Capitalized Bitcoin Fork for National Strategic Reserve

Charanjit S. Jutla
IBM T.J. Watson Research Center
Yorktown Heights, NY

Arnab Roy
Mysten Labs
Palo Alto, CA

March 17, 2025

Abstract

We describe a strategy for a nation to acquire majority stake in Bitcoin with zero cost to the taxpayers of the nation. We propose a bitcoin fork sponsored by the the government of the nation, and backed by the full faith of treasury of the nation, such that the genesis block of this fork attributes fixed large amount of new kinds of tokens called strategic-reserve-bitcoin tokens (SRBTC) to the nation's treasury, which is some multiple (greater than one) of the amount of all Bitcoin tokens (BTC) currently set in the Bitcoin protocol. The BTC tokens continue to be treated 1:1 as SRBTC tokens in the forked chain. The only capital that the nation puts up is its explicit guarantee that the SRBTC tokens of the fork will be accepted as legal tender, such as payment of tax to the treasury.

We suggest that this is a better approach than starting a new blockchain that mimics Bitcoin, as it will be partially fair to the current holders of Bitcoin, which in turn would make it competitive in the space of other such possible forks by other powerful nations. Moreover, such a proof-of-work blockchain retains its egalitarian and democratic nature, which competitively deters the said nation from any dilutions in the future.

To justify our proposal we setup three competitive games, and show strategies for different players that are in Nash equilibrium and which throw further light on these claims. In particular,

1. The first game shows that if the only two alternatives for investors is to invest in BTC or SRBTC, then individuals who have a certain fraction θ of their wealth already invested in BTC, will invest new money in the original chain, whereas the individuals whose current wealth invested in BTC is less than the θ fraction will invest new money in SRBTC.
2. The second game shows that if there is a third alternative for investment, which is cash that is losing value (inflation-adjusted) by a percentage d, then the investors who had less than θ fraction of wealth in Bitcoin, will invest in SRBTC only if the dilution of SRBTC is large enough (as an increasing (linear) function of $1/d$). Here by dilution we mean the new SRBTC tokens that are allowed to be eventually mined in the fork.
3. The third game shows that investors would prefer a fork of Bitcoin over a replica of Bitcoin that doesn't value original BTC, when both are available and even if both are backed similarly by one or more nations.

1 Introduction

As is well known, the field of (egalitarian) crypto-currencies started with publication of a white paper on Bitcoin [9] and its subsequent implementation and wide popularity. While the notion of digital money has existed for a while (see e.g. [4, 10, 3]), and even some based on hash chains that were anonymous and allowed off-line transactions (see e.g. [12, 6]), none of these solved the double-spending problem without the use of a ledger maintained by a trusted authority. The key idea of Bitcoin is to use *proof-of work*, based on solving (computationally) hard problems, to democratize the consensus protocol in a peer-to-peer setting. No registration of protocol participants is required, and hence neither an online availability of pre-defined quorum of participants is required. This allows for a decentralized ledger in an ad hoc network setting [1].

Despite the ingenious use of proof-of-work [5] to implement a peer-to-peer permission-less consensus protocol for a time-stamped ledger of rare tokens, its actual utility to implement a cryptocurrency has been marred by a lack of scalability and other issues such as large concentration of share of the rare tokens amongst its early adopters who are all private individuals or groups. Still, Bitcoin as a proof-of-work cryptocurrency has the potential to at least solve some problems, e.g. as a reliable, highly liquid digital store of value, arguably better than gold itself in some respects such as (digital) liquidity.

This ability of Bitcoin to serve as a digital egalitarian store-of-value has recently been recognized by the US government, which has even mandated (at least as an executive order) a national strategic reserve of Bitcoins. Unfortunately, since the US government (or for that matter any government excluding the possibility that Satoshi Nakamoto is a government entity) has only a tiny fraction of total rare Bitcoin tokens, it precludes the US government from lawfully becoming the majority owner of such tokens. Without the US government (or any government) becoming a substantially major owner of such tokens, it is not in its interest to make it a legal tender.

Why is a digital decentralized "store-of-value" important? While Bitcoin as an enabler of day-to-day use currency is unlikely, outside of off-chain solutions like lightning network [11], because of lack of scalability of transactions, it is hoped that it becomes a store of value similar to gold. Most nations hold gold reserves as capital (or collateral) backing their paper (fiat) currencies. One could envision a similar role for an egalitarian digital store of value. This store of value serves as a good monetary vehicle for inter-nation trade, as well as a good balance sheet asset for raising debt to build national economies etc. For example, countries currently own gold and US dollar as reserve to bolster their balance sheets. However, the store of gold is not easily verifiable and a paper currency can lose its reserve status due to economic downfall. However, value stored on a blockchain, even in an encrypted form, can be proved to one or more parties, almost instantly, using non-interactive zero-knowledge proofs [13]. Thus, an egalitarian digital currency, if properly designed, has advantages over traditional stores of values such as gold and fiat currencies of developed countries.

2 Bitcoin Fork Proposal

Our central proposal is for a nation to initiate a fork of the bitcoin blockchain. Essentially, it's an alternate continuation of the bitcoin blockchain with a common prefix up to a certain agreed-upon block. There will be a strategic reserve committee which is instituted to set the rules of the fork. The rules will be set out as an RFC with public discussions organized and finalized way before (say 6 months) before the fork event. The first alternate block of this fork will be called the SRBTC genesis block. The genesis block will allocate a predetermined large amount of SRBTC tokens

[1] See [2] for a more theoretical universally-composable treatment of Bitcoin functionality.

to the nation's strategic reserve. It also issues SRBTC at 1:1 ratio to pre-fork BTC holders, in other words the BTC tokens in the prefix can be sold as SRBTC. After the genesis block, it will allow regular decentralized mining of SRBTC tokens according to a schedule to be decided by the strategic reserve committee. The schedule of the amount of SRBTC tokens to be awarded per mined block will determine the dilution of the token, and we discuss this important issue and its implications in Section 5. Briefly, to garner interest of individuals of the nation and around the world (as well as other nation's reserves) who are *not* already substantially invested in bitcoin, the new forked blockchain must have a long period of dilution, i.e. mining awards that keep adding to the total SRBTC tokens for a long time.

