BUILDING WEB 3.0 ON BITCOIN

Updated as of September 2021

Table of Contents

Introduction

Internet is this amazing intangible thing that enables the world to be connected, and with every additional user connecting to it, its value increases incrementally. As for the new user who just gained internet access, it's like opening an ever-expanding encyclopaedia and a phone directory that allows you to connect with almost anyone across the globe, all packed into a device the size of your palm. The computing power you possess with this palm-sized device is multiple folds of what Apollo had when it embarked on its mission to send humans to the moon for the first time. It certainly sounds utopian to anyone who first hears about the internet and mobile computing, about the limitless possibilities this innovation can bring to mankind. It surely is, when the public first discovered the internet when the world wide web became mainstream, the euphoria kickstarted the dot com era and a generation of new companies and business models were created that drastically improves our way of life.

The rise of the internet

The internet was originally used by the military, powered by ARPANET which subsequently adopted the TCP/IP protocol standards developed by Robert Kahn and Vinton Cerf[1]. It was only when Tim Berners-Lee invented the World Wide Web which makes accessing data online easier in the form of websites and hyperlinks that we saw wider adoption of the internet. This initiated the digital revolution that we're all part of as commercial use of the internet increases.

The key innovation of the internet was to enable information/data to be transmitted/replicated across the globe at little to no cost once the infrastructures are in place. Relatively fixed costs as public goods, but exponential value gain overtime for any users/entities when scale is achieved. This is where the telephone and fax machines fell short, while they enabled global connection, data transmission was expensive therefore usage was limited thus making innovation and new experiments on them prohibitive. With the internet, it enabled new business dynamics to occur such that a centralized vendor can facilitate a huge amount of activity over the internet with relatively light physical assets and bringing network effects to a global scale (where traditionally network effects have been limited by your physical geographic location).

Dotcom era

Dotcom era euphoria, seen by many as a financial disaster with stock prices plummeting and an abundance of fraudulent claims in the private/public markets with companies going bankrupt weeks/months after going public. However, to a certain extent such euphoria, while short-lived and had lasting implications on market participants that were involved, it accelerated innovation and attracted more talents into the industry. With the likes of Facebook, YouTube, LinkedIn and more started after the dotcom crash, the euphoria certainly created more awareness about what the internet could be, and thereby inspiring the next-generation technology companies to be built[2]. Companies that survived the market boom and bust while keeping their heads down, constantly building and delighting their customers, emerged stronger. Some anecdote examples like Amazon, Microsoft, Apple, Google, Adobe Systems, Nvidia and many more survived the dot-com crash and emerged stronger in their own ways thereafter. During the dot-com peak, the market overreacted too much over a short period of time to the potential the internet could bring to the economy, which led to a steep correction shortly after. However two decades on, we're merely realising the potential of the internet on

[1] https://www.history.com/news/who-invented-the-internet

[2] https://www.wired.com/insights/2013/08/tech-boom-2-0-lessons-learned-from-the-dot-com-crash/

a global scale from productivity gains, improved quality of life, unlocking new business value, etc, and companies surpassing their dotcom peak multiple folds with no signs of stopping. New emerging technologies are often overhyped in the short-term but are underestimated in the long term. The possibilities might be infinite, but it requires, time, talent and resources for these technologies to be built out and for the industry to mature.

Drawing reference from the dot-com era, the crypto industry witnessed its own version of boom and bust on multiple occasions during its short history (13years) with 2017 getting the most attention from mainstream media and the wider market. The euphoria that the bull market brought to the crypto industry certainly excites many and brought awareness to the industry. While it attracted bad actors and opportunist creating subpar/borderline fraudulent projects soliciting funds from the unintended, the awareness the euphoria created have also attracted talents, resources and infrastructures from other industries to be involved. While corrections after a euphoric market can be painful for participants if they are caught on the wrong side of the trade, looking back four years on, you'd realise that a significant number of folks who were drawn into crypto due to the euphoria in 2017. Many stayed on to build/contribute to the wider crypto ecosystem, with various key infrastructures being built during the crypto winter of 2018-2019.

Web 3.0

As more businesses build on top of the internet, value creation and value capture were done on top of the internet, as seen from the various big technology companies operating in the industry now. Value accrues to the gatekeepers of these key services (e.g. Data – online search, e-commerce marketplace, Mobile platform) that the general population have grown accustomed to. Over time, through sheer prowess in execution, deep understanding of the market and strong balance sheet, these companies can fight off competition (or acquire them) to maintain their market position and expand into parallel sectors while gradually increasing their power in the market. Society is coming to terms with the dangers of Web 2.0 limitations, while the internet certainly improved our lives and increased our productivity, it presents a new set of challenges that needs to be overcome. Epic-Apple antitrust case[3] and the other hearings of antitrust cases against Big Tech[4] gave us hints of what is to come as companies build their ecosystem as walled gardens[5]. Social Media companies in 2021 de-platformed the 45th President of the United States[6] is treading on a very fine line of ethics, and have also shown the world that technology companies do have the power to censor users if they deem that there were violations in their terms of use. This creates a scenario whereby the services that big tech companies provide have become so entrenched in our daily lives that to a large extent many users rely on them for their daily livelihood. This changes the balance of power from end users to service providers, where creators, businesses become susceptible to any changes these platforms introduce, with little recourse.

This is where Web 3.0 strives to improve on, to build the next generation of the internet on an open infrastructure that is secure, private and data are fully owned by users, which eliminates the need for gatekeepers and allows more value to accrue to its end users. Blockchain technology offers the ability to do that as it does not require a third party to maintain trust in

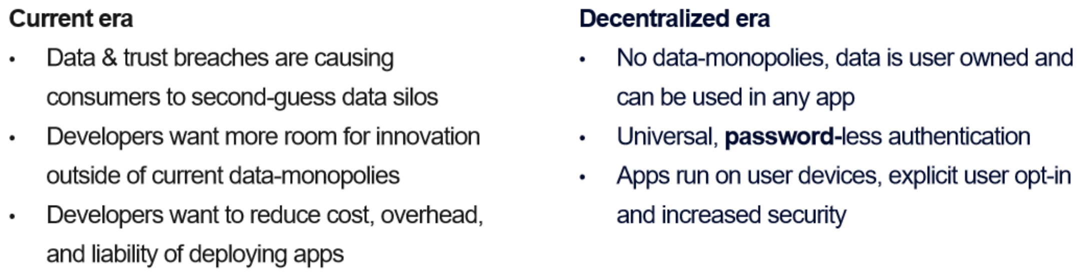
[3] https://www.brookings.edu/blog/techtank/2021/06/02/the-epic-apple-app-case-reveals-monopoly-power-and-the-need-for-new-regulatory-oversight/

[4] https://www.vox.com/recode/2020/10/6/21505027/congress-big-tech-antitrust-report-facebook-google-amazon-apple-mark-zuckerberg-jeff-bezos-tim-cook

[5] https://medium.com/mediarithmics-what-is/what-is-a-walled-garden-and-why-it-is-the-strategy-of-google-facebook-and-amazon-ads-platform-296ddeb784b1

[6] https://www.campaignlive.co.uk/article/social-media-companies-alone-power-ban-donald-trump/1704287

the system, such that users, stakeholders and participants can interact directly with each other, facilitated by smart contracts and settles the transaction in a trustless manner. A great analogy to illustrate this point would be, the inventor of TCP/IP or the creator of the world wide web couldn't capture any value for their creation despite it being the key catalyst to unprecedented wealth creation for many other internet businesses. As applications and other product services begin building on open smart contract layers like Stacks and the Lightning network which uses the Bitcoin Network as the settlement layer it changes the dynamics where economical value can be created while being publicly accessible. Value accrues to the token of the network (bitcoin) as 1) demand for the Bitcoin Network increases, 2) Network Effects increases as more applications rely on the Bitcoin Network as the ultimate source of truth, along with other properties of bitcoin such as 3) Store of Value, 4) Hedge against currency devaluation and 5) Personal Sovereignty.



Current era

- Data & trust breaches are causing consumers to second-guess data silos
- Developers want more room for innovation outside of current data-monopolies
- Developers want to reduce cost, overhead, and liability of deploying apps

Decentralized era

- No data-monopolies, data is user owned and can be used in any app
- Universal, **password**-less authentication
- Apps run on user devices, explicit user opt-in and increased security

Stacks

Blockstack (now known as Stacks) was a research project started by Muneeb Ali and Ryan Shea at Princeton University. They went through Y Combinator in 2014 and raised seed funding to further pursue their research on Blockstack, which includes scalable blockchains and long-term storage. With the completion of Muneeb's PhD thesis on Blockstack, the Blockstack whitepaper was published[7]. They went on to raise their Series A led by Union Square Ventures upon the completion of their research work in 2017. Blockstack believes that developing user ownership and privacy-enhancing technologies has a clear public benefit and have converted into a Public Beneficiary Corp (PBC) to enable an open, decentralized internet. Subsequently, they have also raised USD 47.5million in token offering with several self-imposed milestones as a way to incorporate investor protection on its token offerings[8]. Blockstack then went on to launch Stacks 1.0, thereby meeting the first milestone set in the token offering to unlock a portion of the funding for further development. With the newly unlocked funding, Blockstack launched the App Mining program, to encourage developers to build on Blockstack, and based on monthly app quality ranking, each app will earn a reward. This has led to more than 350 apps being built on Blockstack by 2019 along with research and development for Blockstack 2.0 and partnership with Lambda school to teach Blockstack to student developers. Blockstack 2.0 whitepaper was released to document the progress and changes that have been made since version 1.0 was published, together with a USD 23million SEC qualified token offering, under the recently updated Regulation A offering.

In 2020, Blockstack rebranded to Stacks[9] to have a brand that unifies the ecosystem and is readily identifiable, while the project continues to decentralize. Stacks have also added 300,000 new STX token holders through the collaboration with Blockchain.com and have also released

[7] https://pdos.csail.mit.edu/6.824/papers/blockstack-2017.pdf
[8] https://blog.blockstack.org/blockstack-unlocks-25-million-in-funding/
[9] https://blog.blockstack.org/stacks/

the whitepaper[10] for Proof-of-Transfer (PoX) mining and earning Bitcoin by participating in consensus. In the second half of 2020, Stacks 2.0 achieved code completion and various developer tools were released (e.g. Clarity language tooling, login SDKs, wallet SDKs, etc) to onboard more developers to the Stacks ecosystem. As part of further decentralization efforts, Blockstack PBC underwent a name change to Hiro Systems PBC, with a focus on developer tools for Stacks blockchain and more clearly delineating the company and the ecosystem[11]. Hiro's narrower developer focus also sends a message that just as with the other independent entities, Hiro Systems is one organization within the broader Stacks ecosystem.

Stacks 2.0 mainnet launched 14th January 2021 which brings smart contract capabilities to the Bitcoin Network and Stacking rewards for participation in Proof of Transfer consensus live. This further reinforces the notion that Bitcoin is the foundational layer for Web 3.0 while establishing itself as the clear store of value, with the rest of crypto internet settling on Bitcoin, treating it like a TCP/IP layer. Stacks blockchain anchors to the Bitcoin network via PoX mechanism, while allowing developers to create complex functions/applications on the Stacks blockchain using Clarity smart contract language, and STX token holders to receive pay-outs in bitcoins by stacking their STX tokens to secure the network. This unique combination of 1) leveraging on Bitcoin network security to power smart contract application, 2) introduces scalability to the Bitcoin Network, 3) enabling STX token holders to earn bitcoin (the most dominant cryptocurrency), 4) using a significantly safer programming language allows reinforces the tokenomics flywheel of Stacks blockchain.

To date, as of writing, in less than 6months after the launch of Stacks 2.0, the progress Stacks ecosystem are worth noting. Several key partners are integrating their technologies with Stacks Blockchain (USDC, Chainlink, Wrapped, OKcoin, etc), along with amazing entrepreneurs and developers building on top of Stacks blockchain, clearly illustrates the unique value proposition that Stacks blockchain is bringing to the industry. Feel free to head over to the Stacks Ecosystem section to learn more about the current developments.

[10] https://blockstack.org/pox.pdf
[11] https://blog.blockstack.org/hiro-dedicated-to-the-builders-of-a-better-internet-on-bitcoin

The Bitcoin Network

What is Bitcoin?

Conceptually, Bitcoin stretches across multiple domains of Cryptography, Computer Science and Economics to form the basis of a digital native monetary system[12]. There were 4 key innovations with the publication of the Bitcoin Whitepaper[13] in 2008 by pseudonymous author Satoshi Nakamoto, 1) decentralized peer-to-peer network (the bitcoin protocol), 2) public transaction ledger (the blockchain), 3) set of rules for independent transaction validation and currency issuance (consensus rules) and 4) Proof-of-Work algorithm to achieve a global decentralized consensus on the blockchain.

The introduction of the Bitcoin Network and its corresponding token (bitcoin) sets out to solve several key problems that have plagued previous digital currencies attempts. 1) Trust that digital money is authentic, 2) Prevent double-spending, also known as the "Byzantine Generals' Problem", and 3) Full ownership of digital money.

The use of paper money is constantly faced with the counterfeiting problem[14], where bad actors are constantly using sophisticated techniques to counterfeit paper money, thus making it increasingly difficult for the average user to discern between real paper money and counterfeits.

To solve the double-spending problem in the current monetary system, transactions are cleared electronically through central authorities that have a global view of the currency in circulation. Additionally, the rise of cryptography has also enabled users to sign a digital asset or transaction proving the ownership of that asset, thereby addressing the double-spend issue in a centralized ecosystem.

Prior digital currencies solutions were largely centralized in nature which makes them clear targets of intervention by governments and susceptible to attacks by hackers. Governments have concerns that the rise of an alternative currency may result in the government losing control over their monetary policies[15], which is a significant tool to steer the country's economy. Monetary policies have been a double edge sword historically where in times of an economic downturn, governments through various methods increase the money supply circulating in the economy to stimulate the economy has resulted in varying outcomes[16]. Banks and other financial institutions have the central authority to limit access to financial services for certain demographics of the population for various reasons, resulting in a negative impact on upward mobility for these folks[17]. While some restrictions were rightly justified (e.g. criminal activities) others were less clear, and a more thoughtful approach could potentially yield a net positive result. Therefore, to be robust against intervention by antagonists, whether legitimate governments or with criminal intents, a decentralized digital currency was created to avoid a single point of attack. The Bitcoin Network is such a system, decentralized by design, and free of any central authority or point of control that can be attacked or manipulated. Staying true to Satoshi's ethos, the source code[18] powering the Bitcoin Network was made available

[12] https://github.com/bitcoinbook/bitcoinbook
[13] https://bitcoin.org/bitcoin.pdf
[14] https://www.pmgnotes.com/news/article/4495/Counterfeiting-Paper-Money/
[15] https://opentextbc.ca/principlesofeconomics/chapter/28-4-monetary-policy-and-economic-outcomes/
[16] https://knowledge.wharton.upenn.edu/article/goldstein-research/
[17] https://time.com/nextadvisor/banking/what-to-know-if-you-are-unbanked/
[18] https://github.com/bitcoin/bitcoin

publicly along with the published whitepaper in 2008, allowing access to anyone interested to work on it, review it and contribute to the ongoing development of the Bitcoin Network.

History of Bitcoin

Bitcoin was invented in 2008 with the publication of the paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System," under the pseudonym Satoshi Nakamoto, through the cryptography mailing list[19]. The paper outlines the combination of several prior inventions such as B-money[20] and HashCash[21] to create a completely decentralized electronic cash system that does not rely on a central authority for currency issuance or settlement and validation of transactions.

Before Bitcoin, there have been multiple attempts at creating a digital currency[22], the earliest on record dates to the 1980s in the Netherlands. Where developers created smartcards to store monetary value, to allow freight companies to put money on these cards and give it to their truck drivers. Truck drivers would then carry these cards with them and use them to pay for gas on the road, while also enabling gas stations to keep just small amounts of cash on-site to deter crimes.

Digicash was conceptualized by cryptographer David Chaum where he described an anonymous digital payment system via now a well-renowned research paper[23] published in 1981, titled “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”. The blinding formula developed by David was used to encrypt information passed between individuals and formed the basis of “blind signatures”. Blind signatures conceal the content of a message and use a combination of public and private passwords to confirm a transaction. Today, this concept is widely used in cryptocurrencies in the form of public keys.

B-money developed by Wei Dai in 1998 sets out to be an anonymous, distributed electronic cash system. Two key ideas discussed in the paper were: 1) using computational work to facilitate the digital currency and verified by the community and rewarding the workers for their input, 2) using collective bookkeeping to ensure that transactions are accurate and using cryptographic protocols to authenticate transactions. B-money was never officially launched, but several of its features were evident in most modern-day cryptocurrencies development, with Satoshi referring to B-money several times in the Bitcoin whitepaper.

Bit Gold[24] developed by Nick Szabo in the late 90s revolutionized the concept of digital currencies by proposing a move away from the centralized format using a decentralized system without a third party responsible for transaction confirmation achieved using a proof-of-work system. In many ways, Bit Gold’s concepts mirror today's bitcoin mining process.

Hashcash was first introduced in 1997 by cryptographer Adam Black, initially to prevent spam emails and DDoS attacks but gained significant traction as a digital currency before fading away, due to the increasing need for processing power.

The publication of the Bitcoin whitepaper in 2008, made improvements to the work of digital currencies at that time, with decentralization and blockchain technology as key innovations.

[19] https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html
[20] http://www.weidai.com/bmoney.txt
[21] http://www.hashcash.org/papers/
[22] https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/
[23] http://www.lix.polytechnique.fr/~tomc/P2P/Papers/Theory/MIXes.pdf
[24] http://unenumerated.blogspot.com/2005/12/bit-gold.html

The use of a distributed computation system (called a "Proof-of-Work" (PoW) algorithm) to conduct a global "election" every 10 minutes, allowing the decentralized network to arrive at a consensus about the state of transactions, which solves the double-spend issue. This enables a decentralized digital currency for the first time, as previously the double-spend problem has always been a limitation of digital currencies that were addressed by centralizing transaction settlements.

On 3rd January 2009, the Bitcoin Network came into existence when Satoshi Nakamoto mined the genesis block along with inscribing the following message in the block “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”. A genesis block[25] is the first block of a blockchain (block 0). The genesis block is almost always hardcoded into the software of the applications that utilize its blockchain. It is the first block that forms the blockchain that subsequent blocks will refer to.

Early supporters of Bitcoin include Hal Finney, Wei Dai and Nick Szabo, who were computer scientists, creator of Bit gold and the creator of b-money respectively. The first bitcoin transaction occurred on 12th January 2009 when Satoshi transferred 10 bitcoins(btc) to Hal Finney. Since then a community of believers was formed around bitcoin, largely from the cypherpunk community and individuals drawn to the idea of sound money, the ability to maintain sovereignty over your own money and being censorship-resistant. As bitcoin adoption grew, its community got larger and the bitcointalk.org forum became the go-to place for bitcoin enthusiasts to hang out. The community tried to price bitcoin in the early days based on the amount of electricity consumed in mining them, pricing it at 7.6 US cents for 100 bitcoins[26] in Oct’09. On May 22, 2010, the first bitcoin commercial transaction was recorded, where a bitcoin enthusiast paid 10,000 bitcoins for two delivered pizzas[27].

Since then, bitcoin adoption has grown dramatically, albeit multiple road bumps along the way (bitcoin bug exploit[28], mt gox hack[29], blocksize war[30], etc), are witnessing the beginning of the blockchain industry and a shift in the narrative of bitcoin. From a peer to peer electronic cash system to digital gold and a global settlement layer. This was reiterated by industry researchers[31] in 2020, that based on Bitcoin’s underlying properties it could evolve into the following roles: 1) global settlement network, 2) protection against the seizure of assets, 3) digital gold, 4) catalyst for currency demonetization in emerging markets.

Key Properties of the Bitcoin Network

Tokenomics

Bitcoins are "minted" during the creation of each block at a fixed and diminishing rate. Miners compete to solve mathematical problems and earn the right to mint new blocks on average every 10 minutes and are rewarded by the issuance of new btc and transaction fees collected by the bitcoin protocol. Every 210,000 blocks, or approximately every four years, the bitcoin issuance rate is decreased by 50%, widely termed as “the halving” in the industry. For the first four years of the network going live, each new block issued 50 new bitcoins. The most recent

[25] https://en.bitcoin.it/wiki/Genesis_block
[26] https://www.bullionstar.com/blogs/ronan-manly/dawn-of-bitcoin-price-discovery-2009-2011-the-very-early-bitcoin-exchanges/
[27] https://bitcointalk.org/index.php?topic=137.0
[28] https://bitcointalk.org/index.php?topic=823.0
[29] https://www.wired.com/2014/03/bitcoin-exchange/
[30] https://steemit.com/bitcoin/@tobixen/a-brief-history-of-the-bitcoin-block-size-war
[31] https://research.ark-invest.com/thank-you-bitcoin-2?submissionGuid=9615548e-a97f-40fb-ba5b-d17683537429

halving took place in May’20 when the new bitcoin issuance rate decreased from 12.5 bitcoins per block to 6.25 bitcoins per block. The rate of new bitcoins issuance decreases in the same manner exponentially over 32 "halvings" until block 6,720,000 (approximately in the year 2137), and approximately in the year 2140 where all 21 million bitcoins will be issued. Thereafter, blocks will contain no new bitcoins, and miners will be rewarded solely through the collection of transaction fees. Over the long term, bitcoin is deflationary and cannot be inflated by issuing new bitcoins beyond the expected issuance rate.

