Blockchain Technology: A Decentralized Future

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Lucas Banerji

Fall, 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Rosanne Vrugtman, EN-Comp Science Dept

ABSTRACT

Because blockchain technology in the modern business space has been changing so rapidly, many corporations are having difficulties understanding the different applications of blockchain and how it works. To solve this problem, this technology needs to be more transparent and accessible for businesses and government alike. This paper explores the underlying infrastructure of blockchain technology as well as current and potential applications. The possibilities tied to this technology are both incredibly powerful and frankly limitless as its use cases extend far beyond cryptocurrencies and may change the way data is perceived. Both businesses and governments would benefit tremendously from understanding blockchain and how it can reshape the modern world.

1. Introduction

Blockchain technology follows the trend of revolutionary computing models emerging around every decade. Mainframe computers in the 60s, PCs in the 70s, internet in the 90s, mobile phones in the 2000s; common across each of these models are the plethora of new applications developed which leveraged the strengths of the emergent platforms. First introduced in 2008 through the Bitcoin whitepaper by Satoshi Nakomoto, blockchain technology ensures *trust* between users, developers, and the platform itself through groundbreaking algorithmic and cryptographic mechanisms rather than based on the *trustworthiness* of participants within the network. Through my research I’ve discovered that the applications for such a system are both incredibly powerful and frankly limitless. More specifically, with the emergence of blockchain and the movement towards web3, users have the ability to control and own their own data. This presents a fundamental shift away from the current standard of massive companies owning the data of individual users. With all of the social media buzz and plethora of misinformation online, it can be difficult to traverse through and gather information on how blockchain actually works. As mentioned by Yawar and Shaw, “Since its introduction, blockchain technology has been revered, ridiculed, dismissed, embraced, and presently has become too large to ignore, witnessing exponential growth” [12]. Unlike many other emerging technologies, blockchain has been scrutinized as a sort of pseudo technology due to its apparent correlation with Bitcoin, which has been extremely volatile and subject to lots of negative press. However, unbeknown to the general populace, there are hundreds of applications of blockchain technology that have not yet been implemented. As this technology starts getting more and more integrated into various systems, the importance of understanding it will increase dramatically within the world of business and government alike.

2. Review of Research

Buterik, is his Ethereum whitepaper [1], provides a useful reference and an accurate representation of Ethereum and its vision.
Ethereum blockchain was initially built to provide more and better features to users as compared to Bitcoin. However, Ethereum has many more applications beyond that of just a cryptocurrency. Ethereum allows for the existence of smart contracts and decentralized applications through a Turing-Complete programming language.

Decentralization is one of the words that is used in the cryptoeconomics space the most frequently, and is often even viewed as a blockchain’s entire raison d’être, but it is also one of the words that is perhaps defined the most poorly. In his medium article, *The meaning of Decentralization [2]*, Buterik explains the three types of decentralization. When people talk about software decentralization, there are three separate axes of centralization/decentralization that they may be talking about. While in some cases it is difficult to see how you can have one without the other, in general they are quite independent of each other.

Dixon [3] discusses ideas for bitcoin applications in the field of finance, computing, marketplaces, and software. While the first phase of Bitcoin was about laying the foundational infrastructure - gateways, consumer wallets, developer platforms, merchant services etc., the next phase will be about native Bitcoin apps - building new things that could never have been built before. These will likely be the applications that drive Bitcoin and blockchain adoption into the mainstream.

Hart et al [4] dissects the meaning of a *headless brand*. While brands have traditionally been planned and designed directly by corporations, the rise of networked media has challenged the coherence of centrally-managed brand identities. New blockchain-based decentralized organizations take this a step further by giving users financial incentive to spread brand narratives of their own. Hart et al. introduce the concept of headless brands to explain the community-driven brand dynamics of projects which have no centralized managerial body. They describe some elements of a headless brand's lifecycle, from formation to adoption, and suggest strategies to maintain a brand's coherence.
McCormick [6] dives deep into decentralized autonomous organizations and how they may reshape businesses. Decentralized Autonomous Organizations (DAOs) are a new kind of organizational structure that run as code on blockchains. They're owned and run by members who normally hold tokens that provide decision-making rights and/or economic rights in the organization. DAOs allow members from anywhere in the world to pool capital and code rules for how they would allocate the capital. Governance is meant to be automated by code and de-centralized (in other words, no one can tamper with the rules).

