A Trustless Bitcoin–backed Stablecoin

Version 0.95

October 2, 2017

Abstract

In this paper we describe how to build a blockchain-based, Bitcoin-backed "stablecoin" token whose price is tightly bound to the price of any chosen fiat currency in a way which is decentralized, trustless and permissionless to create. This paper explores the market mechanics of the token and explores the likely effects that would arise from its adoption. This token would represent a necessary bridge between the fiat and blockchain worlds and, aside from enhancing financial markets, may have the power to disrupt the control over money supply presently held by central banks — while driving up the price of the underlying blockchain asset (Bitcoin) in the process.

There is no direct commercial benefit for those who implement this concept; hence, this is envisioned to be a true community project.

1 Overview

1.1 Motivation

Recently, the world witnessed an innovation in decentralised payment systems and e-cash called Bitcoin. It has properties for which it is loved, such as:

- It cannot be censored or confiscated.
- It enables the transfer of arbitrary amounts of wealth around the world in a matter of seconds with no intermediaries.
- It can be used algorithmically in smart contracts which allows for complex interactions in a trustless way.[1]
- It promises enhanced levels of privacy and freedom.
- It cannot be devaluated by creating (printing) more of it.

The use of Bitcoin is growing. Its adoption, however, is hindered by its price volatility, which presently renders it a realtively poor medium of exchange and unit of account (desirable properties of sound money). Furthermore, points where Bitcoin touches the classical financial system are becoming increasingly subject to KYC/AML regulations and other legal restrictions. It was Friedrich Hayek's vision that, in a world of competing paper currencies (including those privately issued), the most price-stable relative to a basket of goods will be the most successful. In a cryptocurrency sense, this concept has been explored by a number of early projects in the field which use various methods to peg volatile crypto-assets to flexible, stable tokens known as "stablecoins".[2] However, the complex mechanics and widely varying incentive systems employed in existing projects, coupled with the present lack of an adequate Bitcoin smart-contract-based solution left us pondering a possible evolution upon the work of these pioneers.

We assume that the reader has a basic understanding of decentralised technologies, including blockchain, and is fully aware of their advantages and disadvantages. We do not assume any prior

[1] Technically this is becoming true only in the very near future with projects like Rootstock.

[2] Notable projects include MakerDao, BitShares, StableCoin, Nubits and Corion. Probably the most used token with a stable value is the centrally managed Tether (USDT) which is centralised and thus not trustless.

knowledge of possible "stablecoin" mechanisms.

In the paper we use, without the loss of generality, the notation bUSD for a blockchain-based token whose value is pegged to the US Dollar. However, the mechanism holds in general and can be used for any FIAT currency, or any other tradeable fungible commodity such as precious metals or even portfolios of such assets.[3]

1.2 Idea

The idea is to create a blockchain–based token, backed by Bitcoin, enabled by smart contracts, with a bounded value pegged to any chosen FIAT currency (such as USD). Such a token would bridge the gap between the FIAT and blockchain worlds because:

- It combines the stability of FIAT price levels with the properties of blockchain–based tokens listed in the previous section, which enables this token's use as a (probably) better medium of exchange than Bitcoin and introduces the possibility of using a blockchain token as a widely accepted unit of account.
- It frees the wealth of billions of people around the world which is presently being regulated by nation states by adding a blockchain layer between the flow of FIAT value and Bitcoin.
- If successful, it will cause substantial appreciation of the price of Bitcoin as it incentivises Bitcoin to be held rather than traded. This will reduce market supply and indirectly increase the demand for Bitcoin through people demanding the bUSD token for its unique properties.

1.3 Implications

The proposed system will create synergies, trust and stability.

- It is sufficient if only Bitcoin users use bUSD as a liquidity resource. This group of Bitcoin holders alone is large enough and needs to store enough value in FIAT equivalents to bring the idea to life.[4]
- It effectively makes negative interest rates and a war on cash unenforceable since bUSD is a new alternative to a bank account (where a negative interest rate can not be enforced). It combines the ease of storing and transferring digital money with the advantages of cash.
- With the rise of decentralised exchanges, bUSD can become the main instrument in BTC trading.
- By connecting many separated markets and allowing participants to move USD value quickly and easily amongst themselves, bUSD will help the market in attaining more efficient price discovery and reduced volatility.
- bUSD will allow the creation of many useful financial products in a trustless way.
- People who are introduced to bUSD and its advantages may be likely to subsequently become Bitcoin holders.
- bUSD can be the ideal (missing) bridge between the traditional world and Bitcoin world.

2 Core Idea

The bUSD token is created (minted) through a smart contract BBTF (Bitcoin–based Traded Fund), backed by Bitcoins which are locked into the BBTF by the minter (Bitcoin holder). The BBTF can be interacted with in three distinct ways:

[3] The mechanism depends on the volatility of the asset price denominated in Bitcoin.
[4] Note that current Tether (USDT) market cap is around $300M.

Minting Any Bitcoin holder (Alice or Bob) can send their Bitcoins to BBTF. BBTF locks in the received Bitcoins and creates (mints) new bUSD with a nominal value according to the current minting rate and sends it to the Bitcoin holder. If the minting rate increases in the future, the locked–in Bitcoin collateral becomes excessive and can be either used to mint more bUSD or released to the minter. (Described in Section 3.1).

Releasing of Bitcoin Collateral If the minter wants to release the locked–in Bitcoins, the amount of bUSD which was minted has to be sent to BBTF. BBTF destroys the received bUSD and releases the collateral. (Described in Section 3.2).

Claiming Backing Any bUSD holder can claim the nominal value on BBTF by sending his bUSD to BBTF. BBTF destroys received bUSD and subtracts the backing proportionally from all minters. The nominal value of the destroyed bUSD is paid to the holder in Bitcoins according to the actual claiming rate. This feature gives value to the token, but is not likely to be used very often. (Described in Section 3.3).

In Section 3.1 we explain that only a fraction of the value of the locked–in Bitcoins is admitted to be used to mint new bUSD with the remainder serving as collateral in the event of Bitcoin price depreciation, to ensure that the total supply of bUSD is adequately backed. Through this method, the minters maintain exposure to Bitcoin but are able to enjoy some of the future prosperity of its value now.

The possibility to claim backing guarantees bUSD a minimal value. That creates inherent value even in the first bUSD token minted. At the same time, the maximum value of the newly created token bUSD is bound by the mechanism of minting of new bUSD. The higher the demand for bUSD, the cheaper it is to mint new bUSD. The long–term value of bUSD should therefore converge to the nominal value of $1 as we explain in Section 5.

Furthermore, in Section 4 we explain different aspects of the BBTF from the Bitcoin holder's point of view.

2.1 Assumptions

We make only a few basic assumptions about the existence of needs which might be served by BBTF and about the demand for bUSD.

2.1.1 Assumptions about Bitcoin Holders

We assume the existence of Bitcoin holders who believe in the long–term price appreciation of Bitcoin and could use BBTF in two different use cases:

Alice , who prefers not to sell her Bitcoin, but from time to time needs to finance her consumption. Presently, her only option is to sell Bitcoins for FIAT currency, which she prefers not to do.

Bob , who has invested in Bitcoin. If he could leverage his Bitcoin exposure without spending more money, he would do so.

2.1.2 Assumptions about bUSD Demand

We assume the existence of people who desire a FIAT representation on blockchain. Presently, their main option is Tether (USDT), which is backed by USD holdings in a traditional bank. The downside is that both the Tether issuing company and the bank holding the backing have to be trusted. Tether is regulated by KYC/AML, which makes it harder to use in the unregulated Bitcoin world. Tether is also susceptible to further "crack–downs". [5]

2.2 Notation

B_t — **Bitcoin Spot Price** — Spot price of Bitcoin, as revealed to the BBTF smart contract by oracles.[6]

[5] E-gold, which was an electronic representation of gold was banned by the United States government, justified by money laundering risk. Liberty Dollar was shut down by US government for unclear reasons.

[6] For historical calculations we have used the data from https://data.bitcoinity.org/export_data.csv?c=e&currency=USD&data_type=price&r=day&t=l&timespan=all. In the smart contract implementation there must be a mechanism dictating how to agree on the worldwide spot price.

B_t^α — **Exponentially smoothed price** — Bitcoin's price exponentially smoothed so that it depends on price history. See Section 2.3.

$$B_t^\alpha = \alpha B_{t-1}^\alpha + (1-\alpha)B_t, \qquad t = 1, \dots, n$$
$$B_0^\alpha = B_0$$

bUSD — New "stablecoin" token based on Bitcoin blockchain with value pegged to USD.

BBTF — Smart contract which creates (mints) new bUSD backed by Bitcoin collateral.

P_t — **Market price of bUSD** — Market price bUSD token is traded at.

p_t — **Quality of backing** — Value of backing over nominal value of issued bUSD, capped at 1. This deems how much a bUSD holder will get if they claim backing. Under normal conditions $p_t = 1$. If the backing is insufficient, $p_t < 1$.

bUSD minter — Bitcoin holder who creates new bUSD by locking their Bitcoins into BBTF.

bUSD holder — Someone who holds bUSD. They may either sell bUSD on the market or claim the nominal value of their bUSD from BBFC (though this is not the intended use).

β — **Mintable Fraction** — For minting purposes, we use an exponentially smoothed heavily historically-dependent price of Bitcoin. We allow only a fraction β of the smoothed price to be used determine the amount of minted bUSD.

$\underline{B_t}$ — **Minting Rate** — Rate new bUSD are minted at, at time t.

$$\underline{B_t} = \beta \min(B_t, B_t^\alpha)$$

$\overline{B_t}$ — **Claiming Rate** — Rate at which bUSD holder can claim backing for his bUSD.

$$\overline{B_t} = \max(B_t, B_t^\delta)$$

E_t — **Exposure Extension** — Amount of exposure increase which a Bitcoin holder can attain using BBTF with one initial Bitcoin.

$$E_t = \frac{1}{1 - P_t \frac{\underline{B_t}}{\overline{B_t}}}$$

2.3 Price Smoothing

Bitcoin is a rather volatile asset and its price has experienced many wild moves. Since we want bUSD to be as useful as USD, we need to construct it in such a way that bUSD has sufficient backing so that its value never (or rarely) drops below $1. We anticipate Bitcoin's price to grow in the long-term, but this growth will likely be volatile, with periods of 'over-hyped' growth followed by corrections. If we exponentially smooth the price, we get a more stable (smooth) price function. We define the exponentially smoothed price of Bitcoin B_t^α as

$$B_t^\alpha = \alpha B_{t-1}^\alpha + (1-\alpha)B_t, \qquad t = 1, \dots, n$$
$$B_0^\alpha = B_0$$

The closer the smoothing factor α is to 1, the larger the weight of price history in determining the smoothed price. The extension to unevenly distributed frequencies of measurement is described in Appendix C and the choice for a possible smoothing parameter α is discussed in Appendix B.1. Keep in mind that smoothing is used to obtain a history–dependent price rather than time series modelling. Smoothing is used in the construction of BBTF twice: once in the minting rate with $\alpha = 0.99883$ and a second time in the claiming price with $\delta = 0.9$.

You can see the smoothed price in Pictures 1 and (zoomed–in) in 2. More details about the minting rate are contained in Section 3.1, where we explain that the minting rate is slightly more complicated than just a smoothed price (though price smoothing is the main component).

