute block targets thereafter

(^13) https://wiki.bitcoin.com/w/Target

(^14) https://www.goldcoin.org/block-rewards/

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

(The values below are post-fork in development/dispute values)

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: 72,245,700

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

Inflation Rate and Comparisons

GoldCoin's inflation rate ensures that the market will not become saturated with newly mined coins and that coin distribution will be balanced across future

generations. More than 80 percent of all bitcoins have been mined, while only 50 percent of all goldcoins have been mined.^15

GoldCoin's inflation rate is slow and consistent as compared to others:

Year	Bitcoin	Litecoin	GoldCoin	Dash	Monero
2017	4.10%	10.40%	1.46%	10.10%	15%
2018	3.90%	9.50%	1.46%	8.50%	8.10%
2019	3.70%	8.60%	1.46%	7.90%	4.60%
2020	3.60%	4.10%	1.46%	6.80%	2.70%
2022	1.70%	3.80%	1.09%	5.20%	0.92%
2025	0.83%	1.70%	1.09%	3.70%	0.85%
2030	0.40%	0.82%	0.73%	2.20%	0.81%

(^15) https://wiki.bitcoin.com/w/Controlled_supply

GoldCoin Represents the Evolution of Money

Cryptocurrency may strike you as being something totally novel and innovative. Like any great idea, however, it's got roots in eons of development. Money has most likely been evolving since prehistory, and cryptocurrency is just the latest, most logical response to its many ills.

Barter Origins: Back to Basics

Most economists agree that the predecessors of today’s monetary systems were barter, or trading, arrangements.^1617 If your cave-dwelling ancestor spent all day gathering fruits while their friend was collecting perfectly rounded stones for ax heads, your ancestor could trade what they had according to an agreement with their friend.

As the seasons turned, these ancient hominids got smarter and probably grew tired of carrying around fruits and rocks. Some forgotten paleolithic economic genius wondered, “Why don't we just use seashells or beads to represent an agreed value that anyone can use to exchange for material goods?” The first money was born, and eventually, people pushed the concept even further by switching to precious metals and paper money.

Problems Along the Way

Unfortunately, not everything was smooth sailing. Even as people invented banks to help their fellow humans keep their money secure, they also came up with things like predatory lending and the discriminatory banking practices that continue to marginalize minority and low-income populations to this day.^1819

Government leaders didn't always make it easier for financial systems to thrive either. For instance, in 1933, U.S. President Franklin D. Roosevelt took the nation off the gold standard that previously let anyone exchange their U.S. dollars (USD) for gold at the Federal Reserve.^20 This action, which followed in the footsteps of similar legislation in Great Britain, was intended to make it easier for the government to artificially inflate the money supply and help the country recover from the Great Depression. It also prohibited private citizens from “hoarding” gold certificates, coins or bullion.

The year 1971 saw U.S. President Richard Nixon put the final nail in the gold standard's coffin.With the total elimination of the gold standard, the government gained the power to print money regardless of the reserves it actually held in the vaults at Fort Knox. The USD became a genuine fiat currency, and those who already had wealth gained even more power to decide what money could buy according to their whims.

(^16) https://www.mint.com/barter-system-history-the-past-and-present

(^17) http://www.pbs.org/wgbh/nova/ancient/history-money.html

(^18) https://www.debt.org/credit/predatory-lending/

(^19) http://atlantablackstar.com/2015/03/03/8-major-american-banks-that-got-caught-discriminating-

(^20) https://www.history.com/this-day-in-history/fdr-takes-united-states-off-gold-standard

GoldCoin vs. USD

By some estimates, the dollar has lost 90 percent of its purchasing power since the mid-20th Century. For this reason, most financial planners advise that if you want to do something wise with your money, you won't hold onto cash: Diversified portfolios that contain assets like precious metals, stocks and other property help you avoid the inevitable swings that fiat currency is known for.

Humanity has grown tired of being enslaved by an unfair and corrupt fractional reserve banking system and will tolerate strangulating inflationary theft no more.

True, the USD is the world's stablest currency for everyday transactions, but it can't compete when it comes to building long-term wealth by storing value online. GoldCoin's developers specifically set out to create a cryptocurrency asset that provides the benefits of the old gold standard without the practical disadvantages or top-heavy government interference.

GoldCoin is:

Cutting through the need for payment and transfer mediums, intermediaries and bankers,

Improving global remittances by making it easy for people to send money back home to their loved ones from other countries, and

Following the lead of cryptocurrencies that are rapidly powering the way the internet does digital commerce.

Did the U.S. dollar become less real when it stopped being backed by gold?

Cryptocurrency is the next step in that same evolution — to make currency more

virtual.

