Bitcoin 1776

Software Version

Kennedys Coin

Unit of Value

 

[www.bitcoin1776.com](http://www.bitcoin1776.com) , [www.bitcoin1776.org](http://www.bitcoin1776.org)

[www.kennedyscoin.com](http://www.kennedyscoin.com) , [www.kennedyscoin.org](http://www.kennedyscoin.org)

[JFKBitcoin1776@gmail.com](mailto:JFKBitcoin1776@gmail.com)

Bitcoin 1776 is a new version of the Bitcoin software to adjust future token dilution for post-2008 economies.

Bitcoin 1776 will be capped to 17,760,000 coins, as opposed to 21,000,000, thereby increasing current ownership of the final product from 82% to 96%.1

**Technical Summary**

Bitcoin is inflating.

**Bitcoin 1776 will decrease the rate of inflation.**

Bitcoin must issue coins until it reaches 21 Million coins. These coins are distributed to outside parties, for the incursion of costs. The costs are variable, such that the higher the value of a Bitcoin, the more costs are incurred, and thus the more selling of coins and pull of resources away from the environment.

There comes a point upon which the environment shall not be able to sustain the allocation and either the value of Bitcoin, or the value of everything else, must collapse.

Bitcoin 1776 reduces the annual strain upon the environment by 98%, for Bitcoin 1776 and every successive version respecting an equal coin max. 2

**Bitcoin 1776 blocks are built better.**

Bitcoin blocks are created, motivated by a fixed subsidy. This fixed subsidy is added to consumer demand to create an ecosystem. Providers in this ecosystem must balance their allocation of resources between obtainment of the subsidy, and providing responsiveness to consumer demand. If factors were weighted equally, 50 / 50, then a doubling in consumer demand would increase block speed, and if unequal than one or the other would not affect the outcome.

Bitcoin weighs the fixed subsidy to minimum consumer demand 99.96% to 0.04%, or 2,500 to 1. 3 Bitcoin 1776 will adjust this scale to achieve a ratio of 56 to 1. By providing a more balanced compensation, block builders will become motivated to respond to demand, and build blocks faster during peak season, improving customer service.

**Objections and Responses - 1 of 2**

* What makes Bitcoin 1776 believe it can value Bitcoin without analyzing its culture?

Bitcoin 1776 recognizes the importance culture plays in the valuation of assets. Analyzing and transferring this value to new projects is a complicated matter indeed. We recognize these shortcomings when performing a purely numerical analysis.

However, considering the size of these numbers, accounting for trillions and billions of dollars of expense, we feel using a base formula, such as Demand over Supply, to be appropriate, even considering its lack of cultural appreciation.

* If you really hate inflation, why not end it entirely?

Bitcoin 1776 does not hate all inflation. Inflation of supply directed toward a purpose which provides greater value to the whole is surely welcome. However, inflation of supply simply to reduce scarcity makes as much sense as robbing a rich man to relieve him of the burden of carrying so much treasure.

By aligning expenses with reasonable real world projections, we better protect the historical accumulated wealth of coins. In time, it shall be recognized that there exists a possibility that someone or an organization shall increase the supply in order to fund a project of some sort or another, to seed the wild world, or to automate such processes.

In such events, so long as historical weights and measures remain unadjusted, Bitcoin 1776 shall be initially neutral, and welcome the matter to be discussed via the forums, public and private, until a quorum is reached and the mattered settled.

**Objections and Responses - 2 of 2**

* How can I come to trust your numerology, and deeper motivations?

There are many things which we cannot comprehend, or value with objectivity. However, numerical equations are experiments which can be repeated. Though individual results differ, in sum they produce a range. Bitcoin 1776 encourages resource nodes to construct their own tables, to replicate our math, or propose alternate formulas. Collectively we shall meditate over such until we achieve a comfortable consensus.

It is natural to project circumstance upon the facade of others, and thus I allow that I will be judged from a multitude of experiences, some kind and others mean. But the outcome of Bitcoin 1776 shall neither be to comfort nor to subdue, for in all aspects of change there exists uncertainty, and for that there is no medicine.

* Where is your programming team, marketing team, or advisory council?

While we anticipate the open source community fulfilling some of these functions, we will regard this as beyond the scope of this endeavor. This is to say, one should anticipate no creation of value inherent in the project, beyond what one is capable of downloading and using today.