There are numerous considerations to maintain the security and price stability of such a fork. These include key management of the private key(s) of the national reserve, handling the dynamic nature of the (human) composition of the government who will jointly custody the keys, prevention of insider and long-range attacks which can compromise the chain, and reactive frameworks to address state- sponsored large scale attacks. It is also important to place security of the chain as a much more important goal as compared to the expressivity of its smart contracts and latency and throughput of its execution. These are critical details to figure out, but will be out of scope of this paper. However, certain important remarks are in order here.

1. Price Stability. While we envision a large predetermined amount of SRBTC to be awarded in the SRBTC genesis block to the treasury, it is probably best that it be legislated that any sale of any portion of this reserve must be announced before hand. This also prevents theft of such tokens. However, to maintain price stability of the SRBTC token, it is possible that a small portion of this reserve can be deemed as tradeable by treasury without notice. Alternatively, if there is a general distrust in the treasury department to maintain price stability via such a tradeable portion, one can modify the Bitcoin award-per-mined-block protocol as described in [7] to intrinsically achieve inflation-tracking price-stability.

2. Hash Difficulty. The genesis block of SRBTC will also be mined in a decentralized fashion by solving the usual cryptographic puzzle based on the pre-fork block in BTC blockchain. However, the difficulty of this puzzle can be set based on estimated mining demand of the new forked chain (which arguably depends on the investment demand for SRBTC as well as the dilution implied in the forked chain).

3. Further Future Dilutions? As indicated in the first bullet point, the treasury can sell some portion of the reserve by first making a public announcement, and hence that can contribute to some dilution as it was not part of the "float". The reason for the treasury taking such a decision can be based on some important circumstance such as war or natural calamity. The very reason investors will flock to SRBTC (of a nation) in the first place is based on the trust in that government to not cause massive dilution or rescinding the legal tender in the medium term, say 20 years. We mention medium term, as beyond medium term, when a decent proportion of the population has stake in SRBTC (see Section 5 for a game-theoretic analysis of this behavior), the SRBTC can survive on its own without requiring the legal tender guarantee. Moreover, any further forking will possibly be rejected by the decentralized community of investors and miners.

2.1 Historical Precedents

Historical practices surrounding a nation's currency underscore a key principle: a nation's currency is bolstered by the assets it can credibly pledge or convert into. In the past, that asset was gold or another nation's strong currency; in modern times it is a basket of fiat currencies and gold. The strategic reserve Bitcoin fork concept echoes the reserve principle – seeking to create a large stock of a valuable asset (Bitcoin-like tokens) under government control – but diverges in execution. Rather than accumulating reserves through economic output or trade surpluses, the proposal suggests essentially creating a reserve asset via a blockchain protocol change. In effect, it is a form of "digital seigniorage" harnessed by forking an existing decentralized currency. Historically, when countries needed to increase reserves or money supply, they might have resorted to printing more fiat money (with inflationary consequences) or revaluing gold, but they could not simply duplicate an external asset without cost. In sum, while the goal of shoring up national reserves aligns with long-standing economic strategies, doing so by forking a cryptocurrency represents a novel departure from historical precedents, blending elements of fiat monetary policy with the ethos of decentralized finance.

2.2 Technical Contributions of the Paper

This paper provides several technical contributions:

1. We formalize the proposed strategic reserve Bitcoin fork (SRBTC) and clearly outline the economic rationale behind its genesis structure, ensuring fairness to existing Bitcoin holders while granting significant initial stakes to the sponsoring government.

2. Using game theory, we model investor behavior through three distinct games that rigorously demonstrate the economic incentives and equilibrium conditions underpinning investor preferences between original Bitcoin and the strategic reserve fork, accounting explicitly for the dilution and inflationary pressures.

3. We derive explicit Nash equilibrium conditions that highlight critical parameters influencing investor decisions, notably identifying a wealth threshold that determines preference between BTC and SRBTC.

4. We introduce a novel economic analysis addressing the optimal dilution strategy in the strategic reserve fork, demonstrating the relationship between dilution rates, inflationary pressures in competing assets, and investor preferences.

Collectively, these contributions provide a rigorous framework for evaluating and potentially implementing national-level blockchain reserve strategies, highlighting the economic viability, practical considerations, and governance models necessary for successful deployment.

3 Economic and Game Theory Preliminaries

Giving a detailed presentation of economic theory models and primitives is beyond the scope of this paper, but we point to the excellent teaching notes of Jonathan Levin [8]. Very briefly, consider N resources and M agents. Each agent i has an endowment of resource j : e^i_j. Each agent has a utility function (of their endowments) : u^i_j. An economy is $\mathcal{E} = (u^i, \vec{e}^i)_{i \in [M]}$. Now consider a vector of market prices (of resources): $\vec{p}$. Each agent tries to maximize their utility under their budget constraint: $\vec{p} \cdot \vec{x}^i \ \leq \ \vec{p} \cdot \vec{e}^i$, where x^i_j is the new allocation of resource j to agent i. A *Walrasian equilibrium* of an economy $\mathcal{E}$ consists of (a) a price vector $\vec{p}$, and (b) a redistribution of resources $\{\vec{x}^i\}_{i \in [M]}$, such that each agent maximizes his/her utlity and markets clear, i.e. for all resources j we have $\sum_i x^i_j = \sum_i e^i_j$.

A feasible reallocation $\{\vec{x}^i\}$ of economy $\mathcal{E}$ is called *Pareto Optimal*, if there is no other feasible allocation $\{\vec{y}^i\}$ such that for all $i \in [M]$: $u^i(\vec{y}^i) \geq u^i(\vec{x}^i)$, with strict inequality for some $i \in [M]$. The first Welfare Theorem [1] states that a redistribution of resources that is in Walrasian equilibrium is Pareto optimal.