In the original Bitcoin whitepaper [7], Nakamoto outlines why he thinks that a trustless cash system is needed in the first place. The main reason stated is that traditional payment systems used in commercial settings operating via financial institutions such as banks have a number of flaws. For one, traditional payments often involve high transaction and mediation costs that may arise if there is a dispute about a transaction, for instance, if a transaction needs to be reversed. Secondly, traditional payment systems are prone to fraud and thirdly, they always require a trusted third party. The Bitcoin Whitepaper proposes a system in which third parties, if any, such as escrow services for the primary transacting parties, can easily be implemented but only if needed, by triggering some type of coded action.

Pruden and Choksi [8] provide a glossary of terminology and key concepts in the blockchain space — it covers the basics of cryptography, smart contracts and applications, security/privacy, and other useful definitions.
Szabo [9] argues that smart contracts provide the blueprint for ideal security. Smart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means. Smart contracts reference that property in a dynamic, often proactively enforced form, and provide much better observation and verification where proactive measures must fall short.

Walden [10] discusses how he would approach building a crypto startup. Crypto founders have a unique challenge in front of them. In addition to building a product that people want, they also need to consider how that product can successfully run in a decentralized manner — that is, as a protocol owned and operated by a community of users. This is a difficult challenge because much of what it takes to build a successful product at the outset — product leadership, rapid iteration, a managed go-to-market — complicates the path to community ownership and regulatory compliance, which guarantee long-term health.

3. Blockchain Elements

This sections contents lie on a spectrum of technical complexity, starting with high level considerations of the advantages of decentralization followed by a detailed description of blockchain mechanics outlined in the original Bitcoin whitepaper. Next, I commence a deep dive into the various categories of derivative applications which the protocols have enabled, specifically smart contracts and decentralized autonomous organizations (DAOs).

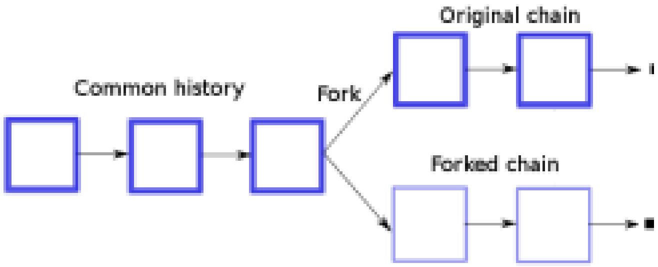
3.1 Decentralization

Vitalik Buterin, the creator of Ethereum, argues that there exist three types of decentralization within computer systems: architectural, political, and logical [2]. Architectural decentralization refers to the number of physical computers comprising a given system and the system's resilience when faced with breakdowns at scale. Political decentralization is defined by the number of individuals or organizations which control the assets of a system. Logical decentralization concerns the actual software structure of a system; does it resemble a monolithic object or is it more akin to an amorphous swarm? Buterin's *gedankenexperiment* aimed at illustrating how logical decentralization works: "if you cut the system in half, including both providers and users, will both halves continue to fully operate as independent units?" [2]. Next consider the multiple advantages to decentralization, specifically fault tolerance, attack resistance, and collusion resistance. If a system relies on many separate components, it follows that it will be less likely to fail accidentally. Many other systems follow this principle including jet engines, generators, and the familiar diversified portfolio of financial assets. Regarding attack resistance, a system lacking vulnerable central points will prove far more expensive to destroy, especially when considering the concept of attack/defense asymmetry. The following example exhibits this idea well: a building which cost $10m to build may in fact cost less than $100k to destroy. Sublinear attack leverage, however, implies that smaller systems appear more robust since a building which cost $1m to build likely would cost closer to $30k to destroy. Before diving into the mechanics of blockchain, it is important to understand another powerful aspect to Bitcoin's decentralization: its *headless brand* [4].Traditionally, companies have imposed a hierarchical brand management model, however, in the context of Bitcoin, all subsequent brand collateral since Nakamoto's whitepaper has been created by stakeholders within the crypto community. The strength of Bitcoin's headless brand primarily derives from the following rigid characteristics of its protocol: only 21m BTC will ever circulate, the currency is non-fiat therefore aligning with anti-authoritarian and economic crisis narratives, and the efficacy of its trustless proof of stake mechanism. More broadly, any cryptographic token must incorporate the views of all its stakeholders to ensure the maintenance, and hopefully growth, of its headless brand.