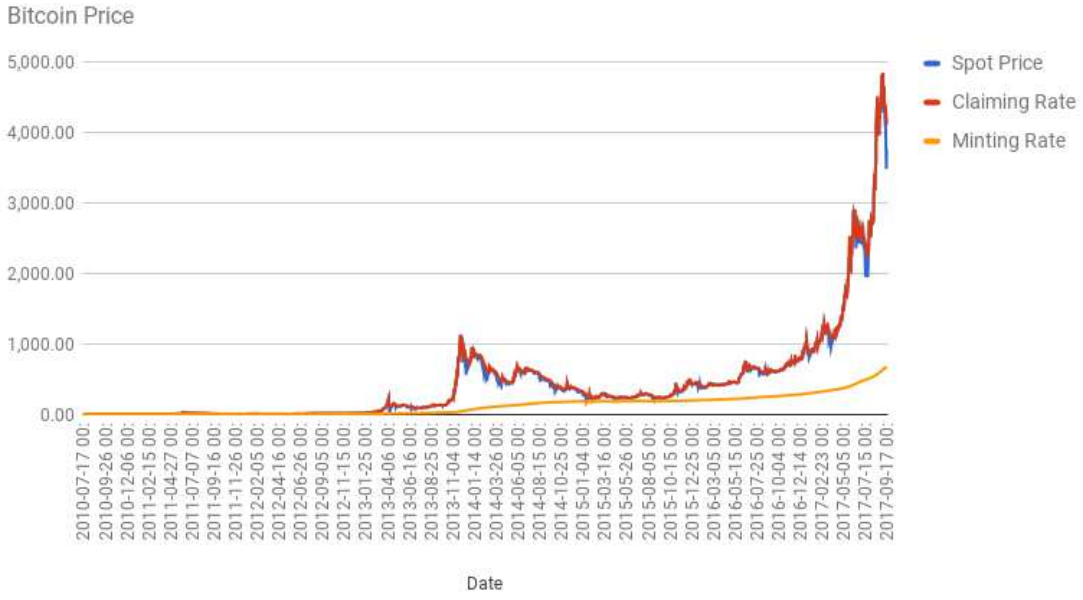

Figure 1: The smoothed Bitcoin price.

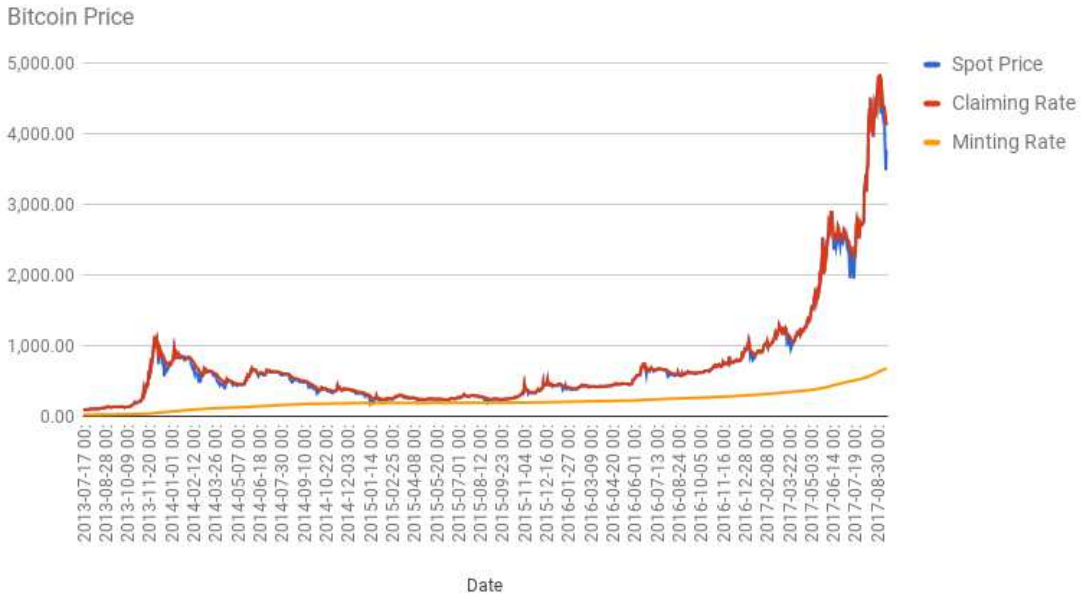

Figure 2: The zoomed smoothed Bitcoin price.

3 BBTF in Detail

BBTF can be used in three distinct ways:

- Minting bUSD by depositing Bitcoin as a collateral (backing) — see Section 3.1.
- Releasing locked–in collateral Bitcoins by depositing minted bUSD — see Section 3.2.
- Claming of backing by any bUSD holder — see Section 3.3.

3.1 The Creation of bUSD — Minting

Minting is the most important function of BBTF. Since the creation of new bUSD is executed via a smart contract, it is a trustless process which anyone can audit.

Any Bitcoin holder can send their Bitcoins to BBTF. BBTF locks in received Bitcoins as a collateral (backing for the newly minted bUSD), creates new bUSD according to the actual minting rate $\underline{B_t}$, and sends it back to the minter. This is the only way new bUSD is created. If Alice sends one Bitcoin to BBTF, she will end up with one Bitcoin locked into the BBTF and will possess $\underline{B_t}$ newly created units of bUSD.

If the minting rate increase in future, Alice can either ask BBTF to mint more bUSD on her existing locked–in Bitcoin collateral or to release the excessive part of her locked–in Bitcoin (since the higher minting rate means less Bitcoins are now required to mint (and back) the same amount of bUSD).

3.1.1 Minting Rate

In 2.3 we established why we have chosen a smoothed price for the minting rate and in Appendix B.1 we argue why we used the choice of smoothing parameter $\alpha = 0.99883$. In determining the minting rate we take the minimum of the smoothed price and spot price and, even then, only mint a fraction $\beta = 0.8$ of the available bitcoin, to ensure adequate backing. Hence, the minting rate is defined as

$$\underline{B_t} = \beta \min(B_t, B_t^{\alpha}) = 0.8 \min(B_t, B_t^{0.99883}). \tag{3.1}$$

Even though we have set conservative parameters, it is still possible that the backing could become insufficient. See 3.4 for a discussion of why even insufficient backing is not a problem. To get an idea what the minting rate would be during Bitcoin's history to date, see Table 3.

The Minting Rate is Increasing Almost All the Time

The construction of the minting rate has positive consequences. For the vast majority of the time, the Bitcoin spot price will be higher than the smoothed price and the minting rate will therefore be increasing. See that from

$$B_t > B_{t-1}^{\alpha}$$

follows

$$\begin{aligned}
\underline{B_t} &= \beta \min(B_t, B_t^{\alpha}) \\
&= \beta \min(B_t, \alpha B_{t-1}^{\alpha} + (1-\alpha) B_t) \\
&= \beta(\alpha B_{t-1}^{\alpha} + (1-\alpha) B_t) \\
&> \beta(\alpha B_{t-1}^{\alpha} + (1-\alpha) B_{t-1}^{\alpha}) \\
&= \beta B_{t-1}^{\alpha} \\
&\geq \beta \min(B_{t-1}, B_{t-1}^{\alpha}) = \underline{B_{t-1}}
\end{aligned}$$

Hence, the minting rate will be increasing almost all the time in quite a predictable manner and minters will know what to expect in the near future.

The minting rate will decrease if, and only if,

$$B_t < B_{t-1}^{\alpha} \qquad \& \qquad B_t < B_{t-1}.$$

That is, if the Bitcoin price drops so low that it goes below the long–term smoothed price, which is very conservative and has never happened in its recorded history.

3.1.2 Bitcoin Exposure Extension

Bob can use BBTF to extend his Bitcoin exposure. Let us compute what Bob can obtain if he continually repeats the following:

1. Lock free BTC into BBTF and mint new bUSD.
2. Sell received bUSD on market for BTC.
3. Repeat steps 1 and 2.

Initially, Bob has one BTC. He sends it to BBTF and receives $\underline{B_t}$ of bUSD units worth $P_t\underline{B_t}$ on the market. He use it to buy

$$\frac{P_t\underline{B_t}}{B_t}$$

additional Bitcoins, which he again uses to mint more bUSD. In general, in the k-th round he mints

$$\left(\frac{P_t\underline{B_t}}{B_t}\right)^{k-1}\underline{B_t}$$

units of bUSD, which he sells on the market for Bitcoins and gets

$$\left(\frac{P_t\underline{B_t}}{B_t}\right)^{k}$$

new Bitcoins. If Bob keeps doing this indefinitely, he will end up with (including his initial 1 BTC)

$$E_t = E(\underline{B_t}, B_t, P_t) = \sum_{k=0}^{\infty}\left(\frac{P_t\underline{B_t}}{B_t}\right)^{k} = \frac{1}{1 - P_t\frac{\underline{B_t}}{B_t}} \tag{3.2}$$

Bitcoins and will create $\underline{B_t}E_t$ units of bUSD. Let us give the label E_t to the exposure extension — how much Bob can extend his BTC exposure by if he uses BBTF to its maximum extent. Of course, Bob does not need to perform the infinite process. He can simply borrow the BTC difference between E_t and his one initial BTC, mint the new bUSD, sell it on the market for BTC (for the same amount he needed to borrow in the beginning) and return it.[7]

It must be noted that building extended exposure is not free profit. It is essentially borrowing FIAT currency (albeit without interest) and investing the borrowed dollars into Bitcoin. Bob's net wealth at the current valuation remains the same. He either has one Bitcoin or uses it to build an extended exposure of E_t while minting $\underline{B_t}E_t$ bUSD, which he will have to obtain at some point in the future to be able to release his Bitcoins. His net wealth in both cases is the same, but the exposure and value dynamics have changed to depend more on Bitcoin. Hence, if Bitcoin appreciates in the future, Bob's wealth will increase faster than if he did not extend his exposure (and vice versa).

Let us examine in detail what influences the extended exposure in (3.2). Note that the crucial component is

$$P_t\frac{\underline{B_t}}{B_t} \tag{3.3}$$

As soon as (3.3) grows to 1, the exposure extension goes to ∞. If it passes 1, Bob would be earning free, riskless money by minting since he would be able to sell the minted bUSD for more Bitcoins than he needed for minting it. It also means that the smaller the ratio between the minting rate and the spot price, the bigger the extension that can be built. In other words, in times when Bitcoin's price is stable or has decreased (and therefore the smoothed price gets closer to the spot price), one can build a bigger Bitcoin exposure. Also, the higher the market price P_t, the bigger the extension. Hence, there is motivation to mint more bUSD when the market price P_t is higher, which plays important role in the market dynamics which we will explore in Section 5.

[7] There could be a service offering to build this exposure for minters. See Appendix D.1.3.

