Triton and Sao: Stable value via consensus mint and burn

Lead Developer:
Harrison Hesslink
harrison@xtri.network
https://xtri.network/

Abstract. A single-chain, dual-coin, peer-to-peer version of electronic cash that gives users the ability to burn and destroy a primary coin with volatile value in order to mint and create an equivalent US dollar value of a secondary coin could result in a stable US dollar pegged secondary coin if these mint and burn mechanisms also ran in the reverse allowing stablecoin redemption for any amount of volatile coin necessary to restore the same market value. Such market conversion rates would be observed by a decentralized oracle monitored by user-hosted service nodes calibrated to reduce the likelihood of black swan failure events. Thus, this concept of market-driven mint and burn could be used to take the volatile cryptocurrency Triton (XTRI) and use it to collateralize the US dollar-pegged value of a second currency on the same blockchain: the Sao Dollar (SAO). While the mint and burn concept was first proposed by Haven Protocol in early 2018, Haven is closed source, has yet to be implemented, and is not overseen by user-validated nodes. Triton will provide the first open-source alternative for a mint and burn stablecoin and will use community feedback during a testnet period to ensure the robustness of the Triton oracle, Triton service nodes, and the XTRI / SAO mint and burn implementation. In this document, we outline the history of stablecoins, the unique challenges we see with mint and burn as a system, and our initial attempts to outline our oracle, service nodes, and mint and burn implementation.

1. Introduction.

Although the advent of Bitcoin and other novel forms of peer-to-peer electronic cash now allows for online payments without the need for trusted third party intermediaries [1], the unrestricted nature of these technologies has resulted in speculative trading markets that create wildly unstable cryptocurrency values. In 2018, Bitcoin at times lost >80% of its value from December 2017 highs with many 'altcoins' falling further [2]. This volatility has created a growing interest in 'stablecoins': cryptocurrencies pegged to established currencies like the US dollar. Such fiat-pegged stablecoins provide the low-volatility necessary for fixed-price transactions and provide stable value storage. Many believe stablecoins will become essential to the overall cryptocurrency ecosystem until it achieves some critical level of mass adoption and maturity. However, there is as yet no consensus on the best way to create a stablecoin.

In early 2019, the most common method of building a stablecoin is via direct asset backing and trusted third parties. The popular stablecoin Tether (USDT) is supposedly backed 1:1 by US dollars held in bank accounts, but this requires not only trust of the company Tether Limited, but their partner banks and the nations in which those banks reside [3][4]. Such trust requirements for Tether and similar asset-backed stablecoins, combined with lack of regulatory oversight, make them unsuitable for everyday transactions or long-term value storage.

In contrast, decentralized stablecoins are ambitious attempts to build a stable store of value via novel methods that do not require third party trust or 1:1 fiat backing. The most successful of these to date is Maker, a protocol that uses Collateralized Debt Positions of contracts locked in Ethereum to mint a stablecoin pegged to the US dollar: Dai [5]. Because the Ethereum collateral backing Dai is unstable in price and cannot be directly created or destroyed by Maker, a complex variety of autonomous feedback and incentivization mechanisms are used to maintain Dai's stable value. The long-term stability of Dai requires flawless execution of these unwieldy mechanisms and requires continued health of the Etherium protocol.

A simpler, private, decentralized stablecoin was proposed in early 2018: Haven Protocol [6][7]. Rather than use a debt collateral like Maker, Haven Protocol proposed a novel mechanism of minting and burning that uses market forces and volatile coin supply to ensure value storage for a stablecoin without complex feedback mechanisms. As proposed, volatile Haven (XHV) could always be burned and destroyed for a market equivalent value of newly minted Haven Dollars (XUSD), and vice versa. This exchange rate would be determined by an oracle that regularly queried exchange values, thus allowing market pressure and the volatile chain to ensure the stable value of Haven Dollars. While the Haven Protocol project has attracted a great deal of attention, the Haven mainnet is not yet live and the oracle and mint and burn mechanisms remain closed sourced. Since a mint and burn stablecoin lacks many of the 'black swan' controls that Maker has implemented, great care must be taken to prevent oracle attacks that could lead to supply inflation and protocol failure. Due to the protocol's closed-source nature, it is unclear whether Haven is taking the sufficient care necessary to ensure success. Additionally, we are concerned by Haven's decision to add multiple stable assets (XEUR, XGOLD, etc.) [8], each of which provides an extra attack surface which could lead to failure of the protocol. A newcomer to the mint and burn concept, BitCash (BITC) [9][10], also hopes to achieve the concept but with few released details and a proposed non-private observational backdoor available for government regulators. While this ability to audit transactions via trusted third parties could benefit certain regulated industries, we expect any such backdoor would also eventually become available for exploitation by malicious actors. For this reason - we have chosen not to include an observational backdoor in the XTRI / SAO protocol.