A normal form Game G consists of a set of players $i \in [M]$, and a set of strategies for each player denoted S_i. Let $S = S_1 \times S_2 \times \cdots \times S_M$. Each user has a payoff function $u^i : S \to \mathbb{R}$. A (mixed) strategy for player i, σ_i is a probability distribution on S_i. A strategy profile $(\sigma_1, \cdots, \sigma_M)$ is a *Nash equilibrium* of G if for every i, and every $s_i \in S_i$, $u^i(\sigma_i, \vec{\sigma}_{-i}) \geq u^i(s_i, \vec{\sigma}_{-i})$.

4 Competition between Original and Strategic Reserve Forks

In this section we will analyze as to which fork, the original or the reserve, is more likely to attract new investment. To model this analysis, we will assume a (worldwide) population M, where each $i \in M$ has a certain current wealth w_i (say, measured in Gold or a currently stable fiat currency, e.g. USD), and further a proportion π_i of i's wealth is currently invested in Bitcoin (say, at its current valuation in USD).

Now, as for new incremental investment into any one of the forks of Bitcoin, one can reasonably argue that individuals who are already invested in Bitcoin are more comfortable investing more, and for this reason we will assume that an individual i is willing to invest a fraction θ_i of their wealth (that is not already in Bitcoin) into one of the forks, where θ_i is an affine function of π_i, say $\theta_i = \alpha + \beta * \pi_i$, where α and β are positive fractions (less than one) and $\beta + \alpha \leq 1$. We will also assume that this decision to invest in one of the forks is split into many periods. We will assume that both forks will maintain their price (inflation-adjusted) after an initial adjustment period, say the first period itself. Thus, we can say that the price of the token in each fork will be determined by the new incremental investment coming in this first period, and further it is a linear function of the total new investment coming into the fork. So, let $P_{\text{BTC}}(W)$ be the price of original chain of Bitcoin if W new investment comes into this chain, and P_{BTC} is a linear function, i.e. $P_{\text{BTC}}(W) = b_0 + b_1 * W$, for some b_0 and $b_1 > 0$ determined by market dynamics. In particular, let b_0 be the price of Bitcoin right before the forking. To be more precise, the price should be $b_0 + b_1 * (W - S)$, where S is the selling pressure, but we will ignore S for this analysis, which will not make a difference as long as S is some constant pre-determined selling pressure. Similarly, let $P_{\text{SRBTC}}(W)$ be the price of strategic-reserve fork chain of Bitcoin if W new investment comes into this chain, and P_{SRBTC} is a linear function, i.e. $P_{\text{SRBTC}}(W) = c_0 + c_1 * W$, for some c_0 and $c_1 > 0$ determined by market dynamics. Here, we can assume that this price is determined by some form of clearing-price auction, and hence the price paid to acquire these tokens is the eventual stable price of these tokens.

We will assume that each individual is interested in their *relative* wealth after a medium time frame, say ten years, with no other gains or reductions in their wealth apart from investing in these two forks or a cash instrument which has a negative return (adjusted for inflation) despite interest payments[2]. Recall, this is the main reason for existence of Bitcoin as it is supposed to be a true store of value as opposed to fiat currencies which are (presumably) constantly debased. For this reason, we will assume that both forks of Bitcoin are not diluted any further (as these will both be democratically managed). There is also a risk in both chain of large scale dumping by Satoshi and/or the government in the reserve fork. However, we will assume that neither of these possibilites have more than negligible probability, although one can introduce these as parameters in the analysis.

Now, for some $x: \ 0 \leq x \leq 1$, consider the following strategy for each $i \in M$.

- If $\pi_i > x$ then invest all of $\theta_i * (1 - \pi_i) * w_i$ in the original Bitcoin.
- If $\pi_i \leq x$ then invest all of $\theta_i * (1 - \pi_i) * w_i$ in the the new strategic-reserve fork of Bitcoin.

In the following lemma to hold we require that $b_1 > c_1$, which should hold as the original Bitcoin blockchain has already mined almost all tokens, and hence the price of that token is highly sensitive to new investment compared to the strategic reserve fork where we expect a large fraction of tokens to yet be mined and hence the price of the token in that fork will be much less sensitive to new investment. In other words, we have $b_1 > c_1$.

Lemma 1 *If $b_1 > c_1$ in the above price structure, then the above strategies for P is a Nash equilibrium, when $x = \frac{1}{2} * (\Psi + \sqrt{\Psi^2 + 4 * \alpha/\beta})$ with Ψ defined as $\Psi = \frac{\sum_{j \in M} \pi_j^2 w_j}{\sum_{j \in M} \pi_j w_j}$.*

Proof: Note that each individual i's utility u^i is their relative future wealth, which is $w_i^* / \sum_{i \in M} w_i^*$, where w_i^* is their future wealth.

We first calculate each individual's future wealth assuming the above strategies were played. The new investment in the original Bitcoin chain is

$$\begin{aligned} &\sum_{i \in M: \pi_i > x} \theta_i * (1 - \pi_i) * w_i \\ = &\sum_{i \in M: \pi_i > x} (\alpha + \beta * \pi_i) * (1 - \pi_i) * w_i \end{aligned}$$

Thus, P_{BTC} is $b_0 + b_1 * \sum_{i \in M: \pi_i > x} (\alpha + \beta * \pi_i) * (1 - \pi_i) * w_i$. Recall b_0 is the price of bitcoin right before the fork. Thus, individual i with $\pi_i > x$, had $\pi_i * w_i / b_0$ original tokens before hand, and now has additional $\theta_i * (1 - \pi_i) * w_i / P_{\text{BTC}}$ tokens in the original chain. Thus, his future wealth $w_i^* = \frac{\pi_i * w_i}{b_0} * (P_{\text{BTC}} + P_{\text{SRBTC}}) + \theta_i * (1 - \pi_i) * w_i$.