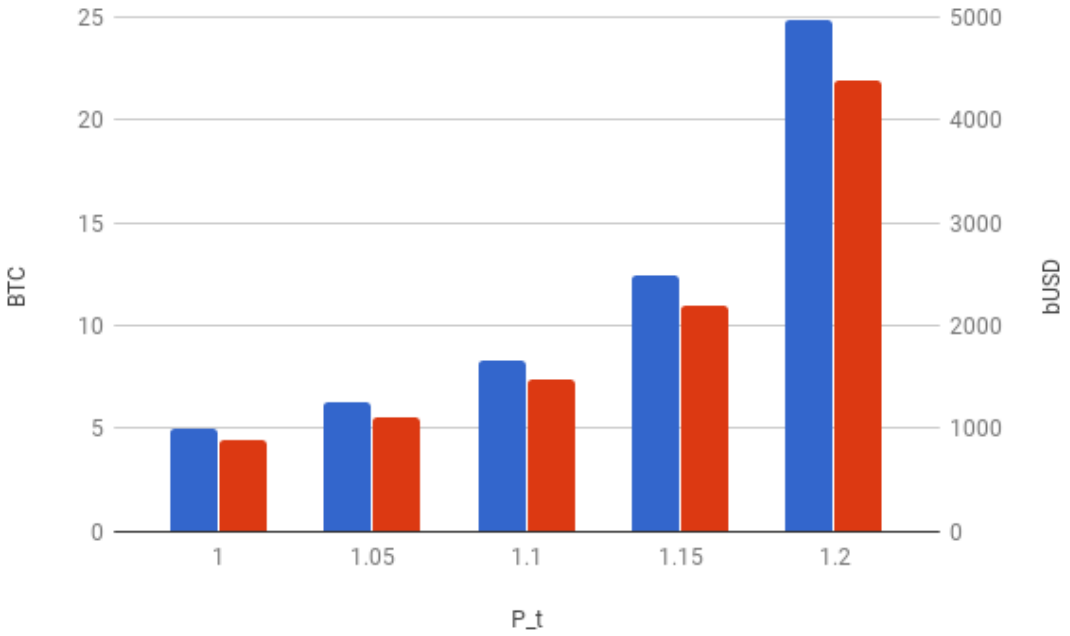

Figure 3: The Bitcoin holdings and bUSD created on 2015-02-01.

3.1.3 Example

Let us follow a hypothetical example using historical price data (see Table 3). The best possible time to build an extended Bitcoin position was on 2015-02-01 when the spot price fell to the level of the long–term smoothed price. Then

$$E_t = \frac{1}{1 - P_t \frac{B_t}{\underline{B_t}}} = \frac{1}{1 - 0.8 P_t}$$

P_t	E_t	$\underline{B_t} E_t$
1.00	5.00	883
1.05	6.25	1104
1.10	8.33	1472
1.15	12.50	2208
1.20	25.00	4415

Table 1: Bitcoin holdings and bUSD created on 2015-02-01.

In Table 1 and Figure 3, one can see that the exposure extension goes up very steeply and, at only $P_t = 1.25$, it explodes. [8]

As another example, we have chosen the recent date 2017-07-01 when $\underline{B_t}/B_t \approx 0.19$. The dynamics seen in Table 2 and Figure 4 show that it grows much more slowly than on 2015-02-01 and explodes only around the value $P_t \approx 5.3$.

3.2 Releasing the Collateral

Bob, who used BBTF to mint bUSD, has a contract with BBTF. His Bitcoin holdings are locked into BBTF and he has minted some amount of bUSD, which he can spend at his will. BBTF keeps records regarding how many Bitcoins each minter locked in and how much bUSD was minted. If the minting rate increases over time, one would need fewer Bitcoins to mint the same amount of bUSD

[8] As the market price approaches 1.25, the exposure extension growths to infinity. If market price hits 1.25, the minter is able to extend his exposure for free or even earn money.

P_t	E_t	$\underline{B_t E_t}$
1.0	1.23	572
1.5	1.40	648
2.0	1.61	747
2.5	1.90	881
3.0	2.31	1074
3.5	2.96	1375
4.0	4.17	1910
4.5	6.74	3129
5.0	18.64	8648

Table 2: The Bitcoin holdings and bUSD created on 2017-07-01.

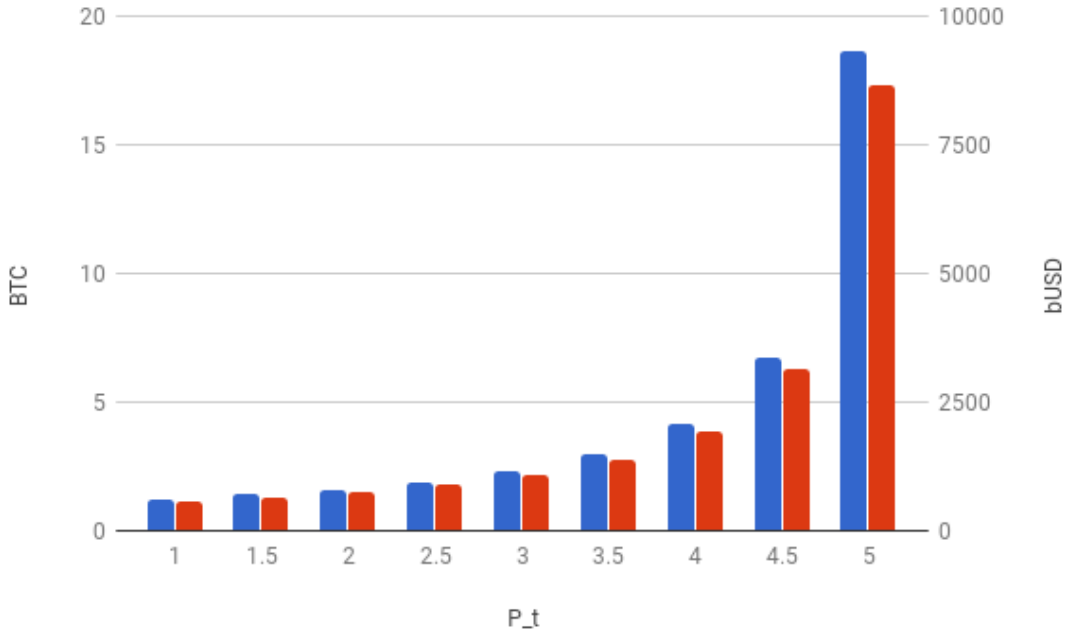

Figure 4: The Bitcoin holdings and bUSD created on 2017-07-01.

than when Bob minted his bUSD. Hence, part of Bob's locked–in Bitcoins becomes excessive and Bob can either ask BBTF to mint more bUSD using the existing locked–in Bitcoins (the excessive part) or he can ask for the excessive part of the backing to be released.

If, for whatever reason, Bob wants his locked–in Bitcoins back, he needs to obtain the exact amount of bUSD which he minted in past. Then, Bob needs to send bUSD to BBTF with a request to release his locked–in Bitcoins. BBTF destroys the received bUSD and sends Bob's originally locked–in Bitcoins back to him. Any relationship between Bob, the bUSD and BBTF disappears. If Bob only sends some fraction of his minted bUSD, he will only release a portion of his locked–in Bitcoins.

3.3 Backing and Claiming the Backing

The backing of bUSD creates the foundation of trust and value of bUSD in the first place. The parameters of the backing are designed (based on historical prices) in such a way that the value of the backing would be always higher than the nominal value of minted bUSD. Backing can be either released back to the minter (see Section 3.2) or claimed by any bUSD holder. This is not the intended use of bUSD, rather it is something which gives value to bUSD. If a bUSD holder wants Bitcoin for their bUSD, they should sell it on the open market for Bitcoin rather than claim any backing. They would probably get a slightly better price thanks to the construction of the

claiming rate.

3.3.1 Claiming Rate

In the case of backing claims, we want to ensure (to the fullest extent possible) price stability and we also want to hedge against temporary flash–crashes or any sudden panic in the market. For claiming purposes, we use a smoothed price with a different smoothing factor δ which utilises a much smaller historical weighting than for the minting rate. We get a smoothed price B_t^δ and define the claiming rate as

$$\overline{B_t} = \max(B_t, B_t^\delta) \tag{3.4}$$

We think that the value $\delta = 0.9$ works well for our purposes. Furthermore, in Appendix B.1, we show that the difference between the claiming rate and the spot rate would flatten out very quickly - in a matter of days. Hence, any rational actor would rather wait a couple days to get more for their money as soon as there is no immediate risk of insufficient backing.

Note that anytime that the backing is claimed only the required part of the backing is accounted for according to the actual minting rate. Any excessive backing held in BBTF is excluded from being used for claiming payouts.

3.3.2 Quality of Backing

Let us define the quality of the backing p_t. Let C_t be the total locked–in Bitcoins in BBTF (excluding all excessive backing) and M_t be the total amount of minted bUSD in circulation. The overall collateral value for claiming purposes is then

$$C_t \overline{B_t}$$

Now let us define the quality of backing p_t as

$$p_t = \min\left(1, \frac{C_t \overline{B_t}}{M_t}\right)$$

In other words, p_t tells us how well is bUSD backed. If $p_t = 1$, bUSD is perfectly backed and any claimer will receive a full face value payout. If $p_t < 1$, the backing is insufficient.

If some bUSD holder claims 1 bUSD, he will get

$$\frac{p_t}{\overline{B_t}} \qquad \text{in Bitcoin}$$

, which is worth

$$p_t \frac{B_t}{\overline{B_t}} \qquad \text{in \$.}$$

If, and only if, bUSD is sufficiently backed ($p_t = 1$), and Bitcoin's price is stable or growing ($\overline{B_t} = B_t$), the claimer will get a full \$1 for his 1 bUSD.

At anytime anyone can observe the total amount of bUSD minted, the amount of Bitcoins held as collateral and the quality of the backing. Keep in mind that it is not rational to claim backing if bUSD is traded on the market with any premium over its claimable value ($P_t > p_t$). A rational bUSD holder gets a better price on the market by selling bUSD for BTC rather than by claiming backing.

3.3.3 Distribution of Claimed Amounts

Any claimed bUSD backing is subtracted proportionally (based on the percentage of their backing against the overall locked–in backing, excluding any excessive backing) from all minters. Similarly, the claimed (and destroyed) amount is subtracted from all minters proportionally based on minted balances. Since the minting rate is increasing almost all the time, minters' proportion of backing is usually same as their proportion of minted bUSD. The two proportions differ only when the minting rate is not at its maximum, in which case the early minters (who received a better minting