In this paper, we propose an open-source mint and burn alternative to Haven Protocol (XHV) and the Haven Dollar (XUSD): Project Triton (XTRI) and the Sao Dollar (SAO). Triton will differ from Haven in being open-source from launch, limiting itself to a US Dollar peg to reduce attack surfaces, and a much more cautious, slow-moving, adaptive mint and burn oracle overseen by service nodes to reduce the chances of black swan failure. We intend for the exact settings of our adaptive oracle's conversion rates to be chosen via empirical observation and experimentation during our upcoming testnet.

2. Oracle

The oracle is an essential component of the SAO protocol. We define our oracle as a 'node' that monitors exchange data and relays that data back to the blockchain. This section will detail how we propose the oracle might query and accumulate exchange data to create a moving average price for use in the mint and burn process. When implemented, we propose the oracle will be run and validated by community run 'service nodes.' These service nodes will be composed of staked volatile-chain Triton (XTRI) coins used as collateral to assure honest behavior of the oracle and the mint and burn exchange rate. For providing this service to the community, service node holders will receive fees from the mint and burn conversion process and be provided with voting rights toward any future protocol changes.

Key Features of the Proposed Oracle.

I. The oracle uses ZeroMQ to connect the blockchain process. ZeroMQ is a high performance asynchronous messaging library that can be used in multiple languages such as Javascript, Golang, C++, and more. By using a request-response system, the blockchain process will reach out to the oracle for data such as block price average (all trades between last block) and to start monitoring the trades.

II. Consensus of prices is essential to the honesty and security of the mint and burn process. This proposal uses oracle blocks that are shared just like regular blocks. A solution for smaller devices is to have 'master public oracles' as remote nodes so devices with less storage space do not have to store oracle blocks. Nodes that do not have at least 480 of oracle blocks cannot submit a new block to the network. Otherwise they would need at least a days worth of prices to create a moving average exchange rate. Oracle hashes will be created and inserted into the regular blocks. This creates a 'link' to oracle blocks (**See Figure 1**). Community discussions and empirical testing will be utilized to refine the consensus mechanism of oracle blocks.