ELI5: Miners compete to mine new bitcoins by solving mathematical problems and are rewarded with bitcoins every 10 minutes. The issuance of new bitcoins decreases by 50% every 210,000 blocks and there will only be a total of 21million bitcoins ever.

Proof-of-Work (Mining)

Mining[32] secures the Bitcoin Network and enables a network-wide consensus to be achieved without a central authority. The reward of newly minted bitcoins and transaction fees is an incentive scheme that aligns the actions of miners with the security of the network, while simultaneously implementing the monetary supply, thus playing a crucial role in bitcoin’s proof-of-work algorithm. Miners validate new transactions and record them on the blockchain which acts as a global public ledger. A new block, containing transactions that occurred since the last block, is "mined" and added to the previous transactions on the blockchain. Transactions that become part of a block and added to the blockchain are considered "confirmed," thereby reflecting the updated balance of bitcoins on the blockchain. Any participant in the bitcoin network may operate as a miner (with mining software), using their computer’s processing power to verify and record transactions. Over the years as more sophisticated participants got involved in bitcoin mining, it became more competitive and required significantly more computing power where only specialized equipment “application-specific integrated circuits” (ASIC) can deliver. The bitcoin protocol’s built-in algorithm regulates the difficulty of the processing task that miners must perform dynamically across the network such that on average, a miner succeeds every 10 minutes regardless of how many miners are competing at any moment. Essentially, bitcoin mining decentralizes the currency-issuance and clearing functions of a central bank and replaces the need for any central clearing authority.

Processing new bitcoin transactions

New bitcoin transactions stream into the Bitcoin Network from user wallets and other applications, which are added into a temporary pool of unverified transactions maintained by each node. As miners construct a new block, they add unverified transactions from this pool to the new block and then attempt to prove the validity of that new block, with the mining algorithm (Proof-of-Work). Transactions[33] are added to the new block, prioritized by the highest-fee transactions first and other criteria. Each miner starts the process of mining a new block of transactions as soon as they receive the previous block from the network, knowing they have lost that previous round of competition. They immediately create a new block, fill it with transactions and the fingerprint of the previous block, and start calculating the Proof-of-Work for the new block. Each miner includes a special transaction in their block, one that pays their bitcoin address the block reward (currently 6.25 newly created bitcoins) plus the sum of transaction fees from all the transactions included in the block. If they find a solution that makes

[32] https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch10.asciidoc

[33] https://www.worldscientific.com/doi/epdf/10.1142/9789811223693_0002

that block valid, they "win" the reward because their successful block is added to the global blockchain and the reward transaction they included becomes spendable.

Bitcoin security

Bitcoin[34] was built from the ground up with decentralization in mind, and that has a strong implication on how security works on the Bitcoin Network. Looking at security from a centralized model wouldn’t work, as fundamentally they are built differently. A centralized model, such as a traditional bank or payment network relies upon access controls and vetting to keep bad actors out of the system. By comparison, a decentralized system like the Bitcoin Network relies on participants/stakeholders to keep the network secure. As proof-of-work is the main mechanism that ensures accuracy on the network and not a vetting through access control, therefore the network can remain open while deterring bad actors from manipulating it. In proof-of-work, whether the transaction data included in a specific block have been tampered with can be easily verified using the Merkle Hash Tree method in the cryptography, thereby allowing an efficient way to keep the network honest while maintaining its transparency.

Bitcoin relies on hash function to incorporate transaction data in mining while ensuring the integrity of the data at the same time. A hash value is generated based on the information that will be used as transaction ID to identify the transaction. The hash value of any input has the same length and any slight changes in the input will cause the resulted hash value to be completely different with no pattern. Such features of hash ensure that as long as we have the same transaction ID, the data and information in a transaction have not been tampered with. The hash function used in bitcoin is SHA-256, which returns a fixed length of 256 bits (32 bytes).

This is in contrast to traditional payment networks (e.g. credit card systems), where the payment process involves the user’s private identifier number (credit card number) to make a charge. After the initial charge, anyone with access to the identifier can charge funds to the owner again and again. Thus, the payment network must be secured end-to-end with encryption to ensure no other unauthorized third party can gain access to the payment traffic, in transit or when it is stored (at rest). If a bad actor gains access to the system, he/she can compromise current transactions and manipulate payment tokens that can be used to create new transactions.
The Bitcoin Network functions differently, a bitcoin transaction authorizes only a specific value to a specific recipient and cannot be forged or modified. It does not reveal any private information, such as the identities of the parties, and cannot be used to authorize additional payments. Therefore, a bitcoin payment network does not need to be encrypted or protected from unauthorized third-party access. Bitcoin transactions can be broadcast over an open public channel, such as unsecured WiFi or Bluetooth, with no loss of security.

Bitcoin’s security relies on decentralized control over keys and independent transaction validation by miners, which puts more responsibilities in the hands of the users in safeguarding the private keys to your bitcoin wallet.

One of the most discussed blockchain security risks in the crypto industry is the likelihood of a 51% attack on a cryptocurrency network. A 51% attack is when a group of miners controls more than 50% of the network’s mining hash rate/computing power. As such the attackers

[34] https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch11.asciidoc

would be able to 1) prevent new transactions from gaining confirmations, allowing them to halt payments between users. 2) They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins. However, in the case of the Bitcoin Network, launching a 51% attack would be extremely difficult[35] due to various constraints such as 1) the cost and availability of equipment, 2) the cost and availability of sufficient electric power and 3) spare hash rate availability for rent. The above constraint factors make a 51% attack on the Bitcoin Network highly unlikely, and as the network difficulty increases over time due to advancement in mining equipment, the harder it becomes to launch a 51% attack on the Bitcoin Network.

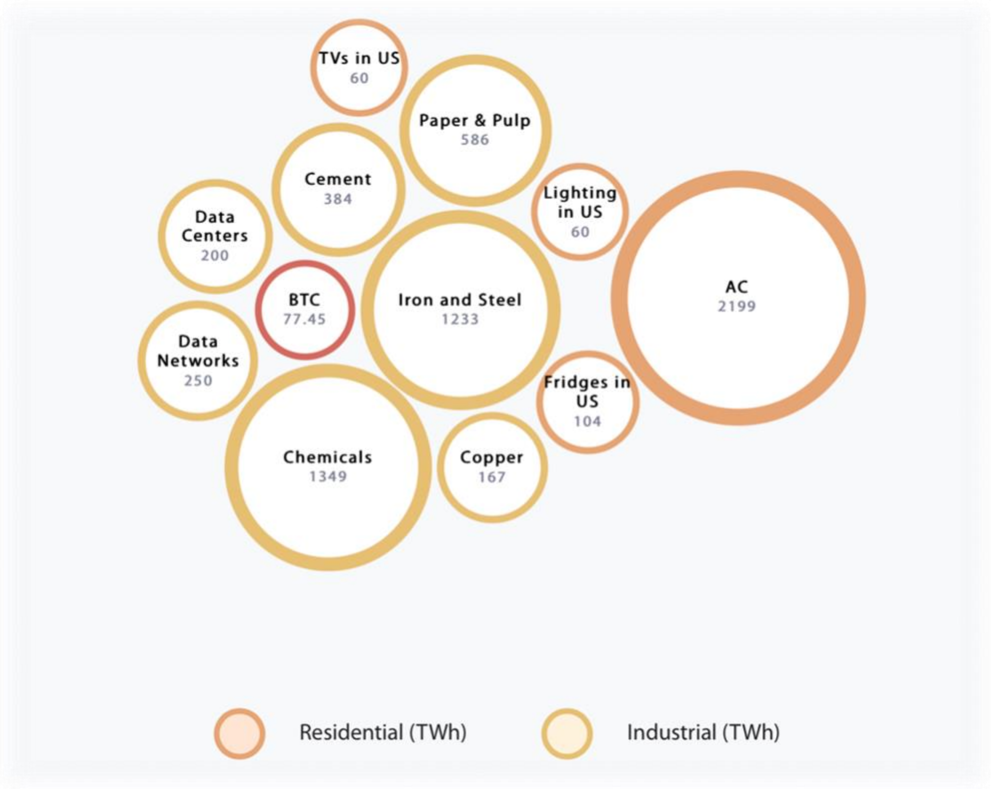
Bitcoin script

Bitcoin Script[36] is a simple, stack-based, Turing incomplete programming language, that enables the processing of transactions on the Bitcoin blockchain. It is important to note that Bitcoin software (also known as Bitcoin Core) is not written in Bitcoin Script. The script itself is implemented using the programming language the Bitcoin software is written in. The original implementation of the Bitcoin software was written in C++. Script gives the Bitcoin software instructions on how coins in a UTXO can be spent. UTXO refers to an “unspent transaction output” and is the result of a transaction that a user receives and can spend in the future. The decision to implement such a restricted scripting language lowers the vulnerability of external attacks on the Bitcoin blockchain as Turing incomplete language is unable to run malformed scripts and do not face the halting problem[37]. However, Turing incomplete language limits the possibility to create smart contracts on the Bitcoin Network as it does not support complex loops. Smart contracts are code snippets, if-then functions, that are run across the blockchain nodes and are necessary to build more complex applications.

Bitcoin Energy Consumption

A key innovation by Satoshi Nakamoto is the use of proof-of-work mechanism to enable a decentralized digital monetary system to function, and has since gained wide adoption after more than 13 years since the white paper was released. As covered in the above section, proof-of-work requires miners to compete using computing processing power to solve mathematical problems, to win the chance of minting a new block and be rewarded with new bitcoin issuance and transaction fees. In the early days, when bitcoin mining was a hobbyist activity there were no concerns over energy consumption as equipment used for mining were mainly PCs or GPUs and insignificant relative to global power consumption. As the Bitcoin Network matures and bitcoin becomes more valuable, it incentivizes more participants to join the bitcoin mining industry, and over time bitcoin mining begins institutionalizing, where miners use specialized equipment to mine. This was largely a positive event as more miners participated in proof-of-work mining the more decentralized the network is, and with more miners and equipment advancements(which increases the net energy consumption of the bitcoin mining industry) more hash power is committed to the network thereby making it more secure. However, as the bitcoin mining industry grew, the consumption of electricity to power mining operations grew along with it and became a material amount that raises concerns[38] among various stakeholders (e.g. environmentalists, politicians, landlords, etc).

[35] https://braiins.com/blog/how-much-would-it-cost-to-51-attack-bitcoin
[36] https://komodoplatform.com/en/academy/bitcoin-script/
[37] https://en.wikipedia.org/wiki/Halting_problem
[38] https://www.ft.com/content/1aecb2db-8f61-427c-a413-3b929291c8ac



CBECI, 2021[39]

Further comparisons from the above chart give a varying perspective to bitcoin's energy consumption relative to a wide range of use cases and industries.

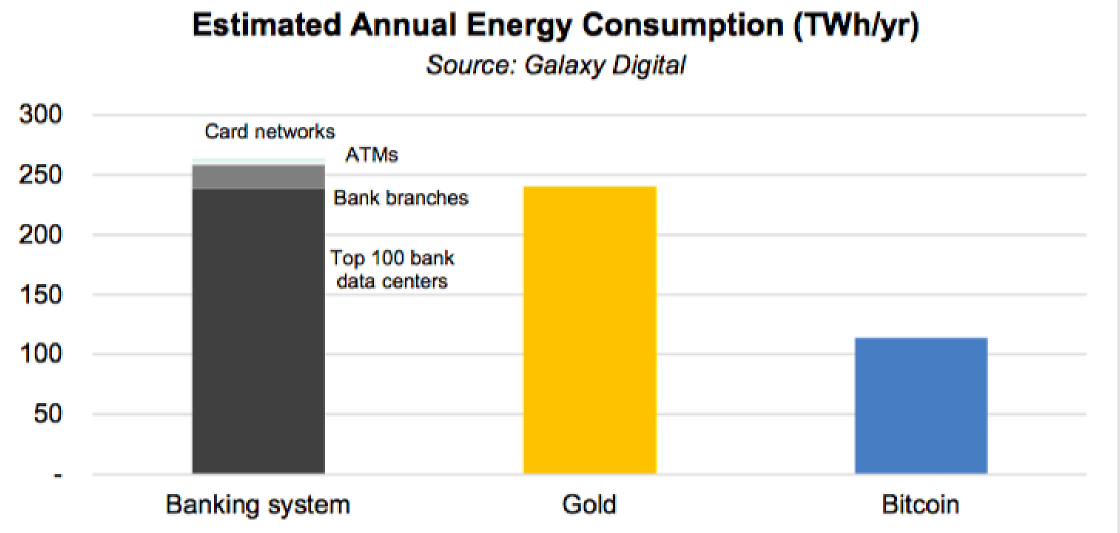
At its peak in May'21, bitcoin electricity consumption was at 130 Terra Hours per year[40] which approximates to 0.5%[41] of global electricity production or roughly the annual energy consumption of a country like Sweden or Norway[42]. Looking at the data in isolation may seem daunting, but to put things into perspective we look at some data below on how much energy is the Bitcoin Network consuming relative to similar industries that bitcoin is most often compared to.

Bitcoin is a novel technology and not a substitute for any specific legacy system, but a cross-section of several use cases as discussed in earlier sections. One facet of Bitcoin to offer significant improvement over the legacy system is to become the global settlement layer, where it is capable of providing high assurance, final settlement that cannot be reversed or censored[43]. Instead of facilitating large volumes of low-value transactions at the point of sale, Bitcoin could act as a base layer to handle large transactions between and among financial intermediaries, and allow other platforms, side-chains, to build on and rely on Bitcoin for finality. One Bitcoin transaction, therefore, can settle thousands or more of off-chain or near-chain transactions on any of these third-party networks. We can think of Bitcoin as a settlement layer similar to Fedwire in the US or TARGET Services in Europe.

[39] https://cbeci.org/cbeci/comparisons
[40] https://cbeci.org
[41] https://ourworldindata.org/electricity-mix
[42] https://yearbook.enerdata.net/electricity/electricity-domestic-consumption-data.html
[43] https://www.coindesk.com/frustrating-maddening-all-consuming-bitcoin-energy-debate

For millennia the world has recognized gold as the most sustainable form of money, through natural selection, where several goods competed with each other for dominance until gold evolved as the global monetary standard. As we transit to a digital economy, a digital native asset could very well find its place within the digital economy and Bitcoin is widely regarded as digital gold because it improves upon many of physical gold's characteristics. Not only is bitcoin scarce and durable, but it also is divisible, verifiable, portable, and censorship-resistant.

The chart below provides more context on the energy consumption of the Bitcoin Network relative to parallel industries that bitcoin is often compared to, the banking and gold industries.



Galaxy Digital 2021[44]

Energy consumption within the banking sector(data centres, bank branches, ATMs and card networks data) is estimated to be 263.72 TWh globally. Separately, prior research on gold's energy consumption is estimated to be around 240.61 TWh. Both of which were significantly higher than the energy consumption of Bitcoin. However, the intent of such a comparison isn't to justify if the usage of energy in one industry is superior to another industry. A direct comparison of electricity consumption between industries has limitations as well, such as the lack of accounting for externalities, second and third-order of value creation deriving from these industries were not taken into considerations too. These statistics provide an interesting context into each industry, however, defining them solely on energy consumption seems reductive as we overlook the benefits each industry brings to the global economy. The banking industry has for centuries enabled civilizations to prosper by providing financial access to the population, despite some of its flaws, has allowed capital to flow more efficiently through the economy. Gold[45] has for a long period of time been the de-facto store of value for the global economy, has enabled upward mobility and promoted trade in the early civilizations.

Likewise, for bitcoin, it can offer financial freedom to people around the world who do not have access to stable financial infrastructure. The network can benefit the energy sector by creating use cases for intermittent and excess energy. Energy utilization is not necessarily a bad thing, as we've witnessed in the rise of new technologies (e.g. agricultural revolution, the industrial revolution, etc) which consumes additional energy but at the same time improves the well-being of humans and the environment if done sustainably. Humans will continue to find

[44] https://docsend.com/view/adwmdeeyfvqwecj2
[45] https://www.focus-economics.com/blog/gold-the-most-precious-of-metals

new technologies that require a significant amount of energy that challenge the status quo, with bitcoin being just another example.

Sustainable Energy

The world is facing an unprecedented challenge towards its climate and environment with a rising risk of severe global warming. In the above section, we've established the case for bitcoin energy usage, so one may wonder if bitcoin can play a positive role in helping the world achieve zero emissions, and drive the use of sustainable energy? In the following section, we shall deep dive into the topic of bitcoin mining using sustainable energy.

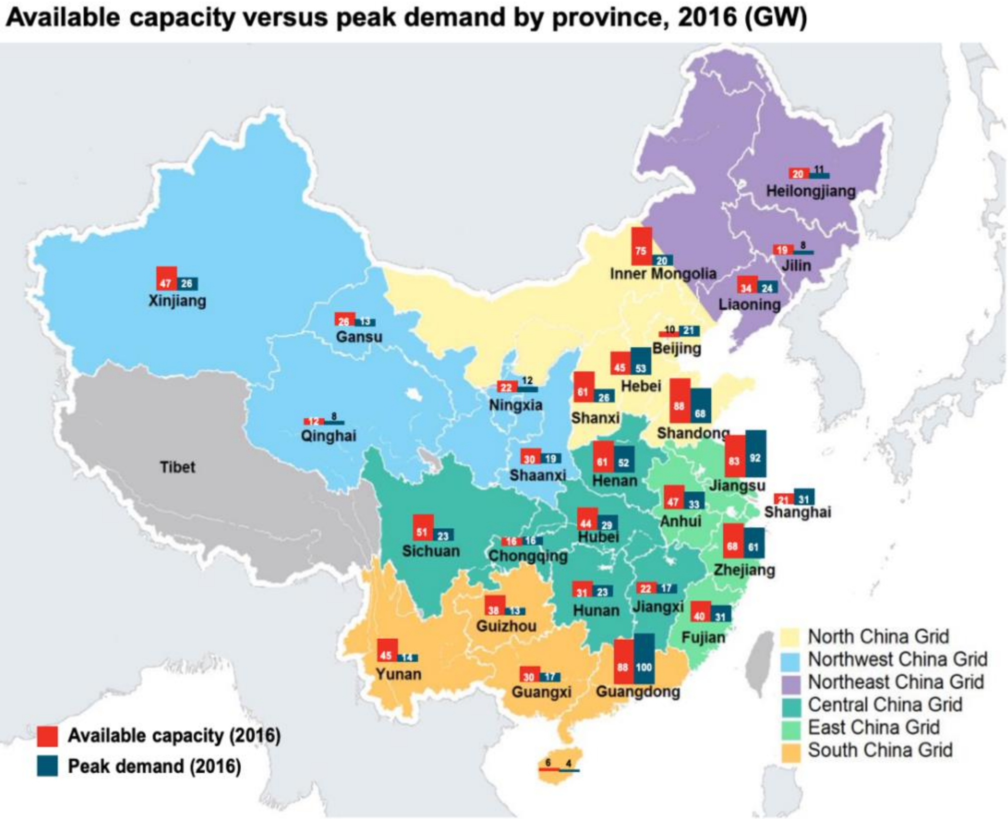
Critics have always been vocal on bitcoin's energy consumption and the sources of those energy used coming from unsustainable sources[46]. While there are some elements of truth in the argument, it fails to present a holistic view on the matter.

A significant amount of energy usage from bitcoin mining was from excess renewable energy that would otherwise have been wasted due to various factors such as 1) difficulty in transporting energy to areas of demand[47], and 2) oversupply of energy concentrated in specific locations due to poor central planning[48].