Similarly, the new investment in the strategic-reserve fork is

$$\begin{aligned} &\sum_{i \in M: \pi_i \leq x} \theta_i * (1 - \pi_i) * w_i \\ = &\sum_{i \in M: \pi_i \leq x} (\alpha + \beta * \pi_i) * (1 - \pi_i) * w_i \end{aligned}$$

Thus, P_{SRBTC} is $c_0 + c_1 * \sum_{i \in M: \pi_i \leq x} (\alpha + \beta * \pi_i) * (1 - \pi_i) * w_i$. Thus, for individual i , with $\pi_i \leq x$, his future wealth is $w_i^* = \frac{\pi_i * w_i}{b_0} * (P_{\text{BTC}} + P_{\text{SRBTC}}) + \theta_i * (1 - \pi_i) * w_i$, the formula being the same in both cases.

[2] We will actually ignore this cash instrument option, and just assume that individuals are risk averse investing in Bitcoin which is reflected in θ_i as defined above.

Thus, in either case the future relative wealth $\hat{w_i^*}$ is

$$\begin{aligned}
\hat{w_i^*} &= \frac{\frac{\pi_i * w_i}{b_0} * (P_{\text{BTC}} + P_{\text{SRBTC}}) + \theta_i * (1 - \pi_i) * w_i}{\sum_{j \in M} \frac{\pi_j * w_j}{b_0} * (P_{\text{BTC}} + P_{\text{SRBTC}}) + \theta_j * (1 - \pi_j) * w_j} \\
&= \frac{\frac{\pi_i * w_i}{b_0} * (P_{\text{BTC}} + P_{\text{SRBTC}}) + \theta_i * (1 - \pi_i) * w_i}{(P_{\text{BTC}} + P_{\text{SRBTC}})/b_0 * \sum_{j \in M} \pi_j * w_j + \sum_{j \in M} \theta_j * (1 - \pi_j) * w_j} \qquad (1)
\end{aligned}$$

To show Nash equilibrium, first consider two cases, based on $\pi_k \leq x$ or $\pi_k > x$:

$k \in M :: \pi_k \leq x$**.** Suppose that such an individual k instead invests all the new money in the original Bitcoin chain. Then with just this change in strategy profile of all of M, the alternate $P^{(k)}_{\text{BTC}}$ is $P_{\text{BTC}} + b_1 * \theta_k * (1 - \pi_k) * w_k$, and similarly the alternate $P^{(k)}_{\text{SRBTC}}$ is $P_{\text{SRBTC}} - c_1 * \theta_k * (1 - \pi_k) * w_k$. Thus, the utility of k in this alternate profile, is

$$\frac{\frac{\pi_k * w_k}{b_0} * (P_{\text{BTC}} + P_{\text{SRBTC}} + (b_1 - c_1) * \theta_k * (1 - \pi_k) * w_k) + \theta_k * (1 - \pi_k) * w_k}{(P_{\text{BTC}} + P_{\text{SRBTC}} + (b_1 - c_1) * \theta_k * (1 - \pi_k) * w_k)/b_0 * \sum_{j \in M} \pi_j * w_j + \sum_{j \in M} \theta_j * (1 - \pi_j) * w_j}$$

We need to show that this quantity is less than $\hat{w_k^*}$ as defined in (1). This follows because this inequality will hold (with some manipulation and using the fact that $(b_1 - c_1) > 0$) iff

$$\begin{aligned}
&\frac{(P_{\text{BTC}} + P_{\text{SRBTC}})/b_0 * \pi_k * w_k + \theta_k * (1 - \pi_k) * w_k}{\pi_k * w_k} \\
&> \frac{(P_{\text{BTC}} + P_{\text{SRBTC}})/b_0 * \sum_j \pi_j * w_j + \sum_j \theta_j * (1 - \pi_j) * w_j}{\sum_j \pi_j * w_j},
\end{aligned}$$

which in turn is equivalent to

$$\frac{(\alpha + \beta * \pi_k)(1 - \pi_k)}{\pi_k} > \frac{\sum_j (\alpha + \beta * \pi_j)(1 - \pi_j) * w_j}{\sum_j \pi_j * w_j},$$

which after some manipulation is equivalent to

$$\pi_k < \Psi + \frac{\alpha/\beta}{\pi_k},$$

which can be seen to be true iff $\pi_k < x = \frac{1}{2} * (\Psi + \sqrt{\Psi^2 + 4 * \alpha/\beta})$.

$k \in M :: \pi_k > x$**.** The analysis is same as the previous case except that now since $(c_1 - b_1) < 0$, and the inequality holds in the other direction in this case.

The above inequalities were shown if the strategy for k was completely reversed to invest the whole amount in the alternate chain. However, the above inequalities are easily seen to hold even with partial re-investment in the other chain, as well as in mixed strategies. □

Example. According to the Federal Reserve, through its Survey of Consumer Finance (SCF), the average net worth [3] in USA is \$800,000. We will assume that there are 200 million individuals

[3] https://financebuzz.com/us-net-worth-statistics

in USA. Thus, the total wealth in the country is about \$160T. The current market capitalization of Bitcoin is 20M × \$100K, which is about \$2T. We will assume that this is the wealth in Bitcoin. In the above terminology, $\sum_i w_i = \$160\text{T}$, and lets say (liberally) that $\sum_i \pi_i * w_i = \$2\text{T}$. So, the average π_i is about 1/80, although the distribution of π_i is more likely to be a Poisson distribution with $\lambda = 1/80$. But, as an example, we want to estimate $\Psi = (\sum_i \pi_i^2 * w_i)/(\sum_i \pi_i * w_i)$, which we can estimate to be about average π_i, and hence 1/80. Thus, the above lemma is approximately saying that all individuals whose net worth invested in bitcoin is less than 1/80 fraction are rationally likely to invest in SRBTC, and others in BTC.