In its purest form, currency is confidence. It's a network effect around an

agreed-upon medium of exchange that has some promise of scarcity. Bitcoin

enforces its scarcity through a combination of cryptography and economic

incentives ("cryptoeconomics"). A lot of people find that more comforting than

relying on the good faith of a government. In math we trust."

- David Sacks, the original COO and product leader of PayPal^21

(^21) https://www.cnbc.com/2017/08/14/david-sacks-cryptocurrency-interview.html

GoldCoin and the Developing World

One of the most interesting aspects of cryptocurrency's development is its potential to help more than just those in wealthy communities. Although some people in places like the U.S. view GoldCoin and other crypto assets merely as passing investment trends that make for interesting news headlines, others recognize their true power. In nations whose economic systems have stagnated for

years, cryptocurrency holds the tantalizing lure of an escape from onerous fiscal regimes.

Countries that suffer from hyperinflation face countless problems. Whether their plights are the results of decades of misguided monetary policies or infrastructural deficiencies, global citizens who struggle under such systems must contend with extreme price fluctuations that make it hard to survive, with some inflationary events even carrying dangers like malnutrition, violence and human rights abuses.^222324

"With GoldCoin, money is stronger, and our freedom is ensured. We finally have a borderless, trustless, permissionless payment system: a gift for the entire world. The time has come for us as a people to begin winning again."

In the modern world, it’s not uncommon for those who've already spent years trying to accumulate wealth to suddenly find their efforts gone to waste when they're unable to make purchases. Sadly, the solutions proposed by traditional banking systems rarely promise anything but more of the same. Some experts even suggest that the time may be ripe for such inflationary currency systems to take their toll on wealthy nations.^25

The GoldCoin team is working to change the relationships between people in the developing world by offering them chances to leverage value systems that aren't subject to unjust manipulation. Since it lets anyone transact with an internet-connected device, it removes the barriers to entry that make it so hard for the underserved to accumulate financial wealth. Our team is

Fully committed to the promise of letting people be their own banks,

Continually working to improve the tools that allow people to store, access and transfer funds, and

Developing software designed to let people retain full control of their affairs from anywhere, at any time and at little to no cost.

(^22) https://www.theguardian.com/inequality/2018/jan/31/human-rights-new-rule-of-law-index-reveals-global-fall-basic-justice

(^23) https://www.project-syndicate.org/commentary/brazil-hyperinflation-real-plan-lawsuits-by-camila-villard-duran-and-arnoldo-wald-2018-02

(^24) https://www.reuters.com/article/us-venezuela-unicef/unicef-sees-growing-signs-of-malnutrition-crisis-in-venezuela-idUSKBN1FF1OF

(^25) https://www.forbes.com/sites/mikepatton/2014/04/28/is-u-s-hyperinflation-imminent/#31825419ad2d

GoldCoin has successfully built the world's most perfect money. The secret was in coupling our globally recognized brand to a hardened, trustless protocol design.

GoldCoin vs. Other Cryptocurrencies

Feature	Bitcoin (BTC)	Litecoin (LTC)	GoldCoin (GLD)
Confirmation Speed	10 Minutes	2.5 Minutes	2 Minutes
Instant Transactions (0-Conf)	No	No	Yes
SegWit Free	No	No	Yes
51% Defense System	No	No	Yes
On-Chain Scaling	No	No	Yes
Difficulty Retarget	2016 Blocks	2016 Blocks	Each Block
Block Size	1 MB	1 MB	2 MB
Satoshi's Vision	No	No	Yes
Multi-Pool Resistant	No	No	Yes
Free Transactions	No	No	Yes

Although cryptocurrencies like Bitcoin were widely hailed for their innovative nature, many fell prey to problems over time. As the ways people used wallets, mining computers and cryptocurrencies evolved, so did the need for novel technological solutions to unanticipated issues. Big challenges for cryptocurrencies like Bitcoin include the fact that:

Transactions take longer than they should, so investors find it harder to sustain profitable portfolios as currency prices change,

Relatively weak algorithms expose the system to theft by allowing an attacker to double- spend funds on a single address, and

Limited block capacities make it hard for some cryptocurrencies to scale up and meet demand as more users try to place transactions.

Breaking Bad: Throttling the Blockchain

From the start, Bitcoin was designed to scale on-chain. It was intended to be a cash payment system with minimal fees, not a dedicated settlement layer. When the block size is sufficient to meet network demand, a natural balance occurs, and transactions can be sent efficiently at little to no cost.

But if the network is throttled, as in the case of Bitcoin, there simply isn't enough block space in the system to meet demand. This results in the network being overloaded with its users forced to pay high fees due to the limited capacity.

When Bitcoin was introduced in 2009, it did not have a block size limit. Later, in 2010, Satoshi decided that there should be a maximum block size for improved security. Otherwise, an attacker might try using an unlimited block size to perform a Distributed Denial of Service (DDoS) assault on the network.