3.2 Blockchain Mechanics

To provide an accurate, comprehensive, yet sufficiently nontechnical description of the blockchain, consider a simple digital ledger system built to track the money owed between a group of friends where any ledger transaction requires an associated digital signature. Without some method to superimpose additional verification, a digital signature is meaningless since it can theoretically be replicated by an identical string of 0s and 1s. The first component of the blockchain addresses this dilemma with digital signatures involving a public key / private key (sometimes referred to as a secret key) pair. Additionally, note that each digital signature changes for different messages regardless of whether they originate from the same sender, i.e. altering a message even slightly would completely change the signature. Next, a signature function takes the message and the secret key as parameters, and outputs the digital signature. To verify this message, another function takes the message, signature, and public key as inputs and outputs true or false, indicating the veracity of the transaction. Each digital signature is 256 bits implying 2^256 possible signatures exist; this is an incredibly large number, comparable to the number of atoms in the universe. Next, note that any given party within the network cannot overspend their allotted *ledger dollars*, i.e. participants are barred from transacting if they've reached exactly zero *ledger dollars*. Therefore, verifying any transaction requires knowledge of the full network's transaction history, or access to the entire ledger. For Bitcoin, this transaction history *is the currency* and each party within the network maintains their own copy of the globally distributed ledger. The next step is for each transaction between individual parties to be broadcast out across the entire network so that each participant can record it on their ledger. This bodes the question: how can one ensure everyone is recording the same transactions in the same order? The answer is to trust whichever ledger has the most computation work put into it, a system better known as *proof of stake*.

The first step to understanding proof of stake is familiarity with the cryptographic hash function, SHA256. Algorithms that ensure the integrity of data in software applications, hash functions have the following key properties: they're deterministic so that the same input results in the same output, they're non-invertible so that the output reveals no information about the input, and they're collision-resistant so that no two inputs should result in the same output [9] . A central component to essentially all modern digital security systems, SHA256 is incorporated within the previously described signature function. The next question to ponder is how this function *proves* a particular list of transactions is associated with a large amount of computational work. Imagine you're given a list of transactions and asked to identify a number that when appended to that list and inputted into the hash function outputs a signature with 30 leading zeros. This would require about 1 billion guesses as 2^30 = 1073741824. Given a number, however, to assess its veracity one simply hashes the combined transaction list and number pair to observe whether the outputted signature starts with 30 zeros. The process of finding this unique number is the core mechanism defining proof of work. Next, imagine organizing a ledger into blocks, each of which consists of a list of transactions together with the proof of stake. Furthermore, a block is only considered valid if it carries proof of stake and must also contain the hash of the previous block in its header. This structure of blocks chained together is, you guessed it, the blockchain. Based on this system, if any block's data is changed or if the order of the blocks is swapped, every proceeding block in the chain would be impacted, requiring all the work to be redone. Within a network, anyone can be a block creator, otherwise known as a miner, and be compensated with cryptocurrency paralleling their computing contributions. Let's now illustrate how proof of stake protects against malicious actors within the network. Imagine participant X is attempting to deceive participant Y by sending them a fraudulent block containing outgoing payments from participant Y to participant X, without broadcasting it to the rest of the network. In order to execute this strategy, participant X would have to find valid proof of stake before all other miners in the system. Keep in mind participant Y still receives broadcasts from the other miners, and when faced with conflicting messages, will fork their own blockchain (depicted below) [6].



Due to the randomized nature of the proof of stake mechanism described previously, unless participant X retains close to 50% of the network's computing resources, the probability becomes overwhelming that the blockchain all other miners are working on grows far faster than the fraudulent chain. Therefore, participant Y will eventually reject participant X's blockchain and avoid being duped. This ingenious system ensures the entire network achieves decentralized consensus.