The initiating coins, or premine, will be donated to the 501(c)3 nonprofit, Midnight Discovery, Inc. which serves the purpose of educating and engineering a robust society. Some of these pledged coins may be restricted as to their use or manner of distribution, and shall not be expected to directly contribute value to Bitcoin 1776.

Some possible examples include:

* Restricting 51,375 Coins, to be sold between values of $2 and $400
* Restricting 100,000 Coins, to be sold between values of $400 and $300,000
* Restricting 300,000 Coins, to be used to sponsor social events
* 100,000 Coins for general use and patronage
  + Released in stages, not to be fully tradable until after 155,500 blocks

**Numerical Equations - 1 of 2**

Assume a Bitcoin value of $100,000, what is the amount of new supply?

144 blocks are created daily (6 per hour, 24 hours per day) and 52,560 blocks are created per year. Until approximately May, 2020, 12.5 Bitcoins are minted per block and then 6.25 Bitcoins for the next four years. Thus, 657,000 Bitcoins are created annually until 2020, and 328,500 until 2024. Over 6 years, this amounts to minting 2,628,000 new coins.

Thus at a value of $100,000, annual new supply amounts to $65.7 Billion, or $180 Million daily, and half this amount after 2020. New supply consumption can either be achieved through the minting new dollars (whereby median wages skyrocket from $30,000 to $300,000) or through the collapse of Bitcoin value. The total funding required over 6 years, to sustain a fixed price of $100,000, would total $263 Billion.

In contrast, Bitcoin 1776 will mint 52,560 new coins over the next 6 years. In sum, at a $10,000 value, Bitcoin 1776 would need $526 Million in funding cumulatively or $5.3 Billion at a fixed value of $100,000. The level of new supply minted by Bitcoin at a $10,000 valuation is $6.6 Billion, annually, until 2020.

However, this type of equating often represents a misunderstanding of the function of markets. Instead, the coin shall increase in value until annual new supply adjusts to equate to annual new demand, less the relaxing of concentrated holdings or change in expectation of future value. Whereby in one calculation, the value is indeterminable, supply indeterminate, and the results are merely one of infinite possibilities, in the other calculation the value is determined by equating demand to supply. Such a method is more considerate to the intelligence of markets, and appreciative of predictive nature of organic demand.

Another common misconception is presuming demand slackens for things that grow more valuable in time. As values grow, concentrated holders sell to better represent their wealth using a variety of assets. This creates temporary downward pressure, but cannot be perpetually sustained. If the new demand for Bitcoin 1776 was consistently $6.6 Billion annually, the coins must grow until they achieve a value of $500,000 to $1 Million, by way of mathematical requirement.

**Numerical Equations - 2 of 2**

Bitcoin transaction fees are set by the minimum divisible unit, the Satoshi.

The cumulative amount paid for Bitcoin transactions is relative to the number of available bytes available per Bitcoin block, and the variable cost per byte, as established by the consumer demand.

Bitcoin is set to a 1 megabyte block size, which allows for 450,000 Bytes to be used for the transferring of Bitcoins. One commonly referenced average for a Bitcoin transaction is 225 Bytes, thus 2,000 Bitcoin transactions can fit per block. If 1 Satoshi is paid per byte, then this amounts to 225 Satoshi, or 450,000 Satoshi per block, pre-Segwit (high uses of scripting can double available bytes).

The fixed subsidy of Bitcoin (added to transaction fees) is set to 1,250,000,000 Satoshi until 2020, and then 625,000,000 per block until 2024. Broken down into Satoshi per byte using a 1 megabyte block, that amounts to 2,777 Satoshi until 2020 and then 1,389 Satoshi until 2024, per byte in fixed subsidies as opposed to 1 Satoshi per byte of minimum consumer demand, creating a significant imbalance. Each incremental rise in fee of 28 Satoshi adds 1% to the block reward, and is represented as 6,300 Satoshi per Bitcoin transaction. At $10,000, this amounts to $0.63 in Bitcoin fees, and $6.30 at $100,000 per Bitcoin.

Bitcoin 1776 improves responsiveness to this uncertain variable by reducing the fixed subsidy to 25,000,000 Satoshi per block, or 56 Satoshi per byte. Each incremental rise in fee of 1 Satoshi adds 2% to the block reward. At $100,000, escalating transaction fees from 1 to 2 Satoshi per byte amounts to $0.23, which is enough to be meaningful but not breaking.