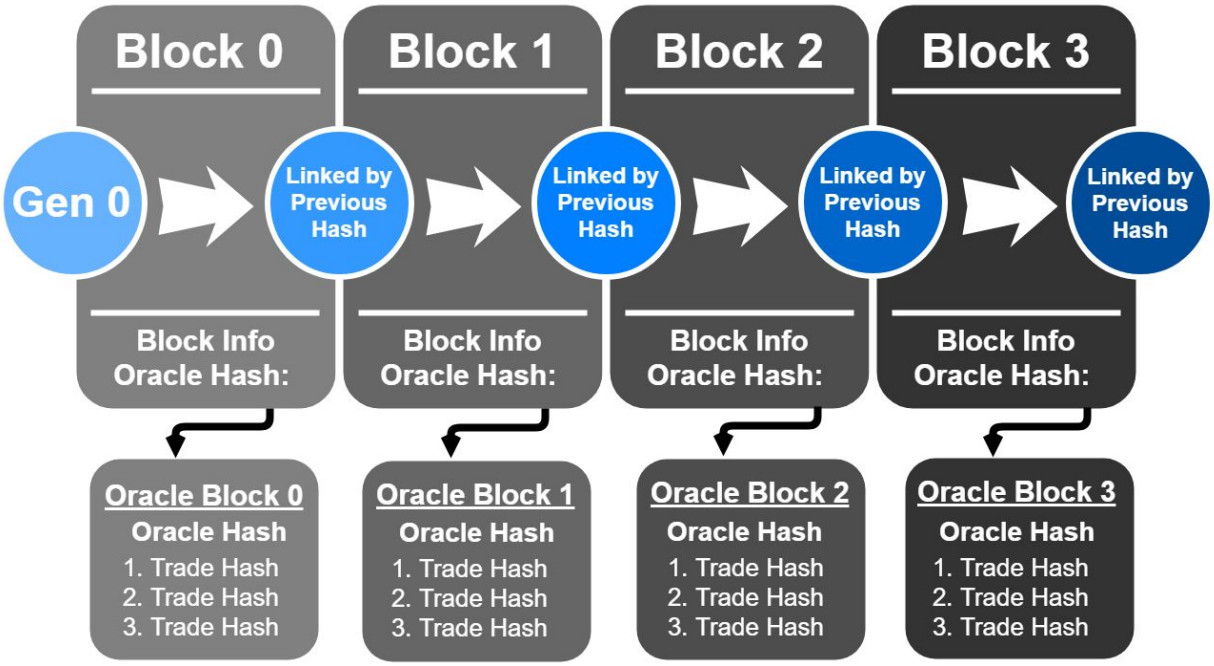

Figure 1. Overview of how hashes will be created and inserted into the regular blocks in the combined Triton (XTRI) and Sao Dollar (SAO) blockchain

III. How is the moving average price found for the mint and burn exchange rate? Price checkpoints are found within every block; these are then used for the next block. The service node consensus oracle polls exchange market history. Trades include: trades between block A timestamp and block B timestamp.

Block A → [trades] → Block B for Block C.

To make sure trades are not added to the array we create a trade signature which is a SHA256 signature of timestamp of trade + price + quantity.

Example Trade:

{price:0.00000145,timestamp:1546677721,quantity:70.91800000,signature:ec344f5d677e69479ceb7180a820a594cdd76cc08fce384289a4f2feb37e02f9}

After the oracle has the trades they will average the price weighted by exchange volume. See weighted average equation below. *ANP* is the price checkpoint for the next block.

*ANP = ((exchange x volume / exchange x + y...) * exchange x average price) + ((exchange y volume / exchange x + y..d.) * exchange y average price)...*

IV. Price checkpoints are created within each block and used to build a 480 block moving average. This 480 block moving average is then used as the mint and burn exchange rate. While this extended block time may create some volatility between the value of SAO and one US dollar, we propose this as a failsafe to increase the cost of any attacks attempting to manipulate the mint and burn market rate. By establishing such an extended moving average for the XTRI / SAO exchange rate, we sacrifice some value precision to significantly reduce the dangers of black swan hyperinflation events and protocol failure. As the protocol becomes more mature and such events become less likely due to increased trading volumes and thus increased attack costs, a 2/3 majority of service nodes will have the ability to vote and reduce the length of the moving average and improve the SAO to US dollar peg.

V: Additionally, mint and burn will be subject to attacks or attempts to insert fake prices into the blocks. More discussion on threats can be found below in the **Risks and Mitigations** section.

3. Mint and Burn

The Triton / SAO protocol uses minting and burning for the creation and destruction of both 'currencies.' A user would burn XTRI to mint SAO and burn SAO to mint XTRI. SAO is differentiated by transaction type. Transactions will be labeled with *isSao* and *unlock_time* will be set to thousands of years away so that transaction is not spendable. Mint transactions will have a return address which is used to send the newly minted coins to. Miners will pick SAO transactions and will then create a coinbase-like transaction in that block to the return address. Transactions that mint SAO or XTRI will have a unlock time of 10 blocks and have a higher fee.

XTRI → SAO. By using the transaction parameter *isSao* we can lock the XTRI forever. This is our 'burn.' Nodes can verify these transactions have been burned by checking the *isSao* parameter.

SAO → XTRI. By using the transaction parameter *isSao* we can lock the Sao forever. This is our 'burn.' Nodes can verify these transactions have been burned by checking the *isSao* parameter.

Privacy. As proposed, this mint and burn system is not perfectly private. You will have to broadcast your return address to the network. However, later development will allow us to create disposable addresses for those users who desire complete privacy. These addresses would be similar to Monero subaddresses, and be easier to keep private. Besides the privacy of users minting and burning, the total amount of the transaction will be known. This will also allow everyone to see how much is minted and burned. Possible development could be made to shroud this number.

4. Risks, Mitigations and Protocol Rules

The authors expect any mint and burn protocol to become subject to various attacks, exploits and risks. The Haven Protocol community has touched briefly on some risks and we will reference attack methods previously discussed by their public community. Oscar is our hypothetical attacker in the following examples.