Date	B_t	$\underline{B_t}$	$\overline{B_t}$	fm$\overline{B_t}$	Date	B_t	$\underline{B_t}$	$\overline{B_t}$	fm$\overline{B_t}$
2010-08-01	0.06	0.04	0.06	0.06	2014-02-01	830.67	82.76	830.67	229.87
2010-09-01	0.06	0.04	0.06	0.06	2014-03-01	564.76	96.63	595.56	229.87
2010-10-01	0.06	0.04	0.06	0.06	2014-04-01	479.03	110.09	548.93	229.87
2010-11-01	0.19	0.04	0.19	0.18	2014-05-01	453.92	119.05	467.02	229.87
2010-12-01	0.22	0.05	0.26	0.23	2014-06-01	643.39	128.77	643.39	229.87
2011-01-01	0.30	0.05	0.30	0.29	2014-07-01	649.66	141.30	649.66	229.87
2011-02-01	0.68	0.06	0.68	0.68	2014-08-01	590.36	153.85	601.71	229.87
2011-03-01	0.92	0.08	0.92	0.77	2014-09-01	483.37	163.62	514.72	229.87
2011-04-01	0.78	0.11	0.82	0.77	2014-10-01	384.97	170.23	419.08	229.87
2011-05-01	3.33	0.14	3.33	2.61	2014-11-01	330.73	174.50	359.27	229.87
2011-06-01	9.03	0.31	9.03	2.61	2014-12-01	379.29	178.63	379.29	229.87
2011-07-01	17.51	0.80	17.51	2.61	2015-01-01	317.27	181.98	327.19	229.87
2011-08-01	13.23	1.18	13.91	2.61	2015-02-01	220.83	176.66	242.72	229.87
2011-09-01	8.23	1.42	9.81	2.61	2015-03-01	252.35	182.81	252.35	230.19
2011-10-01	4.99	1.54	5.54	2.61	2015-04-01	245.68	183.98	257.51	230.19
2011-11-01	3.18	1.59	3.35	2.61	2015-05-01	236.12	184.12	236.12	230.19
2011-12-01	3.14	1.61	3.14	2.78	2015-06-01	227.24	181.79	235.44	230.19
2012-01-01	4.94	1.65	4.94	4.86	2015-07-01	258.89	184.55	258.89	233.48
2012-02-01	5.72	1.77	5.87	4.86	2015-08-01	282.04	185.95	282.86	233.48
2012-03-01	4.94	1.85	4.95	4.86	2015-09-01	229.38	183.51	237.34	233.48
2012-04-01	4.84	1.92	4.86	4.86	2015-10-01	237.83	186.53	237.83	237.83
2012-05-01	4.96	1.99	5.03	5.01	2015-11-01	316.51	187.51	316.51	316.51
2012-06-01	5.18	2.07	5.18	5.15	2015-12-01	366.01	190.69	366.01	357.16
2012-07-01	6.54	2.16	6.54	6.50	2016-01-01	428.94	196.06	430.54	382.98
2012-08-01	9.44	2.31	9.44	9.44	2016-02-01	375.65	200.75	394.30	382.98
2012-09-01	10.07	2.54	10.68	10.55	2016-03-01	434.12	204.84	434.12	413.46
2012-10-01	12.29	2.77	12.29	10.90	2016-04-01	413.77	209.36	415.17	415.17
2012-11-01	11.15	3.01	11.19	10.90	2016-05-01	450.49	214.09	450.49	446.12
2012-12-01	12.50	3.22	12.50	12.50	2016-06-01	524.54	219.62	524.54	524.54
2013-01-01	13.38	3.48	13.38	13.26	2016-07-01	671.87	229.64	671.87	581.59
2013-02-01	20.60	3.81	20.60	20.06	2016-08-01	619.90	240.15	650.77	581.59
2013-03-01	33.87	4.36	33.87	33.55	2016-09-01	580.94	248.11	582.43	582.43
2013-04-01	97.87	5.90	97.87	84.10	2016-10-01	614.11	256.32	614.11	612.71
2013-05-01	129.11	9.26	129.11	84.10	2016-11-01	721.21	265.59	721.21	698.43
2013-06-01	125.70	12.29	125.70	84.10	2016-12-01	749.92	276.63	749.92	749.92
2013-07-01	89.21	14.72	98.46	84.10	2017-01-01	960.50	290.42	960.50	869.55
2013-08-01	98.80	16.66	98.80	95.35	2017-02-01	963.59	305.85	963.59	963.59
2013-09-01	133.09	19.09	133.09	119.33	2017-03-01	1202.99	323.37	1202.99	1064.20
2013-10-01	128.24	21.94	128.24	125.82	2017-04-01	1061.23	343.94	1064.20	1064.20
2013-11-01	202.22	25.61	202.22	202.22	2017-05-01	1399.85	366.10	1399.85	1399.85
2013-12-01	980.51	40.05	980.51	229.87	2017-06-01	2308.19	406.69	2308.19	2308.19
2014-01-01	752.79	61.05	752.79	229.87	2017-07-01	2451.82	464.05	2523.37	2334.69

Table 3: Bitcoin Spot Price, Minting Rate, Claiming Rate and Future Minimum Claiming Rate.

rate) profit from the situation.[9] The subtraction from both the minters' backing and their overall minted amount means that part of their backing will likely become excessive (unless they minted at a higher minting rate and therefore the part of the backing that would otherwise become excessive would still be below the required backing at the current minting rate).

Claiming while the minting rate is at its maximum We assume Alice has 1 Bitcoin and Bob has 2 Bitcoins locked–in as collateral at minting rate $\underline{B_t} = 500$. Hence, Alice minted 500 bUSD and Bob, 1 000 bUSD. Let's say some bUSD holder claims 500 bUSD at a claiming rate of

[9]Remember that minting rate is an (generally) increasing function and the described exception can only happen if the spot price were to drop below the long–term smoothed price and the volatility of the price decrease with the maturing Bitcoin market. See Section 3.1.1 for more.

$\overline{B_t} = 3000$. The claimer receives a Bitcoin payout of

$$\frac{500}{3000} = \frac{1}{6} \quad \texttt{BTC}.$$

Alice and Bob both minted at the same minting rate and therefore the ratio of their respective minted amounts is equivalent to the ratio of their locked–in backing, i.e. 1:2. Hence, the 500 claimed bUSD and the paid out Bitcoin payment (1/6 BTC) are both divided in the of ratio 1:2 between Alice and Bob. In Table 4 we can see that Alice's backing has decreased from 1 BTC to

	Alice	Bob	Total BBTF
BTC	1	2	3
bUSD	500	1000	1500

-500 bUSD claim paid out as $\frac{1}{6}$ BTC

BTC	0.94	1.89	2.83
bUSD	333.33	666.67	1000
Excess	0.27	0.56	

Table 4: Bitcoin claiming example while the minting rate is at its maximum.

0.94 BTC and her minted amount has decreased from 500 to 333.33 bUSD. The required backing for the 333.33 bUSD minted is only 0.67 BTC. Therefore, 0.27 of the locked–in BTC is excessive and Alice can withdraw it or use it to mint new bUSD - similarly for Bob.

Claiming when the minting rate has dropped If Bitcoin's price were to drop so much that the minting rate decreases, the claiming process might be a bit different. We assume that Alice has locked in 1 BTC and has minted at a minting rate of 500 (spot price around \$3 000). Subsequently, the price of BTC drops to \$500. The new minting rate would be $\underline{B_t} = 0.8 \times 500 = 400$. Meanwhile, Bob has locked in 4 BTC and has minted 1 600 new bUSD. There are 5 Bitcoins locked

	Alice	Bob	Total BBTF
BTC	1	4	5
bUSD	500	1600	2100
$\underline{B}$.	500	400	

-500 bUSD claim paid out as 1 BTC

BTC	0.8	3.2	4
bUSD	380.95	1219.05	1600
Excess.	0	0.15	

Table 5: Bitcoin claiming example after a drop in Bitcoin's price.

into BBTF and a total of 2 100 minted bUSD. Since the spot price (and the claiming rate) is \$500, the bUSD is still perfectly hedged ($p_t = 1$). If someone were to claim 500 bUSD, they would get a payout of 1 BTC. As can be seen in Table 5 the 1 BTC payout is divided between Alice and Bob according the ratio of the locked–in Bitcoins, i.e. 1:4. However, the 500 of claimed bUSD is subtracted from their minted balances in a ratio of 5:16. As can be seen in Table 5 only part of Bob's backing became excessive. All of Alice's backing is required.

3.4 Why Insufficient Backing is not a Problem

Under normal conditions — when bUSD is sufficiently backed ($p_t = 1$), the value of the claimable backing creates the natural lower bound for the market value of bUSD

$$P_t \geq p_t$$

If $p_t < 1$, it simply means that the lower bound for the market value of bUSD decreases, in which case bUSD could potentially be less than \$1. Of course, it is possible for the market value to remain above or close to \$1 even while not completely backed.

In following paragraphs we show that:

- Everyone who mints while the backing is insufficient improves the quality of the overall backing.
- Minting while backing is insufficient or close to insufficient is profitable. Hence, there is extra incentive to improve the backing if there is a risk of insufficient backing.
- Pure expectations of improvement in the quality of backing will manifest in the price. That makes claiming irrational since $P_t > p_t$ and also makes minting even more profitable. Therefore the quality of backing improves even faster.

In summary, as long as Bitcoin does not lose all its value, the insufficient backing is not a problem and should fix itself quickly. It is entirely possible that the market price P_t will therefore remain close to \$1 even while insufficiently backed.

3.4.1 Minting during Insufficient Backing

If bUSD backing is insufficient, it means that the current spot price is below its long–term smoothed price ($B_t^\alpha > B_t$) and hence the minting rate is

$$\overline{B_t} = \beta \min(B_t, B_t^\alpha) = \beta B_t = 0.8 B_t.$$

If Bob, as a Bitcoin holder, mints new bUSD under these circumstances, the amount of bUSD able to be minted from 1 Bitcoin is more than in the case of sufficient backing, since the long–term smoothed price (and hence minting rate) is usually much lower than the spot price. Bob can use this situation to immediately build an extended Bitcoin exposure of

$$E_t = \frac{1}{1 - P_t \frac{B_t}{\overline{B_t}}} = \frac{1}{1 - 0.8 P_t}$$

Of course, this situation depends on the price P_t for which the minter can probably sell his minted bUSD.

If P_t is close to, or above, \$1, the situation is especially favorable since Bob can build an extended exposure of

$$E_t = \frac{1}{1 - 0.8} = 5$$

Bitcoins from his 1 initial Bitcoin and will improve the quality of the backing while doing it. This should further motivate other Bitcoin holders to build a substantially larger exposure to Bitcoin. This also creates buy-pressure on Bitcoin which again helps the stability and robustness of the system.

If P_t is well below \$1, the situation is not as advantageous. If $P_t = \$0.2$, the extended exposure would be

$$E_t = \frac{1}{1 - 0.16} \approx 1.2.$$

If any Bitcoin holder exists who believes that Bitcoin will rebound and is interested in building an extended exposure (in this case, 1.2 instead of 1 Bitcoin), they will mint new bUSD.

In fact, as soon as there is reason to expect that the bUSD backing quality is going to improve back to 1 ($p_t \uparrow 1$) with a high probability, any rational actor would want to buy bUSD when it is priced well below \$1 in order to realise a profit as soon as the backing improves, creating a self–fulfilling slingshot upwards in the price. If market participants know that the bUSD backing will improve over time provided Bitcoin does not lose all its value, that knowledge alone should be sufficient to keep the value of P_t within the neighbourhood of \$1, even while insufficiently backed.

Furthermore, if the use of BBTF is attractive enough under insufficient backing for any Bitcoin holder to mint new bUSD, they are going to automatically improve the quality of backing. This is because through minting they lock in more Bitcoin value than newly minted bUSD. That improved backing quality will, in turn, make BBTF sufficiently attractive to further Bitcoin holders to mint new bUSD, which will again improve the quality of backing. This cycle will accelerate the improvment of the backing to above 1. The only assumption is that the Bitcoin price stabilises and does not decline indefinitely (Bitcoin does not need to appreciate and return to previous highs, it merely needs to stabilise).

4 Minter's Perspective

In the previous section we have described how BBTF works technically and how Bob can use BBTF to extend his Bitcoin exposure. In this section we show that every BBTF operation (minting, extending the Bitcoin exposure, and releasing backing or claiming backing[10]) keeps the net wealth of the minter the same and only changes the exposure to different assets (USD vs Bitcoin).

4.1 Minter's Wealth

Let us define a minter's wealth as the sum of their Bitcoins (b_t) plus all bUSD which they own (o_t), minus the amount of bUSD they have minted (m_t) and denote it

$$W[b_t, o_t, m_t] = b_t B_t + P_t(o_t - m_t).$$

The wealth dynamic is given by Bitcoin's spot price B_t and the market price P_t. Let us show that minting bUSD, building extended exposure and even claiming backing[11] preserves a minter's wealth during the process.