3.3 Smart Contracts

The concept of smart contracts is absolutely central to any discussion of the myriad possibilities for decentralized apps. The main idea behind smart contracts is that distinct kinds of contractual clauses can be directly inlaid within software to make breach of contract expensive and retribution automated. Curiously, they're also somewhat analogous to vending machines: "The vending machine is a contract with the bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas" [10]. Extending beyond the vending machine example, smart contracts can theoretically digitally embed contractual obligations concerning any kind of valuable property. Specifically, blockchain protocols would provide cryptographic keys necessary for use of the property to the rightful property owner, based on previously defined contractual terms. The following example of a security system for automobiles perfectly illustrates the utility of smart contracts. A straightforward implementation would simply prevent car theft by prohibiting use without completion of an identity information protocol, however, the beauty of smart contracts reveals itself when credit is introduced. Traditionally, an automobile repossession agent would be hired by a creditor to retrieve property in the case of default, but with the introduction of a *smart lien protocol*, if the car owner fails to make timely payments the smart contract would invoke the protocol and return control of the car keys to the bank. This mechanism would almost certainly prove cheaper, faster, and overall, more effective than employing a repossession agency. To recap, the smart contract would include the following features: a lock to selectively allow access to the owner, as well as a back door for the creditor switched on upon extended nonpayment or default but erased once the owner fully pays off the loan. As demonstrated by the example, blockchain technology has the potential to dramatically reduce inefficiencies related to contractual clause execution and collateral seizure. Significant qualitative differences in types of contractual terms and specific technological differences between property types necessitates creation of a diverse set of smart contract protocols, however.

3.4 Decentralized Applications

Vitalik Buterin initially divided the spectrum of decentralized applications space into three categories in the Ethereum whitepaper: financial, semi-financial, and non-financial applications. Exclusively financial applications of blockchain technology are concerned with providing users better ways of managing money and entering monetary contracts; this category would include sub-currencies, financial derivatives, hedging contracts, savings wallets, wills, and perhaps eventually even employment contracts. Semi-financial applications do involve money in some capacity but also include a significant non-monetary angle; one such example would be bounties rewarded for computational solutions. Finally, examples of non-financial applications would include online voting or decentralized governance.

Venture capitalists drawn to the space also identified several verticals with explosive growth potential even before the introduction of Ethereum. For example, Chris Dixon, a general partner at Andreesen Horowitz, published a blog post exploring decentralized application possibilities as early as 2014, titled, *Some ideas for native bitcoin apps.* In it he proposes five primary ideas: international microfinance, bandwidth/storage/compute allocation, marketplaces, micropayments, and incentivized social software. His thesis regarding international microfinance is simple yet compelling: "Bitcoin removes most of the cost and friction of cross-border transactions and allows anyone with internet access to participate in the global economy [3]."In terms of computer-related resource allocation, Dixon argues blockchain technology could support a protocol by which nodes efficiently and seamlessly pay for networked resources. Today, Filecoin has proven the efficacy of this model; by coincidence, New York City recently announced plans to store public data on the platform in an effort to determine whether decentralized networks can improve government operations [5]. Additionally, Dixon perceives a serious convenience problem for marketplace operators attempting to pay partners and customers with or without a bank account. Instead, using blockchain the possibility of mobile crowdfunding and crowd labor services emerges. Finally, Dixon coins the term *incentivized social software* to refer to social media platforms replacing likes, followers, upvotes, etc. with actual monetary incentives in the form of cryptocurrency. Fascinatingly, at varying levels of efficacy, each of Dixon's main theses has been proven viable since his article.

