Choice Coin: Bitcoin Choices

Hackers[1]
Samuel Tosin | David Kazeem | Brian Haney

2022 MIT Bitcoin Expo Hackathon

May 7th, 2022

[1] Hackers contributed equally to this work.

Table of Contents

Introduction

The Choice Coin DAO was started at the 2021 MIT Bitcoin Expo Hackathon, where our submission Algorand Autonomous won the top prize in the infrastructure track, the Algorand challenge, and the Sia Skynet challenge. During the 2021 Hackathon, we built the foundation and groundwork for what became a global DAO with over 33,000 users and over 100 contributors on GitHub. But one way in which our 2021 submission was lacking was that it failed to incorporate or use Bitcoin and we wanted to change that this year.

Bitcoin Choices is a scalable voting solution for Bitcoin built by a team of developers from the Choice Coin DAO for the 2022 MIT Bitcoin Expo Hackathon. Bitcoin Choices provides a method for using the Algorand blockchain to facilitate fast, secure, and cost-efficient voting for decentralized governance with Bitcoin. The decentralized application is focused on software infrastructure and usability.

At the 2021 MIT Bitcoin Club Expo keynote, Michael Saylor famously asked, can you come up with a better idea than converting all your $BTC into Dollars before you do anything? The problem cuts to the heart of adoption for Bitcoin technology because it challenges us to stop thinking about Bitcoin like an investment and start thinking about it like a key people can use to unlock vaults of value on the blockchain. But the problem is, using Bitcoin as a key is expensive because Bitcoin transactions take a long time and often cost hundreds or thousands of dollars because of the high cost of energy required to validate blocks.[2]

For example, consider Michael Saylor wanted to use Bitcoin as a method for voting on MicroStrategy corporate governance, it would be extremely expensive for his shareholders to have to transfer Bitcoin as a voting token. However, if Bitcoin transactions could happen for less than a penny, then it could save the company a substantial amount of money that would otherwise be spent on governance. Thus, there exists a need for a way to securely vote with Bitcoin in a cost-efficient and timely manner to facilitate governance on the Bitcoin network. Defined, the Bitcoin governance problem is how can Bitcoin be used for fast, scalable, and secure voting with instantaneous results?

The solution is Bitcoin Choices, a scalable, secure, and systemic methodology for voting with collateralized Bitcoin on the Algorand blockchain. Bitcoin Choices allows for Bitcoin governance to happen based on a proportional ownership interest of the total or circulating Bitcoin supply. Perhaps more importantly Bitcoin Choices allows for scalable Bitcoin voting with transactions that cost less than a penny and are recorded on the blockchain near instantly. Global, scalable, and secure – Bitcoin Choices is a tamperproof voting software, leveraging the Algorand blockchain to specifically offer governance as a service to the Bitcoin network.

Part I provides an overview of the Bitcoin Network and the fundamental limitations causing the Bitcoin governance problem. Part II offers analysis of the Algorand blockchain as a scaling

[2] Al-Shehabi Abdullah, "Bitcoin Transaction Fee Estimation Using Mempool State and Linear Perceptron Machine Learning Algorithm" (2018). Master's Projects. 638. DOI: https://doi.org/10.31979/etd.j6zd-an2c https://scholarworks.sjsu.edu/etd_projects/638.

solution for Bitcoin voting. Part III discusses decentralized governance, Choice Coin and the scalable solution to the Bitcoin governance problem.

I. Bitcoin

In the year 2008, an unknown person or persons with the pseudonym Satoshi Nakamoto, published the Bitcoin White Paper, which serves as the foundation for most blockchain technology today. [3] In the Bitcoin White Paper, Nakamoto presents a problem, "Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments."[4] The solution developed is a peer-to-peer network for decentralized transactions called a blockchain. [5]

The design of the Bitcoin network consists of a series of computers connected as new layer of the Internet.[6] According to some, the network architecture is a parasitic function of the Internet.[7] Nakamoto claims what is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a third party.

In the Bitcoin White Paper, Satoshi Nakamoto refers to the blockchain more commonly as a means of solving transactional problems in the financial system and the term cryptocurrency does not appear.[8] They explain for transactions in such a system to be valid, there needs to be a way in which to verify electronic coins are not spent twice. In other words, there must be a method for the payee to know the previous owners did not already spend the electronic coin. Thus, Nakamoto proposes a solution to the double-spending problem using "a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions."[9]

According to one scholar "Perhaps Bitcoin's greatest technological achievement is building a peer-to-peer transaction system relying on cryptographic proof, rather than trust."[10] However, one problem is that mining or solving the necessary cryptographic hash algorithm underlying the Proof-of-Work (PoW) technology requires massive amounts of computing power and brute force search. As a result, PoW blockchains are extremely expensive and economically inefficient. So,

[3] SAIFEDEAN AMMOUS, THE BITCOIN STANDARD xv (2018).

[4] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 1 (2008).