Minting

$$W[b_t, 0, 0] = b_t B_t = b_t B_t + P_t(b_t \underline{B_t} - b_t \underline{B_t}) = W[b_t, b_t \underline{B_t}, b_t \underline{B_t}]$$

Bitcoin Exposure Extension

$$W[b_t, 0, 0] = B_t b_t = \frac{b_t B_t}{1 - P_t \frac{B_t}{\overline{B_t}}} \left(1 - P_t \frac{B_t}{\overline{B_t}}\right) = B_t b_t E_t - P_t b_t E_t \underline{B_t} = W[b_t E_t, 0, b_t E_t \underline{B_t}]$$

Backing Claim We have to distinguish between two cases:

1. **Claiming while the minting rate is at its maximum** Let us recall that the minting rate is almost always increasing[12] and therefore all minters have the same minting rate and the same ratio between their locked–in backing and minted balances. Hence, if a claim of X bUSD occurs, the claimer will get a Bitcoin payout of

   $$\frac{X}{\overline{B_t}}.$$

   Let c be a minter's fraction of the overall backing (and, equivalently, of minted bUSD). Then the minter's backing will decrease by

   $$\frac{cX}{\overline{B_t}}$$

   and his minted balance will decrease by cX. Then for the minter's wealth:

   $$\begin{aligned} W\left[b_t - \frac{cX}{\overline{B_t}}, 0, m_t - cX\right] &= B_t\left(b_t - \frac{cX}{\overline{B_t}}\right) - P_t(m_t - cX) \\ &= B_t b_t - P_t m_t + cX\left(P_t - \frac{B_t}{\overline{B_t}}\right) \\ &= W[b_t, 0, m_t] + cX\left(P_t - \frac{B_t}{\overline{B_t}}\right) \end{aligned}$$

   The last term is non-negative since $P_t \geq 1$ and $B_t \geq \overline{B_t}$; and equal to 0 if, and only if, $P_t = 1$ and $B_t = \overline{B_t}$. Otherwise, the minter would profit from some bUSD holder claiming backing.

[10] Claiming while the minting rate is at its maximum.
[11] Claiming while the minting rate is at its maximum.
[12] For more see Section 3.1.1

2. **Claiming after a substantial drop in Bitcoin's price** If the claiming occurs while Bitcoin's price has dropped below its long–term smoothed price and the minting rate has also dropped, the new minters will potentially mint with a worse minting rate than the early minters. In the previous case we have showed that claiming is wealth-preserving if the minting rate is the same for everyone. Since early minters have a better minting rate than the average minting rate, the claiming is wealth-preserving for them. However, claiming might be wealth-losing for minters who minted only after the minting rate dropped.[13]

The important takeaway is that under normal circumstances (i.e. the minting rate is at its maximum) all three operations above keep the net wealth of the minter untouched and only change their exposure to the different assets (bUSD or Bitcoin).

4.2 Rebuilding Exposure after Claiming

We have proved that under the condition of the minting rate being at its maximum, if someone claims backing, it does not decrease any minter's wealth - it only decreases a minter's exposure to Bitcoin. Let us further explore the situation of reduced exposure after a backing claim.

We assume that the minting rate $\underline{B_t}$ is at its maximum. Since $\underline{B_t}$ is increasing almost all the time (see Section 3.1.1), it is not a restrictive assumption. In fact, historically, there was only a brief period of a few days around 2015-02-01 when the spot price B_t dropped below the long–term smoothed price B_t^α and the minting rate decreased (see Table 3).

Let us assume that Bob has 1 Bitcoin locked into the BBTF. He used it to extend his Bitcoin exposure to the fullest extent

$$E_t = \frac{1}{1 - P_t \frac{\underline{B_t}}{\overline{B_t}}}$$

and thus minted $E_t \underline{B_t}$ worth of bUSD. If someone were to claim bUSD, and the amount which should be subtracted from Bob's locked–in Bitcoins is \$1 (without loss of generality), the following will happen. The \$1 paid in Bitcoin according to present claiming rate means that

$$\frac{1}{\overline{B_t}}$$

is subtracted from Bob's locked–in Bitcoins. His locked–in Bitcoins are now

$$E_t - \frac{1}{\overline{B_t}} \tag{4.1}$$

Also, \$1 is subtracted from his minted bUSD. For his minted

$$E_t \underline{B_t} - 1$$

units of bUSD, he now needs to maintain locked–in backing of

$$\frac{E_t \underline{B_t} - 1}{\underline{B_t}} = E_t - \frac{1}{\underline{B_t}} \tag{4.2}$$

Therefore, he now has excessive backing (4.1) - (4.2)

$$\frac{1}{\underline{B_t}} - \frac{1}{\overline{B_t}}$$

which he can use to again build his Bitcoin exposure

$$E_t \left(\frac{1}{\underline{B_t}} - \frac{1}{\overline{B_t}} \right)$$

[13] See Section 3.3.3 for more details about claiming while minting rate decreased.

In summary, with his required backing (4.2) we get

$$\begin{aligned} E_t\left(\frac{1}{\underline{B_t}}-\frac{1}{\overline{B_t}}\right)+E_t-\frac{1}{\underline{B_t}} &= E_t\left(\frac{1}{\underline{B_t}}-\frac{1}{\overline{B_t}}+1-\frac{1}{\underline{B_t}E_t}\right) \\ &= E_t\left(\frac{1}{\underline{B_t}}-\frac{1}{\overline{B_t}}+1-\frac{1-P_t\frac{B_t}{\overline{B_t}}}{\underline{B_t}}\right) \\ &= E_t\left(1-\frac{1}{\overline{B_t}}+\frac{P_t}{B_t}\right) \geq E_t \end{aligned}$$

since $P_t \geq 1$ and $\overline{B_t} \geq B_t$ and the equality holds if, and only if, $P_t = 1$ and $\overline{B_t} = B_t$. In other words, if someone claims backing, the minter can immediately build the same Bitcoin exposure as he had before (or even bigger, if $P_t > 1$ or if $\overline{B_t} > B_t$) and profit from it. Keep in mind that all of the above actions (claiming and rebuilding) are done with either a zero or positive effect on a minter's net wealth. Both operations only change the exposure.

The above holds under the assumption that the minting rate is at its maximum (at least during the period of Bob's minting). If this were not the case, claiming would not create excessive backing or at least not by enough to rebuild Bob's exposure fully. In that situation, Bob's present wealth would not change but his Bitcoin exposure would decrease, and his dollar exposure increase (the amount of bUSD, which he has minted and needs to return if he ever wants to release his Bitcoins, would decrease). If such a situation were to occur, Bob could use it to build a much bigger Bitcoin exposure (5x bigger, as we showed in example 3.1.3), but he would need to do so with new Bitcoins and a new contract with BBTF.

4.3 Exposure Maximisation over Time

To demonstrate the power of extended exposure, we performed the calculation on historical data. We assume Bob started with 1 Bitcoin on 2011-01-01 when the minting rate was 0.05 and the spot price was 0.30. Of course, we could do the calculation from the beginning of our data series 2010-08-01, but at that time the smoothed price calculation just began and hence the minting rate would be at 0.8 of the spot price and Bob could immediately quintuple his Bitcoin position (as we already showed in example 3.1.3). Therefore, we would rather start at 2011-01-01 where the difference between minting rate and the spot rate was larger and can be considered as the long–term "usual" situation.

As can be seen in Table 6 Bob has almost sextupled his Bitcoin position in six and half years. If he had started on 2010-08-01 when the minting rate was close to 0.8 of the spot price, he would have built an almost 30-times larger Bitcoin position. This also demonstrates the inherent motivation to mint bUSD if the Bitcoin price goes down towards the long–term smoothed price.

4.4 The Worst Case Scenario

If there is demand for bUSD, and Bitcoin is stable or appreciating, the market mechanisms work favourably. We have already discussed why it is not a problem if Bitcoin were to drop in value so much that the backing would become insufficient in Section 3.4. If bUSD suddenly became unpreferred for any reason and bUSD holders were not able to sell it on the market, they would start claiming the backing. As we showed in Section 4.1, the net wealth of a minter would stay the same but the exposure to Bitcoin would decrease. Therefore, the worst possible scenario for a Bitcoin holder (and bUSD minter) is one where they would mint bUSD only to have Bitcoin's price drop below the price at which they minted and then for bUSD to become unpreferred and the majority of it claimed. In this situation, the minter's Bitcoin exposure would be decreased unfavourably. The minter could then try to rebuild their original position as described in Section 4.2 and could do so if Bitcoin's price was above its long–term smoothed price and they could find a bUSD buyer[14]. If Bitcoin's price was so low that it was below its long–term smoothed price and a major backing claiming occurs, the minter would inevitably lose their Bitcoin exposure and would not be able to rebuild it easily. However, the conditions for minting would be very favorable at such time (the minter could quintuple their Bitcoin exposure - see Example 3.1.3), though they must use new Bitcoins to do so, not the presently locked–in ones.

[14] Probably after some "cooldown" period.

date	B_t	$\underline{B_t}$	E_t	$E_t B_t$
2011-01-01	0.30	0.05	1.00	0.30
2011-04-01	0.78	0.11	1.08	0.85
2011-07-01	17.51	0.80	1.18	20.66
2011-10-01	4.99	1.54	1.28	6.39
2012-01-01	4.94	1.65	1.36	6.73
2012-04-01	4.84	1.92	1.47	7.11
2012-07-01	6.54	2.16	1.58	10.32
2012-10-01	12.29	2.77	1.71	20.97
2013-01-01	13.38	3.48	1.85	24.71
2013-04-01	97.87	5.90	2.00	195.82
2013-07-01	89.21	14.72	2.17	193.92
2013-10-01	128.24	21.94	2.36	302.50
2014-01-01	752.79	61.05	2.56	1930.81
2014-04-01	479.03	110.09	2.78	1332.19
2014-07-01	649.66	141.30	3.01	1954.07
2014-10-01	384.97	170.23	3.25	1249.89
2015-01-01	317.27	181.98	3.46	1098.78
2015-04-01	245.68	183.98	3.54	870.12
2015-07-01	258.89	184.55	3.57	925.39
2015-10-01	237.83	186.53	3.65	868.67
2016-01-01	428.94	196.06	3.85	1651.61
2016-04-01	413.77	209.36	4.11	1698.68
2016-07-01	671.87	229.64	4.39	2952.72
2016-10-01	614.11	256.32	4.72	2899.86
2017-01-01	960.50	290.42	5.08	4880.26
2017-04-01	1061.23	343.94	5.48	5810.75
2017-07-01	2451.82	464.05	5.93	14528.79

Table 6: Bitcoin exposure maximisation over time.

5 Market Dynamics

In this chapter we only summarise previous arguments but explore them from the angle of the market value of bUSD. bUSD is a purely decentralised token whose price only depends on supply and demand forces. In this paper, we claim that the proposed process of minting bUSD with Bitcoin as backing has the direct consequence that the market price of bUSD is economically pegged to \$1 from below as well as from above (in such a way that surges in demand can only cause short term increases of the bUSD price above \$1).

Our reasoning is based on only one assumption: the existence of some rational people on both sides (among Bitcoin and bUSD holders) who will realise free profit if they see it.

5.1 The Minimum Value of bUSD

Anyone who holds bUSD can claim part of its backing (as described in Section 3.3) and receive the payout in Bitcoins using the current claiming rate

$$\frac{p_t}{\overline{B_t}}$$

for each claimed bUSD. Hence, it holds that

$$P_t \geq p_t \frac{B_t}{\overline{B_t}} \tag{5.1}$$

unless an arbitrage opportunity exists.

Since bUSD is very well backed, ($p_t = 1$) almost all of the time.[15]. Furthermore, the claiming

[15] Against historical data, the quality of backing would have never dropped below 1.

rate $\overline{B_t}$ is defined as

$$\overline{B_t} = \max(B_t, B_t^\delta)$$

Hence, the claiming rate is equal to the spot price if Bitcoin's price is stable or is growing. The short-term smoothed price B_t^δ is chosen such that the difference between the spot price B_t and the claiming rate $\overline{B_t}$ disappears quickly (in a matter of days). The reasons behind the choice of the parameter δ is explored in Appendix B.1.