5 Is Large Dilution in Strategic Reserve Warranted?

In the previous section, we had analyzed competitive situations ignoring the wealth of individuals retained as cash. In this section, we show that if in the strategic reserve fork, there is not enough dilution, i.e. if c_1 is not much smaller than b_1, then investors who own no or only small proportion of their wealth in Bitcoin are better served to not invest in either fork, even if their cash position is losing value due to inflation. So suppose that over the medium term, say ten years, it is expected that cash will lose total value by a fraction $0 < d < 1$, even assuming the cash instrument was paying interest, and we assume that both forks of Bitcoin will retain their value over this period of time after the initial price was determined as modeled in the previous section, e.g. $P_{\text{BTC}}(W) = b_0 + b_1 * W$.

In the previous section, we had assumed that each individual plans to invest θ_i fraction of their wealth in some form of Bitcoin, and we had assumed that $\theta_i = \alpha + \beta * \pi_i$. In this section, we will make no such assumption. Since large investors pool together their investment strategies using mutual funds, pension funds, wealth funds etc, instead of the usual Nash equilibrium we will seek equilbrium under coalitions. To make the analysis simpler, we will thus have only two parties in this game: a party (or coalition) of current Bitcoin holders and a party (or coalition) of non-Bitcoin holders. Thus, we will assume that the wealth of the world is divided amongst these parties, party 1 and 2, with $\pi_1 = 0.5$ (Bitcoin holders) and $\pi_2 = 0$ (non Bitcoin holders). As mentioned earlier the main point of this game is to show that if c_1 is too large (which would be implied if dilution in strategic reserve is *not* large enough), then party 2 is better off not investing at all in SRBTC.

Lemma 2 *If* $c_1 > \frac{d}{1-d} * \frac{1}{w_2} * (2 * b_0 + c_0 + 1/2 * b_1 * w_1)$*, then the strategy of player* 2*, where it continues to retain money in cash despite it losing value by fraction d, has more utility than a strategy that invests some money in SRBTC. We will assume that party* 1 *invests all its remaining money, i.e.* $(1 - \pi_1) * w_1$ *in BTC.*

Proof: Under the above two strategies, there is no new investment in SRBTC, but there is $1/2 * w_1$ investment in BTC. Thus, $P_{\text{SRBTC}} = c_0$, and $P_{\text{BTC}} = b_0 + b_1 * 1/2 * w_1$. Hence the future wealth of party 1 is $w_1^* = (1/2 * w_1) + (1/2 * w_1)/b_0 * (c_0 + b_0 + 1/2 * b_1 * w_1) = (1 + 1/2 * c_0/b_0) * w_1 + 1/4 * w_1^2 * b_1/b_0$, whereas the future wealth of party 2 is $w_2^* = (1 - d) * w_2$. Also, the relative wealth's are $\hat{w}_1^* = \frac{(1+1/2*c_0/b_0)*w_1+1/4*w_1^2*b_1/b_0}{(1+1/2*c_0/b_0)*w_1+1/4*w_1^2*b_1/b_0+(1-d)*w_2}$, and

$$\hat{w}_2^* = \frac{(1-d) * w_2}{(1 + 1/2 * c_0/b_0) * w_1 + 1/4 * w_1^2 * b_1/b_0 + (1-d) * w_2} \tag{2}$$

Recall, we assume that both forks of bitcoin retain their value after the initial price determination at forking.

Now, suppose that Player 2 instead invests some fraction θ of money in SRBTC. Then, the alternate price of P_{SRBTC} is $c_0 + c_1 * \theta * w_2$. Hence, its wealth in this scenario is $w_2^{**} = (1-d) * (1-\theta) * w_2 + \theta * w_2$. The wealth of party 1 in this scenario is $w_1^{**} = (1/2 * w_1) + (1/2 * w_1)/b_0 * (c_0 + c_1 * \theta * w_2 + b_0 + 1/2 * b_1 * w_1) = (1 + 1/2 * (c_0 + c_1 * \theta * w_2)/b_0) * w_1 + 1/4 * w_1^2 * b_1/b_0$. Thus, the relative wealth of party 2 is

$$\hat{w}_2^{**} = \frac{(1-d) * w_2 + \theta * d * w_2}{(1 + 1/2 * (c_0 + c_1 * \theta * w_2)/b_0) * w_1 + 1/4 * w_1^2 * b_1/b_0 + (1-d) * w_2 + \theta * d * w_2} \tag{3}$$

We need to show that the relative wealth in (2) is more than relative wealth in the alternate scenario (3). But, this is equivalent to $c_1 * w_2 > \frac{d}{1-d} * (2 * b_0 + c_0 + 1/2 * b_1 * w_1)$. □

Remark. Since, b_0 the current price of Bitcoin and c_0 are expected to be much much smaller than w_2 (which is the wealth of the world not invested in Bitcoin), the above criterion for c_1 can instead be stated as $c_1/b_1 > \frac{d}{1-d} * \frac{w_1}{2*w_2}$, which essentially hints that the dilution in the strategic reserve fork, which is well estimated by b_1/c_1, should be at least $\frac{2*w_2}{d*w_1}$ before investors not currently invested in BTC will be interested in investing in either fork. Thus, dilution should be inversely proportional to $1/d$, which makes sense since if d is negligible, there is no incentive to invest in SRBTC unless it is highly diluted so that relative wealth of investors not already in Bitcoin is maintained.