Returning to the Ethereum whitepaper, Buterin elaborated on decentralized financial derivatives and stable-value currencies with the foresight of a Greek oracle, claiming they would likely be some of the most common applications of smart contracts as well as some of the simplest to program [1]. For example, one highly relevant application would be a smart contract that hedges against the volatility of Ether, or any other cryptocurrency for that matter, with respect to the US dollar. Implementing this would require the smart contract to constantly receive updated values for the ETH/USD exchange rate, perhaps from a separate data feed smart contract created in partnership with a specific financial party like NASDAQ. This straightforward yet potent application would be coveted within crypto-commerce for example, where many users and merchants may be attracted to the security and convenience of crypto assets but fear their punishing volatility. Since a trusted third party is necessary to provide the price ticker, the approach is therefore not fully decentralized. Given that a decentralized market of speculators are providing the funds to back an asset rather than a single issuer, however, this system arguably significantly reduces the threat of fraud and lowers infrastructure requirements. In addition to brainstorming DeFi possibilities, Buterin also first introduced the concept of DAOs, or Decentralized Autonomous Organizations. Described as a "virtual entity that has a certain set of members or shareholders which, perhaps with a 67% majority, have the right to spend the entity's funds and modify its code," Buterin indicates a complete DAO would contain fully built out asset management functionality, the ability to buy or sell shares, and the capacity to accept offers using an internal order-matching mechanism [1].

3.5 Decentralized Autonomous Organizations

Simply put, DAOs are a novel way to finance ideas, govern communities, and share value. More technically, they're a series of smart contracts that define which parties own what and how decisions are made within an organization. DAOs are the next step in the natural progression of digitization, where information, money, and now organizations are transformed into a faster, cheaper and more accessible digital alternative: information became the internet, money into cryptocurrency, and now organizations may become DAOs. Labelled decentralized as they leverage the blockchain to transfer decision making power from a traditional management team to community stakeholders and deemed autonomous due to their dependence on smart contracts rather than human intermediaries, DAOs distribute authority and financial rewards by issuing tokens reflective of contribution. Thereafter, token holders can submit proposals, vote on proposals, and engage in other community activities dependent on the DAO's relative complexity. The following section from the Not Boring newsletter by Packy McCormick describes the relationship between various Web3 layers: "If blockchains, NFTs, smart contracts, DeFi protocols, and DApps are tools, DAOs are the groups that use them to create new things. If they're the what, DAOs are the how. They're the Web3 version of a company or community. And as people experiment with new building blocks and structures, DAOs will have emergent properties that we can't predict today" [7]. Simply because a business involves cryptocurrencies doesn't entail that it leverages a decentralized business model, and just because a model is decentralized doesn't imply it is also a DAO. Consider the examples of Coinbase and Uniswap to illustrate how two superficially similar companies actually maintain wildly different operational models. Coinbase is a centralized cryptocurrency exchange which matches orders and extracts a transaction facilitation fee as revenue. It is in every way a traditional centralized company with investors, a board, and a management team which dictates the organization's direction. Uniswap, on the other hand, is a decentralized exchange running on Ethereum, with no say in what can be traded and no hand in providing liquidity. Instead, Uniswap's operations are dictated by a series of smart contracts which state that anyone can serve as a liquidity provider by locking up capital in any pair of supported tokens. In exchange, these liquidity providers receive liquidity tokens proportional to their share of liquidity in any given cryptocurrency pair and capture the corresponding fee stream resulting from Uniswap's .3% transaction fee. Only recently, however, did Uniswap become a DAO after announcing the UNI token which gives holders governance rights, or the ability to directly influence the protocol's future.

The point of DAOs is to maximize stakeholder value since users and contributors are simultaneously investors and owners. The concept seems alien, even anti-capitalist, but Mr. McCormick quite persuasively argues "it's actually a more natural model than a few outside investors and board members dumping a bunch of money into a company and deciding what it should do [7]. Let's explore exactly how DAOs may prove superior to traditional operational structures and build sustainable moats. Surprisingly, DAOs benefit from economies of scale as they give groups of people across the world the ability and incentive to pool resources, therefore driving costs lower as they acquire more users and produce more units. Additionally, DAOs experience tremendous network effects since each new user within the protocol theoretically drives the DAO's token value higher, therefore benefiting all current users who are also all token holders. Finally, DAOs have strong counter-positioning as incumbent competitors are highly unlikely to suddenly transform their traditional company into a DAO, in fact this maneuver is infeasible for the vast majority of companies.