If Bitcoin is stable or is growing

$$\frac{B_t}{\overline{B_t}} = 1 \tag{5.2}$$

If there was a downward move in Bitcoin's price, the ratio (5.2) would fall below 1, but only temporarily. A rational actor would know that the difference would disappear quickly and simply the pure expectation of this would disallow the price P_t to go below 1 (if there is not an immediate worry that the backing could become insufficient). Therefore, it should hold

$$P_t \geq p_t.$$

and almost all of the time

$$P_t \geq 1.$$

5.2 The Maximum Value of bUSD

We know that the bUSD token has a minimum bound, however demand could potentially drive the price up far higher than \$1 and make it impractical for usage as a USD representation on blockchain.

Fortunately, there is also an upper bound of the value. It comes from the exposure extension (see Section 3.1.2). Recall that Bob can use BBTF to build an extended exposure to Bitcoin

$$E_t = \frac{1}{1 - P_t \frac{B_t}{\overline{B_t}}}$$

As soon as P_t would be worth more than $B_t/\underline{B_t}$, an arbitrage opportunity would be created. A rational person would then borrow $1/\underline{B_t}$ of BTC in order to mint 1 bUSD and sell it on the market for more than the initial cost, and would therefore get free profit. Hence, it holds that

$$P_t \leq \frac{B_t}{\underline{B_t}}.$$

In Table 7 we can see how the attractiveness of the Bitcoin exposure extension depends on the ratio between the minting rate $\underline{B_t}$, the spot price B_t and the bUSD market price P_t. If we look at Table 3, we see that in the last three years the ratio $\underline{B_t}/B_t$ was roughly around 0.3, on average. Therefore, if P_t starts growing too much, market forces will push it back due to Bitcoin holders using the opportunity to extend their exposure. If P_t goes to 1.5, Bitcoin holders can almost double their exposure.

The possibility for P_t price growth exists only in the case where Bitcoin's price grows substantially in a short period of time. However, even that does not necessary mean that P_t will climb because the market knows that unless the rapid appreciation of Bitcoin continues, the ratio $\underline{B_t}/B_t$ is going to start shrinking and pushing P_t down. The mere expectation of this happening should act as a market force in preventing P_t from climbing.

As Bitcoin's volatility reduces in the future, so too will the potential volatility of P_t.

The upper bound might be more loose in the beginning, when the market is in its infancy and is not efficient enough, and also might become more loose when Bitcoin appreciates heavily in a short time period. However, in the long–term it should always be contained due to people wanting to maximise their exposure to Bitcoin (see also Section 4.3). In the beginning, we suggest starting the BBTF with an artificially higher minting rate so as to help keep P_t close to \$1 even with a small market - and to promote minting at the same time (see Section 8.1). In the longrun, the pure expectations of self-correction should correct the price efficiently.

		$\underline{B_t}/B_t$							
		0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8
P_t	1	1.11	1.25	1.43	1.67	2	2.5	3.33	5
	1.5	1.18	1.43	1.82	2.5	4	10		
	2	1.25	1.67	2.5	5				
	2.5	1.33	2	4					
	3	1.43	2.5	10					
	3.5	1.54	3.33						
	4	1.67	5						
	4.5	1.82	10						
	5	2							
	5.5	2.22							
	6	2.5							
	6.5	2.86							
	7	3.33							
	7.5	4							
	8	5							
	8.5	6.67							
	9	10							
	9.5	20							

Table 7: Bitcoin exposure extension.

6 A Detailed Example

Let us go through a step-by-step example to demonstrate how the smart contract algorithm works. The details surrounding each event in the 'life' of our example BBTF are in Table 8. Everything is calculated under the condition that bUSD does not trade with any premium above the value of the backing ($P_t = p_t$) - thus, the most conservative scenario is assumed. If there were any premium, the exposure extension would be more powerful and the wealth of minters would grow faster.

1. There are two actors, both with 1 Bitcoin who want to use BBTF. The BBTF is empty - there are no locked–in Bitcoins or minted bUSD in the beginning. Alice and Bob have both sent 1 BTC each to BBTF. Alice used her 1 Bitcoin to mint 2.72 bUSD. Bob used his 1 Bitcoin to extend his exposure to 1.29 Bitcoins. Their respective net wealth is the same, but they opted for different asset exposures. Hence, the dynamics of their respective wealth will be different in the future.

2. Both the spot price and minting rate have increased. Part of Alice and Bob's backing is now excessive.

3. Alice has minted more bUSD with her excessive backing. Bob used the excessive backing to extend his Bitcoin exposure. Bob's net wealth is significantly different to that of Alice.

4. Spot price has decreased, but minting rate has increased and part of locked–in backing is now excessive.

5. Alice again minted more bUSD using the excessive backing. Bob has used it to extend his Bitcoin exposure. A new minter Carol has locked in her 5 Bitcoins and minted new bUSD.

6. Some bUSD holder (not minter) has claimed 100 bUSD. 100 bUSD were destroyed and BBTF made a Bitcoin payout according to current claiming rate. Every minters' locked–in Bitcoins were subtracted proportionally according to their locked–in Bitcoins (note that only the required portion is accounted for, not the excessive part). Net wealth of minters remain the same, only their Bitcoin exposure was reduced.

7. Alice has used her newly excessive backing to mint new bUSD, Bob to extend his Bitcoin exposure, and Carol to mint more bUSD. Note that Bob was able to regain his previous Bitcoin exposure.

8. Price has changed. All minters' backing is partly excessive.

Date	B_t	$\underline{B_t}$	$\overline{B_t}$	BTC	Required	bUSD	Backing
Step	Minter	Free BTC	locked–in BTC	bUSD minted	Excessive	bUSD	Wealth
2012-09-24	12.03	2.72	12.03	2.29	2.29	6.22	4.43
1	Alice	0.00	1.00	2.72	0.00	2.72	12.03
	Bob	0.00	1.29	3.51	0.00	0.00	12.03
2014-02-06	792.78	86.11	821.49	2.29	0.07	6.22	9.54
2	Alice	0.00	1.00	2.72	0.97	2.72	792.78
	Bob	0.00	1.29	3.51	1.25	0.00	1020.41
2014-02-06	792.78	86.11	821.49	2.44	2.44	210.44	9.54
3	Alice	0.00	1.00	86.11	0.00	86.11	792.78
	Bob	0.00	1.44	124.33	0.00	0.00	1020.41
2014-12-03	379.33	178.92	379.33	2.44	1.18	210.44	2.12
4	Alice	0.00	1.00	86.11	0.52	86.11	379.33
	Bob	0.00	1.44	124.33	0.75	0.00	423.40
2014-12-03	379.33	178.92	379.33	8.11	8.11	1451.56	2.12
5	Alice	0.00	1.00	178.92	0.00	178.92	379.33
	Bob	0.00	2.11	378.02	0.00	0.00	423.40
	Carol	0.00	5.00	894.62	0.00	894.62	1896.65
2014-12-03	379.33	178.92	379.33	7.85	7.55	1351.56	2.12
6	Alice	0.00	0.97	166.60	0.04	178.92	379.33
	Bob	0.00	2.04	351.98	0.08	0.00	423.40
	Carol	0.00	4.84	832.99	0.18	894.62	1896.65
2014-12-03	379.33	178.92	379.33	7.92	7.92	1416.68	2.12
7	Alice	0.00	0.97	173.11	0.00	185.44	379.33
	Bob	0.00	2.11	378.02	0.00	0.00	423.40
	Carol	0.00	4.84	865.55	0.00	927.18	1896.65
2017-07-27	2581.76	509.02	2581.76	7.92	2.78	1416.68	5.07
8	Alice	0.00	0.97	173.11	0.63	185.44	2510.19
	Bob	0.00	2.11	378.02	1.37	0.00	5076.55
	Carol	0.00	4.84	865.55	3.14	927.18	12550.96
2017-07-27	2581.76	509.02	2581.76	7.63	7.63	3882.18	5.07
9	Alice	0.63	0.34	173.11	0.00	185.44	2510.19
	Bob	0.00	2.45	1246.69	0.00	0.00	5076.55
	Carol	0.00	4.84	2462.39	0.00	2524.02	12550.96
2017-07-28	300.00	240.00	2280.25	7.63	7.63	3882.18	4.48
10	Alice	0.63	0.34	173.11	0.00	185.44	302.58
	Bob	0.00	2.45	1246.69	0.00	0.00	-511.93
	Carol	0.00	4.84	2462.39	0.00	2524.02	1512.89
2017-09-25	300.00	240.00	303.95	7.63	7.63	3882.18	0.60
11	Alice	0.63	0.34	173.11	0.00	185.44	297.61
	Bob	0.00	2.45	1246.69	0.00	0.00	-9.68
	Carol	0.00	4.84	2462.39	0.00	2524.02	1488.06
2017-09-25	300.00	240.00	303.95	7.23	7.23	3682.18	0.60
12	Alice	0.63	0.32	164.19	0.00	185.44	297.68
	Bob	0.00	2.32	1182.46	0.00	0.00	-9.19
	Carol	0.00	4.59	2335.53	0.00	2524.02	1489.05
	Dan	5.00	0.00	0.00	0.00	0.00	1500.00
2017-09-25	300.00	240.00	303.95	20.03	20.03	6753.78	0.90
13	Alice	0.63	0.32	164.19	0.00	185.44	304.15
	Bob	0.00	2.32	1182.46	0.00	0.00	-369.14
	Carol	0.00	4.59	2335.53	0.00	2524.02	1546.42
	Dan	0.00	12.80	3071.60	0.00	0.00	1070.30

Table 8: Bitcoin holdings and bUSD created.

9. Alice has released her excessive backing. Bob used it to extend his Bitcoin exposure. Carol minted more bUSD.

10. Price has dropped almost 90% in a single day. It will take a couple of days for the claiming rate to adjust. Backing is sufficient only because the claiming rate has not yet adjusted. In a couple days it will be insufficient. Bob's net wealth is negative since he is maximally exposed to Bitcoins and does not hold any bUSD.

11. Low price of Bitcoin persists. Claiming rate has adjusted and backing is insufficient.

12. Some bUSD holder has claimed 200 bUSD. Since the backing is insufficient, the claimer has received only 0.6 of the claimed face value. Backing per issued bUSD remains the same. Every minter's net wealth was slightly increased because it was claimed with a claiming rate higher than the spot price, hence they have profit on the claim. The subtraction from backing and from the minted balance was done in the same ratio since all minters minted before the big drop in price. New minter Dan has entered.

13. Dan has used his 5 Bitcoins to mint new bUSD and extend his Bitcoin exposure to the maximum. Since the price of Bitcoin has dropped 90% recently, minting rate is very close to spot rate, which allows Dan to build a much larger Bitcoin exposure, even while bUSD is insufficiently backed. Dan has also improved the quality of backing towards 1.

7 Inherent Dynamics and Advantages of the System

The mechanism of minting leads to several inherently favourable dynamics which support each other.

High demand for bUSD will lead to increased supply of bUSD — The demand for bUSD will drive up the price of bUSD and make minting more profitable for Bitcoin holders.Therefore, the supply will increase to come into balance with bUSD demand. This mechanism also creates the upper bound for the bUSD price.

Bitcoin price drops create buy-pressure on Bitcoin — If Bitcoin's price starts dropping and approaching the long–term smoothed price B_t^α, minting for the purpose of extending the exposure to Bitcoin becomes much more attractive. A Bitcoin exposure of up to $5\times$ larger can be built and this would cause buying pressure on Bitcoin.

Demand for bUSD creates buy-pressure on Bitcoin — The demand for bUSD drives the price P_t up and attracts Bitcoin holders to use the opportunity to extend their Bitcoin exposure. That again pushes Bitcoin's price up.