6 Bitcoin Replica vs Bitcoin Fork

In this section, we will consider competition between two variants of Bitcoin "forks", one as studied in earlier sections which is a legitimate fork that respects original BTC tokens 1:1 as SRBTC tokens in the forked chain, and second a brand new blockchain which is a replica of Bitcoin and in which the original Bitcoin tokens are not accepted. To model the competition between these two variants more accurately, in contrast to earlier sections, we will now assume that both variants have a similar incentive mechanism to attract investors. This incentive mechanism will be similar to the Bitcoin incentive mechanism where over time the reward per mining block decreases, and hence as there is lesser dilution as time goes by, it causes the price of BTC to go up. Without specifying how this mechanism is implemented, we will just model the price of BTC in the two variants as follows. Recall, in earlier sections we had modeled the starting price of token as an affine function of the net new investment, e.g. $c_0 + c_1 * W$. We had then assumed that for the rest of life of the blockchain these tokens just maintain their value (as a store of value). In this section we will assume that after the forking event and the setting of price at that event to be $c_0 + c_1 * W$, there is a second future epoch where the price goes up proportional to this investment W. Thus, the price at the second epoch will be modeled as $c_0 + c_1 * W + c_2 * W$. It is reasonable to make it linear in W, as one can expect that the early investment is actually spread out over time in multiple smaller intervals upto the second epoch.

For the Bitcoin Replica, which we will denote as RepBTC, its price will be modeled as $c_0 + c_1 * W + c_2 * W$ as well, that is with the exact same linear coefficients, thus making all things equal except for the fact that in this blockchain the original BTC tokens are worthless.

As in section 4, we will assume a set of individuals M, and for each individual i we will assume that π_i fraction of their wealth w_i is already invested in BTC. In contrast to section 4, we will now assume that all investors invest all their remaining wealth in either of the two options, i.e. SRBTC or RepBTC. We could make this investment a fraction of their wealth, but results will be more nuanced and less clearer to understand.

In this modeling, we will also assume that real high net worth individuals, wealth funds etc already have an alternate store of value such as Gold or land, and hence will only invest a small fraction of their wealth in the two options here. Thus, we will assume that for all individuals k, $\sqrt{\Omega * c_0/c_1} > \theta_k * (1-\pi_k) * w_k$, where $\Omega = \sum_{i \in M}(1-\pi_i) * w_i$ (i.e. the total wealth not in Bitcoin). Recall θ_k is the fraction that individual k will invest in these two options. For individuals, with non-huge net worth, we can even assume $\theta_k = 1$ in the below analysis. [4]

Lemma 3 *Focusing on $k \in M$ such that $\sqrt{\Omega * c_0/c_1} > \theta_k * (1-\pi_k) * w_k$, consider strategy of k where it invests all its θ_k fraction of remaining wealth, i.e. all of $\theta_k * (1-\pi_k) * w_k$, in SRBTC and zero in RepBTC. Then these strategies are in a Nash equilibrium.*

Proof: With the above strategy, the total investment in SRBTC is $\sum_{j \in M}(1-\pi_j) * w_j$, which we denote by Ω. Thus, the price of SRBTC at the first epoch is $c_0 + c_1 * \Omega$, and its price at the second epoch is $c_0 + (c_1 + c_2) * \Omega$. Thus, whatever is invested at epoch one has a value at epoch two that is a multiple $(1 + \frac{c_2 * \Omega}{c_0 + c_1 * \Omega})$ of the investment. Hence i's wealth at the second epoch is

$$w_i^* = \pi_i * w_i / b_0 * (c_0 + (c_1 + c_2) * \Omega) + (1-\pi_i) * w_i * \left(1 + \frac{c_2 * \Omega}{c_0 + c_1 * \Omega}\right)$$

The individual k's relative wealth at the second epoch is

$$\hat{w}_k^* = \frac{\pi_k * w_k / b_0 * (c_0 + (c_1 + c_2) * \Omega) + (1-\pi_k) * w_k * \left(1 + \frac{c_2 * \Omega}{c_0 + c_1 * \Omega}\right)}{\sum_i \pi_i * w_i / b_0 * (c_0 + (c_1 + c_2) * \Omega) + (1-\pi_i) * w_i * \left(1 + \frac{c_2 * \Omega}{c_0 + c_1 * \Omega}\right)} \tag{4}$$

Now suppose that individual k invests all its money in RepBTC instead. Then the total investment in RepBTC is $(1-\pi_k) * w_k$, and hence its price at the first epoch is $c_0 + c_1 * (1-\pi_k) * w_k$, and its price at the second epoch is $c_0 + (c_1 + c_2) * (1-\pi_k) * w_k$. Thus an investment made at the first epoch has value a multiple $1 + \frac{c_2 * (1-\pi_k) * w_k}{c_0 + c_1 * (1-\pi_k) * w_k}$ larger. Let $\Omega_k = \Omega - (1-\pi_k) * w_k$. Thus, in this scenario, k's wealth at epoch two is $\pi_k * w_k / b_0 * (c_0 + (c_1 + c_2) * \Omega_k) + (1-\pi_k) * w_k * \left(1 + \frac{c_2 * (1-\pi_k) * w_k}{c_0 + c_1 * (1-\pi_k) * w_k}\right)$. The wealth of all other individuals is same as before except for Ω replaced by Ω_k. In otherwords, now w_i^* is

$$w_i^* = \pi_i * w_i / b_0 * (c_0 + (c_1 + c_2) * \Omega_k) + (1-\pi_i) * w_i * \left(1 + \frac{c_2 * \Omega_k}{c_0 + c_1 * \Omega_k}\right)$$

Then, the new w_k^* differs from this by $\delta = (1-\pi_k) * w_k * \frac{-c_0 * c_2}{c_1 * (c_0 + c_1 * (1-\pi_k) * w_k)}$, assuming $c_0 \ll c_1 * \Omega_k$.