[5] Riley T. Svikhart, *Blockchain's Big Hurdle*, 70 STAN. L. REV. ONLINE 100, 101 (2017). *See also* Emily Wells, et al., Blockchain Benefits and Risks, The Military Engineer, 62 (2018), https://www.researchgate.net/profile/Igor_Linkov/publication/325385235_Blockchain_Benefits_and_Risks/links/5df6b251a6fdcc2837245f1e/Blockchain-Benefits-and-Risks.pdf. ("Blockchain technologies are being considered as solutions to various cybersecurity and information technology threats and challenges.") *See also* Elona Marku, et al., General Purpose Technology: The Blockchain Domain (2019).

[6] David Mills et al., Distributed Ledger Technology in Payments, Clearing, and Settlement 10 (Fed. Reserve Bd. Fin. & Econ. Discussion Series, Working Paper No. 95, 2016), https://perma.cc/UUU6-R2SY.

[7] PAUL E. CERUZZI, COMPUTING: A CONCISE HISTORY 121 (2012).

[8] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 2 (2008).

[9] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 1 (2008).

[10] Ryan Farell, *An Analysis of the Cryptocurrency Industry*, University of Pennsylvania Scholarly Commons (May 2015).

the cost for transactions is unnecessarily high and, in some instances, can cost hundreds of dollars for a single transaction.

II. Algorand

Algorand's technical and structural model gives it a certain advantage when compared to PoW blockchains and corresponding cryptocurrencies. Algorand's proof-of-consensus (PoC) blockchain improves security and power efficiency across blockchain networks by eliminating miners and validating transactions based on a staking consensus.[11] Algorand is the most technically advanced and sophisticated blockchain technology, utilizing advanced post-quantum cryptographic mechanisms and zero-knowledge proofs (ZKPs). The proof-of-consensus mechanism incorporates a timestamp signature,[12] relying on ZKPs instead of hashing for validation.

AlgoMint is a decentralized finance platform on the Algorand blockchain. AlgoMint provides software products and services that allow for Bitcoin to be collateralized and used on the Algorand blockchain.

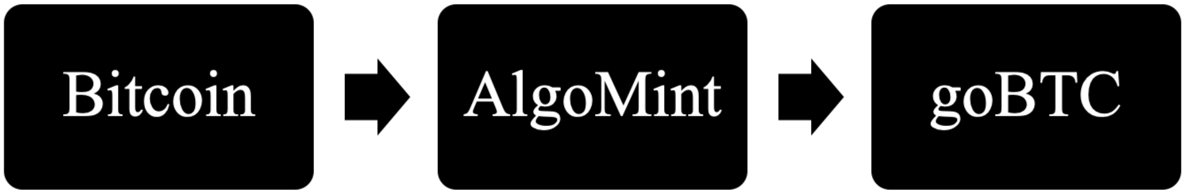

Figure 1

Once on the blockchain, the collateralized Bitcoin $goBTC may be sent in Internet transactions and smart contracts at a fraction of the cost.

The term smart contract is defined in wide variance among blockchain developers and professionals. For example, the Founder of Ethereum, Vitalik Buterin defines smart contract as, "systems which automatically move digital assets according to arbitrary pre-specified rules."[13] Another example, the former MIT professor and current Commissioner of the SEC Gary Gensler, adopts Nick Szabo's definition of smart contract, "A set of promises, specified in digital

[11] Yossi Gilad, et al., Algorand: Scaling Byzantine Agreements for Cryptocurrencies, 53 (2017). *See also* Emily Wells, et al., Blockchain Benefits and Risks, The Military Engineer, 62 (2018). ("Blockchain technologies are being considered as solutions to various cybersecurity and information technology threats and challenges.")

[12] Tal Rabin, A Simplified Approach to Threshold and Proactive RSA, 90, Annual International Cryptology Conference (1998). ("Proactive signature schemes use threshold signature schemes as the basis but drastically reduce the assumption concerning failures.") *See also* Scott J. Shackelford, Steve Myers, Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace, 19 Yale J. L. & Tech. 334, 351 (2017). *See also* Tal Rabin, Verifiable Secret Sharing and Multiparty Protocols with Honest Majority (1989).

[13] Vitalik Buterin, Ethereum White Paper, A Next Generation Smart Contract & Decentralized Application Platform (2013).

form, including protocols within which the parties perform on these promises."[14] On Algorand, smart contracts are software systems that can be used for transactions and applications development.[15] Generally, and for the purposes of Choice Coin technology, a smart contract is a computer program which transfers data between addresses on the blockchain using a digital signature.

Algorand smart contracts are much faster and more efficient for transferring Bitcoin when compared to smart contracts on other blockchain networks such as Ethereum, due to the heterogeneous way in which the network is programmed.[16] The low transaction fees are possible because of Algorand's innovative proof-of-consensus PoC mechanism, which validates blocks more efficiently and swiftly than the PoW mechanism. Specifically, Bitcoin Choices use Algogeneous smart contracts, which is a new type of software we invented to bridge the gap between technical, business, and legal understandings of contracts – and to provide efficiency improvements for voting applications.[17]

III. Governance

Voting is important because it is a key method by which collective information is processed to make decisions.[18] In fact, the right to vote is the central tenant of modern democracy and a principle means for asset allocation across both public and private markets. Some suggest, voting is a central feature for a free society because it provides the only mechanism for a democracy under a rule governed by the people. Now decentralized voting is a key to DAO infrastructure in the growing decentralized Internet.