The price volatility of Bitcoin does not matter — If Bitcoin appreciates in a phase of over-hyped growth, the minting rate would follow with a huge delay which leaves a lot of time for Bitcoin's price to correct. Therefore, the stability of bUSD is not threatened by future corrections following over-hyped growth periods. On the other hand, in stable times minting is easier which could drive Bitcoin appreciation.

It is a community project — There is no need to compete about who will implement the project. The whole community will profit from its existence. If other cryptocurrencies want to implement the same smart contract, they may, but their backing parameters should be more conservative because of their higher volatility. More conservative parameters would make them less attractive for holders. With no fees and no ICO, there is little incentive aside from persuasive marketing for any actor to create and push adoption of a alternative cryptocurrency–backed stablecoin.

8 Road to Implementation

Of course bUSD is a project which would benefit greatly from the network effect. The more people use it, the better it works - especially the market forces which pegs the price around $1. This is where a decentralised, trustless coin faces a greater challenge in "building the snowball" perhaps than a centralised stablecoin that can be promoted onto large exchanges through commercial negotiations. Let us see how BBTF might attract its first users and bootstrap from there.

8.1 The Initial Period

When BBTF goes live, the market for minted bUSD will be small and the market forces pushing price P_t close to \$1 will be quite weak. Therefore, we suggest to artificially increase the minting rate depending on the amount of minted bUSD in existence. Let us denote the amount of minted bUSD as M_t and choose a constant $C = 100M$.[16] We define the initial minting rate $\underline{\hat{B}_t}$ as

$$\begin{aligned} \underline{\hat{B}_t} &= 0.8 \left(\frac{C - M_t}{C} \right)^2 (B_t - \underline{B_t})^+ + \underline{B_t} && \text{for } M_t < C \\ &= \underline{B_t} && \text{otherwise} \end{aligned}$$

where $(\cdot)^+$ denotes the positive part. In simple words, the initial minting rate is artificially elevated closer to 0.8 of the spot price. Hence, early participants can easily almost quintuple their exposure when there is not much bUSD in existence (see Example 3.1.3). Minting under such favorable conditions will probably result in an over-supply of bUSD in the beginning and will press the price P_t down close to \$1, even with the small market. Potentially high demand for bUSD (which would drive P_t up) would only make minting and extending Bitcoin exposure even more attractive. With the growing monetary supply of bUSD, this advantage would fade away and disappear completely upon reaching 100M bUSD.

8.2 The First Use Cases

Let us ponder where bUSD can find its first uses. It sould be noted that there is no need for wide-scale early acceptance - the network effect will help to propel bUSD a lot. As soon as even small group of people will start using bUSD for any purpose, the system will grow from there. See Appendix D for a examples of useful services which could be build on top of BBTF right away.

Decentralised BTC/bUSD Trading Since bUSD is based on the same blockchain as Bitcoin[17], Bitcoin can be traded for bUSD through smart contracts in a trustless way without the need to have an account with a centralised exchange which must adhere to KYC/AML regulations. In practice, this means that one can trade BTC for bUSD (and vice versa) anonymously.

Crypto-trading in General Traders can use bUSD as the liquidity resource when they want to reduce their crypto exposure in favour of FIAT price stability. As soon as bUSD is implemented on more crypto exchanges, it will become a great tool for arbitrage and could make the whole sphere of Bitcoin more efficient in arbitrage clearing and price discovery. Being decentralised and trustless, bUSD represents a superior alternative to the incumbent stablecoin solutions offered on major exchanges.

Financial Engineering The existence of a blockchain-based token with its price denominated in USD could commence a complete remake of all sorts of financial derivatives built using smart contracts which utilise bUSD. Derivatives built in this way would not have counterparty risk, could easily be audited and could be settled immediately. One could start building products like options, swaps and so on between Bitcoin, bUSD and other tokens pegged to other FIAT currencies built using BBTF.

International Wiring bUSD could be used to move USD value around the world with all the advantages of blockchain, bringing more opportunities for people and companies to trade internationally.

Fight Capital Controls In many countries capital is not allowed to move outside of the country. bUSD could change that.

[16] The choice of $C = 100M$ is arbitrary, but we think it is high enough for the market to work well but at the same time is not *too* high. For reference, the current market cap of Tether (USDT) is over \$300M.

[17] Practical implementations will probably be based on the Rootstock (RSK) platform, which is a side-chain to Bitcoin that uses Bitcoin as its main token. Other implementations using different smart contract platforms on top of Bitcoin will also be possible. The main scripting language of the Bitcoin blockchain is not sophisticated enough to allow a practical implementation on top of the main Bitcoin blockchain.

Community Insurance and Community Financial products Community insurance concepts are being built on blockchains already. Their disadvantage is that they are supposed to help with financing events in the real world which are denominated in USD (or other FIAT currencies) rather than in Bitcoins or other cryptocurrencies. Building such systems using bUSD would get rid of the volatility risk.

Free Markets In various economical transactions the parties desire to remain anonymous but can not do presently without using price-volatile cryptocurrencies. The more stable bUSD would be a preferable choice for them.

bUSD Worldwide Escrow and the Use of Smart Contracts in International Business Companies often need to pay their suppliers for products worldwide and they are forced to take risks related to doing business with unknown counterparties or relying on foreign jurisdiction and its protection (which is often not functional, especially in third world countries). Smart escrow and using smart contracts in a trustless way with USD value could have the potential to make significant improvements in this area.

Online Betting and Gaming Some strategies in betting and gaming are based on only slight probability advantages. The expected return is often small and any change in Bitcoin's price can ruin it. The more stable bUSD would be preferred in such cases.

Irreversible payments denominated in a preferred unit of account Irreversible payments help avoid chargeback risks for merchants and allow for cheaper trade. This use case already requires some sort of network effect, but when merchants start accepting payments in bUSD they do not have to recalculate prices in stores and can receive payments directly pegged to their preferred unit of account.

A Comments on General BBTF

In the paper we have demonstrated the concept using USD as the prime example since it has very low volatility and is considered as a worldwide reserve (and unit of account) currency. However, the concept holds in general and can be used to create a token pegged to any tradeable asset or portfolio of assets. The only assumption is that there must be a price in Bitcoins of the asset (or portfolio). Also, the more volatile the pegged asset is, the more conservative the backing parameters must be. In general, there is no reason why cryptocurrencies other than Bitcoin could not be used (for example, Ether or Litecoin). However, since Ether and other cryptocurrencies are more volatile than Bitcoin (and have a shorter recorded history of market price), the backing parameters would have to be more conservative than in the case of Bitcoin. That makes Bitcoin a more attractive choice for now.

B Bitcoin Backing

B.1 Smoothing Parameters

For claiming purposes we want to have some short–term stability which would also create an incentive not to claim backing during any period of panic regarding Bitcoin - therefore protecting the token against flashcrashes. Let us recall that the claiming rate is defined as the maximum of the spot price and the smoothed price with the parameter δ

$$\overline{B}_t = \max(B_t, B_t^\delta)$$

During periods of Bitcoin price growth, the claiming rate will be equal to the spot price. During any declines, the claimer should need to some short period of time until the spot price equals the smoothed price and claim without any loss. To choose an adequate δ we have looked at the length of time until the difference between the spot price and the claiming rate vanishes.

In Table 9 we see different choices of parameter δ and its impact on the calculations on historical data. For different choices of δ we have calculated the longest gap in days, the average length of the gap, the maximum ratio of claiming rate over the spot price and the mean ratio.

B.1.1 Claiming Parameter δ

We can see that all metrics depend on the choice of δ in quite a smooth way. There are no sudden changes. The maximum gap and maximum ratio both happened during the crash in the beginning of 2014. Even then, with the rather extreme volatility, it was only a matter of time to wait until the difference between the claiming rate and the spot price disappeared. The higher the choice of δ, the more stable the system in the case of a sudden market change. We feel safe to choose $\delta = 0.9$; where the mean length of the gap is around one week. However, we could also take any other constant in the neighbourhood of 0.9 and the system would not change much - the choice of the minting parameters α and β are more important.

B.1.2 Minting Parameters

The credibility of bUSD depends on making a good choice regarding minting parameters. The smoothing parameter α should be close to 1 so that it is heavily history-dependent, smooths out most over-hyped growth and accounts for possible crashes. On the other hand, if it were too conservative, it would not be attractive to use. Hence, for different choices of α we have calculated what the maximum possible β could be so that bUSD would be still completely backed during Bitcoin's entire recorded history. We have also calculated how much bUSD would be minted with the chosen α and corresponding maximum β by using 1 BTC every day. Furthermore, we have calculated the current minting rate with those parameters and how many days in Bitcoin's history the spot price would have dropped below the long–term smoothed price (denoted as "days at spot" in the tables).

In Tables 10, 11, 12 and 13 we subsequently observed that the maximisation of overall minted coins is equivalent to the maximisation of the current minting rate and culminates at $\alpha = 0.99883$, for which the β could be set to 1 and bUSD would still be perfectly hedged for Bitcoin's entire recorded history. You may note that for $\alpha = 0.99883$ there were 70 days when the spot price was

δ	Max Gap	Mean Gap	Max Ratio	Mean Ratio
0.70	23	4.60	1.63	1.01
0.71	23	4.93	1.64	1.01
0.72	29	5.07	1.64	1.01
0.73	28	5.09	1.65	1.01
0.74	28	5.19	1.65	1.02
0.75	28	5.36	1.65	1.02
0.76	29	5.60	1.65	1.02
0.77	29	5.64	1.65	1.02
0.78	29	5.87	1.65	1.02
0.79	29	5.92	1.64	1.02
0.80	35	6.23	1.64	1.02
0.81	35	6.31	1.64	1.02
0.82	42	6.47	1.66	1.02
0.83	49	6.91	1.67	1.02
0.84	49	6.83	1.68	1.02
0.85	49	7.26	1.69	1.02
0.86	61	7.39	1.69	1.02
0.87	65	7.77	1.69	1.02
0.88	85	7.99	1.69	1.03
0.89	84	8.00	1.68	1.03
0.90	84	8.49	1.69	1.03
0.91	81	8.89	1.73	1.03
0.92	82	9.25	1.80	1.03
0.93	82	9.59	1.88	1.03
0.94	143	10.99	1.99	1.04
0.95	143	12.00	2.14	1.04
0.96	137	15.89	2.36	1.05
0.97	141	21.20	2.70	1.06
0.98	127	21.47	3.12	1.07
0.99	327	41.41	3.22	1.09

Table 9: The different choice of smoothing parameter δ for claiming price.

α	Max β	Minted	Minting Rate	Days at Spot
0.90	0.15	125152	307	1028
0.91	0.15	127859	314	1014
0.92	0.15	128575	318	990
0.93	0.16	129898	323	978
0.94	0.16	132222	331	965
0.95	0.17	136218	345	932
0.96	0.18	143314	369	914
0.97	0.19	150870	398	853
0.98	0.22	162504	447	777
0.99	0.29	197799	499	705

Table 10: The different choices of smoothing parameter α for minting.

below the long–term smoothed price whereas β was still 1. This is because the claiming rate during that period was higher than minting rate and hence, the backing was sufficient.