[4] Recall, By Lemma 2, c_1 must be $\frac{d}{1-d} * \frac{1}{w_2} * (2 * b_0 + c_0 + 1/2 * b_1 * w_1)$ for investors not in Bitcoin to be interested in SRBTC. Here we can interpret $w_1 = \sum_{i \in M: \pi_i > \Psi}(1-\pi_i) * w_i$, which we will just approximate as $1/2 * \sum_{i \in M} \pi_i * w_i$ and $w_2 = \sum_{i \in M: \pi_i < \Psi}(1-\pi_i) * w_i \approx \Omega$. Also, a good estimate of b_1 is that $b_1 * \sum_i \pi_i * w_i \approx b_0$, so $b_1 * 1/2 * w_1 \approx b_0$. Thus, we have $c_1 < \frac{d}{1-d} * \frac{1}{\Omega}(2 * b_0 + c_0 + b_0)$, or $c_1 * \Omega < d * (3 * b_0 + c_0)$. Assume $b_0 = 10 * c_0$, so we get $c_1 * \Omega < 31 * d * c_0$, or $c_0 / c1 > \Omega / (d * 31)$. Thus, $\sqrt{\Omega * c_0/c_1} > \Omega / \sqrt{d * 31}$. Thus, for $d < 1/2$, $\sqrt{\Omega * c_0/c_1} > \Omega/4$.

Hence, the alternate relative wealth of k is

$$\hat{w}_k^{**} = \frac{\delta + \pi_k * w_k/b_0 * (c_0 + (c_1 + c_2) * \Omega_k) + (1 - \pi_k) * w_k * \left(1 + \frac{c_2 * \Omega_k}{c_0 + c_1 * \Omega_k}\right)}{\delta + \sum_i \pi_i * w_i/b_0 * (c_0 + (c_1 + c_2) * \Omega_k) + (1 - \pi_i) * w_i * \left(1 + \frac{c_2 * \Omega_k}{c_0 + c_1 * \Omega_k}\right)} \tag{5}$$

Again, we need to show that $\hat{w}_k^* \geq \hat{w}_k^{**}$. Since $c_0 \ll c_1 * \Omega$ and $c_0 \ll c_1 * \Omega_k$, we can simplify both expressions by replacing $c_0 + c_1 * \Omega$ by $c_1 * \Omega$ etc. Thus, (5) simplifies as

$$\hat{w}_k^{**} = \frac{\delta + \pi_k * w_k/b_0 * (c_0 + (c_1 + c_2) * \Omega) + (1 - \pi_k) * w_k * (1 + c_2/c_1 - \tau_k)}{\delta + \sum_i \pi_i * w_i/b_0 * (c_0 + (c_1 + c_2) * \Omega_k) + (1 - \pi_i) * w_i * (1 + c_2/c_1)} \tag{6}$$

where $\tau_k = \pi_k * w_k/b_0 * (c_1 + c_2)$. Thus, we need to show

$$\begin{aligned} & \frac{\delta - (1 - \pi_k) * w_k * (c_1 + c_2)/b_0 * \sum_i \pi_i * w_i}{\sum_i \pi_i * w_i/b_0 * (c_0 + (c_1 + c_2) * \Omega_k) + (1 - \pi_i) * w_i * (1 + c_2/c_1)} \\ > & \frac{\delta - \tau_k * (1 - \pi_k) * w_k}{\pi_k * w_k/b_0 * (c_0 + (c_1 + c_2) * \Omega) + (1 - \pi_k) * w_k * (1 + c_2/c_1)} \end{aligned}$$

Since δ is negative, this is better written as

$$\begin{aligned} & (-\delta + \tau_k * (1 - \pi_k) * w_k) * \left(\sum_i \pi_i * w_i/b_0 * (c_0 + (c_1 + c_2) * \Omega_k) + (1 - \pi_i) * w_i * (1 + c_2/c_1)\right) \\ > & \left(-\delta + (1 - \pi_k) * w_k * (c_1 + c_2)/b_0 * \sum_i \pi_i * w_i\right) * \\ & \quad (\pi_k * w_k/b_0 * (c_0 + (c_1 + c_2) * \Omega) + (1 - \pi_k) * w_k * (1 + c_2/c_1)) \\ & + \quad (1 - \pi_k) * w_k * (c_1 + c_2)/b_0 * \sum_i \pi_i * w_i \end{aligned}$$

which is equivalent to

$$\begin{aligned} & (-\delta) * \left(\sum_i \pi_i * w_i/b_0 * (c_0 + (c_1 + c_2) * \Omega_k) + (1 - \pi_i) * w_i * (1 + c_2/c_1)\right) \\ & + (\tau_k * (1 - \pi_k) * w_k) * \left(\sum_i \pi_i * w_i/b_0 * (c_0 + (c_1 + c_2) * \Omega_k) + (1 - \pi_i) * w_i * (1 + c_2/c_1)\right) \\ > & (-\delta) * \quad (\pi_k * w_k/b_0 * (c_0 + (c_1 + c_2) * \Omega) + (1 - \pi_k) * w_k * (1 + c_2/c_1)) \\ & + \left((1 - \pi_k) * \tau_k/\pi_k * \sum_i \pi_i * w_i\right) * \\ & \quad (1 + \pi_k * w_k/b_0 * (c_0 + (c_1 + c_2) * \Omega) + (1 - \pi_k) * w_k * (1 + c_2/c_1)) \end{aligned}$$

which again simplifies as

$$\begin{aligned}
&(-\delta) * \left(\Omega * (1 + c_2/c_1) + \sum_i \pi_i * w_i/b_0 * (c_0 + (c_1 + c_2) * \Omega_k)\right) \\
&+ (\tau_k * (1 - \pi_k) * w_k) * \Omega * (1 + c_2/c_1) \\
> \ &(-\delta) * \ \ (\pi_k * w_k/b_0 * (c_0 + (c_1 + c_2) * \Omega) + (1 - \pi_k) * w_k * (1 + c_2/c_1)) \\
&+ \left((1 - \pi_k) * w_k * (c_1 + c_2)/b_0 * \sum_i \pi_i * w_i\right) * \ (1 + (1 - \pi_k) * w_k * (1 + c_2/c_1))
\end{aligned}$$