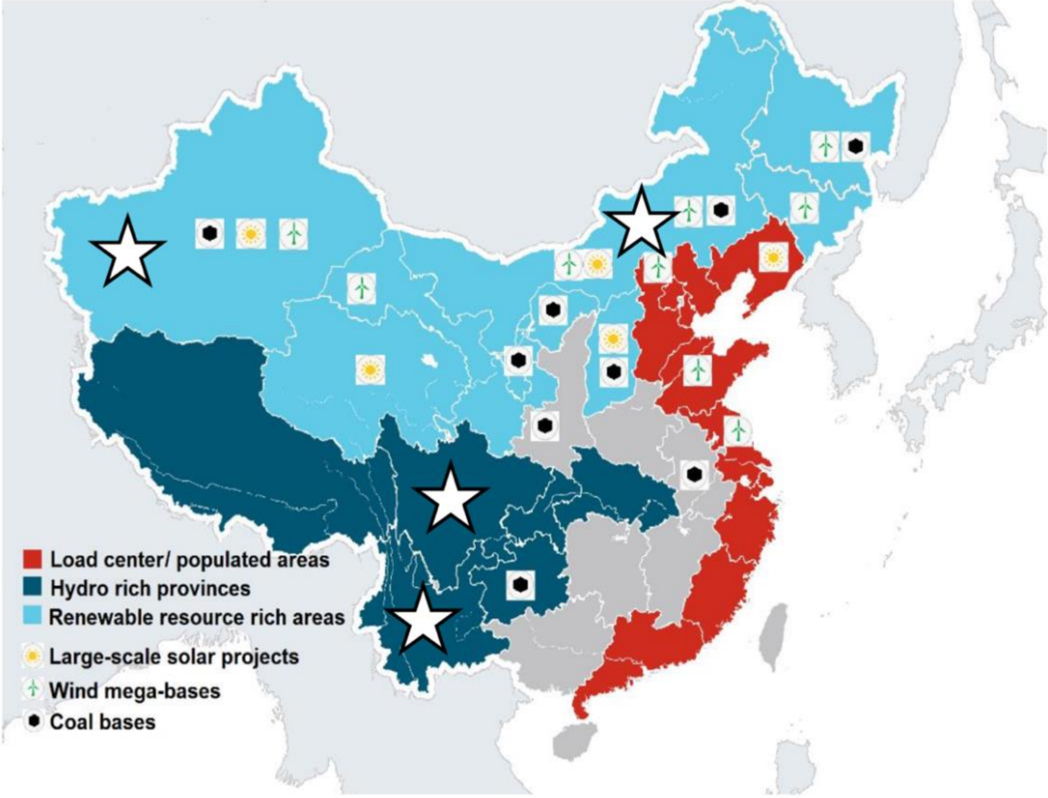
Drawing reference from an insightful point that Nic Carter (General Partner at Castle Island Ventures) made[49], critics extrapolate Bitcoin's energy consumption to the equivalent CO2 emissions is inaccurate as Bitcoin actively seeks out otherwise-curtailed energy (which in most cases are relatively green), to reduce the cost of mining given that it is an intensely competitive industry. Any reliable estimate must take this into account.

Historically bitcoin mining has concentrated in certain parts of China (up to 76% of total hash rate[50]) and Inner Mongolia largely due to the availability of cheap energy and excess energy in remote parts of China/Inner Mongolia which makes transporting energy to in-demand areas extremely costly. With an abundance of energy supply but nowhere to sell them, bitcoin mining became the natural fit in such circumstances. The map below indicates the availability of energy capacity in China and the key areas with high electricity demand, which explains why bitcoin mining has largely been in areas such as Xinjiang, Inner Mongolia, Sichuan and Yunnan.

[46] https://www.ft.com/content/1aecb2db-8f61-427c-a413-3b929291c8ac
[47] https://data.worldbank.org/indicator/EG.ELC.LOSS.ZS
[48]https://www.reuters.com/article/us-china-hydropower/dam-nation-big-state-projects-spared-in-chinas-hydro-crackdown-idUSKCN1LF2RG
[49] https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume
[50] https://cbeci.org/mining_map



Zhou and Lu, 2017[42]


Load center/ populated areas
Hydro rich provinces
Renewable resource rich areas
Large-scale solar projects
Wind mega-bases
Coal bases

Zhou and Lu, 2017[51]

[51] https://data.bloomberglp.com/bnef/sites/14/2017/10/Chinas-Renewable-Curtailment-and-Coal-Assets-Risk-Map-FINAL_2.pdf

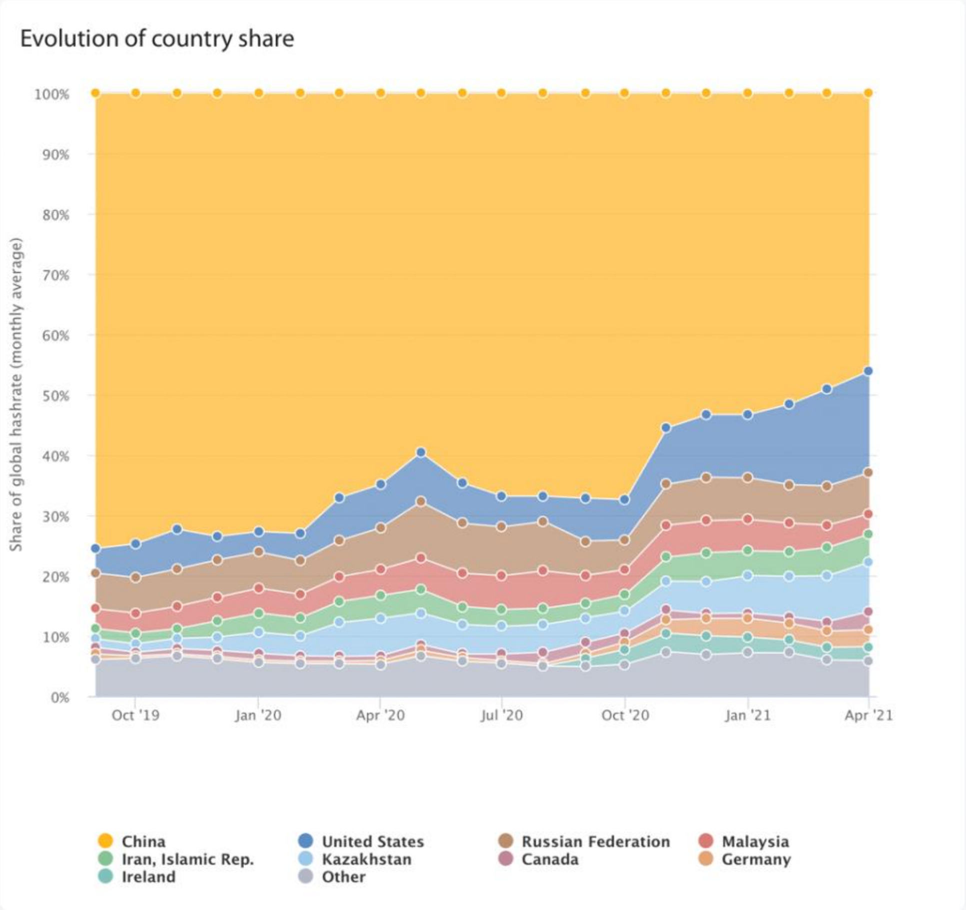
CCAF's report[52] specifies that an estimate of approximately 39% of bitcoin mining activity comes from renewable sources (higher than the 25% global average[53] share of renewables in electricity generation in 2019), with coal and natural gas coming in at a close second and third energy sources that miners favour the most. Among renewable sources, hydropower is the most commonly used renewable energy source at 62%, with wind and solar energy at 17% and 15% respectively. It is estimated that hydroelectricity is 30% cheaper than other options during the rainy season in Sichuan & Yunnan and when the rainy season ends at the end of October, they will migrate back to regions with cheap electricity powered by coal in Inner Mongolia or Xinjiang

China banning bitcoin mining[54] in Jun'21 came at a time where concerns are rising within the crypto industry that mining is centralizing within a jurisdiction. Since the ban, we've seen China's mining market share has dropped from its peak of 76% to 46% as of Apr'21 and it is predicted to drop even further as more up to date data streams in. In fact, the ban on mining in China has enabled mining to further decentralize as miners seek other suitable locations to set up operations.

Unlike other industries, Bitcoin mining is relatively mobile. In their quest for cheap and abundant energy sources, miners can set up new facilities fairly quickly all over the world, including the most remote areas. As a result, Bitcoin miners can tap into so-called 'stranded' energy assets that cannot easily be put to productive use by other industries. In those cases, Bitcoin miners are not competing with other industries or residential users for the same resources but instead soaking up surplus energy that would otherwise have been lost or wasted. Globally there are multiple options where miners can pursue renewable energy setups, while some may still use grid power, however it is encouraging to see various initiatives signalling their intent of using clean energy to pursue bitcoin mining. E.g. Square's Bitcoin Clean Energy Investment Initiative[55] and Aker's Seetee initiative[56]. In July'21, the Bitcoin Mining Council reported that the global mining industry's sustainable electricity mix had grown to approximately 56%, during Q2 2021.

Countries like the US witnessed an increase in the share of hash rate from 4% in Sep'19 to 16% in Apr'21, with on the ground sentiment shows that it'll continue to increase especially after the ban. With mining manufacturers reporting that in recent years around 60% of the machines sold have been for outside of China and to the US[57], and the proportion will likely increase further as updated data after China's ban are accounted for. Below is a chart showing the evolution of countries' share of hash rate from Sep'19 to Apr'21.

[52] https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study
[53] https://irena.org/-/media/Files/IRENA/Agency/Publication/2021/March/IRENA_World_Energy_Transitions_Outlook_2021.pdf
[54] https://www.reuters.com/technology/chinas-ban-forces-some-bitcoin-miners-flee-overseas-others-sell-out-2021-06-25/
[55] https://www.coindesk.com/square-to-support-greener-bitcoin-mining-as-part-of-zero-carbon-pledge
[56] https://www.seetee.io/static/shareholder_letter-6ae7e85717c28831bf1c0eca1d632722.pdf
[57] https://onthebrink-podcast.com/bixin/



CBECI, 2021[58]

Hydroelectricity is prominent elsewhere apart from China, where approximately 60% of bitcoin mining in Europe, 67% in Latin America and the Caribbean (LAC) and 61% in North America are powered by it. The share powered by coal in these regions is much lower. Just 20% do so in Europe, 28% in North America and none in LAC. Therefore with miners migrating out of China to other countries, renewable sources of energy are more prevalent and encouraged, along with stronger political and socio-economic willpower of various stakeholders in using and advocating for renewable energy sources.

Additionally the notion of "pipe to crypto" is increasingly common where bitcoin mining uses methane, a natural by-product of oil extraction to power their operations. In most cases, natural gas is either vented or flared at rig locations. As these oil wells are frequently remote, off-grid, with no pipeline infrastructure, and unviable economics for capturing (due to low prices of natural gas), oil rig operators often combust waste gas on site. Methane is a worse greenhouse gas than CO2, thus flaring is a net positive by combusting methane gas into CO2 and releasing it into the atmosphere. However, flaring is a very inefficient method[59] in converting methane gas into CO2 therefore, Bitcoin mining presents a better alternative such that methane gas is fully combusted in a generator(to ensure a full burn) to power bitcoin miners. Given the baseline situation of venting/flaring, a clean, supervised burn in a generator is a net positive from a carbon perspective. The scale of flared gas is massive, presenting opportunities for

[58] https://cbeci.org/mining_map
[59] https://www.crusoeenergy.com/emissions-reduction

bitcoin miners to tap on the availability of these energy sources. In the U.S. alone, 538 billion cubic feet of natural gas[60] were vented and flared in 2019, and this is likely underreported[61].

Nic Carter sums up the situation of bitcoin mining succinctly with the following paragraph[62]

"Imagine a topographic map of the world, but with local electricity costs as the variable determining the peaks and troughs. Adding Bitcoin to the mix is like pouring a glass of water over the 3D map – it settles in the troughs, smoothing them out. As Bitcoin is a global buyer of energy at a fixed price, it makes sense for miners with very cheap energy to sell some to the protocol. This is why so many oil miners (whose business results in the production of lots of waste methane) have developed an enthusiasm[63] for mining Bitcoin. From a climate perspective, this is a net positive[64]. Bitcoin thrives on the margins, where energy is lost or curtailed."

Additionally, Crypto Climate Accord (CAA)[65] is a private sector-led initiative that promotes the decarbonization of the crypto industry. Two main objectives of the CAA are to reach net-zero emissions from electricity consumption by 2030 and to reach net-zero greenhouse gas emissions by 2040. Alongside the Bitcoin Mining Council (BMC)[66], another private sector-led initiative to provide an open forum where bitcoin miners could promote transparency, share best practices and educate the public on the benefits of Bitcoin and Bitcoin mining enabling the industry to transition to full sustainable energy.

Bitcoin mining brings economic resources to fund the development of renewable energy infrastructure. Currently, renewables face two key limitations that limit their scalable and mainstream adoption, which we've briefly alluded to in early sections. 1) Renewable energy is often not stable in its energy production. For example, solar power receives a surplus of energy during the sunny time but receives no energy in the evening, while hydropower & wind is seasonal, and geothermal availability is limited to a very specific geolocation. Battery technology is not advanced enough that it can hold an abundance of energy and release them on an on-demand basis in a large scale setting. 2) Many of the renewable energy stations are located in remote areas, far away from key demand loads where the land is large to build out solar power, hydro energy, and wind farms. Infrastructures necessary to transport these energies efficiently are costly to build thus making renewables extremely costly for mainstream adoption.

This is where bitcoin mining comes into the equation, as it is not constrained by location making it a global buyer of energy at a fixed price, allowing miners to utilize power sources that are inaccessible for most other applications. Along with global initiatives pushing for greater use of clean energy, the demand for clean energy by the miners will incentivize utility companies to expand their renewable energy capacity, knowing that there is a global buyer ready to tap on the additional supply generated by these companies before battery technology and other infrastructures are ready to make it viable to run the world fully on clean energy.

[60] https://www.eia.gov/dnav/ng/ng_prod_sum_a_EPG0_VGV_mmcf_a.htm
[61] https://medium.com/@nic__carter/noahbjectivity-on-bitcoin-mining-2052226310cb
[62] https://www.coindesk.com/the-last-word-on-bitcoins-energy-consumption
[63] https://trib.com/business/energy/the-unlikely-marriage-of-cryptocurrency-and-crude/article_b6e3fd6c-e485-5e22-9a16-3e292dc79cfc.html
[64] https://bitcoinmagazine.com/business/oil-field-alchemy-how-bitcoin-can-turn-waste-emissions-proof-work
[65] https://cryptoclimate.org
[66] https://bitcoinminingcouncil.com

Regulations

The rise of every new technology or industry comes with added regulatory scrutiny, as we've witnessed with the internet[67], social media[68], ridesharing[69] and many other sectors. Regulators are treading a fine line between regulating it with the right approach, which will enable the industry to prosper and gain mainstream adoption, or by over-regulating it, which may inhibit its potential. Finding the right balance when navigating through areas for regulation in new technologies can be challenging but a task that regulators need to embrace. New technologies and industries can bring massive benefits to the community through economic growth, improved quality of life, etc but at the same time without adequate regulations, bad actors may thrive in extracting value from genuine participants. The following quote illustrates the thinking behind regulating with the right approach: "Speed limits and traffic lights provided public safety but also helped cars become mainstream. It is only with bringing things inside—and sort of clearly within our public policy goals—that new technology has a chance of broader adoption". The current regulation outlook revolves around two key areas: 1) KYC/AML compliance and 2) classification of securities.

KYC/AML

Know-your-customer/Anti-money laundering (KYC/AML) procedures are put in place to identify their customers and are measures to deter money laundering. These procedures were meant to deter money launderers from using the said service to launder money, which could potentially be used to fund various nefarious activities. In traditional finance, KYC/AML has been in place for decades under various legislation such as the Bank Secrecy Act[70], Patriot Act[71] in the US and the 5th Anti-Money Laundering Directive (AMLD5)[72] in the EU and other similar legislation worldwide. Implementing KYC/AML is a matter of cost & benefit analysis on how thorough due diligence are conducted on customers and partners against the effectiveness of preventing money laundering activities. While there are ways to sidestep these procedures, financial institutions are also mindful[73] in implementing excessive checks that will significantly add to their operational costs and inefficiencies.

In 2019, the Financial Crimes Enforcement Network (FinCEN), the Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC) issued a joint statement[74] that defined cryptocurrency exchanges as money service businesses (MSBs), thus making them subject to AML and KYC regulations under the Bank Secrecy Act. This was followed by new regulations[75] for cryptocurrency wallets and cryptocurrency holdings at foreign exchanges. AMLD5 in Europe have also made it clear that cryptocurrency exchanges that are trading them to adhere to KYC/AML legislation. KYC/AML legislation in the crypto industry is relatively new and exchanges[76] are applying KYC/AML measures retrospectively to remain compliant with regulators across various jurisdictions. Like traditional finance, KYC/AML are commonly applied to on-ramps and off-ramps, thus centralized crypto exchanges (CEXs) are impacted the most with KYC/AML procedures. The

[67] https://www.tandfonline.com/doi/abs/10.1300/J103v26n01_06?journalCode=wbss20
[68] https://www.cfr.org/in-brief/social-media-and-online-speech-how-should-countries-regulate-tech-giants
[69] https://www.barrons.com/articles/regulatory-headaches-arent-going-away-for-uber-and-lyft-51598642257
[70] https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html
[71] https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf
[72] https://ec.europa.eu/info/law/anti-money-laundering-amld-v-directive-eu-2018-843_en
[73] https://www.mckinsey.com/business-functions/risk/our-insights/the-new-frontier-in-anti-money-laundering#
[74] https://www.natlawreview.com/article/cftc-fincen-and-sec-warn-crypto-aml-enforcement
[75] https://decrypt.co/52021/us-treasury-apply-bank-secrecy-act-rules-crypto-wallets
[76] https://www.forbes.com/sites/martinrivers/2021/07/28/not-your-bitcoin-binance-stops-users-withdrawing-more-than-006btc-without-kyc-checks

Financial Action Task Force (FATF) has recently updated the Travel-Rule guideline[77], which recommends Virtual Asset Service Providers (VASPs), including exchanges, banks, OTC desks, hosted wallets and other financial institutions, to share certain identifying information about the recipient [78]and receiver for cryptocurrency transactions over USD/EUR 1000 globally. Since the issuance of FATF's virtual asset guidance, some jurisdictions, such as Singapore, Switzerland and Hong Kong, have already forbid exchanges from operating without licenses that enforce Travel Rule compliance—regulations that require Virtual Asset Service Providers to securely share certain sender and receiver information with each other for cryptocurrency transactions. Exchanges are also complying with the new guidance by deploying new tools to scan addresses associated with incoming crypto transactions.

The rise of decentralized applications (dApps) built on various blockchain protocols adds a unique mix to the equation, by design there is no central authority responsible for operating those applications as they are solely managed by smart contracts. Having witnessed multiple hacks on smart contracts where hackers cashed out their loot via decentralized exchanges (DEXs)[79] sidestepping any KYC/AML procedures placed on CEXs. This further makes the case for regulators to consider enforcing KYC/AML requirements on dApps. However contradicting this may sound, the enforcement of KYC/AML could undermine the pseudonymous or anonymous nature of cryptocurrencies. The uncertainty that the industry is facing on the regulation front is inevitable as stakeholders and regulators are coming to grasp how the technology functions and what blind spots within the industry are, to implement the right policies to regulate the industry.

Securities

Securities are commonly defined as fungible and tradable financial instruments used to raise capital in public and private markets[80]. In the US, the Securities Act of 1933 is the federal law that requires that securities sold to the public be registered with the SEC and that complete information about the seller and the stock offering is made available to investors.

The Howey Test is often used to determine if a transaction qualifies as an "investment contract," and therefore would be considered a security and subject to disclosure and registration requirements under the Securities Act of 1933 and the Securities Exchange Act of 1934. In recent years as blockchain technology matures and the issuance of tokens became more prevalent, the need to define the scope of a security and if the issued tokens come under the scope became ever more imperative. The SEC came up with a framework for "Investment Contract" Analysis of Digital Assets to give a clearer definition of what constitutes a security. The application of the Howey Test on digital assets remains applicable with the following three criteria: 1) The Investment of Money, 2) Common Enterprise and 3) Reasonable Expectation of Profits Derived from Efforts of Others. In most cases, whether a digital asset qualifies as an investment contract largely relies on whether there is an "expectation of profit to be derived from the efforts of others."

Token Issuance

The focus on defining the scope of a security within the crypto industry is essential as unregistered security can only be traded by an accredited investor, which is largely not the case

[77] https://ciphertrace.com/the-complete-guide-to-the-fatf-travel-rule-for-cryptocurrency/
[78] https://www.nasdaq.com/articles/binance-deploys-ciphertrace-tool-for-travel-rule-compliance-2021-07-01
[79] https://modernconsensus.com/cryptocurrencies/kucoin-hackers-dump-stolen-funds-on-defi/
[80] https://www.investopedia.com/terms/s/security.asp

in the current environment. A recent case further reinforces this point where DEXes[81] are delisting tokens that may be at risk of being classified as securities by a regulator.

Given the importance regulators placed on entities offering a public sale of securities to fundraise, there are various crypto projects (e.g Stacks) that applied to the SEC for an exemption from registration for public offerings under the SEC Regulation A+ framework. Regulation A is an exemption from registration requirements—instituted by the Securities Act—that apply to public offerings of securities that do not exceed $50 million in any one-year period. Projects that have met the criteria of not being a security can also make an application to the SEC to no longer treat it as a security[82], thereby allowing non-accredited investors to purchase them.

Regulation Landscape

Cryptocurrencies and Digital Assets have evolved tremendously since the publication of the Bitcoin Whitepaper in 2008, which kickstarted the industry to life. Simultaneously, as the industry grew to attract more participants, capital, and other resources into the mix, regulating the landscape needs to evolve to accommodate it. Crypto is at the cross juncture now as regulators see the need to implement tighter policies to regulate the industry in the interests of participants in the industry, while participants, builders in the industry are iterating at breakneck speed and are worried that regulations may impede their progress.