Based on the transaction volume at the time, Satoshi decided that a 1 MB block capacity would be more than sufficient. Then as the volume grew, he would increase this size to allow the network to scale. He even provided a formula to be used in the code that would trigger this increase based on block height.^26

It was never intended for the block size to remain at 1 MB, as this would effectively break the system, cause the network to become overloaded and send fees skyrocketing. There were several proposals set forth to raise the block size after his disappearance, such as BIP 100 and BIP 101, but none of these solutions were adopted by the core development team.

Proponents of small blocks promote the idea that the block size, if allowed to grow, would become unmanageable. These same voices reason that ordinary users would be unable to afford machines capable of running full nodes and that this condition would lead to network centralization.

While it is true that full nodes would eventually require high-end computers, mining is a capitalist enterprise and commercial mining operators will always compete for a share of network revenue.

Transaction Backlog and Rising Fees

When there isn't enough capacity on the network to handle transaction demand, users are required to pay growing fees in order to compete for limited block space. The has led to the development of an unnatural fee market.

This has resulted in instances where transaction fees have exceeded the cost of the items being purchased. In some cases, users are paying fees that are 10X to 20X more than the actual item's cost. If you don't pay a high enough fee, your

transaction could be delayed for days or weeks. Or it might never be confirmed at all.

(^26) https://cointelegraph.com/news/satoshis-best-kept-secret-why-is-there-a-1-mb-limit-to-bitcoin-block-size

Compromised Protocol: What is Segregated Witness?

In 2016, the Bitcoin Core development team came up with a compromise for increasing the capacity of the network without increasing the block size. Segregated Witness, in short, means to separate transaction signatures. SegWit is also a prerequisite of the Lightning Network.

Since SegWit transactions take up less space than regular transactions, it's possible for the network to process a greater number of transactions per block. By some estimates, this could lead to virtual block sizes approaching 1.7 MB.^27 However, it's important to realize that this scheme doesn't come without a cost.

Since the signature info gets separated and discarded with SegWit, it could be harder to prove the legal validity of transactions and adhere to evidence laws. For investors facing government declarations that virtual currencies are properties for tax purposes, having such evidence might prove essential, which means that recordless schemes could pose major problems.^28

Even worse, only newer SegWit-supporting software can handle the modified transaction format. Older software will receive the transaction in the old format without the witness data. This means older nodes can no longer validate the blockchain since they are unable to see these transactions.

At best, SegWit is a complicated means of scaling on-chain transactions. In practice, it's far easier to increase the block size limit, which is exactly what GoldCoin did in 2016.

Introducing Dependency: The Lightning Network

The Lightning Network (LN) is another attempt at allowing an overloaded network to scale without changing the 1 MB block size limit. In this secondary network, channels are created between two users when one user creates a special transaction in the blockchain with a certain amount of coins that funds a new multisig address. The users can then send coins to each other and to other users that are also connected via other channels.

"Throttling the main chain and forcing Bitcoin transactions onto external networks creates operational dependency and effectively breaks autonomy."

These transactions are not recorded in the blockchain, and unlike on-chain transactions, recipients must be online to receive payments. By forcing independent parties or networks to keep their own side-chain records, solutions that split the blockchain may weaken the system, introduce potential inaccuracies and make users more likely to face regulatory interference.

(^27) https://segwit.org/is-segwit-a-block-size-increase-705df6a8731d

(^28) https://www.coindesk.com/the-risks-of-bitcoins-segregated-witness-problems-under-us-contract-law/

Dwindling Fees: Miners Get the Shaft

When you send someone a blockchain payment, any fee you include gets added to the miner's reward. By limiting the block size, you're limiting the number of transaction fees that can be sent through the network.

This means that miners are subsidizing every transaction that occurs off chain. With this unnatural bypassing of the blockchain, miners are forced to provide more work for less pay. This could lead to greater centralization if mining operations are forced to consolidate in order to remain profitable.

And things only get worse. When Bitcoin mining ends in the year 2140, transaction fees must fully support the network. If the Lightning Network progresses to the point where channels are rarely closed, miners will have no remaining revenue and thus no incentive to provide work for the blockchain.

Increased Regulatory Exposure

It's likely that Lightning Network node operators will be exposed to strenuous KYC/AML requirements since they'll fulfill the roles of currency custodians, like banks, and money transmitters, like exchanges. This means that central nodes will mostly be made up of banks and large merchants that serve as regulatory actors by demanding that end-users provide identity information.

Unsolved Routing Issues

Multiple routing issues with the network also remain as-yet unresolved. Liquidity across the network could vary considerably. This could mean that at certain times and particularly with larger payments it might be difficult or even impossible to find a payment route.^29

The Lightning Network was intended to avoid the necessity of paying high transaction fees in a congested network. But as with complicated SegWit solutions, increasing the block size renders the Lightning Network unnecessary.