Add more, during seasonal consumer peaks, blocks could become generated in an average of 7 minutes, and 13 minutes off peaks, for several days at a time. Thereby creating a market reactive block (from a human perspective), which can increase the quantity of transactions processed per day seasonally, without adding long-term node strain or substantially increasing the chance orphaned blocks (both of which can be problems from having too short of block times).

**Hash Power**

Hash power is the rope which holds Bitcoin together. Without hash, or a low amount of hash, one cannot be certain they are connected to a proper line of nodes.

In an ideal world, that of Satoshi Nakamoto, mining and node operating could never be decoupled. However, it is recognized that this is an unreasonable expectation as each successive technological advance creates a multibillion dollar competitive edge, and to arrogantly shame those who do not simply share such with the world openly and freely is to purport a level of social sacrifice from the industrious intellectuals that will forever leave one bitter and in misery. Steps were taken in designing this code to reduce future payouts of Bitcoin algorithm from 16% to 1%, thereby limiting their financial control over the platform, by way of hacking or elsewise.

**Price finding and the arrival of market equilibrium**

Blockchain tokens are notably volatile. There are many factors which effect markets overall, or which are specific to one project. There are matters public, in which many actors act independently, and matters private in which a small collection act in concert against.

One force which creates the appearance of a controlled market is supply cornering. When a small group, or single entity, controls an unusually high percentage of supply, then presumably these units must become divided over time, into an increasing number of hands, reducing general demand, or put upon the trading floor, overloading supply. In either situation, the syphoning of future demand or the overloading of supply, the public is largely excluded from knowledge of the decision driving such exchanges, and are left to speculation.

Bitcoin 1776 shall initiate through the awarding of 96% of all possible coins in equal ownership to those of Bitcoin. This process shall reduce the ability for any new entity, or future entity, from seizing over 5% of the coin supply, separated from that of Bitcoin.

**Local Terminology and responses to common or controversial social norms**

**Bitcoin** – Bitcoin shall generally refer to the dominate version of the Bitcoin blockchain, or “Bitcoin Core”. Bitcoin 1776 and Bitcoin are similar into that their software is similar, and their histories are similar. Bitcoin has many peripheral products, such as BISQ, BTCPay, Lightning, Block Explorers, Node Explorers, Scheduled Updates, Communication Channels, etc, not shared by Bitcoin 1776. Likewise, the ways in which Bitcoin derives its value, and the ways in which Kennedys will derive their value will be nothing similar. The price and value of a Bitcoin should have little to do with the price of a Kennedy.

**Units and Subunits** – Within the development of culture, the units are as follows

1 Kennedy = 100,000,000 Franklins = 1 Bitcoin

1 Malcolm = 1,000,000 Franklins

1 Paine = 1,000 Franklins

1 Franklin = Indivisible Unit = 1 Satoshi

**Lambo holding** – Generally speaking, we shall discourage flashy treasure to front, or lord over, those of lower social class and the reinforcement of inferior social rank. Through our actions, we hope to promote the acquisition of human energy, holistically, as it will prove more rewarding than tools or trophies. Similarly, we encourage all investors to hold a diversified portfolio, improving market breadth and responsiveness to volatile movements in price. Lastly, we will promote the acquisition of fiat, and all things, which may prove of service to Bitcoin 1776.

**Midnight Discovery, Inc** – A 501(c)3 nonprofit organization. Their purpose is to socially engineer a more robust society, through education and culture.

**Bitcoin 1776**  – Bitcoin 1776 is the name of this version of the Bitcoin software.

**Kennedys Coin** – A “Kennedy” is our unit of measure, ticker JFK.

Created by Keller Barnette (fork block 530,500) first published in August, 2018.

**Summary – For Quick Reference**

Bitcoin mints more tokens in one year than Bitcoin 1776 will, ever. Bitcoin 1776 is a balance change to the Bitcoin code, executing on block 530,500, which was mined on July 4th, 2018, 10am EST, 4pm UTC (at 17,131,250 tokens). Bitcoin 1776 began with 17,682,625 tokens and will continue until 17,760,000 tokens have been issued. Initiating tokens of 551,375 will be pledged to Midnight Discovery, Inc, a 501(c)3 nonprofit. Possible future pledges restrictions include:

* Restricting 51,375 Coins, to be sold between values of $2 and $400
* Restricting 100,000 Coins, to be sold between values of $400 and $300,000
* Restricting 300,000 Coins, to be used to sponsor social events
* 100,000 Coins for general use and patronage
  + Released in stages, not to be fully tradable until after 155,500 blocks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Bitcoin 1776 | | Bitcoin | |
| Spot Price | $10,000 | $1,000,000 | $10,000 | $100,000 |
| 2019 costs | $0.13 Bil | $13 Bil | $7 Bil | $65 Billion |
| 2021 costs | $0.07 Bil | $7 Bil | $3 Bil | $32 Billion |

**Notes on Merchandising and Unit Exchange**

Transference of values less than $10,000 is unlikely to create a Rewind Attack risk. However, for larger amounts between unfamiliar third parties, we recommend waiting until at least 25% of the value transferred has been paid toward security. In many cases, than can mean waiting over a week for the transference of $100,000 or more, when the risk of fraud is significant. If the tokens appreciate in value to say $100,000 per unit, then this means only several minutes.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Distribution | Bitcoin 1776 | 17,760,000 | Bitcoin | 21,000,000 |
| BTC Holders | 96.5% | 17,131,250 | 81.6% | 17,131,250 |
| Nonprofit | 3.1% | 551,375 | 0% | 0 |
| ASIC Miners | 0.4% | 77,375 | 18.4% | 3,868,750 |

Bitcoin 1776 began issuing 1 BTC per block, halving every 210,000 blocks. At the time of activation, this amounts to 0.25 BTC per block, or a dilution rate of 0.07%.

**Attack Vectors**

Generally speaking, we hope that the code development for Bitcoin 1776 does not materially differ from that of Bitcoin, and we hope the two groups work together. Thus, regarding attack vectors they will largely be the same for both.

**Rewind Attack**

A “Rewind Attack” is when one party pays some amount to submit a new blockchain with more proof of work than the previous recognized blockchain. However, in the newly submitted blockchain, some exchange of value is omitted, and allowed to be spent again, to a separate address. In particular this is a risk for exchanges that may credit an account millions of dollars instantly, and allow one to withdraw said amount instantly as well. The cost to perform a Rewind Attack, in a free market, is approximately equal to Number of Blocks x Subsidy x Price. At a $10,000 value, to Rewind a blockchain 4 hours, it would cost approximately $3 Million for BTC and $60,000 for JFK.

This attack is created through abuse of the orphan system. The orphan system allows for occasional desync of nodes, which for Bitcoin generally amounts to 3 blocks or less, but has no cap, and then to settle this dispute by ruling in favor of the higher cumulative proof of work. However it is possible, using a Check Point system, to prevent any node from accepting a blockchain which alters blocks more than 2 hours old, no matter the amount of new work provided. In such a way, one is stating that orphaned chains will only be considered if less than 12 blocks different, as opposed to infinity. With the known attack on Bitcoin Gold, using a similar system to that of Bitcoin, their blockchain was Rewound 22 blocks, or 3 hours and 40 minutes, leading to $1.75 Mil in transferences getting reverted, and double spent, for a cost approximating $22,000, plus setup fees.

This can be stopped in its entirety through implementation of a Check Point system, either into the protocol or at the wallet level, which prevents abusing the orphan system beyond the usual 3 blocks all the way through infinity. I might recommend a Check Point every 2 hours, or 12 blocks. Development of this process will fall upon the collective open source communities of Bitcoin.

**Attack Vectors**

**Transaction Fee Spam**

In the event that mining becomes highly centralized and well-coordinated, as it is with Bitcoin and will be with Bitcoin 1776, an attack vector is created which allows for the sudden and dramatic increase of transaction fees at little cost. Generally referred to as spam, these fees prevent the average user from executing transactions without paying exorbitant costs. Over the holidays of 2017, the BTC fees rose from $0.05 to $50 temporarily, or an increase of 1,000%. It should be noted, this could have been the result of user error, and not even represent an orchestrated attack. Fees however, pass on to miners, 100% coin for coin, without any degree of loss.

Assuming that it becomes impossible to prevent an abusive monopoly from arising, which takes over the Bitcoin system, we suggest burning or redistributing some portion of transaction fees, so that there is some portion of loss. We recommend this amount to be approximately equal to 25% of Transaction Fees. As it stands, a miner with 50% control over the Bitcoin network receives a 50% discount on fees to utilize the network, or a miner with 80% control receives an 80% discount. It is quite possible to manipulate fees into such a way, so that Transaction Fee Spam becomes profitable for a miner with significant network control, or through coordination. By implementing a system where 25% of fees are redistributed, a miner could never exceed a discount rate higher than 75%, whereas a coordinated group representing 99% receives a collective discount of 99%, as it stands today.