In the US[83], at the state level, there are 50 attorneys general and various state agencies that enforce digital asset-related laws (or other general laws that may apply to digital assets) passed by state legislatures and applied by the courts. Individual states are taking different approaches, and the laboratory of ideas is actively at work. For example, the New York State Department of Financial Services has enacted the Virtual Currency Business Activity regulatory framework (e.g., the "BitLicense" framework), which covers substantially all virtual currency activity by New York firms and residents. On the opposite end of the spectrum, Wyoming has passed legislation exempting virtual currency transactions from its money transmitter regulations, utility tokens from certain state securities registration and money transmitter laws and virtual currencies from property taxation laws. Colorado recently issued guidance exempting certain types of digital asset exchanges from the state's money transmitter licensing requirements. It remains unsettled whether federal regulation will supersede state regulation in respect of digital assets and FinTech more generally, as the courts have not yet ruled on many aspects of crypto regulation.

The EU and Switzerland have taken different approaches to the regulation of distributed ledger-based security issuance and trading[84]. In September 2020, the Swiss Parliament adopted the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT). In the same month, the European Commission adopted several legislative proposals as part of its Digital Finance Strategy.

Switzerland’s new regulation enables the issuance of securities using DLT as of 1 February 2021. The Swiss ledger-based security (Registerwertrecht) is a new type of uncertificated security, which can serve as an alternative to the existing intermediated securities (Bucheffekten). Both types are immaterialised securities, but intermediated securities require

[81] https://cointelegraph.com/news/uniswap-delists-100-tokens-from-interface-including-options-and-indexes
[82] https://blog.blockstack.org/stacks-cryptocurrency-securities-filing/
[83] https://www.reuters.com/legal/transactional/whos-charge-an-overview-us-digital-asset-regulation-2021-06-14/
[84] https://www.area2invest.com/security-token-regulation-europe/

a regulated institution such as a bank, securities firm, or a Central Securities Depository (CSD) for issuance and transfer of the security. The new Swiss ledger-based security (Registerwertrecht) can be issued and transferred without an intermediary.

The European Commission adopted four proposals: The Market in Crypto-Assets Regulation (MiCA) [85], the Pilot DLT Market Infrastructure Regulation (PDMIR), the Digital Operational Resilience Regulation (DORA), and a directive to amend existing financial services legislation. According to the new legislation, security tokens issued using DLT will be subject to MiFID II and, therefore, other financial market regulations will apply as well, namely the Market Abuse Regulation, Prospectus Regulation, Transparency Directive, Short Selling Regulation, Settlement Finality Directive and the Central Securities Depository Regulation. However, the specific laws that apply depending on which country the issuer is in, which country the investors are in, and what type of investment contract is being tokenised. There are eight main types of security tokens:

1. Tokenised profit participation rights
2. Tokenised revenue participation rights
3. Tokenised subordinated loans
4. Tokenised commitments to use
5. Tokenisation of a limited liability company (GmbH)
6. Tokenisation of a stock corporation
7. Tokenisation of real assets such as precious metals or apartment buildings
8. Tokenisation of voucher entitlements

The European Union first published its Digital Finance Package[86] on 24 September 2020 which includes legislative proposals on crypto-assets to ensure the EU's financial sector remains competitive by simplifying the rules and emphasising consumer safety. MiCA Proposal is a regulatory framework developed to help regulate currently out-of-scope crypto-assets and their service providers in the EU and provide a single licensing regime across all member states by 2024. The Markets in Crypto-assets proposal has 4 broad objectives:

- To provide legal certainty for crypto-assets not covered by existing EU financial services legislation, for which there is currently a clear need.
- To establish uniform rules for crypto-asset service providers and issuers at the EU level
- To replace existing national frameworks applicable to crypto-assets not covered by existing EU financial services legislation
- To establish specific rules for so-called 'stablecoins', including when these are e-money.

Singapore's digital assets regulations fall under The Payment Services Act (PSA)[87] and The Securities and Futures Act (SFA)[88], implemented by The Monetary Authority of Singapore (MAS). The regulation covers various segments including, KYC/AML, Digital Payment Token activities (DPT), DPT service providers, transfer of DPTs, provision of custodial wallet services for DPTs, and the facilitation of the exchange of DPTs. With DPT service providers being granted an exemption[89] to provide services to retail and institutional investors while they await a formal licence.

[85] https://www.sygna.io/blog/what-is-mica-markets-in-crypto-assets-eu-regulation-guide
[86] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en
[87] https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220#Sc1-
[88] https://sso.agc.gov.sg/Act/SFA2001
[89] https://www.ft.com/content/4b8aba07-6035-4bdb-a6bb-cb64624d0ac6

Hong Kong in May’21 published the Consultation Conclusions[90] on legislative proposals to enhance anti-money laundering and counter-terrorist financing (“AML/CTF”) regulations in Hong Kong, including a proposal to introduce a licensing regime for virtual asset services providers (“VASPs”). The Hong Kong authorities are focused on promoting the protection of market integrity and investor interests, and the regulatory requirements for licensed VASPs extend beyond AML/CTF requirements by seeking to regulate matters including customer type (i.e. professional investors only), prevention of market manipulative and abusive activities, and prevention of conflicts of interest.

Thailand introduced the Digital Asset Decree (the “Decree”)[91] that establishes the requirements for a business to offer or provide operations for digital assets in 2018. The Decree covers both cryptocurrencies as well as digital tokens and is overseen by the Securities and Exchange Commission of Thailand (“SEC Thailand”). The Decree clearly segments between primary issuance activities (e.g. fundraising), applicable to token offerors and issuers, and secondary market activities (e.g. trading), applicable to token exchange and trade-related intermediaries. Thailand has also established 3 types of licenses: (i) Digital Asset Exchange License; (ii) Digital Asset Broker License; and (iii) Digital Asset Dealer License.

China has expressed their position with decentralized crypto networks[92] with the banning of 1) crypto mining, 2) provision of crypto trading and payment services and 3) ICOs, but remains receptive to Chinese investors holding and trading of cryptocurrencies. China has been encouraging the use of China’s own Central Bank Digital Currency (CBDC) Digital Renminbi and showed great enthusiasm towards the application of blockchain technology in modernizing China’s financial systems.

India is taking a more calibrated approach towards regulation crypto, after initially floating the idea of outright banning it in the country[93]. Similar to other jurisdictions, India takes on a tough stance towards money laundering and has issued a show-cause notice to India’s biggest crypto exchange – for facilitating money laundering, specifically for infringing the Indian Foreign Exchange Management Act (FEMA)[94]. However, India has yet to issue any clear regulatory guidance on crypto assets.

In developments…

As of writing, the US is about to take the most significant steps from a regulatory standpoint, in the coming months. Changes were made to cryptocurrency tax provisions that were intended to improve tax compliance among those trading digital currencies were drafted as part of a larger Infrastructure Bill, to be passed into law by the US government[95]. There were some key contentious points within the draft that were causing concerns within the cryptocurrency and blockchain industry. In particular, The bill defines a broker broadly as "any person who is responsible for regularly providing any service effectuating transfers of digital assets on behalf of another person". Therefore, under the U.S. tax code, brokers are required to collect and report information on transactions.

[90] https://www.fstb.gov.hk/fsb/en/publication/consult/doc/consult_conclu_amlo_e.pdf
[91] https://www.sec.or.th/EN/Documents/EnforcementIntroduction/digitalasset_decree_2561_EN.pdf
[92] https://www.mondaq.com/china/fin-tech/944330/regulation-of-cryptocurrency-in-china
[93] https://www.businesstoday.in/latest/economy-politics/story/india-today-conclave-not-all-windows-to-be-shut-for-cryptocurrency-says-fm-nirmala-sitharaman-290882-2021-03-15
[94] https://www.livemint.com/companies/news/wazirx-gets-ed-notice-nischal-shetty-says-investors-funds-safe-11623406433211.html
[95] https://www.politico.com/news/2021/08/04/cryptocurrency-tax-provisions-502435

Even proposed fixes were fraught with complications as they would "pick winners and losers" according to critics. The Wyden-Lummis-Toomey amendment, which did not pass, made it explicitly clear that validators and software developers are not “brokers”. However, even that amendment only exempted proof-of-stake and proof-of-work validators while unknowingly excluding the many other consensus mechanisms that exist. The definition of "broker" may also encapsulate blockchain developers and does not acknowledge that many such developers are developing platforms and applications that have little or nothing to do with financial instruments.

The overarching concern amongst stakeholders is that innovation could be stifled if all teams working on blockchain-related projects are required to collect detailed information on their users and provide tax returns as if they were brokers of financial instruments.

In the same week, Rep. Don Beyer (D-Va.) introduced draft legislation for crypto consumer protection[96]. The “Digital Assets Market Structure and Investor Protection Act”
Specifically, the bill would:

- Create statutory definitions for digital assets and digital asset securities and provide the Securities and Exchange Commission (SEC) with authority over digital asset securities and the Commodity Futures Trading Commission (CFTC) with authority over digital assets;
- Provide legal certainty as to the regulatory status for the top 90% of the digital asset market (by market capitalization and trading volume) through a joint SEC/CFTC rulemaking.
- Require digital asset transactions that are not recorded on the publicly distributed ledger to be reported to a registered Digital Asset Trade Repository within 24 hours to minimize the potential for fraud and promote transparency;
- Explicitly add digital assets and digital asset securities to the statutory definition of “monetary instruments,” under the Bank Secrecy Act (BSA), formalizing the regulatory requirements for digital assets and digital asset securities to comply with anti-money laundering, recordkeeping, and reporting requirements;
- Provide the Federal Reserve with explicit authority to issue a digital version of the U.S. Dollar, clarify that digital assets, digital asset securities and fiat-based stablecoins are not U.S. legal tender, and provide the U.S. Treasury Secretary with authority to permit or prohibit US Dollar and other fiat-based stablecoins;
- Direct the Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), and Securities Investor Protection Corporation (SIPC) to issue consumer advisories on “non-coverage” of digital assets or digital asset securities to ensure that consumers are aware that they are not insured or protected in the same way as bank deposits or securities; and,
- Require legislative recommendations from FinCEN, SEC and CFTC to provide clarity on dividing lines between who must register as a money services business versus who must register as a securities or commodities exchange.

On 3rd August 2021, SEC chairman Gary Gensler shared his thoughts about crypto regulation with the key consideration being to protect investors in crypto and also gave his views on several key crypto products in the space[97]. 1) Stock tokens which give exposure to underlying securities are subject to securities law and need to adhere to current securities regulations. 2)

[96] https://beyer.house.gov/news/documentsingle.aspx?DocumentID=5307
[97] https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03

Crypto trading platforms not only implicate the securities laws, but some platforms will also implicate the commodities laws and banking laws. A typical trading platform has over 100 tokens trading on them and each token's legal status depends on its facts and circumstances, therefore the probability is quite remote that of the 100+ tokens none of them is a security given that there is no clear gatekeeping mechanism in enforcing the security criteria before listing on those platforms. 3) Nearly 75% of training on crypto trading platforms occurred between a stablecoin and another token, thus the use of stablecoins on these platforms may facilitate those seeking to sidestep a host of public policy goals connected to the banking and financial system. E.g. KYC/AML, Tax compliance, Sanctions, etc, thus the intent is to apply the full investor protections of the Investment company Act and other federal securities laws on these products. Additionally, he mentioned the need for more legislation on crypto trading, lending and DeFi platforms and granting regulators additional authorities to regulate the crypto ecosystem.

DeFi Regulation

Decentralized Finance (DeFi) have largely been unregulated in major jurisdictions, as participants interacts with smart contracts to trade and conduct other financial activities without a middleman or centralized entity. Developers of these applications believe that DeFi applications are not subjected to current regulation requirements as core developers will step away from the project after writing software that automates and facilitates users transactions with the protocol thereby achieving decentralization in the process, similar to the SEC's stance on Bitcoin. However, SEC chairman Gary Gensler takes on a different view such that "there's still a core group of folks that are not only writing the software, like the open source software, but they often have governance and fees," where "there's some incentive structure for those promoters and sponsors in the middle of this." Mr Gensler also added that "these platforms facilitate something that might be decentralized in some aspects but highly centralized in other aspects." Regulators stance on protecting investors interest in crypto has been clear, while DeFi currently do not require KYC/AML, or any safeguards against money laundering or other criminal activities, there may be some regulatory gaps that will be filled as regulators find a balance between regulating decentralized applications and ensuring investors interests.

It is clear that the crypto industry needs better defined public policies to take it mainstream and the current developments in the US will be watched by the world, and what eventually comes out of it will likely influence how regulators around the world view crypto.

Stacks Blockchain

What is Stacks Blockchain?

Stacks[98] is an open-source network of decentralized apps and smart contracts built on Bitcoin. Stacks unleashes Bitcoin's full potential as a programmable base layer.

This describes Stacks, but as simple as this definition is, there's a lot to unpack here, let's, deep-dive, into it.

Introduction

The internet is the most significant technological revolution in human history. Tim Berners-Lee's[99] Internet was meant to be *"a collaborative medium, a place where we [could] all meet and read and write."*

However, with all of the amazing updates, the Internet world changed. It felt amazing when everything we desired arrived in our hands in a matter of seconds, thanks to the Internet. The threat to digital privacy, on the other hand, became very real at the same time.

- We began to lose our privacy from phones in our pockets to biometric databases used to mark us to government officials.
- Our online browsing is being tracked and logged in. More Internet-connected devices are making their way into our homes.
- These innovations have provided us with many daily conveniences and "free" services. But the data they generate is being crunched, archived, and repurposed for marketing and surveillance.
- We are now facing risks that were unthinkable only a decade ago. Many companies & governments are acquiring and using data in ways that are not in people's best interests. Unfortunately, those we entrust with our data can sometimes let us down.
- Digital Privacy issues are severe, and we are all becoming the victims.

With the threat to digital privacy growing, the tech world is trying to find the solution with decentralized blockchain technology.

Why Decentralized technology (Crypto and Blockchain World)?

Although platforms such as Facebook, Whatsapp, and other messaging and email platforms improve their privacy policies, these applications' centralization framework has allowed platform handlers and hackers to target our personal data and harvest our private information. People's privacy concerns about using centralized networks like Facebook, Google, clouds, and other mediums of connection are growing. There is a need for a decentralized platform that addresses all of their privacy concerns.

Unlike early web applications, which are generally maintained at no cost to developers (or large tech companies), the decentralized protocol layer such as blockchain is transparent. Everything is public and auditable here.

[98] https://www.stacks.co
[99] https://us.corwin.com/sites/default/files/upm-binaries/10848_Chapter_1.pdf

What is Stacks?

Stacks[100] (originally Blockstack) – see Introduction (Stacks) section for backstory; was co-founded in 2013 in the Princeton computer science department by Muneeb Ali[101] and Ryan Shea[102]. They built this ecosystem with the base of Stacks blockchain. Stacks blockchain is a layer 1 virtual blockchain built on top of the Bitcoin blockchain. This enables the most durable and secure blockchain known so far, the Bitcoin blockchain programmable.

Stacks have a native token with the ticker **STX**. This is the first SEC-approved non-security token[103]. STX tokens act as fuel for Clarity smart contracts running on the Stacks blockchain along with the money value. Plus, the STX tokens also ensure the network is stable with the novel Stacking mechanism.

Why build Stacks on top of Bitcoin?

Bitcoin is the strongest sovereign blockchain. Bitcoin is a tamper-proof source of truth, a value settlement protocol. Once you have the ultimate truth source, other decentralized protocols and use cases can be built on it.

The world is converging on Bitcoin, and the demand for use cases around Bitcoin is increasing. Instead of competing with Bitcoin's underlying protocol, Stacks builds on and extends Bitcoin. This enables Stacks to grow with Bitcoin and leverage Bitcoin's capital, security, and network. Also, A transaction is impossible to reverse or change once it has settled on Bitcoin. These settlement assurances are critical to decentralized apps.

If Bitcoin is so powerful and secure, why not build directly on Bitcoin? Why a separate blockchain?

There are two fundamental challenges to building apps and smart contracts on Bitcoin.

- Scalability: The base Bitcoin blockchain has a limited capacity for transactions.
- Secure contracts: The Bitcoin blockchain has a limited scripting language and does not allow general smart contracts. This design choice ensures security at the base layer.

The Stacks blockchain addresses the limitations of scalability and secure smart contracts and enables apps and smart contracts for Bitcoin. This is possible through a unique consensus algorithm called Proof-of-Transfer that runs between two blockchains. Enabling scalable smart contracts directly on Bitcoin has been a long-standing bottleneck, and the Stacks blockchain unlocks that functionality.

What will happen to Stacks blockchain if the security of the Bitcoin blockchain is compromised? – Even though this scenario is most unlikely, if it happens, then it won't affect Stacks much. That is because Stacks is a virtual blockchain.

[100] https://gaia.blockstack.org/hub/1AxyPunHHAHiEffXWESKfbvmBpGQv138Fp/stacks.pdf
[101] https://twitter.com/muneeb
[102] https://twitter.com/ryaneshea
[103] https://www.sec.gov/Archives/edgar/data/1693656/000110465919039908/a18-15736_1253g2.htm

What is a Virtual blockchain?

Have you heard of virtual machines, fondly called as VMs? Virtual machines are the software that emulates the computer. VMS is utilizing the hardware of the base machine and gets bootstrapped. Why are they doing this? Say you are running Linux VM on top of a Windows machine and something happens to your Windows machine. Still, you can access your Virtual machine from another Base Windows machine, and your work is not lost.

Similarly, the Stacks Blockchain is a virtual chain that is bootstrapped by utilizing the power of the base Bitcoin blockchain. This is an excellent concept that makes Stacks even more powerful. In the future, if something happens to the Bitcoin blockchain, then Stacks blockchain can easily migrate stacks blockchain to another base blockchain.

This acts as a powerful solution for longevity and scalability for Stacks blockchain. This unlocks great potential for apps built on top of the Stacks blockchain with App Chains' concept.

What are App Chains?

Like how Stacks is built as a virtual chain on top of the Bitcoin blockchain, the Apps built on Stacks can also have their own virtual chains on top of the Stacks blockchain. This will solve the scalability issues of the apps.

Microblocks

Microblocks enables near-instantaneous transaction time on the Stacks blockchain[104]. How do microblocks work? As part of Stacks mining process, a leader is elected every 10mins via the verifiable random function (VRF) to mint a new Stacks block, along with broadcasting the batched transactions associated with the new block. In addition to sending batched transaction data, an elected miner leader can "stream" a block throughout its tenure by selecting transactions from the mempool as they arrive and packaging them into microblocks[105]. These microblocks contain small batches of transactions, which are organized into a hash chain to encode the order in which they were processed. If a leader produces microblocks, then the new chain tip the next leader builds off of will be the last microblock the new leader has seen.

In this setup, streaming of transaction data allows for lower latency, as transactions can be included in between the current epochs and the next epoch that will be mined. Each newly minted Stacks block settles on the Bitcoin blockchain as the ultimate source of truth via Proof-of-Transfer consensus, with microblocks providing a new lower-latency global view of the Stacks blockchain transaction state. Therefore, Microblocks improves the experience for users and developers and are a step further in scaling bitcoin.

[104] https://www.hiro.so/blog/microblocks-reduce-transaction-processing-times

[105] https://github.com/stacksgov/sips/blob/main/sips/sip-001/sip-001-burn-election.md

Stacks 2.1

Stacks 2.1[106] will be the next major upgrade introduced to Stacks blockchain, with several added features that would improve the functionality of Stacks blockchain and user experience. Some of the key improvements are:

- Stacking Improvements – continuous stacking, fine-grained bidding and unlocked unused STX automatically.

- Better In-band upgrades – voting to stop the network, Voting to extend the PoX sunset date, Voting on which contract is the PoX contract.

- Better Clarity APIs – Expose PoX reward set info, Handle PoX STX locking in Clarity, Native Merkle proof verification, More Clarity Built-ins

- Reliability Improvements – Fix mean-of-min-and-median sortition logic, Better tolerance for flash blocks in the prepare phase, Order-independent multisig signing and verification, Adjusted runtime costs

A vote-to-upgrade feature[107] will be introduced before the upgrade to Stacks 2.1, where STX token holders and miners can collectively vote on when Stacks 2.1 should go live.

Proof-of-Transfer

Stacks blockchain made Bitcoin programmable with the consensus algorithm Proof-of-Transfer.

What is a consensus algorithm?

Cryptocurrencies and blockchains are both decentralized networks with no centralized authority. The desired, one-of-a-kind features are enabled by decentralization (censorship resistance, seizure resistance, trust minimization, etc.). However, there is a cost to decentralization: how do we ensure that network participants agree on the “truth” when no one is “in charge?”. That is where the consensus algorithm helps. In the absence of a centralized authority, trust is established through “consensus protocols.”

Consensus protocols can be thought of as a set of rules that incentivize actors to create a record of the truth, such as which funds belong to which addresses in a public ledger system, allowing everyone else to verify the truth. As seen in the previous chapter, Bitcoin is the most secure blockchain because of its consensus algorithm Proof of Work (PoW), which has high decentralization and security levels.