(^29)
https://www.coindesk.com/lightning-network-may-not-solve-bitcoins-scaling-trilemma/

On-Chain Scaling: A Return to Intelligent Design

After many years of carefully studying the known writings of Nakamoto, the developers of GoldCoin have come to the rational and sane conclusion that, “Satoshi Nakamoto knew what he was doing.”

While the “new” Bitcoin is being converted into a dedicated settlement layer dependent on complex scaling solutions and external networks, GoldCoin realizes that the market favors simplicity and autonomy over complexity and dependence.

We understand the delicate balance of the ecosystem and approach problems of scaling with solutions that stay on the blockchain to ensure that the ecosystem remains balanced and keep the public record as incorruptible as possible.

This isn’t to say that the original protocol can’t be improved upon or that secondary network layers are all inherently bad. It just means that on-chain scaling is the lifeblood of the protocol and the heart of the system. The main chain must never be cut off, restricted or forced to rely on some external mechanism.

Thin Clients Vs. Full Nodes

The private key is the bearer instrument, not the node. The node is the validation mechanism only. Satoshi never intended for each user to run a full validating node: Miners perform that task. Expecting every user to run a full node would be like requiring every Internet user to store a complete search index locally, or asking Usenet users to keep the entire newsfeed on their own machines.

The blockchain was designed to grow. As the cost of running a full node increases, nodes will move to distributed data centers. This design allows users to just be users. This transition isn’t controlled by some fallible human administrator either; it’s about individuals reacting to market forces on their own.^30

Increased Network Capacity

GoldCoin's faster confirmation times also improve network capacity. Since its 2 MB blocks are twice as large as Bitcoin's 1 MB size and the system's two-minute

confirmations are five times faster than the ten-minute time in Bitcoin, the GoldCoin network already has 10X greater network capacity.

(^30) https://bitcointalk.org/index.php?topic=532.msg6306#msg6306

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 each block is reserved for free transactions. This allows for approximately 300,000 free transactions per day.

This means that users in developing worlds will have the option to opt-out of paying a transaction fee, while others can include a fee to prioritize transaction speed. As demand grows, overall transaction capacity shall be increased via the block size.

0-Conf Transactions

Instead of taking records off the blockchain and raising the chances of record discrepancies or questionable motives, GoldCoin scales on-chain by using the originally specified standard: 0 - Conf. The GoldCoin protocol broadcasts messages about payments that haven't made it into the blockchain yet. This feature was abandoned in Bitcoin and is no longer possible due to network congestion and replace-by-fee, or RBF.^31

Even though 0-conf transactions haven't formally been inserted into the

blockchain record, they're still in the official network instead of a private,

compromisable sidechain. In essence, they've just received zero

confirmations.^32

When trying to generate a block, a network node only accepts the first version of a transaction it receives for incorporation into the chain. If you broadcast a transaction and someone else broadcasts a double-spend at the same time, then it's a race to propagate to the most nodes first. If one has a slight head start, it will geometrically spread through the network faster and win the race.^33

Regardless, most merchants will use payment processors. The payment processor has connections with many nodes. When it gets a transaction, it blasts it out and simultaneously monitors the network for double-spends. If it receives a double-spend on any of its many listening nodes, then it can alert the merchant that the transaction is bad.

A double-spend transaction wouldn't get very far without one of the listeners hearing it. The double-spender would have to wait until the listening phase was over, but by then, the payment processor's broadcast would have reached most nodes. In other words, it'd be so far ahead in propagating that the double-spender would have no hope of grabbing the needed percentage of remaining nodes.

(^31) https://www.yours.org/content/bitcoin-s-dead-sea-scrolls---disabled-opcodes-to-be-resurrected-by-bit-3eea068c604c/

(^32) https://www.reddit.com/r/Bitcoincash/comments/7dtdr1/0conf_what_does_it_mean/

(^33) https://bitcointalk.org/index.php?topic=423.msg3819#msg3819

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.

A Philosophy in Practice: GoldCoin Is Hard Money

GoldCoin is about more than mere ideas. It's about using code to achieve the philosophical goals that drove the initial creation of coins like Bitcoin. Cryptocurrency may have changed dramatically since its earliest days, yet the spirit of the hard money tradition remains alive and vibrant in the way GoldCoin works.

Living Up to the Hard Money Tradition

Why is money valuable? It's not just because governments say that it's worth something. An equal amount of power lies in public trust, which prompts people to agree on money's value and implement systems for its use. Being able to use said money, in turn, further raises user confidence.

For holding money to be a worthwhile prospect, money must have a certain

utility, namely, the ability to be accessed or exchanged reliably and freely.

Paper money, commonly referred to as soft money, would be next to worthless if it was just paper. Coinage, on the other hand, is known as hard money because coins are actual assets that bear their own intrinsic value pegged to the worth of the precious metals that comprise them. True, both assets have fungibility, or the quality

of individual units being interchangeable, such as when someone trades one dollar for another. This may not be enough, however.