4. Future Work

Blockchain technology is inextricably intertwined with Bitcoin and other cryptocurrencies. Most of the people currently interacting with blockchain networks do so only because that's how they buy and sell cryptocurrencies. But most people have not yet purchased crypto, and a future in which you can make all your everyday purchases with Bitcoin, or another cryptocurrency seems far away. Cryptocurrency alone is not sufficient to push blockchain to its full potential. If that's all blockchain is good for, that's why blockchain will fail to become a mainstream technology. But there is more. Much more. A compelling decentralized financial app could propel blockchain into the mainstream. Hundreds of DeFi apps are now available, with more appearing every day. Non-fungible tokens have brought many new users to the blockchain world through games, artworks, collectibles, and investments that are implemented with NFT technology. Some of these fields are composed of millions of potential users, so one of them might turn out to be blockchain's killer app. The metaverse could turn out to be the gotta-have-it service that brings blockchain to the masses. Many of the metaverses currently under development use blockchain technology under the hood, if only to verify identity and represent personal belongings as NFTs. Blockchain technology meets real needs in all of these fields, and any one of them could explode into consumer consciousness and make blockchains omnipresent. It's hard to predict which it might be. How big is the blockchain future? It's potentially huge.

5. Conclusion

Blockchain technology found its first real-world application with the launch of Bitcoin in 2009. Since then, entrepreneurs in a variety of industries have begun exploring the technology's potential. Blockchain technology is finding its way into fields as diverse as health records management, digital identity verification, supply chain tracking, and video games. The ability of Ethereum and other blockchains to store and execute computer code has multiplied the number of use cases for this innovative technology.

This paper was largely aimed at building a robust conceptual framework for Web3; a lens through which rapid crypto/blockchain innovation could be understood and compared to the current technological status quo. I expect I'll frequently revisit this piece and iteratively improve the now skeletal frameworks within it as I continue to learn more about the industry.

6. REFERENCES

[1] Buterin, V. (2014). *Ethereum whitepaper*. ethereum.org. Retrieved December 1, 2022, from https://ethereum.org/en/whitepaper/

[2] Buterin, V. (2017, February 16). The Meaning of Decentralization [web log]. Retrieved December 1, 2022, from https://medium.com/@VitalikButerin/the-meaning-of-decentralization-[illegible].

[3] Dixon, C. (2014). *Some ideas for native bitcoin apps*. cdixonorg RSS. Retrieved December 1, 2022, from https://cdixon.org/2014/10/04/some-ideas-for-native-bitcoin-apps

[4] Hart, S., Lotti, L., & Shorin, T. (2019). *Headless brands*. Headless Brands. Retrieved December 1, 2022, from https://otherinter.net/research/headless-brands/

[5] Johnston, R. (2021, December 16). *Crypto-affiliated platform to store copies of New York City open data*. StateScoop. Retrieved December 1, 2022, from https://statescoop.com/new-york-city-filecoin-cryptocurrency/

[6] Leoussis, A. (2021). *All about Forks.* Coinomi Support. Retrieved December 1, 2022, from https://coinomi.freshdesk.com/support/solutions/articles/29000018129-all-about-forks%203

[7] McCormick, P. (2021, March 22). The Dao of DAOs. Retrieved December 1, 2022, from https://www.notboring.co/p/the-dao-of-daos

[8] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved December 1, 2022, from https://bitcoincash.org/bitcoin.pdf

[9] Pruden , A., & Chokshi, S. (2022, June 2). *Crypto glossary: Cryptocurrencies and Blockchain*. Andreessen Horowitz. Retrieved December 1, 2022, from https://a16z.com/2019/11/08/crypto-glossary/

[10] Szabo, N. (1997). *The Idea of Smart Contracts*. Nick Szabo -- the idea of Smart Contracts. Retrieved December 1, 2022, from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

[11] Walden, J. (2022, June 2). *Progressive decentralization: A playbook for building crypto applications*. Andreessen Horowitz. Retrieved December 1, 2022, from https://a16z.com/2020/01/09/progressive-decentralization-crypto-product-management/

[12] Yawar, S. M., & Shaw, R. (2022, July). *Augmenting blockchain with competition law for a sustainable economic evolution*. Frontiers. Retrieved September 14, 2022, from https://www.frontiersin.org/articles/10.3389/fbloc.2022.931246/full