What is Proof-of-Transfer

Proof-of-Transfer (PoX) is the first consensus algorithm between two blockchains. For participating in PoX based Stacks mining, the miners don’t need any specialized hardware. All they need is Bitcoin. In a way, PoX helps to bootstrap the new blockchains securely.

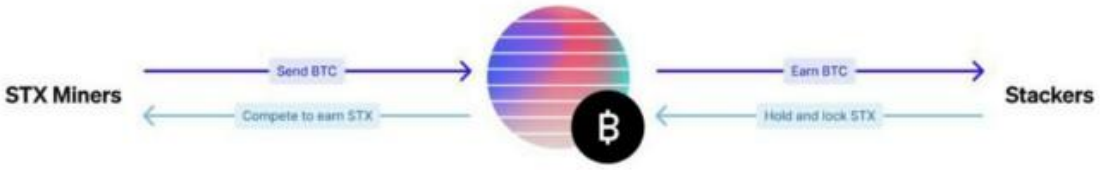
[106] https://github.com/stacksgov/sips/discussions/16?sort=new

[107] https://github.com/blockstack/stacks-blockchain/discussions/2687

In PoX, leader election happens on the Bitcoin blockchain. Instead of burning electricity on proof of work, PoX reuses already minted bitcoins as “proof of computation” and miners represent their cost of mining in bitcoins directly.

In a PoX-based Stacks Blockchain, there are 2 major network participants.

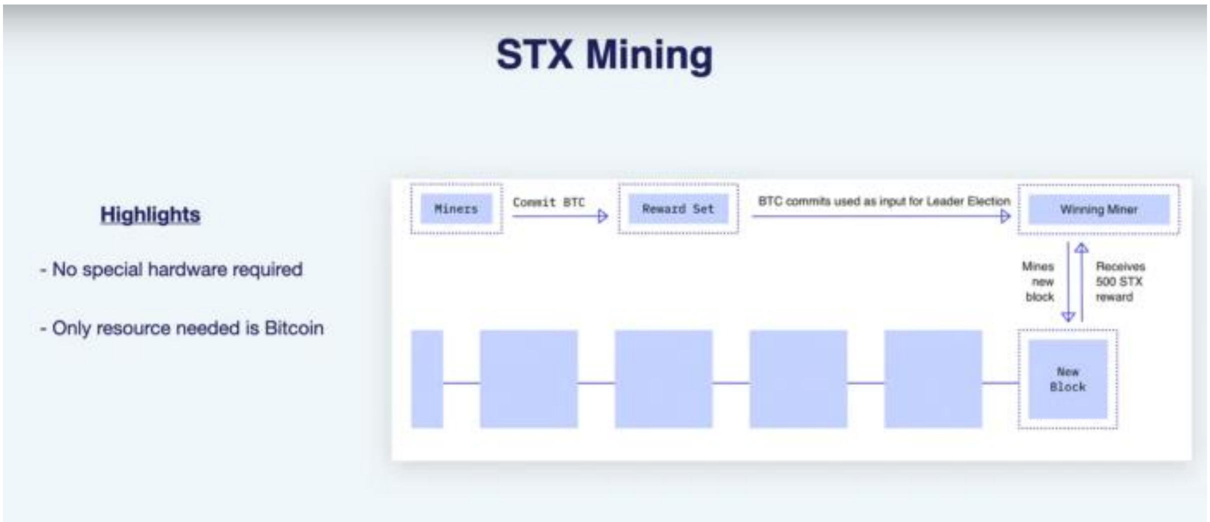
1. Miners – They spend Bitcoin and earn new Stacks tokens, smart contracts, and transaction processing fees.
2. Stackers – They signals their support by Stacking STX tokens and earn Bitcoins.



Proof of Transfer consensus mechanism

Mining & Stacking

STX miners bid for becoming the leader in mining the next block. For this process, they spend Bitcoins. The protocol selects the winning miner (i.e., the leader) around using a verifiable random function (VRF). This is made to ensure a fair chance. Once elected, the leader writes the Stacks blockchain's new block and mints the rewards: newly minted Stacks for the block, fees for smart contracts, and transactions.



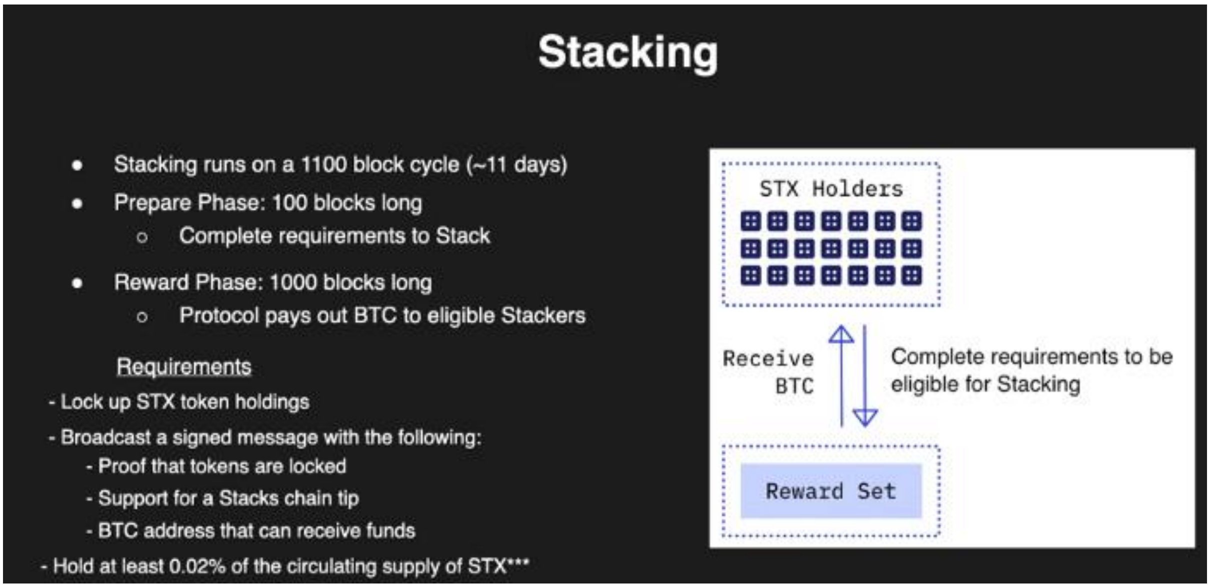
STX Mining

Highlights

- No special hardware required

- Only resource needed is Bitcoin

Bitcoins used for miner bids are sent to specific addresses corresponding to Stacks STX tokens holders that actively participate in consensus. Again these reward addresses are also random and are selected with the help of VRF. Thus, the bitcoins consumed in the mining process go to productive Stacks holders as a reward based on their holdings of Stacks and participation in the Stacking algorithm. This is called Stacking.



Stacking

- Stacking runs on a 1100 block cycle (~11 days)
- Prepare Phase: 100 blocks long
  - Complete requirements to Stack
- Reward Phase: 1000 blocks long
  - Protocol pays out BTC to eligible Stackers

Requirements

- Lock up STX token holdings
- Broadcast a signed message with the following:
  - Proof that tokens are locked
  - Support for a Stacks chain tip
  - BTC address that can receive funds
- Hold at least 0.02% of the circulating supply of STX***

STX Holders

Receive BTC

Complete requirements to be eligible for Stacking

Reward Set

However, does the Stacking portion resembles Staking in certain respects? Furthermore, why is Stacks built on a PoW-based blockchain rather than a Proof-of-Stake (PoS) based blockchain? – To answer this, let's understand PoS first.

Proof-of-Stake (PoS)

In this mining, the network participants will stake some tokens to prove they are interested in securing. This system has the below limitations.

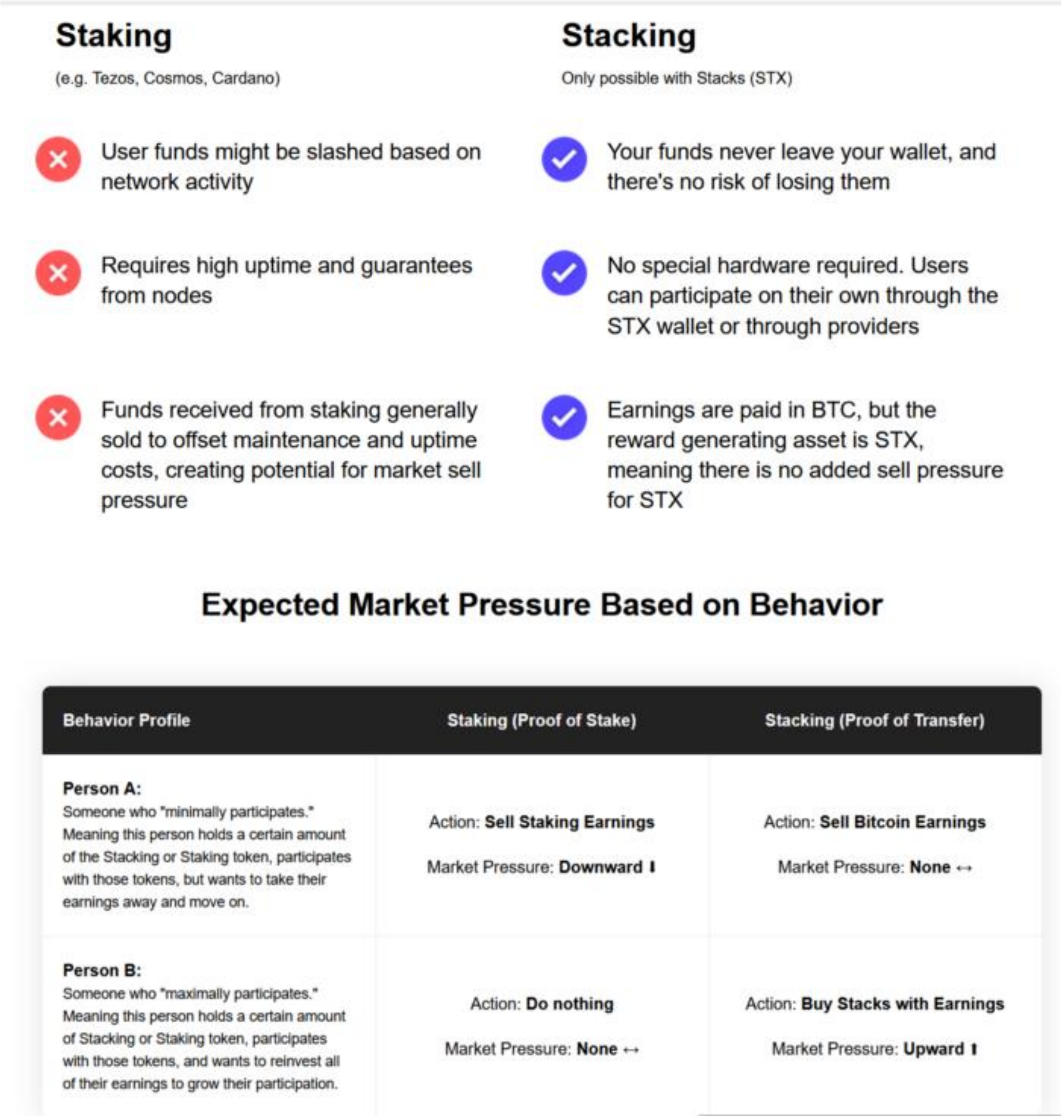
Lack of initial Liquidity: The initial validating nodes are reluctant to transfer coins to other nodes as the opportunity to mine is directly proportional to the value of coins accumulated by the node

- *Second Spend Chain:* There is a possibility that the second spend may get recorded as a valid transaction. A corrupt node can secretly build & grow an alternative chain using that second spend block. Once it grows bigger than the valid chain, the network will have to accept it as the main chain, and hence sanity of consensus will be destroyed.
- *51% risk:* If an entity owns 51% or more of the currency, it can corrupt the blockchain by gaining most of the network.
- *Restricted Liquidity:* As the miners' network grows more, native cryptocurrency becomes idle and can't be traded as more mining nodes hold it.

Why Proof-of-Transfer is not based on Proof-of-Stake

PoX is an extension to PoW based blockchain to make it more programmable. There is a reason why Stacks is not being based on top of a PoS blockchain.

In PoS, if a node has been disconnected for a sufficiently long time or is bootstrapping and presented with two conflicting transaction histories, the network can't determine which one is the "true" chain without some external input. This is because it is impossible to know whether or not the "committee" that validates the chain is majority-honest and not post-facto corrupted (i.e., attacker-controlled). This is not the case for PoW blockchains, where the valid chain with the most cumulative proof-of-work is always the “true” chain. This is not to say that PoS is insecure or is a bad idea. But, PoS has undesirable security assumptions compared to PoW[108].



Staking

(e.g. Tezos, Cosmos, Cardano)

- ✗ User funds might be slashed based on network activity
- ✗ Requires high uptime and guarantees from nodes
- ✗ Funds received from staking generally sold to offset maintenance and uptime costs, creating potential for market sell pressure

Stacking

Only possible with Stacks (STX)

- ✓ Your funds never leave your wallet, and there's no risk of losing them
- ✓ No special hardware required. Users can participate on their own through the STX wallet or through providers
- ✓ Earnings are paid in BTC, but the reward generating asset is STX, meaning there is no added sell pressure for STX

Expected Market Pressure Based on Behavior

Behavior Profile	Staking (Proof of Stake)	Stacking (Proof of Transfer)
Person A: Someone who "minimally participates." Meaning this person holds a certain amount of the Stacking or Staking token, participates with those tokens, but wants to take their earnings away and move on.	Action: **Sell Staking Earnings** Market Pressure: **Downward ⬇**	Action: **Sell Bitcoin Earnings** Market Pressure: **None ↔**
Person B: Someone who "maximally participates." Meaning this person holds a certain amount of Stacking or Staking token, participates with those tokens, and wants to reinvest all of their earnings to grow their participation.	Action: **Do nothing** Market Pressure: **None ↔**	Action: **Buy Stacks with Earnings** Market Pressure: **Upward ⬆**

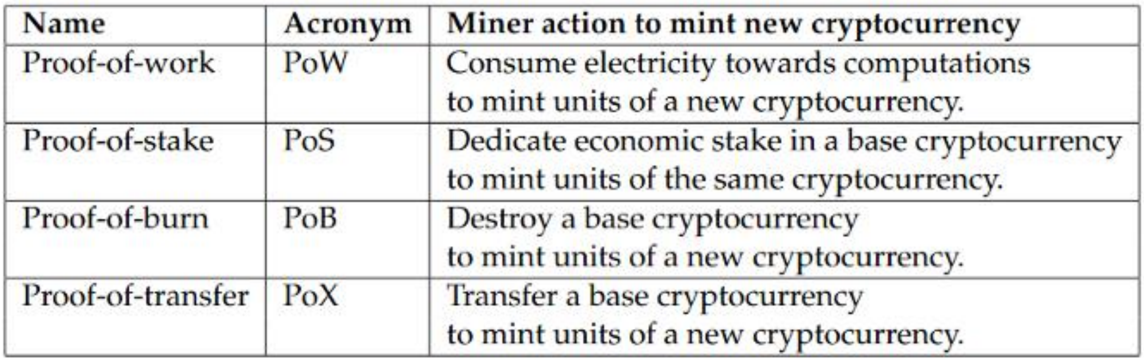
Also, one more notable point here is Stacking is a part of the consensus. Stacks chain will make progress even if no one participates in Stacking. Also, the network security is much better in PoX. One example, as per the PoX consensus, PoX will fall back to Proof of Burn (PoB)[109] when there is an act of a malicious miner.

What is Proof-of-Burn (PoB)

This is the consensus algorithm proposed before PoX for the Stacks 2.0 blockchain.
In PoX, the miners transfer the tokens to Stackers, whereas in PoB, before Stacks 2.0, this will be in the form of miners burning bitcoin and are rewarded in a new cryptocurrency (STX

[108] https://forum.stacks.org/t/pos-blockchains-require-subjectivity-to-reach-consensus/762
[109] https://github.com/stacksgov/sips/blob/main/sips/sip-007/sip-007-stacking-consensus.md

token). PoB is destructive, requiring miners to destroy value to secure the blockchain. So, PoB suffers from a potential bootstrapping problem. This is because, before the PoB chain matures and the new cryptocurrency gains value and stability, miners may be unwilling to destroy Bitcoin to participate.



Name	Acronym	Miner action to mint new cryptocurrency
Proof-of-work	PoW	Consume electricity towards computations to mint units of a new cryptocurrency.
Proof-of-stake	PoS	Dedicate economic stake in a base cryptocurrency to mint units of the same cryptocurrency.
Proof-of-burn	PoB	Destroy a base cryptocurrency to mint units of a new cryptocurrency.
Proof-of-transfer	PoX	Transfer a base cryptocurrency to mint units of a new cryptocurrency.

Table 1: *Comparison of proof-of-work with other mechanisms.*

Why PoX is the best tool for a user-owned Internet?

For building a user-owned Internet, PoX based Stacks blockchain is truly a powerful tool. In this process, network participants are incentivized to hold the tokens so long as the service/network resource given back is worth it. If that changes, they can leave their creations and connections intact. Also, this is secured by the PoW based blockchain. This model of digital ownership is what will fix our broken internet and become the standard. It rewards power and value to the people responsible for making it what it is in the first place.

Consensus protocols are a set of instructions that keeps the blockchain secure. Different consensus algorithms are available and have their own pros and cons. PoX is a novel consensus algorithm on the Stacks 2.0 blockchain that helps solve the new blockchain's potential bootstrapping problems. Also, it rewards its network participants, thus ensuring sustainability.

Imagine the possibilities with such a setup, allowing you to use web apps, all without the risk of mass data breaches, loss of user privacy, and the lack of data portability. Physical assets and new forms of assets can be digitized on the blockchain and be transferred freely, with the Bitcoin network's security, thus allowing for new business models, governance, and funding mechanisms.

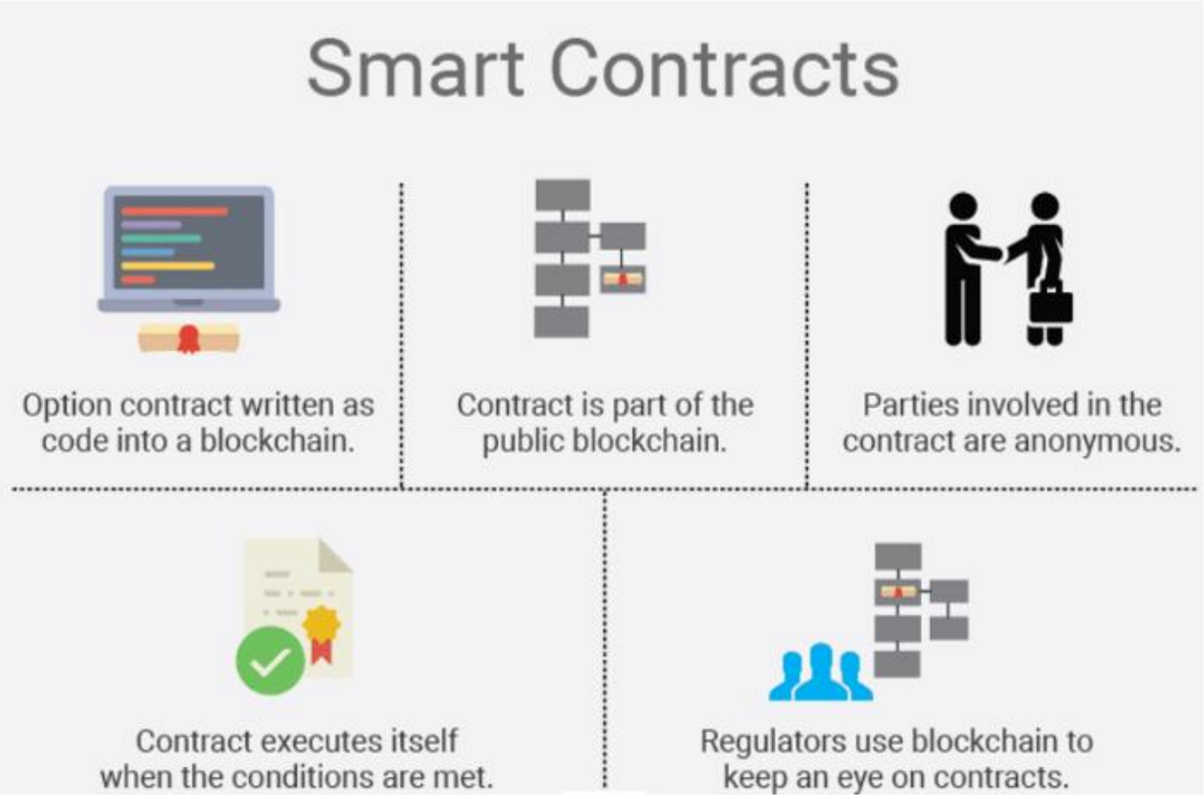
Clarity Smart Contract

In the previous chapter, we learned all about the consensus mechanism of the Stacks blockchain Proof-of-Transfer (PoX). We also understand that PoX makes Bitcoin programmable. To recap, we learned that the Bitcoin blockchain is secure because it has a minimal scripting language with a small attack surface, among other properties. Introducing new features to the Bitcoin core protocol is hard and not desirable as these features add complexity. Stacks has solved this problem with the help of PoX, and it's a native smart contract programming language, Clarity[110]. Let's understand all about Clarity smart contracts in this chapter.