Traditional soft and hard money are both relatively weak long-term value stores. Their worth rests in the hands of people who have vested interests in ensuring that they profit from valuations. In other words, these kinds of money can never achieve true impartiality or fairness.

GoldCoin Strives to Be the Best of Both Worlds

Because GoldCoin combines an electronic coin with a trustless cash payment system, it grants anyone who downloads the free wallet software instant access to the power of spendable hard money. GoldCoin outpaces other crypto alternatives by minimizing transaction times and improving network performance and security, so spending utility always remains available and dependable. As free and open-source software, it cultivates a community of participants who get to decide how it works and contribute to its betterment.

GoldCoin is evolving into a high-value platform that offers a lasting foundation

for the world's financial systems.

Under the Hood: Unique Features

GoldCoin employs a wide range of specialized technologies created by the GoldCoin team to improve the cryptocurrency's functional convenience, utility as a value store and security. Although some of these elements were derived from the inspiring open-source code implemented in earlier versions of Bitcoin and Litecoin, many of the aspects that differentiate GoldCoin from other cryptocurrencies aren't found elsewhere. Totally exclusive, these code- based features speak to the spirit of innovation with which the earliest cryptocurrency visionaries sought to transform global monetary systems.

Securing the Network

It's not enough to simply want to change the way cryptocurrencies and financial systems operate. To realize positive impacts, it's also necessary to support such desires with sound computer science, smart cryptography and secure network communications.

Today's digital currencies also require robust algorithms that can withstand malicious interference, outright attacks, and high or unpredictable usage rates. Two of GoldCoin's critical features, the Golden River Difficulty Algorithm (GRDA) and the 51 percent defense system, are perfect examples of these principles in action:

The Golden River Algorithm

If cryptocurrency miners whose computers solve math problems get rewarded with new coins, what's stopping one miner from simply finding all of the solutions first? After all, many people wonder, why wouldn't some billionaire just purchase a super-fast computer so that they could continually beat everyone else to the punch?

The solution lies in difficulty algorithms. To control the rate at which new blockchain blocks, and therefore currency coins, are minted, crypto developers ensure that each problem is hard to solve.

Even the fastest modern computers still operate at predictable rates. For instance, your laptop or phone runs at a certain number of GHz or MHz, and a supercomputer can perform a specific number of basic floating-point math operations per second, or FLOPS. Given that these machines are rate-limited, it's possible to intelligently estimate how long it will take each one to solve each block. From there, the network determines how many machines are working on the problem and corrects the difficulty variables as needed.

Multi-Pool Resistant

Multicoin pools are mining pools that mine the most profitable coins at any given time, and many have rather high hash rates. They continually switch between coins with low difficulty and mine them profitably, which has the side effect of raising the difficulty of mining each coin. The multipool keeps mining a particular coin until its mining rate slows down to a point where another coin can be mined faster. Once the multipool switches to another cryptocurrency, the last coin's difficulty is often left much higher than what its network can normally handle, leading to abnormally lengthy confirmation times. Users of the coin need to wait longer for confirmations on their transactions. In some cases, it could take hours or even days to receive a single network confirmation.

This action of the multipool is like strip mining: The miner gains many coins, but they leave the environment in a state that takes a long time to repair, or return to a normal confirmation time. Additionally, a malicious actor or group of actors may be less interested in profit and more interested in raising the difficulty of a coin to slow down the network.

Cryptocurrency developers have sought to combat the issues caused by multipools by designing many types of difficulty adjustment algorithms. The main purpose of such algorithms is to target a specific block solving time. For GoldCoin, this target is two minutes.

If more miners join the network, then the average block solving time goes down, so the algorithm raises the difficulty. If miners leave the network, then the difficulty

is lowered to maintain the specified time. Some adjustment algorithms change the network difficulty every few days or weeks, and others change it every block. Unfortunately, multipools and malicious actors can take advantage of either strategy.

GoldCoin developer Amir Eslampanah created Golden River as the second part of a two-pronged approach to dealing with multipools and other types of attacks. It works together with the 51% defense system (discussed in the next section) to reduce the profitability of multipool mining. When these large miners discover that they're not reaping the rewards of their added hash power, they leave without significantly changing the difficulty for other miners.

Golden River vs. Other Algorithms

Golden River outperforms many self-adjusting difficulty algorithms, including Kimoto Gravity Well, or KGW. GoldCoin's unique algorithm is also a vast improvement over the original Bitcoin algorithm, which makes adjustments every 2016 blocks.^3435

(^34) https://www.cryptocompare.com/coins/guides/what-is-a-kimoto-gravity-well-dark-gravity-wave-or-digishield/

(^35) https://bitcoin.stackexchange.com/questions/21730/how-does-the-kimoto-gravity-well-regulate-difficulty

Torture-tested in the Wild

The development team ran numerous test cases before implementing Golden River to make sure it would perform flawlessly under even the most extreme network conditions. Since then, it's survived countless trials in the real world.