Bitcoin Choices draws inspiration from the simplicity of the first voting machine, which was invented by Thomas Edison, "...to produce an apparatus which records and registers in an instant, and with great accuracy, the votes of legislative bodies...", in the year 1869.[19] *Simplex sigillum veri* stands for the principle, simplicity is the sign of truth – complexity only confuses. The simplicity principle was Edison's North Star – and it is the same North Star for Bitcoin Choices.

One of the main problems with smart contracts on Algorand is that most smart contracts on Algorand are not smart and they are not contracts. Of course, that doesn't mean they aren't smart contracts – it's a term encompassing a massive body of academic research and professional industry. Still given the complexity and lack of usability, we needed to build a new type of smart contract on Algorand to vote.[20]

[14] Gary Gensler, Blockchain and Money, Lecture 6 Smart Contracts and dApps, MIT OpenCourseWare (Fall 2018).

[15] Massimo Bartoletti, A formal model of Algorand smart contracts 1, arXiv:2009.12140 (2021). ("Smart contracts are agreements between two or more parties that are automatically enforced without trusted intermediaries.")

[16] Massimo Bartoletti, A formal model of Algorand smart contracts, 1 (2021), https://arxiv.org/abs/2009.12140v3. ("Smart contracts are agreements between two or more parties that are automatically enforced without trusted intermediaries.")

[17] Archie Chaudhury and Brian Haney, Algogeneous smart contracts (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3887719.

[18] A consensus is a defined majority or agreement.

[19] U.S. Patent No. 90,646 to Edison, Electric Vote-Recorder (June 1, 1869).

[20] U.S. Patent Application 17,375,542, Algogeneous smart contracts (2021).

Algogeneous smart contracts represent a technical convergence of stateless and stateful smart contracts on the Algorand blockchain.[21] Figure 2 is an information flow model for Bitcoin Choices voting technology.

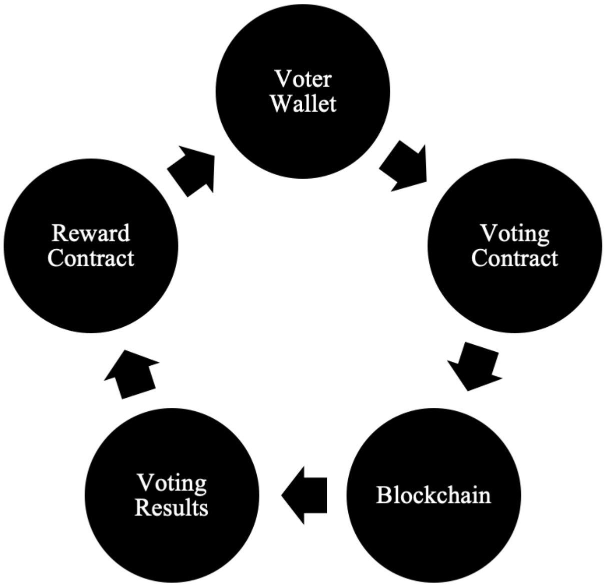

Figure 2

The voting contract is an Algogeneous smart contract that receives an amount of Satoshis with which the voter intends to vote and then sends the Satoshis from the voter's wallet to the blockchain automatically on the push of a button. The blockchain then records the collective number of votes stored on the blockchain. Then, the reward contract reads the results and calculates a proportional distribution of a reward pool for each voter. Finally, the reward contract returns the committed votes to the voter's wallet, plus a proportional reward from the reward pool.

The voting algorithm treats 1 Satoshi, which is the smallest unit of Bitcoin, as 1 vote. This allows for a democratic consensus based on proportional ownership and still supports participants with smaller sums of Bitcoin.

$$v \in V : r \in R$$

The reward contract automatically calculates each voter's rewards *r*, using a proportion *v* of the vote *V*, compared to the reward pool *R*, then returns committed Satoshis and the proper reward amount to the voter's address.

$$d = \{v : r\} \in \{V : R\}$$

The reward contract distribution returns both the voter's votes, *v*, and rewards *r*, as a set of the total votes *V* and the total rewards *R*.

[21] Archie Chaudhury and Brian Haney, Smart Contracts on Algorand, SSRN 3887719 (2021).

Conclusion

Part I introduced an high-level view of Bitcoin and its limitations causing the Bitcoin governance problem. Part II introduced analysis for Algorand's ability to act as a scaling solution for Bitcoin governance using AlgoMint to bridge assets. Part III discussed distributed governance, the Choice Coin DAO, and our scalable solution to the Bitcoin governance problem – Bitcoin Choices.