[110] https://clarity-lang.org

What are Smart Contracts?

A Smart Contract is an agreement between two or more parties in the form of computer code. Contracts are stored on the blockchain and cannot be modified. In the physical world, the transactions are being processed with centralized authority/intermediaries. Transactions in a Smart contract are processed by the blockchain, allowing them to be sent automatically without a centralized authority/intermediaries' intervention. There is no need for a confidential advisor when you agree with a smart contract. The transactions take place only if the terms of the agreement are met. Smart contracts enable us to exchange money, stock, or anything else of value in a transparent, trustless manner, all while avoiding the services of an intermediary and the risk of conflict.


Smart Contracts
Option contract written as code into a blockchain.
Contract is part of the public blockchain.
Parties involved in the contract are anonymous.
Contract executes itself when the conditions are met.
Regulators use blockchain to keep an eye on contracts.

The quote below by Vitalik Buterin, Founder of Ethereum Blockchain, explains Smart Contracts eloquently.

"Smart contracts — It's like a vending machine. You put money in, and candy comes out. A vending machine is a physical device that executes the rules of the agreement. But a vending machine can be broken. By digitizing the concept, cryptography makes these contracts far more secure and powerful."

The most important features of a smart contract are:

1. Digital Agreement — A Smart Contract is an agreement in the form of a computer code.
2. Blockchain — Transactions are processed by a public database based on blockchain technology.
3. Confidentiality — A transaction can only take place if the conditions in the agreement are met.

When implemented, a smart contract can replace the need for an attorney or a notary to sign a document that can be upheld in court. These contracts execute themselves when all the clauses in the contract are met.

Clarity Programming Language

Clarity is a *decidable programming language* designed as "*non-Turing complete* " and "*Not intended to compile.* "

What is a Non-Turing complete programming language?

To understand why Clarity is designed as a non-Turing complete programming language, we should first know what Turing complete language and its limitations are.

What is Turing complete programming language?

A programming language is considered as Turing complete if it can do what a Turing machine can do.

What is a Turing machine?

Alan Turing was a mathematician who created a theoretical machine called the Turing Machine. This mythical machine has access to an infinite amount of RAM and runs using a finite program that determines when it should write, read, and move within its memory. The machine's programming also dictates under what conditions it should terminate and what it should do next. Programming languages that fit these conditions are known as TC (Turing complete) languages.

A language will be deemed Turing complete if it satisfies the below conditions.

- Has the ability to implement any computable function.
- It always includes a function that won't terminate by itself.
- Includes a function that, theoretically, could use an infinite amount of memory.

Refer to the Turing Complete-Computerphile video[111] to understand the Turing machine functioning. Most of the language which we are using to date is Turing complete.

What harm does a Turing complete smart contract programming language cause?

Smart contracts are powerful, but they cannot be fully entrusted due to the history of bugs reported. The most popular blockchain for smart contracts is Ethereum, and its widely used smart contract language is Solidity. Solidity is a statically typed, contract-oriented, high-level language. It is a very effective language but had several issues reported, a few of them listed below. One of the reasons is that this is Turing complete programming language.

1. DAO hack[112] (recursive call exploit)
2. Re-entrancy attacks[113] (caused by the poorly implemented contracts)
3. Halting problem[114]
4. Predicting the transaction fee is very difficult since the static analysis[115] cannot be performed.

[111] https://www.youtube.com/watch?v=RPQD7-AOjMI
[112] https://medium.com/@ogucluturk/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562
[113] https://eprint.iacr.org/2016/1007.pdf
[114] https://en.wikipedia.org/wiki/Halting_problem
[115] https://www.perforce.com/blog/sca/what-static-code-analysis

What is Clarity?

Clarity is Stack's smart contracting language for use with the Stacks blockchain. Clarity supports programmatic control over digital assets within the Stacks blockchain (BNS names, Stacks tokens, and so forth). Unlike the Turing complete programming languages known so far, Clarity is a non-Turing complete language intended to avoid all the above-said issues of a Turing complete programming language. Also, it aims to provide the users with an option to do static analysis well before the code is being implemented.

The following are some key differences of Clarity, being a non-Turing complete and interpreted programming language.

1. *Turing incompleteness enables static analysis* to determine the cost of executing a given transaction. This will help the network calculate the transaction fee well in advance, which will be conveyed to the user.

2. *Turing incompleteness* allows static analysis to find out which other contracts a particular transaction ever invokes. By analyzing this, the possible side-effects can be predicted and avoided. This improves user experience and helps the clients to gain credibility from users.

3. *Improved and accurate static analysis* will help the developers analyze and find out possible bugs before implementing /executing the code, which avoids many future issues. The quality of the code can be improved.

   In Clarity, static analyses run before ever broadcasting the smart contract can provide information such as:

   1. The cost to broadcast a given transaction as a function of input size.
   2. The sets of transactions that will be able to modify any particular table. Future work could support even more advanced analysis features, such as the ability to automatically check proofs on smart contracting code.

4. *Clarity is interpreted language*, which means it's not intended to be compiled. As per blockchain, "code is law," and rules committed to a blockchain are the source of ultimate truth. But is it exactly showing what was there in the developer's mind? The answer to this question is not 100 %. Ultimately, bugs can be introduced during compilation as well. Also, if there is a bug in the source code, it is easy to directly fix it in the interpreter and restart the nodes rather than fix it in the compiler. That's why, in Clarity, the intermediate step of compilation is avoided, and this language intends to publish the developer's exact intention, written as a contract(source code), to be directly published/ deployed in the blockchain.

Much like concurrency primitives, well-designed smart contracts can prevent bugs, but poorly designed contracts, however, can exacerbate hard-to-debug problems. This is especially important given smart contracts manage billions of dollars[116] for people. With Clarity, Stacks took the WYSIWYG — what you see is what you get — approach. This approach is providing a base platform for building endless decentralized apps on Bitcoin that puts users in control.

[116] https://www.coinschedule.com/stats

Clarity Language Design

The basic parts of Clarity are *data spaces* and *functions*. Clarity is a LISP (List Processing language), and it has its native types. Also, in Clarity, by default, all the functions are private unless declared as public.

Atoms and Lists

The basic building blocks of Clarity are “atoms” and “lists.”

An *atom* is a number or string of contiguous characters. Atoms can be native functions, user-defined functions, variables, and values that appear in a program.
For example:

- Token-amount
- 324314
- SP2HRJRFVK7MSDJ3T1RWG8385FKRJEWR59BPS014

A *list* is a sequence of atoms enclosed with `()` parentheses. Lists can contain other lists.

For example:

```
(is-none? (get id (fetch-entry names-map (tuple (name
\”clarity\”)))))
```

Data Spaces

The data in Clarity is handled as below.

1. Each smart contract has its own data space. Data within this data space are stored in maps.
2. These stores relate a typed-tuple to another typed-tuple (almost like a typed key-value store).
3. As opposed to a table data structure, a map will only associate a given key with exactly one value.
4. Any smart contract may fetch data from any other smart contract maps. However, only a smart contract may directly update data within its own maps.

Data maps’ interface ensures that the return types of map operations are fixed length, which is a requirement for static analysis of smart contracts’ runtime, costs, and other properties.

Functions

In Clarity, functions can be either public, read-only or private.

1. Public functions — Public functions can be called from other contracts.
2. Private functions — Private functions can only be executed by the current smart contract.
3. Read-only functions — Read-only functions are also public, but as the name implies, they cannot change the contract’s state, like variables values, data maps, or token transfers.

Some of the notable Clarity language features

- The Clarity language uses a strong static type system. Function arguments and database schemas require specified types, and the use of types is checked during contract launch. The type system does *not* have a universal supertype.

- *Principals* are a Clarity native type that represents an entity that can have a token balance.
- In Clarity, if a function mutates data, it is terminated with an! Exclamation point. For example, *change-name!*
- Clarity supports comments using ; (double semicolons). Inline and standalone comments are supported.

Note: Refer to the Stacks docs on Clarity language[117] to learn more.

Clarity Language Limitations

- The only primitive types are booleans, integers, buffers, and principals.
- Recursion is illegal, and there are no anonymous functions.
- Looping may only be performed via map, filter, or fold.
- There is support for lists; however, the only variable-length lists in the language appear as function inputs; there is no support for list operations like append or join.
- Variables are immutable. Meaning, Variables are created by 'let,' binding and mutating functions like 'set' are not supported.

Clarity is designed to protect the code from common security vulnerabilities in other smart contract languages thus making Clarity more safe and secure.

Bitcoin Native Swap

Allows users to do trustless BTC swaps to stablecoins, derivatives, perpetuals and other crypto assets on the main Bitcoin Network[118], by sending bitcoins from one address to another. With Bitcoin Native Swap, DEXes, AMMs can now be built with direct interaction with the Bitcoin main chain, with the security of Bitcoin. Friedger, a Stacks community developer have executed a trustless swap, Swapping the NFT for Bitcoins works with a Clarity smart contract on the Stacks chain that has knowledge about the Bitcoin blockchain. This type of swap is called catamaran swap because - unlike submarine swap[119] - Catamaran swaps are three leg swaps where two transactions happen on the Stacks chain and one transaction happens on the Bitcoin chain. In contrast to Submarine swaps where some actions happen on-chain (over water) and some off-chain (underwater), all actions happen on-chain just on two different blockchains, hence Catamaran.

ELI5: You can pay someone in bitcoin and their house title, car ownership (via NFTs) can be transferred to you, all happening through smart contracts with direct interaction with the Bitcoin Network without a separate third party.

Solidity

Another commonly used smart contract programming language is Solidity[120]. Solidity was initially proposed in 2014 by Gavin Wood and later developed by the Ethereum project's Solidity developer team. Solidity is an object-oriented, high-level language for implementing smart contracts. Solidity is a curly-bracket language. It is influenced by C++, Python and JavaScript, and is designed to target the Ethereum Virtual Machine (EVM). Many wild

[117] https://docs.blockstack.org/en-US/write-smart-contracts/overview
[118] https://app.sigle.io/friedger.id/A-l0d8h0Bq7uEGTWl004B
[119] https://wiki.ion.radar.tech/tech/research/submarine-swap
[120] https://soliditylang.org/

frameworks, such as Truffle or OpenZeppelin, help developers quickly get started with Solidity. However, Solidity's syntax is not very clear, thus requiring longer audit periods.

Rust

Rust programming language has traditionally been a widely-used programming language among software developers, as the blockchain industry matures, various blockchains have adopted Rust as the smart contract programming language (e.g. Solana)[121]. Rust is a multi-paradigm, high-level, general-purpose programming language designed for performance and safety, especially safe concurrency. Rust is syntactically similar to C++ but can guarantee memory safety by using a borrow checker to validate references. Rust achieves memory safety without garbage collection, and reference counting is optional.

With multiple smart contract programming languages available on different blockchains, we've compiled a quick summary table of three of the more commonly used smart contract languages for reference.

Parameters/Language	**Clarity**	**Solidity**	**Rust**
Blockchain	Stacks	Ethereum	Solana
Requires Compilation	No	Yes	Yes
Turing Complete	No	Yes	Yes
Supported Types	integers, Booleans, buffer, list, principal, tuple, optional and response	integers, Booleans, buffer, list, principal, tuple, optional, and response	scalar, integers, floating-point, Booleans, character, tuple and array
Complex Types	mappings, fixed-size arrays	structs, mappings, fixed-size & dynamic-size arrays	Structs, slices, trait objects
Gas Estimation	Precise	Approximate	Approximate
Design Style	LISP like	JavaScript like	C++ like
Re-entrancy Attack Vulnerability	Not vulnerable	Vulnerable if coded	Limited to direct self-recursion capped at a fixed depth[122]

Building Web 3 Apps on Stacks

The Internet as we know it today has some clear limitations where users do not have ownership over their data. Our data architectures are still based on the idea of stand-alone computers, where data is centrally stored and maintained on a server and sent or retrieved by a client, even though the Internet has been widely adopted for thirty years. Additionally, in Web 2.0 we do not have a native value settlement layer as we transact digitally.

Crypto and Blockchain tech is complex, and there never existed an easy stack for application developers to build products for the user-owned internet. With 'Stacks', anyone can build 'Can't Be Evil' Web 3 apps with or without smart contracts. The most significant advantage of

[121] https://docs.solana.com/developing/on-chain-programs/developing-rust
[122] https://docs.solana.com/developing/programming-model/calling-between-programs#reentrancy

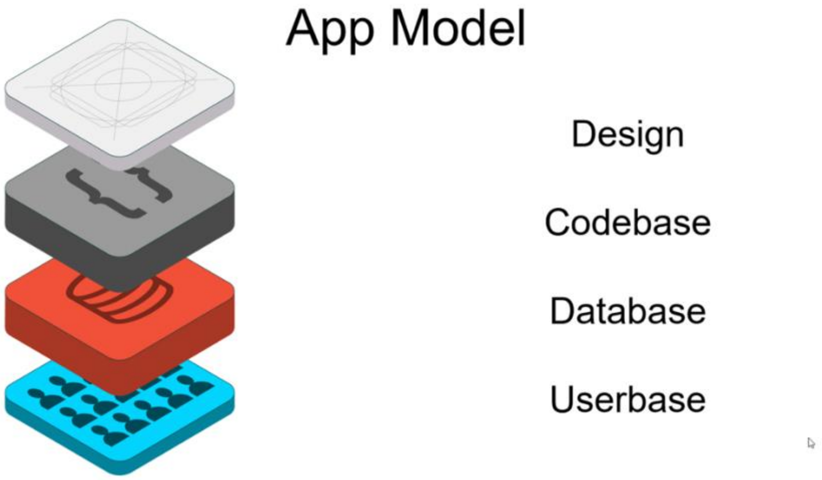
the apps being built on Stacks is that they have zero friction, and an average person can use it without even knowing that it is a dApps (Decentralized Applications). Stacks make the blockchain programmable friendly for developers.

Traditional App Model Vs. Stacks dApp model

For any application, there are always two main areas of focus as application developers.

1. Identity management
2. Storage management

App Model in traditional apps, developers have to maintain multiple layers as referenced below:



App Model

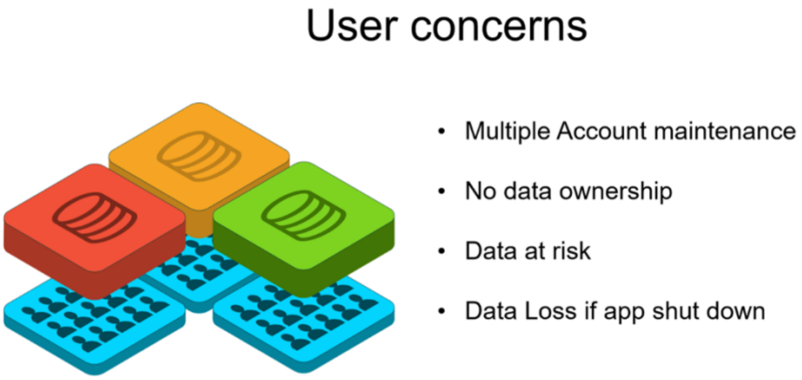
Design

Codebase

Database

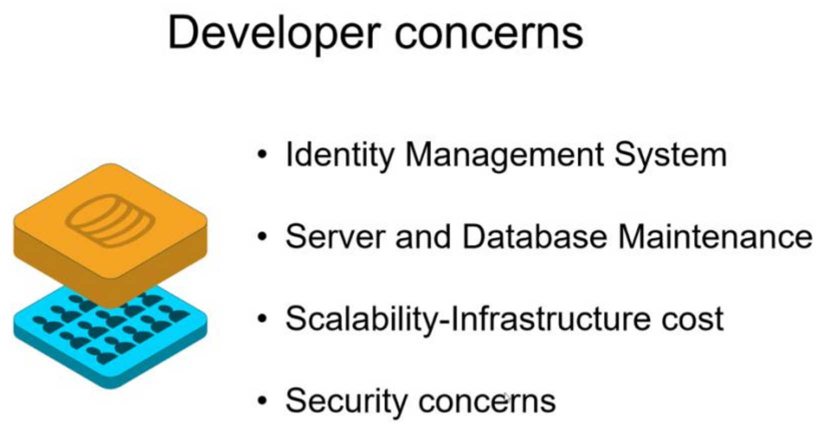
Userbase

Due to the nature of the structure design for traditional apps, there are several limitations that stakeholders face:



User concerns

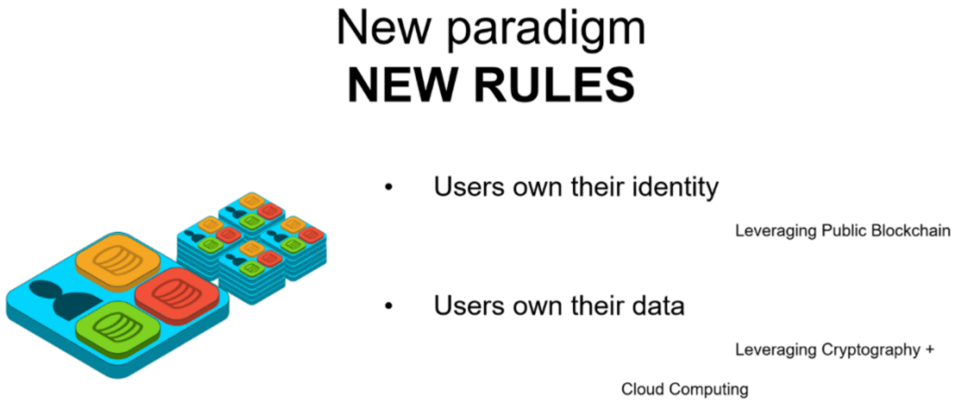
- Multiple Account maintenance
- No data ownership
- Data at risk
- Data Loss if app shut down



Developer concerns

- Identity Management System
- Server and Database Maintenance
- Scalability-Infrastructure cost
- Security concerns

Whereas, in the dApps built using Stacks, there are no such concerns at all.



New paradigm
NEW RULES

- Users own their identity

Leveraging Public Blockchain

- Users own their data

Leveraging Cryptography +
Cloud Computing

Here there is no need for a separate database or userbase management. With the identity created on the blockchain, we can access all the apps within the ecosystem.

Identity Management using Blockchain naming System (BNS)

We rely on naming systems in everyday life, and they play a critical role in many different applications. Be it a username, application name, or domain name; names play a key role. In the Stacks ecosystem, the naming/identity system is being managed by BNS.

Blockchain Naming System (BNS)[123] is a network system that binds Stacks usernames to an off-chain state without relying on any central points of control. BNS is implemented through a smart contract loaded during the genesis block.

Names in BNS have three properties:

1. *Names are globally unique.* The protocol does not allow name collisions, and all well-behaved nodes resolve a given name to the same state.
2. *Names are human-meaningful. Its* creator chooses each name.
3. *Names are strongly owned.* Only the name's owner can change the state it resolves to. Specifically, a name is owned by one or more ECDSA private keys.

[123] https://docs.blockstack.org/build-apps/references/bns

Now with the help of BNS, we can create identities such as test.id.stacks. Here, .stacks is called namespace(the top-level hierarchy of BNS system), followed by BNS names. In this case, it is .id. The last hierarchy is BNS subdomains, represented as a test here. The important point to be noted here is that BNS namespaces and names are part of the blockchain consensus rules, whereas BNS subdomains are not part of the blockchain consensus rules.

If subdomains are not part of consensus rules, how the off-chain name states are stored?

This is happening with the help of the Atlas network[124]. Atlas is a part of BNS.
BNS allows each name to store a small amount of state — in the order of 20 bytes. The size is so small because the state must be recorded to a public blockchain, where the cost per byte is high, and the blockchain protocol limits the size of transactions.

To compensate for this, Stacks developed an off-chain storage system that allows BNS names to bind and store a large number of states to each name in a way that preserves the security properties of having written that state to the blockchain. Atlas's reference implementation currently allows up to 40kb of state to be bound to a BNS name instead of a measly 20 bytes. The 40kb of data is replicated to each BNS node, where it is stored forever. With the help of BNS+Atlas, the identities are being managed efficiently in the Stacks blockchain.

Storage management using Gaia

Blockchains require consensus among large numbers of people so that they can be slow. Additionally, a blockchain is not designed to hold a lot of data. This means using a blockchain for every bit of data a user might write and store is expensive. For example, imagine if an application were storing every tweet in the chain.

The Stacks blockchain addresses performance problems using a layered approach.

1. The base layer consists of the Stacks blockchain and the Blockchain Naming System (BNS), where the identities are created.
2. *Atlas*: The identities correspond to routing data, and that is stored in Atlas Peer Network.
3. *Gaia Storage*: Stacks uses the routing data to associate identities (domain names, user names, and application names) with a particular storage location in the Gaia Storage System's final layer.