Price Manipulation. The first area of concern is price manipulation. The 'mint and burn' price is currently averaged over 480 blocks or close to 1 day. This gives a long period of time where attacker Oscar would need to spend lots of money to suppress the price to be able to mint more XTRI than he burned. This attack was showcased in Haven Protocol's white paper.

1. Burn *i* XTRI into *k* SAO (*k* = *i* / *MBP*(480 block averaged price))
2. Sell *x* XTRI to lower price down by *z*% for 480 blocks
3. Burn *k* SAO into *j* XTRI (*j* = *k* * *MBP)*
4. *j* * *current market price* > expenses

Oscar would have to gamble that the price would go back up to a price high enough where his newly *minted coins* * *current price* would be greater than his expenditures. By having a much longer mint and burn moving average than that proposed by other protocols, we intend to sacrifice some precision of value for dramatically improved protocol security. In order to test this, we plan to create a fake exchange along with our testnet that would allow users to 'buy / sell' coins to test out the responsiveness of the moving average and use the data to alter mainnet calculations if necessary.

Oracle Manipulation. Direct manipulation using the oracle could happen if exchange data is tampered with at the exchange level. Making sure only using trusted exchanges are included in oracle moving average prices is key for this system to work. This is to avoid fake volume and possible API manipulation. Adding exchanges or removing exchanges would be done by hard fork.

Mint and Burn Exploit. If the Mint and Burn code has been exploited Oscar could infinitely mint and burn coins. By open sourcing the code, it can be reviewed by anyone and we expect the community to help us find any bugs during the open source testnet period.

Protocol Rules. Implementing additional protocol rules could allow for better security. There are no set in stone protocol rules currently. Protocol rules would be placed / removed by hard forks.

Service Nodes. Using service nodes could provide the protocol with better security (**See Figure 2)**. To run a service node, users would need to stake a certain x amount of coins. The stake needs to be big enough to disincentivize node holders from trying to disrupt the network, but the exact value has not yet been decided. After staking their coins, users running service nodes can get block rewards for approving blocks and obtain limited voting rights for certain protocol rule changes. Service nodes will be rewarded with a block % and from the mint and burn transaction fees.mint and burn transaction fees will be larger than regular transaction fees. Protocol rules would need to be adopted by a ⅔ majority of service node holders. Here are some examples of rules that could be applied: suspend mint and burn for x blocks, volume control or market cap control on mint and bern where only a certain amount of XTRI minting per day is allowed based on the volume or current market cap. There are numerous ways service nodes could be implemented and this is currently under investigation.