Like KGW, 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.

Calming the Storm: Smooth Flowing Adjustment

When problems get too hard for the computers on the network and the amount of time needed to solve a block increases above the two-minute target, GRDA smoothly and securely reduces the mining difficulty. This uniquely smooth flowing action is how the algorithm got its name.

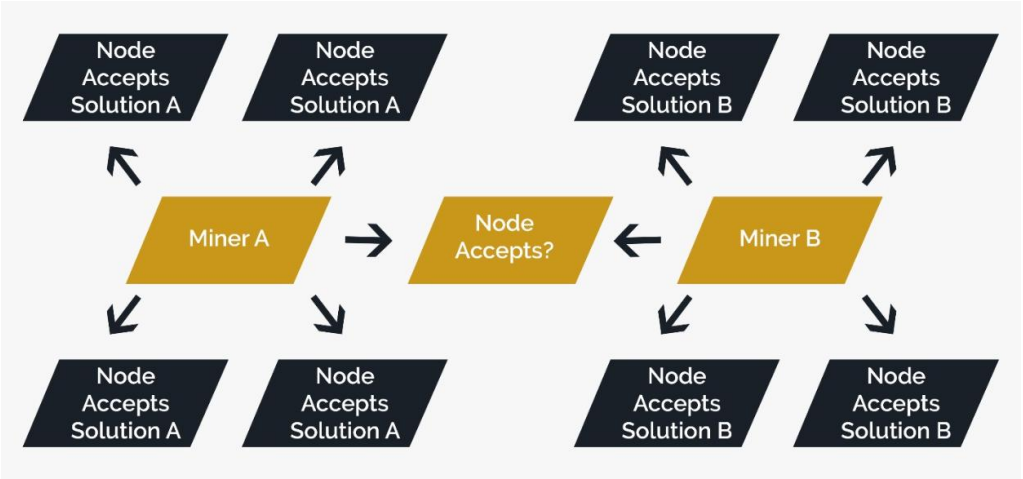
Golden River is also programmed to be adaptive. Some difficulty algorithms operate according to inflexible, predefined formulas. This practice makes it possible for someone to learn how to game the network over time. Golden River's difficulty retargeting is designed to intelligently choose between various mathematical options to ensure that performance responds correctly in a broader range of situations.

Finally, Golden River's self-correctional accuracy means that block generation times are more dependable than they are with other coins. Since users can depend on new blocks appearing every two minutes almost on the dot, they get the advantage of holding a cryptocurrency that has more stable inflation rates and increased value consistency.

The 51% Defense System

As anyone who's ever voted for a losing political candidate knows, “majority rules” doesn't always produce the results you might prefer. In the realm of cryptocurrency, this can have unintended effects with dire consequences.

There are multiple acceptable solutions to each block’s cryptography math problem. Blockchains are designed to accept only one solution and incorporate it as the building block for the remainder of the chain, but what happens if you and another miner publish different solutions at nearly the same time?

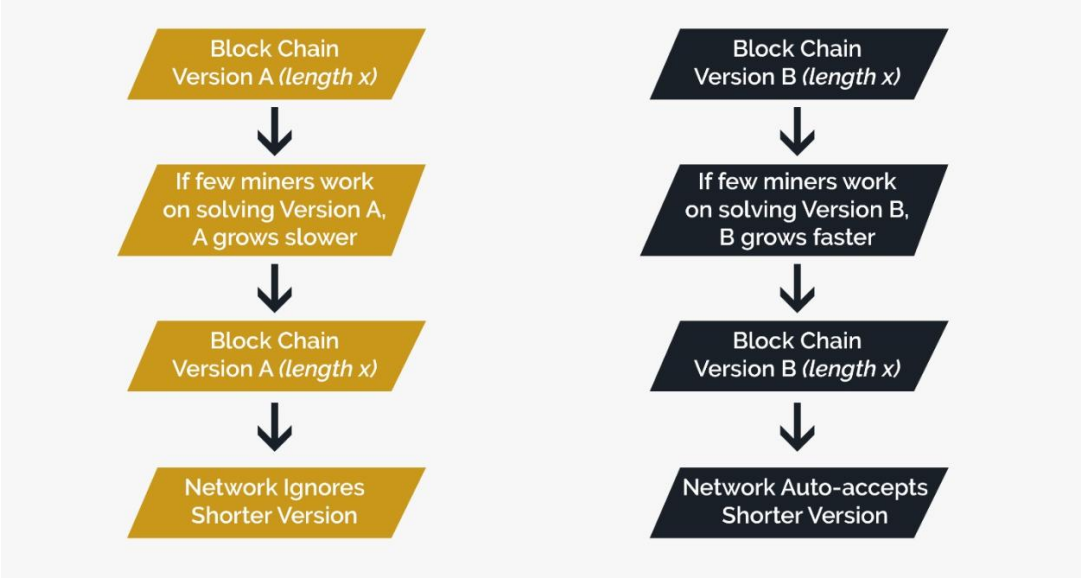


The other computers in your section of the network might see your solution as the right answer while those in your mining competitor's vicinity might be inclined to go with theirs.