Another issue with Transaction Fee Spam is that the Bitcoin blockchain is unreactive to changes in transactions fees, unless truly egregious. Bitcoin 1776 fixes this issue by reducing the fixed subsidy, and making it so that miners become highly incentivized to drive up usage and to allocate more resources toward mining during times of high demand. Effectively making the blockchain reactive to the fee rate, and to put this is into line with consumer expectations. Lastly, a small bit of excess profit using the Bitcoin subsidy can fund a significant portion of transaction fee spam. By reducing subsidy, one reduces potential for transaction fee spam abuse. Improvements of these processes will fall upon the collective open source communities of Bitcoin.

**Attack Vectors**

**Generalized Disruption**

Generically this is referred to as the “51% Attack”; however this creates quite a different picture from that of reality. Some typical methods to disrupt a blockchain are to censor transactions or to frequently submit newly orphaned blockchains, thus censoring miner payouts to anyone other than oneself (I believe referred to as Ghost Blocks). However, it should be noted these concepts are generally not profitable.

One notable example occurred with Bitcoin, when a large mining pool refused to process transactions which paid less than $0.05 for processing, or 5 Satoshi per byte. One possible example of miner censoring occurred when one miner had accumulated 5 Bitcoin blocks, and submitted them all at once, found within seconds of one another. This could have been random luck, or it could have represented a miner attempting to dissuade others from participation, by invalidating their reward for the prior 4 blocks.

Censoring transactions is largely unproductive as anyone paying a high enough fee (say 50 cents), will get included in any uncensored mined block. Thus if one controls 90% of the Bitcoin hashing rate, and censors a particular address, it would still be included within 2 hours, with a high enough fee. Ghost Blocking is also not hugely profitable. Granted, it can make censoring more effective, but neither strategy has a clear-cut profit incentive.

Disruption can be profitable, however, if one controls a significant interest in a similar financial instrument, and is able to create panicked demand, or is able to short Bitcoin using financial derivatives. This is of particular interest, considering a large mining collective owns a significant interest in the Bitcoin competitor known as Bitcoin Cash. It should be noted, performing a profitable attack would create a similar effect, generally for far less cost. All the same, the best techniques Bitcoin can use to prevent this is to have a backup plan turn-key ready, able to be executed within minutes to hours, and to regularly improve its code base. Another technique is to break the monopoly on hash by returning to a consensus model which is Byzantine Consensus secure, like that of Bitcoin Gold or Monero.

**Attack Vectors**

**Exchange Rate Volatility**

Over in the lands of fiat, in which centralized planners seek to control inflation and reduce price variability, one faces the risk of losing their stores of value, such as what has happened in Turkey and Venezuela, they risk of poor investment decisions, such as the housing bubble in the US, and they risk of poor distribution regarding the issuance of new fiat. Jill Stein has noted several times that the US must print and distribute new fiat to such an extent that annually, that it could eliminate the entirety of student debt. In the modern world this is referred to as quantitative easing as opposed to printing money. Generally the amount of new money a nation must print is relative to an increase in a nation’s profit, or increases in GDP, created either through the improvement in labor, increase in quantity of labor, extraction of minerals, or acquisition of foreign assets.

Banks engaging in poor investment decisions, causing consumer loss, are generally referred to engaging in factional reserve lending, and becomes abusive when the credit analyst forgo risk of loss or skin in the game, or otherwise become corrupted. Elsewise, it should be noted investment banking is more economically wise than eliminating it entirely, in favor of hard asset or foreclosure lending, only. This is to say lending a sum between the value of unrefined trees and the value of the constructed house promotes more development than not lending anything above the value of the trees, ever. Collectively, these amount to risks of fiat.

Regarding hard assets, such as Gold and Bitcoin, a new risk develops, which is exchange rate volatility. Excess movement in exchange rate, unrelated to a long-term change in value, creates the potential for users of a product to experience significant financial loss, similar to circumstances created by fiat. Some users of Gold products are still recovering from losses of purchases made in 2010. In so much a wise collective, such as a government, is able to predict these changes in value, they could potentially increase their holdings significantly, without adding any more dollars to the Gold network, simply through optimal trading and propaganda.