B.2 Parameter β

Finally, we must decide about the parameter β. A choice of $\beta = 0.8$ means there is an additional buffer on the calibrated smoothed price. The lower the β, the larger and more conservative the resulting buffer would be. Recall that the parameter β also influences the attractiveness of BBTF,

α	Max β	Minted	Minting Rate	Days at Spot
0.990	0.29	197799	499	705
0.991	0.31	204628	507	708
0.992	0.33	212800	516	708
0.993	0.36	223365	528	708
0.994	0.39	237365	544	671
0.995	0.44	256250	566	608
0.996	0.51	282307	595	527
0.997	0.59	301033	598	460
0.998	0.72	324093	599	342
0.999	1.00	321501	556	2

Table 11: The different choices of smoothing parameter α for minting.

α	Max β	Minted	Minting Rate	Days at Spot
0.9980	0.72	324093	599	342
0.9981	0.74	326962	599	313
0.9982	0.77	330100	600	302
0.9983	0.79	333542	602	279
0.9984	0.82	337253	604	258
0.9985	0.85	341153	606	229
0.9986	0.89	345376	609	208
0.9987	0.94	349907	612	164
0.9988	0.98	352473	613	87
0.9989	1.00	340798	590	12
0.9990	1.00	321501	556	2
0.9991	1.00	300508	519	1
0.9992	1.00	277710	480	1
0.9993	1.00	252911	437	1
0.9994	1.00	225885	391	1
0.9995	1.00	196377	340	1
0.9996	1.00	164099	285	1
0.9997	1.00	128726	224	1
0.9998	1.00	89891	157	1
0.9999	1.00	47181	83	1

Table 12: The different choices of smoothing parameter α for minting.

since for the exposure extension it holds that

$$E_t = \frac{1}{1 - P_t \frac{B_t}{\overline{B_t}}}$$

which is equal to

$$E_t = \frac{1}{1 - \beta}$$

if the spot price were to drop below the long–term smoothed price. At that time we would need minting to be very attractive to motivate more people to mint bUSD and consequently increase the quality of the backing. The closer β is to 1 the better. We think that the choice of $\beta = 0.8$ is a good compromise which creates additional 20% buffer while also allowing the possibility to quintuple one's exposure.

α	Max β	Minted	Minting Rate	Days at Spot
0.99875	0.96	351251	612	134
0.99876	0.96	351512	612	126
0.99877	0.97	351767	612	120
0.99878	0.97	352013	613	102
0.99879	0.98	352246	613	93
0.99880	0.98	352473	613	87
0.99881	0.99	352602	613	80
0.99882	0.99	352719	613	76
0.99883	1.00	352835	612	70
0.99884	1.00	351472	610	58
0.99885	1.00	349754	607	53
0.99886	1.00	348014	603	44
0.99887	1.00	346248	600	31
0.99888	1.00	344454	597	20
0.99889	1.00	342637	594	17
0.99890	1.00	340798	590	12

Table 13: The different choices of smoothing parameter α for minting.

C Exponential Moving Average at Unevenly Distributed Intervals

Let us consider the time series $B_0, B_1, \ldots, B_n$. Recall how exponential smoothing is derived: we count all the past terms with weights which are exponentially decreasing, i.e.

$$\frac{\sum_{i=0}^{k} B_i \alpha^{k-i}}{\sum_{i=0}^{k} \alpha^{k-i}} \tag{C.1}$$

For the denominator, the following holds:

$$\sum_{i=0}^{k} \alpha^{k-i} = \sum_{i=0}^{k} \alpha^{i} = \frac{1-\alpha^{k+1}}{1-\alpha} \xrightarrow{k\to\infty} \frac{1}{1-\alpha}, \qquad 0 < \alpha < 1.$$

From (C.1) we know that by sending the denominator to its limit at infinity we get

$$\begin{aligned} B_k^{\alpha} &= (1-\alpha)\sum_{i=0}^{k} B_i \alpha^{k-i} \\ &= (1-\alpha)\left(B_k + \sum_{i=0}^{k-1} B_i \alpha^{k-i}\right) \\ &= (1-\alpha)B_k + \alpha(1-\alpha)\sum_{i=0}^{k-1} B_i \alpha^{k-1-i} \\ &= (1-\alpha)B_k + \alpha B_{k-1}^{\alpha} \end{aligned}$$

This is the classical exponential smoothing

$$\begin{aligned} B_k^{\alpha} &= \alpha B_{k-1}^{\alpha} + (1-\alpha)B_k, \qquad k = 1, \ldots, n \\ B_0^{\alpha} &= B_0 \end{aligned}$$

where α is the smoothing factor.

However, this situation implicitly assumes that the time series is measured at evenly distributed time intervals $0, 1, \ldots, n$ which is often too restrictive for real world data. Let us derive the generalisation when we have a time series $B_0, B_1, \ldots, B_n$ measured at intervals $0, t_1, \ldots, t_n$. Then,

for the exponentially smoothed time series $B_0^e, B_1^e, \ldots, B_n^e$ we want factor the observation B_k according to how old it is with an exponentially decreasing weight (compared to (C.1)), i.e.

$$B_k^e = \frac{\sum_{i=0}^{k} B_i e^{-\frac{t_k - t_i}{\mu}}}{\sum_{i=0}^{k} e^{-\frac{t_k - t_i}{\mu}}} \tag{C.2}$$

Here μ plays the same role as in the discrete time the factor α, only on a different scale. If the time between sampling intervals is constant Δ_t, we could set $\alpha = e^{-\Delta_t/\mu}$ and derive our simple exponential smoothing.

For practical purposes we need to use a recursive formula for (C.2), so it can be computed efficiently. Let us define

$$\begin{aligned}
\pi_k &= e^{-\frac{t_k - t_{k-1}}{\mu}} \\
w_k &= \sum_{i=0}^{k} e^{-\frac{t_k - t_i}{\mu}} = 1 + e^{-\frac{t_k - t_{k-1}}{\mu}} \sum_{i=0}^{k-1} e^{-\frac{t_{k-1} - t_i}{\mu}} = 1 + \pi_k w_{k-1} \\
s_k &= \sum_{i=0}^{k} B_i e^{-\frac{t_k - t_i}{\mu}} = B_k + e^{-\frac{t_k - t_{k-1}}{\mu}} \sum_{i=0}^{k-1} B_i e^{-\frac{t_{k-1} - t_i}{\mu}} = B_k + \pi_k s_{k-1}
\end{aligned}$$

Therefore we can define an algorithm

1. We initialise the algorithm as

$$\begin{aligned}
B_0^e &= B_0 \\
t &= 0 \\
k &= 1 \\
w &= 0 \\
s &= B_0
\end{aligned}$$

2. Compute k-th step

$$\begin{aligned}
\pi &= e^{-\frac{t_k - t}{\mu}} \\
w &= 1 + \pi w \\
s &= B_k + \pi s \\
B_k^e &= \frac{s}{w} \\
t &= t_k
\end{aligned}$$

3. Increase k and repeat.

If we have some idea about α, we can get the parameter μ through simple inversion as

$$\begin{aligned}
\alpha &= e^{-\frac{\Delta_t}{\mu}} \\
\mu &= -\frac{\Delta_t}{\ln \alpha} = -\frac{24 \times 60 \times 60}{\ln 0.99883} \approx 73802945
\end{aligned}$$

and for $\delta = 0.9$, we find the corresponding ν to be

$$\nu = -\frac{24 \times 60 \times 60}{\ln 0.9} \approx 820041$$

D Possible Extensions

As soon as the BBTF exists and people can mint a FIAT representation in a trustless way, there are plenty of additional extensions that the community can build on top of it. In an evolutionary sense, one can achieve a complete replication of the present financial system, but do so in a trustless and auditable way. Suddenly the possibility of creating derivatives or other financial instruments is no longer possible only for regulated big players – anyone can do it. The counterparty risk is mitigated and everything is transparent and auditable.

D.1 BBTF Additional Services

BBTF is designed to be as simple as possible and provide a valuable FIAT representation on blockchain in a trustless way. There are some obvious extensions which can be done immediately and which allow for a more comfortable use of BBTF. They could be part of BBTF right from the beginning, but from the (IT) security perspective, it is likely better to implement them as separate services. All of the following services can be built as smart contracts in a trustless way.

D.1.1 Collateral Unlocking Service

There will be situations when someone needs his locked–in collateral, but does not possess the necessary bUSD to release it and also has no money to buy bUSD on the market. He is willing to use a service which would pay (by sending bUSD to BBTF) for releasing his collateral and deduct the costs of the required bUSD along with some fee from the released collateral.

D.1.2 Automatic Minting from Newly Excessive Collateral Service

We anticipate that many people will be interested in maximising the minted bUSD from their locked–in Bitcoin holdings. The service could potentially watch the minting price and their position, and if there was a possibility of minting more bUSD, the service would automatically initiate the minting process.

D.1.3 Exposure Extension Service

The process of Bitcoin exposure extension described in Section 3.1.2 is performed through infinitely many steps or can be done in one step with borrowed capital. An obviously helpful service would be to use one's capital to build extended position for someone else and charge some fee for doing that.

D.1.4 Maximum Exposure Building Service

There will be people who would like to mint as much bUSD as possible from their Bitcoin holdings whenever it becomes possible and immediately use it to extend their Bitcoin exposition. This is simply a combination of the previous two services. One could easily start with 1 Bitcoin and only few years later find out that the service had built a total exposure for them of several multiples.

D.1.5 Collateral to Bond Conversion Service

If there was a smart contract which allows for the creation of bonds as described in Section D.2, there would be people who have already spent all the bUSD minted by their Bitcoin holdings and need some more money, but still prefer not to sell their Bitcoin. They are willing to pay interest for the possibility of keeping their Bitcoin. A helpful service could be to unlock their Bitcoin collateral for them without selling any of the Bitcoin and then create a bond which would allow them to get more bUSD with the same collateral.

D.2 Trustless Bonds

Probably the most basic financial instrument is a zero–coupon bearing bond[18]. One could create a smart contract which has its backing in Bitcoins, a face value denominated in FIAT and which would settle itself by paying the face value at maturity or when the collateral value drops below some pre-defined trigger value. The creation of such derivative would be done by a smart contract and every Bitcoin holder could create such derivative and sell it on the market for bUSD for a face value discounted by the time to maturity — the process is similar to how fixed–term derivatives work nowadays. There is almost no default risk involved (except for a rapid flash-crash of Bitcoin price) and with the existence of bUSD it can be created and traded in a trustless way.

[18] More complex financial products are often approximated by series of zero–coupon bearing bonds.

D.3 Decentralised BTC/bUSD trading

The recent crackdown on crypto exchanges in China is probably not the last attempt of regulators to take the crypto-world under their control. Decentralised exchanges are emerging and are already preferred by many Bitcoin users. The problem with most decentralised exchanges come from the properties of FIAT. It is hard to process the trade in a trustless way. The decentralised exchanges are forced to use the assistance of some escrow account or arbitration process in case of a dispute, or to use centralised representations of FIAT currencies, such as Tether (USDT). bUSD could radically change that and allow trades to happen on a smart contract basis only, without the need for any intermediaries, escrows or arbitration process.

E Contact and feedback

We would appreciate any feedback to this whitepaper. If you have corrections, suggestions or have different opinion about the construction of BBTF and bUSD, let us know.

Our website is http://cryptopeg.org/. There you can subscribe to a low-traffic newsletter to stay in touch and learn about our implementation of the BBTF smart contract.

You can contact us at mailto:cryptopeg@cryptopeg.org. We prefer PGP-encrypted e-mail. Our PGP key can be found at https://keybase.io/cryptopeg with keyid and fingerprint:

```
0x3C9885520FF20001 fingerprint: 01AB 5270 A0A6 4A10 3E91 90C9 3C98 8552 0FF2 0001
```

You can also create issues at https://github.com/cryptopegorg and follow us on Twitter https://twitter.com/CryptoPeg_Org.