The answer lies in achieving a majority consensus. If the blockchain splits into two competing chains based on different solutions, individual miners can try to solve

the new problems associated with each new block. If all else is equal, and more miners are using one of the solutions, then that problem is more likely to get solved first, which would add a new block to that version of the chain. When one of two competing chains grows longer, it becomes the official chain, and miners automatically switch because it's the longest.

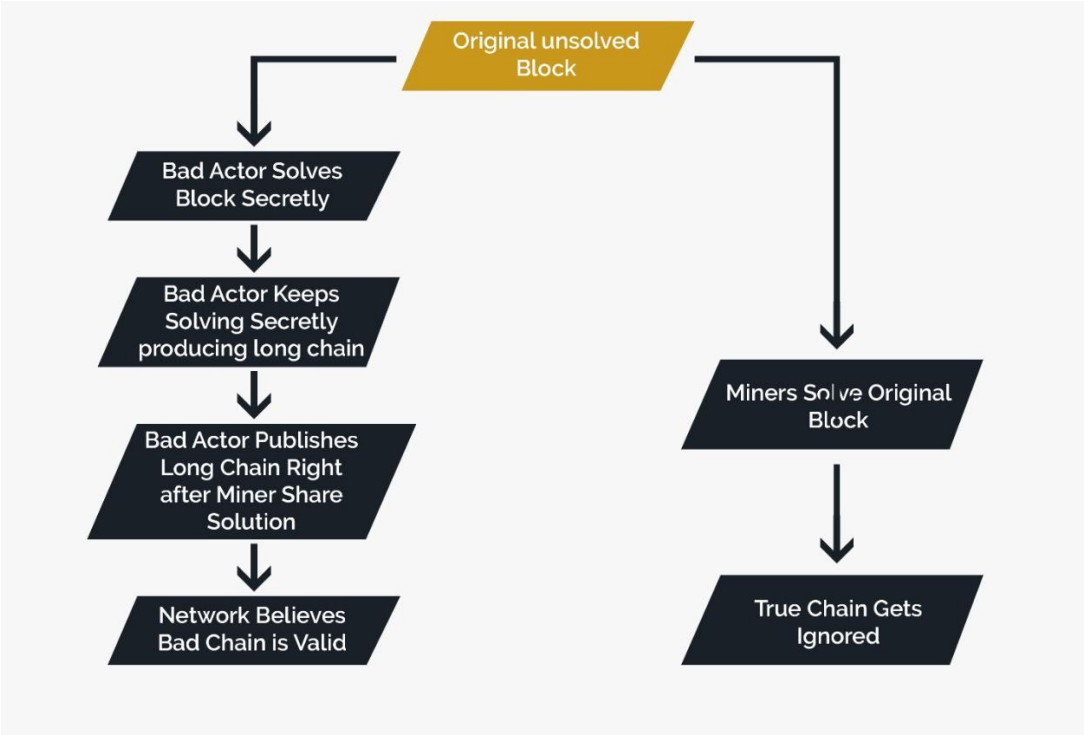
What Happens with Competing Blockchains:



Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

How 51 Percent Attacks Work

In 51 percent attacks, a bad miner takes advantage of the consensus mechanism by solving a block's math problem in secret and then racing to solve the problems associated with the next blocks after that.



If the bad actor's hardware can keep getting way ahead, it just has to wait until the other miners publish the answer to the problem that it originally solved in secret. Then, it publicizes its answer with a longer record of subsequent answers to fool the network into thinking that it should switch to the longest solution.

This is called a 51 percent attack because someone could accomplish it by gaining control of the 51 percent of all mining computers needed to indicate majority consensus. Because these bad actors would also control the record, they could then double-spend the same currency without anyone catching on.

How GoldCoin Stops 51 Percent Attacks

The risks of 51 percent attacks have long been recognized. Since 2013, GoldCoin's revolutionary 51 percent defense system has relied on three laws to stop attackers from distributing their fraudulent blockchains around the network and fooling the system into thinking that everyone else agrees with them:

Law 1: No one node may transmit more than six blocks every 10 minutes based on the block timestamps regardless where the blocks originated.

Law 2: The block timestamp of a block cannot be more than 45 seconds ahead of the current network time.