**Attack Vectors**

**Exchange Rate Volatility (continued)**

It has been noted that the propaganda issued by certain US news stations have mislead Bitcoin investors 95% of the time, or more. Such woeful analysis by professionals paid millions of dollars is more indicative of organized propaganda as opposed to collective ignorance. By suggesting to the unorganized users of Bitcoin they should hold at high prices, and sell at low prices, another group is capable of collecting excess profits, and then using these profits to acquire more Bitcoin, for free, while distributing the cost to ordinary users of Bitcoin. Afterwards, after acquiring significant financial interest, one is capable of causing prices to stagnate on hard asset for years, despite ordinary expectations. Gold is one of the best examples, which has not shown a value gain in over 7 years.

To combat this risk for Bitcoin 1776, a restricted pledge is to be issued requiring the selling of a certain amounts of coins at specified prices, to prevent rapid price inflation. Likewise, a frequent rebuy will be issued at some lower value after the sale of coins, to prevent rapid price deflation. Through the focus of creating a stabilized price and value, centralized organizations are prevented from gaining significant advantage by misleading the public, acquiring a significant interest without financial cost, or causing undue stress through erratic price movements. To aid in this purpose, a pledge of 151,375 coins will be issued to Midnight Discovery, Inc.

Another method to solve this dilemma is to develop a culture of intelligent trading, in which believers sell at high prices and rebuy more coins at low prices. Creating this culture, however, requires some amount of centralized planning, but would make the followers profitable, and thus is likely to be sustaining for a long time to come.

Lastly, Bitcoin and Bitcoin 1776 have an internal method to prevent long periods of drought, by reducing issuance every 4 years. No matter how centralized and manipulated ownership interests become in the short-term, the average user should not experience financial loss beyond 4 years, without an extreme decline in popularity and public interest.

**Attack Vectors**

**Fear of Responsibility, Loss of Discipline, Societal Isolation, and Civil Strife**

While many Americans are accustomed to recognizing the heroes of our society printed upon our monetary units, in other cultures scientific achievements, landmarks, or a modern oppressor is printed instead. However, we are the sum of all those who have gone before, the creators of worlds, the sowers of seeds, the preservers of culture, and the leaders of man. In many instances, these heroes risked not fame alone, not fortune alone, not life alone, but their existence in the entire. Should they have failed, their memory would have be washed away until forgotten in time, their descendants eliminated, and all their supporters punished for generations to come. While one thinks of a loss as temporary, a defeat can have repercussions for decades. Notably, the Korean population is growing in stature at an alarming rate, unrelated to genetics, but as a form of recovery from decades of torture, malnutrition, and punishment. For so long they suffered, many thought their diminished stature a curse of nature, instead of by man.

On the American continent, it is said that the Andros Rebellion led to punishment from their European captors that lasted nearly a century, set back scientific advancement, and led to significant periods of population decline, widespread death, and the destruction of treasured inheritances, affecting generations to come. These lessons hardened the wits of the colonists during their next act, and it was not death they feared, but the ensuing peace should they fail. At other times on the American continent, assassins have worked to kill social leaders, like Malcolm X, and even the American President, John Kennedy. For some believe that through such brutal force, the brave will cower and the uncommitted will fear association, lest he be judged a criminal or lune, and hide beliefs in public.

To combat such systems of oppression, Midnight Discovery, Inc, will organize an annual pilgrimage to a wild land, to remind ourselves from wince we came. It shall sponsor the development of self-reporting organizational units, of exactly 8 members, and develop a system of semi-random election and collective leadership to reduce assassination risk. Lastly, the participants in the development of such a process shall be rewarded in prizes, and recognition. Over half of the initiating coins will be used to implement this system, worldwide. Should it prove successful, we welcome the budding heroes of man.

**Attack Vectors**

**Reduced Scientific Achievement, Public Interest, and Youthful Vigor**

At one time, Bitcoin utilized a consensus model that was described as “one-cpu-one-vote,” for it was stated in their White Paper that allowing any single individual to accumulate an excess of power could lead to destruction. This system, inspired by Byzantine Consensus, which requires uncoordinated actors, interested actors, and easily available & reliable sources of knowledge, has been replaced by Largest Army Consensus, which in effect suggests that if one acquires more than 51% of all available military units at all times, then one should deter any war through assured destruction. In the White Paper, it suggests that a mutiny of the mercenaries would be unlikely, because then they would lose their most valued employer, and source of their wealth. However, today, Bitcoin Cash, and other coins offer potentials for employment, and their wealth is not attached to Bitcoin alone. Not only are mercenaries disloyal, they are also extremely costly, and create significant financial strain upon the social network.