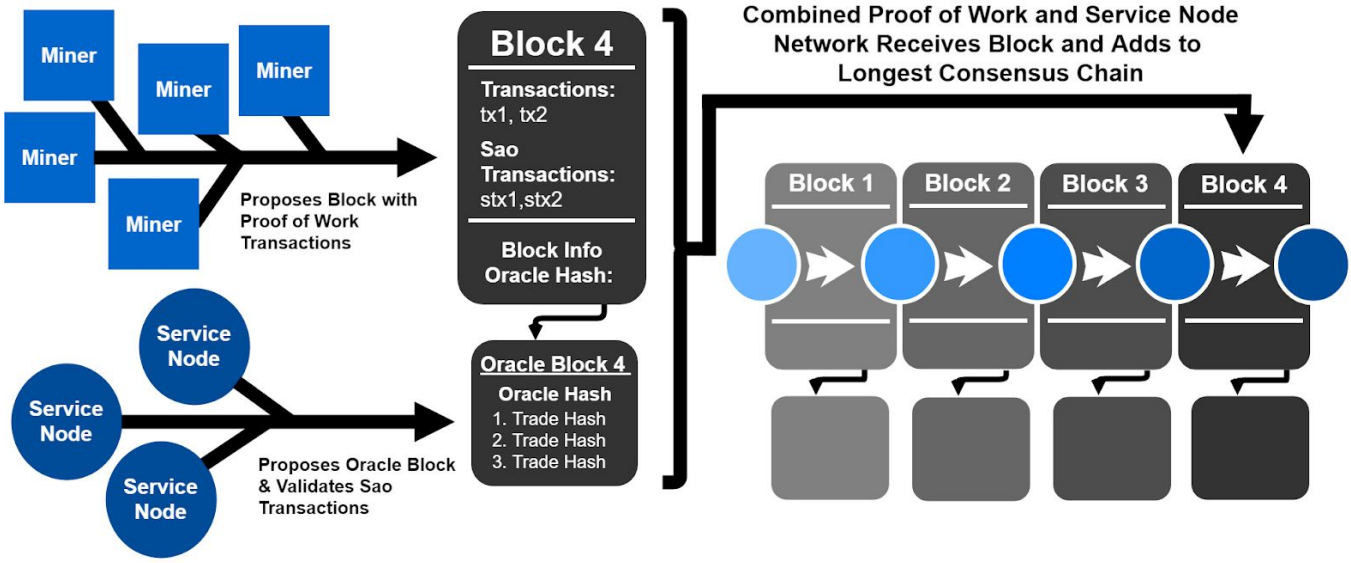

Figure 2. Overview of how service nodes participate in the network.

5. State of the Project

Triton and Neptune. The Triton (XTRI) blockchain is already live. Triton (XTRI), is a decentralized cryptocurrency based on Monero released in early 2018 with a vibrant community and an extant use-case within the Neptune streaming platform. Neptune is a platform which allows streamers to receive tips in Triton and get mining rewards from viewers who mine with the Neptune Extension. Within the Neptune platform, the Sao Dollar (SAO) stablecoin implementation means streamers will get tipped with SAO instead of Triton and thus be buffered from price volatility. In addition to Neptune, Project Triton is working on development of Proteus: an ESports tournament platform where players use computing power to mine Triton. Users will have the option of accepting their prize pool payments in Sao Dollars. We envision

the Sao Dollar (SAO) to both ensure stable value for our streamers and to be useful to the broader cryptocurrency community in ways analogous to the proposed Haven Protocol (XHV). For more information on Neptune or to try it out for yourself - please visit:

neptune.xtri.network

Open Source Code and Testing. This protocol is theoretical and has not been fully implemented into a mint and burn stablecoin cryptocurrency. By opening up the source code we hope to begin community driven discussions as to the specific features of protocol implementation and become more prepared to anticipate the greatest possible variety of attack methods. Initial XTRI / SAO mint and burn protocol rules will be set via experimental testing. Post-launch, mint and burn rules will be open to limited changes by vote of the community of service node holders. Further testing and development, and a final pre-launch technical paper, will be released upon mint and burn mainnet launch. The Triton and Sao Dollar developers encourage you to join our Discord and contribute your thoughts to the broader Sao Dollar stablecoin development community:

https://discord.gg/6VkyUqw

Contributions. Overall concept of dual-coin single-chain mint and burn controlled via service node oracle and draft code by Harrison Hesslink. Support with concept development, stablecoin overview, and manuscript revisions by Tyler W. Hulett, PhD. A sincere thank you to all current and former supporters of Project Triton including Thomas D. Parker, my parents and my sister.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf, 2008.

[2] http://coinmarketcap.com/, 2019.

[3] A. Tan, B. Robertson, M. Leising, “Why Crypto Traders Are So Worried About Tether,” The Washington Post, https://www.washingtonpost.com/business/why-crypto-traders-are-so-worried-about-tether/2019/01/14/8cca36b6-186d-11e9-b8e6-567190c2fd08_story.html?utm_term=.3eddc654760c, 2019.

[4] Tether Limited, “Tether: Fiat currencies on the Bitcoin blockchain,” https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf, 2016.

[5] Maker Team, “The Dai Stablecoin System,” https://makerdao.com/whitepaper/Dai-Whitepaper-Dec17-en.pdf, 2017.

[6] Havenprotocol, “Haven Protocol: untraceable payments x stable value storage,” https://bitcointalk.org/index.php?topic=2989487.0, 2018.

[7] Haven Protocol, “Haven Protocol Public Testnet with Decentralized Oracle Announcement,” https://medium.com/@havencurrency/haven-protocol-public-testnet-with-decentralized-oracle-announcement-8ff8718d7981, 2018.

[8] https://www.havenprotocol.com/, 2019.

[9] C. Kassler, “Announcements, BitCash Stable,” https://discordapp.com/invite/7P4YcXU, 2019.

[10] https://www.choosebitcash.com/, 2019.