Law 3: If a miner or other node submits a block to the network that does not meet Law 1 or 2, then the receiving node will ban the sending node for a period of time.

How do these rules help? Block timestamps have to be extremely close to the network time and adhere to the six-block per ten-minute maximum to be counted as part of the valid chain by the network, so it's far more difficult for someone to hide a secret solution and submit it to the network later.

Since individual wallets can only propagate their solutions so far, those who want to control the network have to work much harder to spread their results and gain a false consensus.

GoldCoin's 51% percent defense works in conjunction with the Golden River algorithm to reduce the profitability of multipools. It also minimizes the network influence wielded by large miners or bad actors who have significant hash power when they leave. Difficulty climbs slowly when someone tries to launch a large-scale assault as the 51% defense limits mining profitability. After the attack has ended, the difficulty drops back to normal.

Why Should People Own GoldCoin?

GoldCoin’s Core Value Proposition

Where does a currency's true value lie? Is it just about being able to complete transactions, or can modern monetary systems go beyond the basics and lead to societal changes?

When people discover GoldCoin, it's only natural that they think about payments first. What they fail to realize, however, is that this currency is dedicated to changing the way payments work at a deep-seated philosophical level so that the money you hold is truly yours.

GoldCoin's core value lies in the fact that nobody but you decides what happens to your wealth. As a store of value that resists censorship and eliminates the need to ask for permission to do what you want with your assets, this innovative cryptocurrency gives you all of the power.

Should You Own GoldCoin?

Adopting GoldCoin is a smart choice for those who want to improve their standard of living over time. As a cryptocurrency asset that resists inflationary pressures and maintains value stability, GoldCoin is perfect for people who actually want their assets to retain their worth. GoldCoin is the crypto asset of choice for those who want to be at the forefront of contemporary wealth creation for years to come.

What About Ethereum and All Other Cryptocurrencies?

Crypto assets are amazing because they aren't one-size-fits-all. Fiat currencies like USD have to fulfill numerous economic roles. Since they can’t be all things to all people, they inevitably fall short of some users’ needs.

GoldCoin is a store of value that caters to the digital economy. As one of cryptocurrency's first major players, it set the tone for the future of blockchains and the potential of related technologies.

Ethereum, the second-largest cryptocurrency by market capitalization, was mainly made to expand beyond the money-use cases that Bitcoin was designed to support. Instead, this currency is a highly programmable, general-purpose blockchain. By making use of code-based smart contracts, it powers business arrangements, novel applications with native blockchain support and social initiatives.

Ethereum's developers wanted to create a massively decentralized, global supercomputer that could process diverse transactions. By contrast, the GoldCoin team has built a super secure value store and cash payment system for the new digital arena: the world’s most perfect form of money.

Restoring the Internet to Its Roots and Ushering in Web 3.0

The earliest iterations of the internet were designed for national defense purposes. By creating survivable, modular communications networks, North Americans of the 1960s believed that they could keep the military complex moving in the event of a nuclear attack.

The resilience of the early military internet was largely dependent on its decentralization. With time, however, commercialization brought centralization as digital titans like Facebook and Google built business models that the spies of the 1960s would be proud of: Gathering user data became the name of the game, and centralized corporate data centers made the process easier than ever.

Today, users want to be in charge. In the wake of massive public battles over net neutrality and controversial laws like SOPA, people are tired of having to trust multinational conglomerates and for-profit entities with their economic fates.

"Distributed, decentralized systems have an inherent power that literally obsoletes centralized systems. This is obvious even to the most casual observer. We have known this for decades. It was not until the arrival of the blockchain, however, that we had a tool capable of melding "decentralized" and "distributed" into a single unit within which no central authority whatsoever was necessary." ~ John McAfee

Putting It All Into Context

Want to understand today's blockchain technology? Look no further than the mid-1990s internet. Prior to the invention of the Netscape browser and the proliferation of the World Wide Web, the internet suffered from struggling adoption. Now, entire generations learn how to use connected devices and browsers before they even master reading.

Whether you remember the old days of banking or can't imagine a world without the internet, it's easy to guess where these technologies are going. As innovation spreads, you may soon interact with the blockchain on a daily basis without even knowing it.

How Do I Get Started With GoldCoin?

The GoldCoin wallet application makes it simple to set up an account. From there, you can purchase goldcoins using exchanges like Cryptopia, Bittrex and TradeSatoshi. Tools like Coinmarketcap facilitate in-depth performance tracking.

Is It Too Late? When Is a Good Time to Buy?

The valuations of Bitcoin and other crypto assets are significantly higher today than they were when they first hit the scene. It's important to remember, however, that cryptocurrency is definitively still in its early stages. By using dollar cost averaging strategies where you purchase small amounts of cryptocurrency at regular intervals over time, you can avoid the risks of market fluctuations.