Let $\sum_i \pi_i * w_i = \mu * \Omega$. For example, currently for Bitcoin μ is at most $1/80$. We also expect c_2 to be same order as c_1, so for simplicity assume $c_1 = c_2$. Then, the above simplifies to

$$\begin{aligned}
&- \delta * (2 + \mu * (c_0 + 2 * c_1 * \Omega_k)/b_0 - 2 * c_1 * \pi_k * w_k/b_0) + 2 * (\tau_k * (1 - \pi_k) * w_k) \\
> \ &- \delta * \ \ (\pi_k * w_k/b_0 * c_0 + (1 - \pi_k) * w_k * 2)/\Omega \\
&+ ((1 - \pi_k) * w_k * 2 * c_1/b_0 * \mu) * \ (1 + (1 - \pi_k) * w_k * 2)
\end{aligned}$$

Since, $\mu * \Omega \geq \pi_k * w_k$ for any k, the above is implied by

$$\begin{aligned}
&- \delta * (2 + \mu * 2 * c_1 * \Omega_k/b_0 - 2 * c_1 * \pi_k * w_k/b_0) + 2 * (\tau_k * (1 - \pi_k) * w_k) \\
> \ &- \delta * (1 - \pi_k) * w_k * 2/\Omega \\
&+ ((1 - \pi_k) * w_k * 2 * c_1/b_0 * \mu) * \ (1 + (1 - \pi_k) * w_k * 2)
\end{aligned}$$

Expanding Ω_k we get

$$\begin{aligned}
&- \delta * (2 + \mu * 2 * c_1 * \Omega/b_0 - 2 * c_1 * \pi_k * w_k/b_0) + 2 * (\tau_k * (1 - \pi_k) * w_k) \\
> \ &- \delta * (1 - \pi_k) * w_k * (2/\Omega + 2 * \mu * c_1/b_0) \\
&+ ((1 - \pi_k) * w_k * 2 * c_1/b_0 * \mu) * \ (1 + (1 - \pi_k) * w_k * 2)
\end{aligned}$$

Now we expect $c_1 * \pi_k * w_k$ to be less than b_0 (the current price of BTC), noting that $c_1 * \pi_k * w_k$ is the effect on price of bitcoin by an individual investing $\pi_k * w_k$, i.e. amount equal to his/her current ownership of Bitcoin wealth. For the same reason, we can also say that $c_1 * \mu * \Omega = b_0$. Thus, the above is implied by

$$\begin{aligned}
&- \delta * 2 \\
> \ &- \delta * (1 - \pi_k) * w_k * (2 + 2)/\Omega \\
&+ ((1 - \pi_k) * w_k * 2 * c_1/b_0 * \mu) * \ (1 + (1 - \pi_k) * w_k * 2)
\end{aligned}$$

This will follow if $1 > (1 - \pi_k) * w_k * 4/(\Omega)$ and $-\delta > (1 - \pi_k) * w_k * c_1/b_0 * \mu * \ (1 + (1 - \pi_k) * w_k * 2)$. Now the first inequality holds unless there is an individual k such that its wealth (not invested in Bitcoin) is greater than $\Omega/4$, which is unlikely.

As for the second inequality, it is implied by

$$\frac{c_0}{c_0 + c_1 * (1 - \pi_k) * w_k} > \ c_1/b_0 * \mu * \ (1 + (1 - \pi_k) * w_k * 2)$$

Now, as argued earlier, $c_1 * \mu * \Omega = b_0$, so the right hand side is much smaller than one, essentially $(1 - \pi_k) * w_k * 2/\Omega$. Thus, as long as $c_1 * (1 - \pi_k) * w_k$ is not too large compared to c_0 (the premium in the price of SRBTC), this inequality holds. More precisely, the inequality holds for $c_0(\Omega - (1 - \pi_k) * w_k) > c_1 * ((1 - \pi_k) * w_k)^2$. Since $\Omega >> (1 - \pi_k) * w_k$, this is approximately same as $c_0 > c_1 * ((1 - \pi_k) * w_k)^2/\Omega$. □

References

[1] Kenneth J Arrow. An extension of the basic theorems on classical welfare economics. In *Proceedings of the Second Berkeley Symposium on Mathematical Statistics and Probability*, page 507—532. Berkeley & Los Angeles: University of California Press, 1951. 3

[2] Christian Badertscher, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas. Bitcoin as a transaction ledger: A composable treatment. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 324–356, 2017. 1

[3] Mihir Bellare, Juan Garay, Charanjit Jutla, and Moti Yung. Varietycash: A multi-purpose electronic payment system. Third Usenix Workshop on Electronic Commerce, 1998. 1

[4] David Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, California, USA, August 23-25, 1982*, pages 199–203, 1982. 1

[5] Cynthia Dwork and Moni Naor. Pricing via processing or combating junk mail. In *Proc. CRYPTO*, 1992. 1

[6] Charanjit Jutla and Moti Yung. Paytree: "amortized-signature" for flexible micropayments. Second Usenix Workshop on Electronic Commerce, Nov 1996. 1

[7] Charanjit S. Jutla. Inflation-tracking proof-of-work crypto-currencies. *IACR Cryptol. ePrint Arch.*, page 1605, 2021. 2

[8] Jonathan Levin. General equilibrium, 2006. `http://web.stanford.edu/~jdlevin/teaching.html`. 3

[9] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`, 2008. 1

[10] Tatsuaki Okamoto and Kazuo Ohta. Universal electronic cash. In Joan Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, volume 576 of *Lecture Notes in Computer Science*, pages 324–337. Springer, 1991. 1

[11] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2016. 1

[12] Ronald Rivest and Adi Shamir. Payword and micromint: : Two simple micropayment schemes. `https://people.csail.mit.edu/rivest/pubs/RS96b.pdf`, May 1996. 1

[13] Alfredo De Santis, Silvio Micali, and Giuseppe Persiano. Non-interactive zero-knowledge proof systems. In *Advances in Cryptology - CRYPTO '87, A Conference on the Theory and Applications of Cryptographic Techniques, Santa Barbara, California, USA, August 16-20, 1987, Proceedings*, pages 52–72, 1987. 1