We suggest Bitcoin learn from the pioneers of Monero and Bitcoin Gold. With Monero it was believed 20% of their hash power was ASIC, as few ASICs had been made available to the public, when in fact it was closer to 80%, most of which secretly manufactured and privately controlled. With Bitcoin Gold, through inventing a system which returned Byzantine principles, they have been able to secure their system for far less, and safer, than others. Eliminating the use of monopolist technology is a fundamental requirement to restoring Byzantine consensus. Furthermore, Bitcoin mining equipment has depreciated by over 90% since January, with rising hash rates. This suggests someone has developed a new technology or manufacturing operation, and is keeping it secret.

Lastly, we believe it is important for Bitcoin to pay developers, and to reward the public at large as well. We suggest doing so by allocating 20% of Transaction Fees toward a public reward system, and 5% toward a developer reward system. By paying developers in units convertible to money, young people can earn the money they so desperately need, and learned people will contribute more frequently, not feeling a fanatic or slave. Such a system could take years to develop, but it is worth the effort and attention, and one can use the public involvement to select the awards for which contributors, and so on.

**Attack Vectors**

**Financial Control and Manipulation**

With any asset, such as Diamonds, it is possible for a single entity to become in control of large portions of that asset. For Bitcoin, this can happen either through natural purchase, volatility trading, mining, merchandising, or other. Bitcoin is to distribute 18% of future coins to miners. If the technology the miners use to produce coins is monopolistically controlled, then the price technology should be equal to the expected value, over a period of time, less some percentage for profit. Add more, the monopolist can control production at will, compete against the miners internally, and is incentivized to create excess expectation. The monopolist can withhold shipments during times of bounty, and create price shocks to encourage over investment. It is also well known that these monopolists have taken to selling miners exclusively to private collectors, to disguise their extreme controlling interest in the financial rewards of Bitcoin.

Bitcoin 1776 solves this issue by reducing future issuance to ASIC monopolists from 18% to 0.4%. Even in the event a manufacturer is capable of acquiring 2x the average reward through added scandal, this would amount to no more than 1% of tokens. Another solution is to switch PoW to a Byzantine Consensus system, such as that of Monero or Bitcoin Gold.

Another method to gain financial control is through volatility trading. A restricted pledge issued to Midnight Discovery, Inc, is set to sell a certain amount of coins at specified values, and use these proceeds to rebuy coins at lower values, until exhausted, or the coin achieves a specified price check point. This process will begin at $2 to $400, with another value set beginning at $400 until $300,000. By reducing the degree of price volatility, we allow for consistent purchasing and selling all throughout the year, reduce stress, and better distribute financial ownership.

Regarding natural purchase, by making the coin very scarce, price should change quite erratically. Any attempt to purchase 5% of the total supply of coins would cause the price to skyrockets. Either they did it with Bitcoin, or it cannot be done quickly in Bitcoin 1776 without creating a noticeable change in value.

**Final Thoughts**

**Benjamin Franklin’s 13 Virtues**

1. **Temperance -** Eat not to dullness; drink not to elevation.
2. **Silence** - Speak not but what may benefit others or yourself; avoid trifling conversation.
3. **Order** - Let all your things have their places; let each part of your business have its time.
4. **Resolution** - Resolve to perform what you ought; perform without fail what you resolve.
5. **Frugality** - Make no expense but to do good to others or yourself; i.e., waste nothing.
6. **Industry** - Lose no time; be always employed in something useful; cut off all unnecessary actions.
7. **Sincerity** - Use no hurtful deceit; think innocently and justly, and, if you speak, speak accordingly.
8. **Justice** - Wrong none by doing injuries, or omitting the benefits that are your duty.
9. **Moderation** - Avoid extremes; forbear resenting injuries so much as you think they deserve.
10. **Cleanliness** - Tolerate no uncleanliness in body, cloths, or habitation.
11. **Tranquility** - Be not disturbed at trifles, or at accidents common or unavoidable.
12. **Chastity** - Rarely use venery but for health or offspring, never to dullness, weakness, or the injury of your own or another's peace or reputation.
13. **Humility** - Imitate Jesus and Socrates.

**Benjamin Franklin’s Junto**

To qualify as a member each person was also asked to stand up, and lay his hand on his breast,

And answer the following questions as indicated.