Gaia Storage system

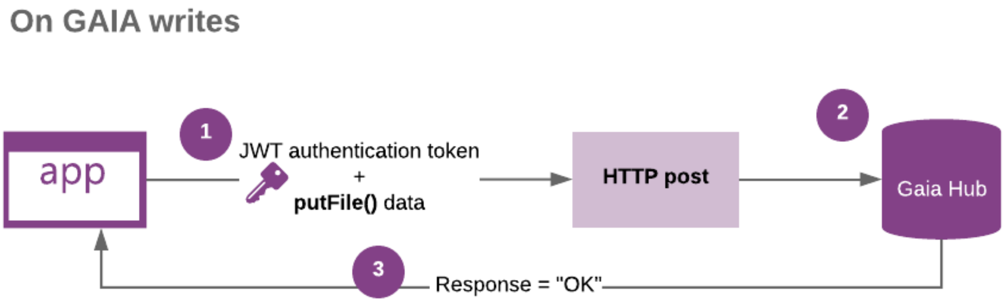
A Gaia Storage System consists of a *hub service* and storage resource on a cloud software provider. The storage provider can be any commercial provider such as Azure, DigitalOcean, Amazon EC2, etc. When an identity is created, a corresponding data store is associated with that identity on Gaia. When a user logs into a DApp, the authentication process gives the application the URL of a Gaia hub, which then writes to storage on behalf of that user.

Applications will read/write data to the Gaia hub on behalf of a user (if and only if the user allows). The user himself can own the user Gaia hub or use the default storage space provided by Stacks. In Stacks default, a hub is used to store user data encrypted by the user’s public key. In this way, storage providers only see data blobs, not the data.

[124] https://docs.blockstack.org/understand-stacks/atlas-overview#architecture

Understand Data Storage in Gaia

A Gaia hub stores the written data *exactly* as given. It offers minimal guarantees about the data. It does not ensure that data is validly formatted, contains valid signatures, or is encrypted. Rather, the design philosophy is that these concerns are client-side concerns. Client libraries (such as Stacks.js) are capable of providing these guarantees. A liberal definition of the end-to-end principle guides this design decision. When an application writes to a Gaia hub, an authentication token, key, and data are passed to the Gaia hub.



The token ensures the app has the authorization to write to the hub on the user's behalf. So, as an application developer, if a data crash happens at the application level, the developers have nothing to lose. From the user's perspective, we are the owners of our data.

Authentication

An app and authenticator, such as the Stacks Wallet[125], communicate during the authentication flow by passing back and forth two tokens. The requesting app sends the authenticator an authRequest token. Once a user approves authentication, the authenticator responds to the app with an authResponse token.

These tokens are JSON Web Tokens, and they are passed via URL query strings. The authenticator generates the app's private key from the user's *identity address private key* and the app's domain. The app private key serves three functions:

1. It is used to create credentials that give the app access to a storage bucket in the user's Gaia hub.
2. It is used in the end-to-end encryption of files stored for the app in the user's Gaia storage.
3. It serves as a cryptographic secret that apps can use to perform other cryptographic functions.

Finally, the authenticator will always generate the same private key for a given Stacks address and domain during the authentication. An important point to note here is that Users own the keys here, and the application developers have no clues to the password associated with a username. This way, it is more secure. With this kind of structure, for application developers, there is no infrastructure cost and maintenance. This makes building ethical apps on Stacks much easier.

Stacks ecosystem helps developers build an ethical web app, putting users in control of their identity and data. Data handling in the blockchain is a costly operation, and the more the data

[125] https://www.hiro.so/wallet/install-web

being stored, the more heavy the chain will be. Stacks addresses this issue with the help of 3 layers.

1. The identity management is being managed by BNS smart contract in Stacks blockchain.
2. The off-chain name state is being managed by a peer-to-peer network management Atlas.
3. The Data is being handled in the Gaia storage.

Stacks helps application developers build ethical apps without worrying about scalability, data loss, or infrastructure costs with this structure. At the same time, Stacks helps users to own their data and identity. Thus, Stacks is a perfect platform to build a user-owned Internet.

Stacks Ecosystem

Stacks Foundation

Stacks Foundation was set up with the aim of making it easier for experiments to happen. Their work seeks to support builders, entrepreneurs, researchers, & contributors to the user-owned internet economy. Stacks Foundation funds development, education, and community initiatives to build that vision together.

As of writing, Stacks foundation has awarded more than USD 600,000 in grants to more than 40 contributors across 15 different countries. Reach out to the foundation if you have something in mind to find out if you're eligible for their grants program[126]. Stacks foundation provides grants of up to USD100,000 non-equity grants for open source contributions with special consideration for Stacks accelerator companies.

Stacks foundation is also actively running various stacks related events[127] to help 1) aspiring contributors work through their grants application via Stacks grants office hours, 2) SIP reading club to go through the technical specificity of Stacks blockchain and 3) Stacker chats, The Crypto Internet Show are more casual, light-hearted way to interact and answer any questions the community may have.

The foundation is also home for the governance[128] of Stacks open-source technology, serving as a neutral ground for various independent parties to come together.

Stacks Accelerator

Stacks accelerator is a 3-month mentorship-driven program for teams building the internet of our future. In the first month of the accelerator program, teams go through a product development camp where you get mentoring on Lean Startup Training, Stacks Tech Support, Branding & Marketing Strategy and Product & UX Feedback.

Subsequently, in the next month, teams will be put through the Pitching & Fundraising Camp to craft an impactful pitch and pitch deck, learn about fundraising strategies and network with 50+ mentors.

[126] https://stacks.org/grants
[127] https://stacks.org/#events
[128] https://github.com/stacksgov/pm

Lastly, teams will be preparing for the demo day in the third month, with product launches along with the support of the stacks community, PR support and the chance to pitch in front of 100+ investors.

As of writing, the 1st cohort of 25 startups[129] have been selected to be part of the Stacks accelerator program, with extremely high quality of entrepreneurs aspiring to build the next generation product/service offerings to solve some of the hardest problems, ranging from DeFi solutions to NFTs & Art and other utility services such as hiring, messaging and healthcare management.

Upon gaining acceptance into Stacks accelerator, each startup receives up to USD50,000 in cash investment with no valuation cap and joins their 3-month acceleration program. Stacks accelerator works hand in hand with the Stacks foundation grants program to deliver flexible, fair, and efficient funding options.

Stacks Community

Apart from the companies, initiatives and projects built around Stacks blockchain which are all crucial parts of Stacks ecosystem, likewise Stacks community plays a crucial role in ensuring a vibrant ecosystem.

Stacks communities are made up of multiple key segments that together create a vibrant community across all fronts. Stacks forum[130] is the go-to place for long-form discussion and deep dive on key subject matters relating to Stacks. These can be research topics, technical specifications regarding Stacks, tokenomics/economic models, etc. Where discussions take on a slower pace but with more well thought out replies and in-depth context to the matter. Stacks Discord group[131] with over 6,000 members, Stacks Telegram group[132] with over 55,000 members and r/stacks at 2,900 members are other ways in which one can be involved with the Stacks community, with thoughtful moderators and welcoming community members makes the experience an enjoyable one.

There are also key Stacks community Twitter accounts constantly generating great content within Crypto Twitter that keeps the community engaged.

- @DocumentingStx provides interesting Stacks related information and facts that keep the community up to date.
- @StacksTrade constantly provides insightful charts and commentary on price actions which makes it a constant joy to consume its content.
- @StxMeme posting top quality memes all the time, engaging the community in a light-hearted manner.
- @StacksDeveloper has been always sharing information and resources with community developers.
- @stxstats[133] dishing out key metrics (unique addresses, no. of transactions and transaction fees) of Stacks blockchain on a regular basis.

[129] https://newsletter.stacks.org/issues/building-on-bitcoin-meet-the-first-stacks-accelerator-cohort-650254
[130] https://forum.stacks.org
[131] https://discord.gg/XYdRyhf
[132] https://t.me/BlockstackChat
[133] https://www.stxstats.co

Apart from the social media front, Stacks Chapters[134] play a huge role in nurturing the Stacks community. The Stacks Chapter program is designed to empower local leads to build their community through activities and content with measurable impact[135]. The program is geographically focused around a city or region and is very flexible from chapter to chapter, relying upon local leaders to set relevant goals. As of writing, more than USD110,000 funding has been awarded to Stacks local chapter contributors across 13 countries. Some key Stacks Chapters are Stacks Turkey[136], Stacks China, Stacks Korea and Stacks Mena, each with local leads leading community development efforts with localized content and activities.

Stacks community have come together to champion for causes, such as lowering STX withdrawal fees on exchanges[137], advocating for crypto-twitter influencers to write about STX[138] and generally making the Stacks community a great place to hang out. Sites like stx.fan[139] made it easy for community members to keep track of the latest developments of the Stacks ecosystem and also a one-stop shop for key information regarding Stacks. Recently Lunar Crush a data analytics company focused on the social media impact cryptocurrency market named Stacks as one of the top coins for June'21[140] due to its strong social engagements on various social media outlets.

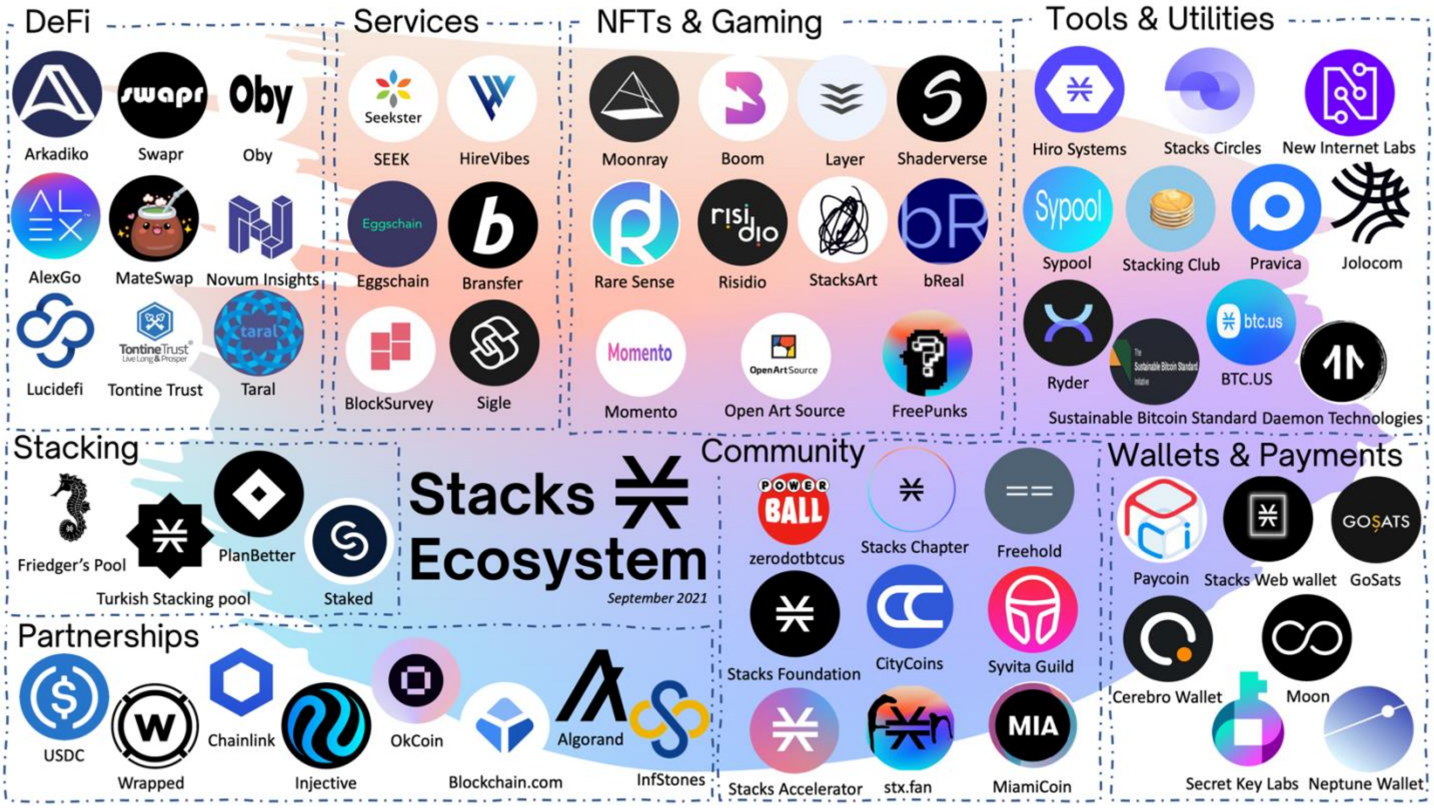
Decentralized Applications

Stacks dApps Overview

Applications built on top of Stacks blockchain have been growing since the launch of Stacks 1.0 Blockchain in 2018. Through its app mining initiative[141], the number of decentralized applications building on Stacks blockchain grew from 27 applications to more than 350 applications[142]. With the launch of Stacks 2.0 mainnet in Jan'21[143] where both clarity smart contract and Proof-of-Transfer consensus went live on the Stacks blockchain, Stacks Foundation[144] and Stacks Accelerator[145] was set up to provide further support to aspiring entrepreneurs and developers who would like to build on Stack Blockchain.

[134] https://stacks.org/chapters
[135] https://stacks.org/stacks-chapters-collective-impact
[136] https://stacksturkey.com
[137] https://twitter.com/stackstrade/status/1367586217647247361?s=21
[138] https://twitter.com/danheld/status/1415805825889841155?s=20
[139] https://stx.fan
[140] https://twitter.com/lunarcrush/status/1421098392323772422?s=21
[141] https://blog.blockstack.org/introducing-app-mining/
[142] https://www.app.co
[143] https://stacks2.com/register
[144] https://stacks.org
[145] https://stacks.ac

The following is a snapshot of companies/initiatives built around Stacks blockchain, showcasing the Stacks ecosystem map.



Updated as of September 2021

DeFi on Bitcoin

Decentralized Finance, more commonly known as DeFi at its core refers to the ecosystem comprised of financial applications that are being developed on top of blockchain systems. DeFi in a community context is usually seen as more of an ethos that promotes the use of decentralized networks and open-source software to create multiple types of financial services and products. It is to enable the development of financial applications on top of a transparent and trustless framework, such as permissionless blockchains and other peer-to-peer (P2P) protocols. Therefore with the rise and maturing of blockchain technology, it became a natural fit where innovators, builders and market participants look to blockchain technology as the fundamental infrastructure to build out the future of finance.

Currently, the three largest functions of DeFi are:

1. Creating monetary banking services (e.g., issuance of stablecoins)
2. Providing peer-to-peer or pooled lending and borrowing platforms
3. Enabling advanced financial activities such as trading via DEXes, tokenization platforms, derivatives, insurance and predictions markets

How DeFi differ from Traditional Finance?

In traditional finance, institutions such as banks act as intermediaries, and courts provide arbitration. DeFi applications do not need any intermediaries or arbitrators. The code specifies the resolution of every possible dispute, and the users maintain control over their funds at all times. This reduces the costs associated with providing and using these products and allows for a more open and frictionless financial system.

What is the underlying technology that powers DeFi on Blockchain?

Smart contracts are pre-specified agreements on the blockchain that evaluate information and automatically execute when certain conditions are met. As they exist on the blockchain, they are deemed immutable (can't be changed) and verifiable (everyone can see them), guaranteeing a high level of trust among parties that they accurately reflect the stated parameters of the agreement and will execute if, and only if, those parameters are met.

Rise of DeFi

Ethereum with its first-mover advantage(went live in 2014), provided developers with the tools(smart contracts, programming language) to execute the kind of complex functionality required by modern finance applications. As of writing, more than USD80bn[146] locked in Ethereum powered smart contracts and millions in dollar value transactions taking place across various DeFi protocols clearly shows that DeFi has found product-market fit, and Ethereum despite its shortcomings served as the platform for developers to build out new DeFi products. However, would DeFi be solely built on Ethereum blockchain? – It is unlikely, as we begin to see blue-chip DeFi products going multichain[147] due to 1) high gas fees on the Ethereum blockchain, 2) limited/complex scalability options on Ethereum and 3) Vulnerability in Solidity programming language.

DeFi on Bitcoin

Bitcoin Network as discussed in previous chapters was created to be a secure and decentralized way for users to store value, thus possessing limited scripting language capabilities. This limits the type of applications that developers can build on top of the Bitcoin network, however, the launch of Stacks Blockchain, brings smart contracts capabilities to the Bitcoin network through Stacks 2.0, Proof of Transfer mechanism and Clarity smart contracts. With billions of value locked in smart contracts, one would expect the underlying technology powering and securing these smart contracts to be secure, immutable and battle-tested. The idea of using Bitcoin to secure DeFi applications became a natural fit, given that Bitcoin has stood the test of time[148], with no security compromises[149] on the Bitcoin network itself. Additionally through the Proof-of-Transfer consensus mechanism which uniquely enables Stacks Blockchain to operate alongside the Bitcoin Network, leveraging its security and allowing developers to innovate on Bitcoin through Clarity smart contracts eliminates a whole class of smart contract bugs and provides for greater predictability.

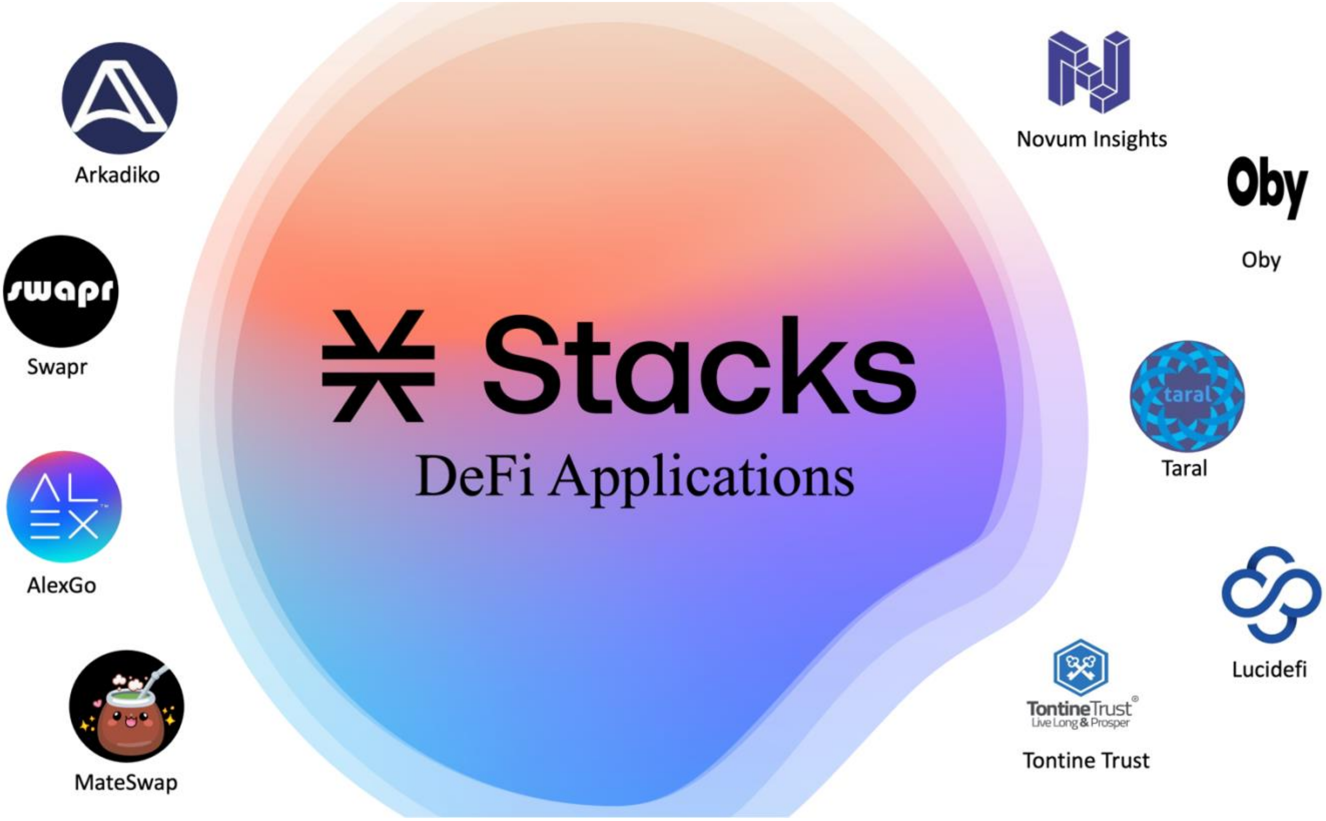
Native Bitcoin swaps

DeFi ecosystem has grown tremendously over the years and there has been demand for DeFi-like products for Bitcoin, however, due to Bitcoin's limited scripting language complex functions cannot be executed on the Bitcoin Network. Developers have come up with several workarounds using derivatives backed by Bitcoin often relying on centralized counterparties or other blockchains. However, those aren't perfect workarounds as using a centralized custodian just defeats the purpose of building decentralized finance around the product and the security of other blockchains do not have the same level of security as the Bitcoin Network.

[146] https://defipulse.com
[147] https://dappradar.com/blog/moving-away-from-ethereum-as-defi-goes-multi-chain-defi
[148] https://bitcointalk.org/index.php?topic=4971039.0
[149] https://help.coinbase.com/en/coinbase/privacy-and-security/other/is-bitcoin-secure-has-the-bitcoin-network-ever-been-hacked

There has been a breakthrough[150] when Stacks community members Friedger Muffke[151], Asteria[152], and Jude Nelson[153] in collaboration with other Stacks community developers, deployed working Bitcoin swaps with NFTs and other crypto-assets. A native bitcoin swap refers to the ability to send an on-chain Bitcoin transaction and execute logic in a smart contract, thus removing the need for a central intermediary. This unlocks new possibilities for developers to create DeFi applications around the native Bitcoin asset, and with bitcoin's market cap close to USD 1 trillion at the time of writing, developers, DeFi products and the wider ecosystem can now tap into this pool of capital with new possibilities. While DeFi on Bitcoin is still at its nascent stage due to Bitcoin's limited scripting language which prevented the execution of complex logic, there are already an increasing number of applications and projects leveraging on Stacks unique technology to build DeFi products and services secured by the Bitcoin Network.

The map below shows some of the current DeFi offerings powered by Stacks blockchain and secured by the Bitcoin Network.



Updated as of September 2021

Alex[154] – An open-source DeFi protocol built on the Stacks blockchain, enabling collateralized lending and borrowing without a third party, and for the first time able to access the liquidity, power and safety of the Bitcoin Network. Which could potentially unlock up and tap into close to USD 1 trillion of locked value.

[150] https://www.hiro.so/blog/bitcoin-defi-is-here-a-deep-dive-into-trust-less-swaps
[151] https://friedger.de/
[152] https://github.com/SyAsteria
[153] http://www.judecnelson.com/
[154] https://alexgo.io

Novum Insights[155] – DeFi data analytics and yield farming allowing end-users to gather more information about DeFi to make informed decisions when participating in the DeFi ecosystem. Aggregating yielding farming information and interest rates help users to find the best liquidity pool and DeFi token pairs.

Swapr[156] – Swapr finance, the first Stacks token exchange to enable trustless token exchange on top of Stacks 2.0.

The above are just some examples of DeFi offerings built on Stacks blockchain, along with stablecoins, derivatives, trade finance and more. We're still in the early phases of DeFi on Bitcoin as the industry comes around to understanding the benefits of building using clarity programming language and Bitcoin as the secured settlement layer, DeFi products that we're accustomed to today will take on new forms and play a more integrated role in the wider Web 3.0 ecosystem.

NFTs on Bitcoin

Non-fungible token(NFT) has been the talk of the town since the turn of the new year, especially with the sale of Beeple's US$69 million[157] NFT art at Christie's. NFTs was largely popularized by Rare Pepes[158], Crypto Punks[159] & Cryptokitties[160] on the Ethereum blockchain in 2017 but do you know that the history of NFTs can be traced back to 2012 on the Bitcoin blockchain(Colored Bitcoin[161]). Where Yoni Assia discussed coloured coins as unique and identifiable and was part of the "Genesis bitcoin transaction".

So what exactly is a Non-fungible token?

Fungibility is most commonly defined as "an item is replaceable by another identical item". E.g. Fiat currencies, a 20 dollar bill has the same value as another 20 dollar bill where users do not differentiate them and counterparties do not possess any discrimination against one over another 20 dollar bill. Non-fungible is the exact opposite of this, where each item is unique on its own, and people place different values on each item. In the physical world, items that are non-fungible range from artwork, music, to personal items where they are largely non-fungible. A non-fungible token represents ownership of a digital asset that is unique on its own on the public blockchain. A more in-depth discussion about what NFTs are can be found in the NFT bible[162].

Do NFTs have value?

Lots of chatter has been going on about the value of NFTs, especially with the sale of Beeple's artwork of US$ 69million, where sceptics argue that artwork on the internet can simply be copied, thus no real value lies in the NFTs itself. NFTs touches on a profound topic of how one can establish authentic ownership over a digital asset that is scarce. Satoshi Nakamoto first introduced digital scarcity to the world through proof-of-work mechanism powering the Bitcoin blockchain, NFTs takes it a step further where seemingly small and miscellaneous items in the digital world can be uniquely labelled, and verified for authenticity and ownership.

[155] https://novuminsights.com
[156] https://swapr.finance
[157] https://www.wsj.com/articles/beeple-nft-fetches-record-breaking-69-million-in-christies-sale-11615477732
[158] https://rare-pepe.com/
[159] https://www.larvalabs.com/cryptopunks
[160] https://www.cryptokitties.co/
[161] https://yoniassia.com/coloredbitcoin/
[162] https://opensea.io/blog/guides/non-fungible-tokens/#What_is_a_non-fungible_token

Much like how the real world values collectables, limited edition items, art, or other seemingly trivial items but possesses a huge amount of value when authenticity and scarcity can be established. James Wang[163] did a great piece explaining how NFTs are certificates of authenticity which is where the value resides in an artwork.

NFTs on Bitcoin

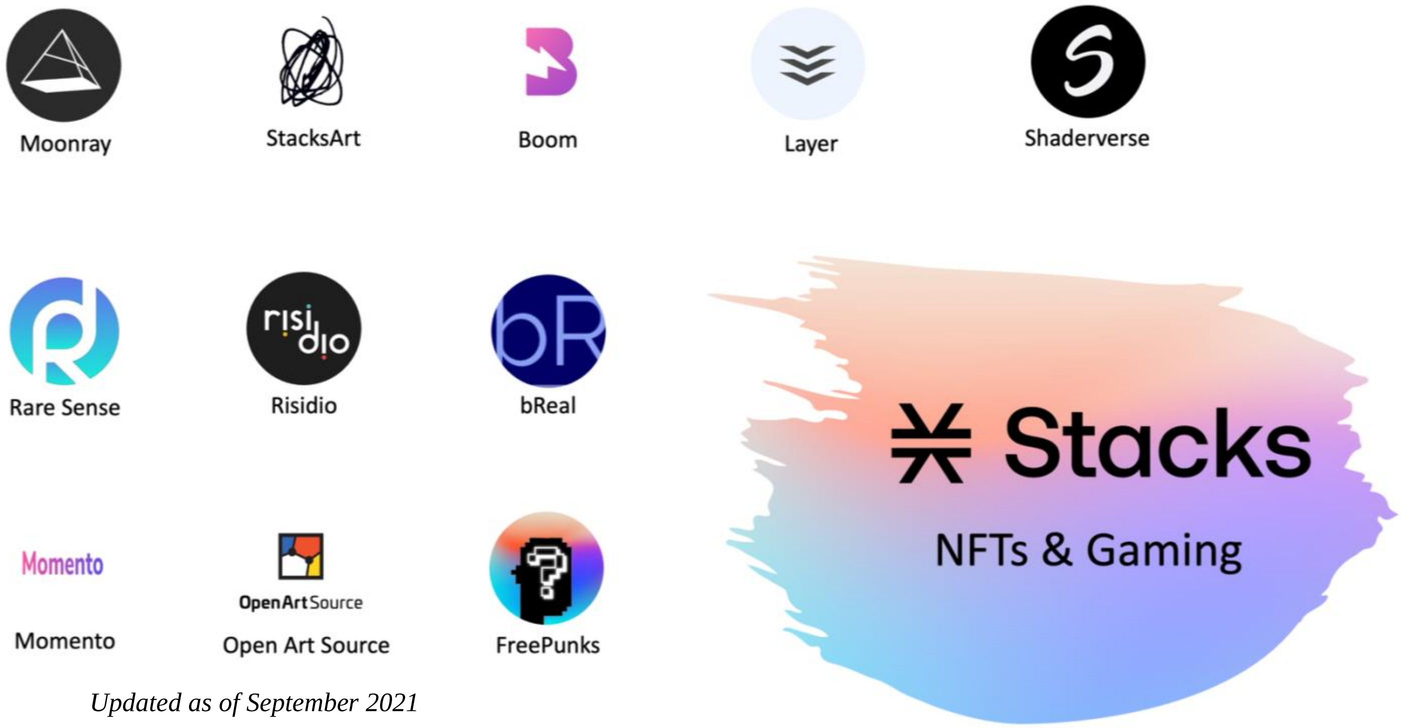
As we've established the value of NFTs, it would then be best practice to build NFTs on the most secure network in the industry that will withstand the test of time. The Bitcoin network by far is the most secure network in the industry with its ever-increasing hash rate, however by design Bitcoin's scripting language was never meant for such functionalities within its network, as security was the utmost priority when designing Bitcoin. The launch of Stacks 2.0 changes everything, bringing programmability and scalability to the Bitcoin network enabling decentralized apps and smart contracts to inherit Bitcoin's security and capital pool. In addition, with clarity smart contract language, which is an interpreted and decidable programming language that is non-Turing complete, brings about clearer execution outcomes and fundamentally a more secure set of codes, thus making NFTs on Bitcoin a much more compelling prospect. Currently, on Stacks blockchain smart contract, Clarity has built-in language primitives to define and use non-fungible tokens. "define-non-fungible-token"[164] function on clarity is used to define a new non-fungible token class for use in the clarity smart contract. Lastly, SIP-009[165] aims to provide a flexible and easy-to-implement standard that can be used by developers on the Stacks blockchain when creating their own NFTs.

Similar to DeFi, we're still at the nascent stages of blockchain technology, where infrastructure to better utilize blockchain technology are still being built out, likewise new use cases for NFTs have yet to be discovered. What we're observing now are first-generation use cases that the market is porting over from the physical world, such as art, collectables, limited editions proprietary ownership to the digital world. E.g. Marketplace for arts(Christie's, Sotheby) < > NFTs marketplace (Opensea, Rarible), Real-world Collectibles (Pokemon cards, Magic the gathering) < > Digital Collectibles (Cryptokitties, CryptoPunk), NBA trading cards < > NBA Topshot. As more talent flows into the blockchain industry, innovative use cases and technologies will be created, where crypto-native use cases and business models will start to emerge and new NFTs use cases will be introduced.

Building NFTs on Bitcoin allow creators, collectors and businesses to take advantage of the growth of the industry as 1) Bitcoin is the most secure network, 2) Most established network effects in the industry ranging from individuals to institutions and governments, 3) largest pool of capital in the network, which is all key ingredients for taking a piece of technology mainstream. We're seeing some of these innovation taking place, where Boom introduced a new type of NFT built on Stacks[166]. Boomboxes enable STX token holders to delegate stacking of their STX and receive an NFT which acts as an automatic claim certificate on their portion of stacking rewards. These Boomboxes can then be traded freely on open marketplaces and the owner of the NFT during the reward distribution phase will receive the rewards, thereby blurring the lines between DeFi and NFTs. This unique combination was achieved through clarity programming language, along with PoX consensus mechanism and SIP-009 NFT standards, which together opens up new possibilities for builders to create innovative products.

[163] https://draecomino.substack.com/p/nfts-are-signatures-that-come-with
[164] https://docs.blockstack.org/references/language-functions#define-non-fungible-token
[165] https://github.com/stacksgov/sips/blob/friedger-main/sips/sip-009/sip-009-nft-standard.md
[166] https://boom-wallet.medium.com/how-to-get-your-first-boombox-d97a9404e759

The map below shows some of the current NFTs products and services built on Stacks blockchain and secured by the Bitcoin Network.



Updated as of September 2021

Risidio[167] – A creators lab with the core purpose of empowering artists with Web 3.0 technology using the power of NFTs and crypto. They are the folks behind This is #1. a decentralised digital marketplace of curated celebrity NFTs built on the Stacks Blockchain, that facilitates the collaboration of artists with DeadMau5, Cara Delavingne, Chemical X, and others

Momento[168] – TikTok for NFTs, powered by the Bitcoin Network via Stacks, where more intimate and valuable content will be created once centralized hierarchy of ownership is removed. Uniquely designed to enable streamline content management, royalties management via smart contracts, transforming content into an asset class for creators.

Moonray[169] – Moonray is a far-future, surreal sci-fi Action-RPG built on the Stacks blockchain.

In addition to these offerings of one-click NFTs minting, art pieces with artists collaboration, NFTs marketplace, music, certificates authentication, the unexplored new possibilities that blockchain technology creates when these industry-leading technologies are placed into the hands of creative individuals are sure to excite. Some potential use cases of NFTs on Bitcoin could see art no longer be a one-off purchase, instead recurring revenue models could take shape (e.g. purchase of a movie ticket vs Netflix subscription) paid for with sats via Bitcoin Native Swap, timelock ownership measured by blocks instead of time, micro royalty payments through the ownership of collectables (sats streaming to your wallet in real-time). NFTs will venture into the B2B space, where design IPs can be protected and enforced via NFTs, thereby eliminating piracy and copyright issues.

[167] https://risidio.com
[168] https://www.momentonft.com/
[169] https://moonraygame.com

DAOs on Bitcoin

"It makes the most sense to see Bitcoin [...] as a decentralized autonomous organization". – Vitalik Buterin (Ethereum co-founder)

Bitcoin represents the first real-world implementation of a "decentralized autonomous organization" (DAO) and offers a new paradigm for organization design[170]. In contrast with traditional organizations, DAOs do not have a structural setup that resembles a company, with well-defined decision-makers such as senior management, middle managers, etc. Instead, governance rules are written into smart contracts, which makes up the backbone of a DAO. The contract defines the rules of the organisation and DAOs are commonly used to govern a project's treasury but not limited to treasury governance only. Once the contract is live on the blockchain, no one can change the rules except through a vote. If anyone tries to do something that's not covered by the rules and logic in the code, it will fail. A crypto treasury defined by smart contracts would also be safeguarded as no one can spend the money without the group's approval. Therefore DAOs do not need a central authority to function. Instead, the group makes decisions collectively and payments are authorised automatically when votes pass.

In essence, a DAO is a commitment to share value with a community[171], where it enables 1) members within the community to have a voice through governance, 2) flatten hierarchy and create fluid workstreams and 3) allocate resources to achieve a core mission. Today, more than 100s DAOs are managing over $10B in assets, largely built on the Ethereum network, taking on different forms. Such as Protocol DAOs, Grants DAOs, Investment DAOs, Service DAOs, Media DAOs, Collector DAOs and DAO operating systems.

As we transit to a digital economy, DAOs can be seen as an internet-native organization that's collectively owned and managed by its members, with rules built into smart contracts which forms the basis of governance and decisions are made via proposals and voting to ensure everyone in the organisation has a voice. DAOs addresses the coordination problem of starting an organization in a digital native and decentralized environment that involves handling money in one way or another which requires trust in the people you're working with[172]. This opens up new ways for global collaboration across different settings.

DAO	A traditional organisation
Flat hierarchy and democratized.	Usually hierarchical, with complex structure and power distribution.
Voting is required by members for any changes to be implemented.	Depending on the structure, changes can be demanded from a sole party, or voting may be offered.
Votes tallied, and outcomes implemented automatically without a trusted intermediary and in a transparent manner.	If voting is allowed, votes are tallied internally, with manual handling of the outcome.
Services offered are processed automatically in a decentralized manner (for example distribution of grants, philanthropic initiatives).	Requires human intervention, or centrally controlled automation, prone to manipulation.
All activities are transparent and fully public.	Activities are typically private and limited to the public.

[170] https://core.ac.uk/download/pdf/215383528.pdf
[171] https://coopahtroopa.mirror.xyz/_EDyn4cs9tDoOxNGZLfKL7JjLo5rGkkEfRa_a-6VEWw
[172] https://ethereum.org/en/dao/#how-daos-work

Similar to DeFi & NFTs on Bitcoin, DAOs built on Bitcoin is not widely implemented due to limited scripting capabilities on the Bitcoin Network, however as alternative solutions begin to come online and be available open-source to the community, more applications and tools for DAOs management that relies on Bitcoin infrastructure for settlement and security will increase over time. This is evident particularly within the Stacks community as we witnessed multiple projects leveraging on Clarity programming language and Stacks blockchain infrastructure to build out DAOs as their main governance mechanism for their projects. Additionally tools to help better create and manage DAOs are also being built by the community to enable better coordination on more complex decision making.

Arkadiko[173] – A decentralized, non-custodial liquidity protocol and stablecoin issuer building on Stacks blockchain and settles on the Bitcoin Network, integrates DAOs setup to enable governance voting. It is the main coordination mechanism that Arkadiko uses within the ecosystem.

MateSwap[174] – Decentralized exchanges building on Stacks blockchain and secured by the Bitcoin Network leveraging on DAOs to grow their ecosystem, enabling the community to have a share of the fees captured by the exchange, loyalty programs and participate in the governance of the platform.

daoOS[175] – Tools are currently being built to enable a more streamline deployment of DAOs on the Stacks blockchain. Recognizing the need for communities to organize themselves across different causes, lowering the barrier to set up DAOs bring immense value to the community as it empowers the community to organize and self-govern thereby allowing more grassroots initiatives to take place.

The future of DAOs

DAOs take on a vastly different form as compared to traditional organization structures, however, it still serves the same underlying purpose which is to enhance coordination among a group of individuals to pursue a common set of objectives. Therefore one may wonder would similar corporate actions such as mergers and acquisitions of DAOs, companies going public via DAOs, etc be applicable? We are seeing early signs of such corporate actions happening in the DAO space with ShapeShift, one of the earliest cryptocurrency exchange dissolving their corporate structure and decentralizing it by issuing tokens (FOX token) as a representation of ownership[176]. Fox Governance – token holders will be the ones guarding and running the exchange, essentially a DAO governed by its users. In essence, it can be seen as a private company taking itself public via DAOs and distributing governance tokens to the public. However, several nuances need to be addressed above, as this cannot be seen as a like for like comparison of a private company going public via traditional ways (IPOs, Direct listing, SPACs etc). Instead with ShapeShift, they took on the path of an open-source governance model via FOX token, instead of shareholders and equity. While the corporate entity goes away, the product, the software that people use becomes open source and becomes a community-governed project.

Separately, we’re also witnessing DAO-to-DAO acquisitions happening in recent times where synergistic mergers were taking place to further solidify their position in the market and

[173] https://www.arkadiko.finance
[174] https://www.mateswap.io/indexUS.html
[175] https://github.com/syvita/daoos
[176] https://shapeshift.com/shapeshift-decentralize-airdrop

unlocking further value for all stakeholders involved. One such event happening was the acquisition of Stake.gg a global, permissionless, and open-source prediction market platform built for gamers, to integrate with Pulse Ecosystem, a community-owned prediction market platform[177].

This sets a significant precedent for future blockchain mergers and acquisitions and other traditional business practices, where synergistic corporate actions can take place while staying true to the ethos of crypto. Which is about being truly borderless, being truly immutable, being decentralized and being open for everyone in the world, and that just cannot be done as a centralized company. Similarly, it'll be interesting to observe and learn from these pioneering cases as they play out on how various operational challenges can be resolved. For example, 1) integrating two different communities when a DAO-to-DAO acquisition takes place, 2) remain aligned on for-profits objectives such as revenue, growth and profit margins when a private company decentralizes ownership through governance token, 3) navigate any potential legal ramifications through such actions. It's a new type of economic organization, which could potentially be utilized by global digital companies that want a more open model and in which their users can become part of the economic engine. As DAO tools like daoOS get built, which enables communities to better self-manage or even enabling corporate actions to take place using these tools, we'll be seeing more DAOs directed events taking place as we transit to a digital economy.

Closing Remarks

Thank you and great work for making it this far! We've come to the end of the book and hope that you've gained some valuable insights into the topics covered in the book. From the basics about the Bitcoin Network to Stacks blockchain and the wider crypto ecosystem. We hope your crypto journey does not end here, instead use this book as the catalyst to kickstart your crypto journey with us and dive deeper into your areas of interest.

As the saying goes, crypto never sleeps, trading goes on 24/7/365 while teams are heads down building relentlessly as the crypto community matures and develops with the necessary infrastructure and applications for Web 3.0 gets built-out. If you're looking to get involved in crypto, excited to work on solving challenging problems with great impact, or build the next decentralized application for Web 3.0 that could potentially disrupt an industry, there are multiple ways to do so, Stacks discord channel[178] is a great way to start, crypto-twitter, or crypto-native jobs portal like Hirevibes[179], Pomp Crypto Jobs[180] and more. The developments in crypto take place at breakneck speed, with a wide range of opportunities to get involved from solving infinitely complex smart contracts problems to community moderation, there's always something for all levels of crypto proficiencies.

Lastly, as you may know, that the crypto industry is constantly evolving, with new ideas, developments and moonshot projects taking place every other day. We make every effort to ensure that the content in this book has the most up-to-date information, however, due to the nature of the industry, some of the content written in this book may be outdated when this book is published. Nonetheless, we hope you'll be able to get some free alphas from reading this book, and also use it as a reference point for your future crypto work!

[177] https://medium.com/@pulsemarkets/pulse-acquires-stake-gg-in-the-first-dao-to-dao-acquisition-78c720da2ca1
[178] https://discord.com/invite/XYdRyhf
[179] https://www.hirevibes.io
[180] https://pompcryptojobs.com

Brought to you by:

Stacks Community

Made by the community for the community ❤

Core contributors: Ethan Tan, Harini Rajan and STX Freehold Community