1. Have you any particular disrespect to any present members? Answer. I have not.
2. Do you sincerely declare that you love mankind in general; of what profession or religion so ever? Answer. I do.
3. Do you think any person ought to be harmed in his body, name or goods, for mere speculative opinions, or his external way of worship? Answer. No.
4. Do you love truth’s sake, and will you endeavor impartially to find and receive it yourself and communicate it to others? Answer. Yes.

-----------------------

1. Have you met with anything in the author you last read, remarkable, or suitable to be communicated to the Junto? Particularly in history, morality, poetry, physics, travels, mechanic arts, or other parts of knowledge?
2. What new story have you lately heard agreeable for telling in conversation?
3. Has any citizen in your knowledge failed in his business lately, and what have you heard of the cause?
4. Have you lately heard of any citizen’s thriving well, and by what means?
5. Have you lately heard how any present rich man, here or elsewhere, got his estate?
6. Do you know of any fellow citizen, who has lately done a worthy action, deserving praise and imitation? Or who has committed an error proper for us to be warned against and avoid?
7. What unhappy effects of intemperance have you lately observed or heard? Of imprudence? Of passion? Or of any other vice or folly?
8. What happy effects of temperance? Of prudence? Of moderation? Or of any other virtue?
9. Have you or any of your acquaintance been lately sick or wounded? If so, what remedies were used, and what were their effects?
10. Who do you know that are shortly going [on] voyages or journeys, if one should have occasion to send by them?
11. Do you think of anything at present, in which the Junto may be serviceable to mankind? To their country, to their friends, or to themselves?
12. Hath any deserving stranger arrived in town since last meeting that you heard of? And what have you heard or observed of his character or merits? And whether think you, it lies in the power of the Junto to oblige him, or encourage him as he deserves?
13. Do you know of any deserving young beginner lately set up, whom it lies in the power of the Junto any way to encourage?
14. Have you lately observed any defect in the laws, of which it would be proper to move the legislature an amendment? Or do you know of any beneficial law that is wanting?
15. Have you lately observed any encroachment on the just liberties of the people?
16. Hath anybody attacked your reputation lately? And what can the Junto do towards securing it?
17. Is there any man whose friendship you want, and which the Junto, or any of them, can procure for you?
18. Have you lately heard any member’s character attacked, and how have you defended it?
19. Hath any man injured you, from whom it is in the power of the Junto to procure redress?
20. In what manner can the Junto, or any of them, assist you in any of your honorable designs?
21. Have you any weighty affair in hand, in which you think the advice of the Junto may be of service?
22. What benefits have you lately received from any man not present?
23. Is there any difficulty in matters of opinion, of justice, and injustice, which you would gladly have discussed at this time?
24. Do you see anything amiss in the present customs or proceedings of the Junto, which might be amended?

**Citations**

1 “Bitcoin 1776 will be capped to 17,760,000 Bitcoins, as opposed to 21,000,000, thereby increasing current ownership of the final product from 82% to 96%.”

Approximate Bitcoins created by the time of the fork 17,131,250.

17,131,250 / 17,760,000 = 96.4% 17,131,250 / 21,000,000 = 81.6%.

2 “Bitcoin 1776 reduces the annual strain upon the environment by over 95%, for Bitcoin 1776 and every successive fork which is created out of its codebase.”

Each new coin created must be absorbed by the Bitcoin community.

Coin Creation

2019 - Bitcoin 657,000 Bitcoin 1776 13,140 2%

2020 - Bitcoin 657,000 Bitcoin 1776 13,140 2%

2021 - Bitcoin 328,500 Bitcoin 1776 6,570 2%

2022 - Bitcoin 328,500 Bitcoin 1776 6,570 2%

2023 - Bitcoin 328,500 Bitcoin 1776 6,570 2%

3 “Bitcoin weighs the fixed subsidy to minimum consumer demand 99.96% to 0.04%, or 2,500 to 1”

Fixed Subsidy (0.9996) 1,250,000,000 Satoshi

Minimum Consumer Demand (0.0004) 450,000 Satoshi

(at 1 Sat / Byte, 450,000 usable bytes) 1,250,450,000 Total

**Acknowledgements and special thanks to**

Satoshi Nakamoto, and contributing developers to the Bitcoin White Paper

Bitcoin Gold, for improved consensus and issuance of polite social treaties

The developers unrewarded and forgotten

The destressed plotting and persevering

The forefathers and foremothers who improved this world

And the grandchildren who honor them