Blockstack Token Whitepaper

Ryan Shea
Muneeb Ali

A Token Mechanism for Growing the Blockstack Ecosystem of Decentralized Applications

https://blockstack.com
Token Whitepaper Version 1.0
October 12, 2017

BLOCKSTACK

This paper assumes familiarity with the current design of Blockstack. We highly encourage the readers to first read the Blockstack technical whitepaper:

- M. Ali, R. Shea, J. Nelson, and M. J. Freedman,
  "Blockstack: A New Internet for Decentralized Applications",
  Technical Whitepaper Version 1.1, October 2017.
  https://blockstack.org/whitepaper.pdf

DISCLAIMER: The attached whitepaper is meant to describe the currently anticipated plans of Blockstack Token LLC (the "Token LLC") and its affiliates (together, "Blockstack") for developing a new blockchain token mechanism ("Token") that will be used on the network sponsored by Blockstack ("Network"). Nothing in this document should be treated or read as a guarantee or promise of how Blockstack's business, the Network, or the Tokens will develop or of the utility or value of the Network or the Tokens. This White Paper outlines Blackstock's current plans, which could change at its discretion, and the success of which will depend on many factors outside Blackstock's control, including market-based factors and factors within the data and cryptocurrency industries, among others. Any statements about future events are based solely on Blackstock's analysis of the issues described in this document. That analysis may prove to be incorrect.

This document does not constitute an offer or sale of the Tokens or any other mechanism for purchasing the Tokens (such as, without limitation, a fund holding the Tokens or a simple agreement for future tokens related to the Tokens). Any offer or sale of the Tokens or any related instrument will occur only based on definitive offering documents for the Tokens or the applicable instrument.

Purchasing the Tokens or any related instrument is subject to many potential risks. Some of these risks will be described in the offering documents. These documents, along with additional information about Blockstack and the Network, are available on our website at www.blockstack.com. Purchasers of Tokens and related instruments could lose all or some of the value of the funds used for their purchases.

A Token Mechanism for Growing the Blockstack Ecosystem of Decentralized Applications

Ryan Shea Muneeb Ali

http://blockstack.com
Token Whitepaper Ver 1.0

October 26, 2017

Abstract

The traditional internet was designed over 40 years ago and has certain design flaws. End-users need to trust hidden middlemen like domain name servers and certificate authorities and trust remote data stores with their personal data. Blockstack is a new internet for decentralized applications that removes the need for trusted intermediaries and enables users to own their application data directly. For the long-term success of the Blockstack network, there is a need for (a) governance structures that ensure that no single party can control the protocol and (b) incentive mechanisms for developers and users to participate in a new two-sided market for decentralized applications. In this paper, we present Stack—a blockchain token protocol that improves upon the earlier design of the Blockstack blockchain. Stack introduces decentralized governance and incentive mechanisms for ecosystem growth, and enables new features like support for mobile/light clients and atomic swaps. Stack is a major upgrade to the Blockstack network and, like earlier major upgrades, will be proposed as a network hard fork.

1 Introduction

The internet was originally meant to be a decentralized network without any central points of failure or control. However, certain design limitations of the traditional internet resulted in a dependency on centralized internet infrastructure, like root servers of the Domain Name System (DNS) or Certificate Authorities (CAs) used for digital certificates. Further, the economic incentives of today's internet resulted in an oligopoly, where a few large companies (Google, Facebook, Amazon, etc.) have ended up hosting most end-user data in centralized data silos. These centralized data stores are enticing targets for attackers and have frequent data breaches, as was the case with the recent hacks of Yahoo! [1] and Equifax [2]. Blockstack is an open-source effort to re-decentralize

the internet; it builds a new internet for decentralized applications and enables users to own their application data directly [3]. Blockstack uses the existing internet transport layer (TCP or UDP) and underlying communication protocols and focuses on removing points of centralization that exist at the application layer. Alternate transport layer protocols, like new mesh networking protocols [4], can be supported with Blockstack.

The Blockstack network removes central points of failure and trust from the internet, like domain servers and certificate authorities, and enables high-performance personal storage for end-users. The network has been running in production for over three years, and more than 74,000 domain names have been registered on it. Blockstack uses blockchains, replicated data logs synchronized over peer networks [5], for propagating secure data bindings and discovery information. We encourage the readers to read the Blockstack whitepaper [6] for details on how the Blockstack network is designed to be fully decentralized, uses blockchains as a simple base layer, and can give comparable performance to centralized cloud systems.

Developers have already started building decentralized applications, like decentralized home-sharing [7] and decentralized micro-blogging [8], on Blockstack. For the long-term success and sustainable growth of the network, there is a need for:

- **Governance Structures** that ensure that no single entity can control the network/protocol and stakeholders of the network can vote on protocol upgrades.
- **Incentive Mechanisms** for a "two-sided market" for decentralized applications that overcome the problem where neither developers nor users have an incentive to participate, at scale, unless the other participates first.

In this paper, we address the challenges of decentralized governance and incentive mechanisms for ecosystem growth. We present *Stack*, a blockchain token protocol that improves upon the earlier Blockstack blockchain design. Stack adds a new mining system to the protocol that enables (a) independent verification of the longest Blockstack blockchain, a feature important for mobile clients and "light" nodes, (b) incentive mechanisms for developers, and (c) incentive mechanisms for users. Blockchain protocol tokens serve two purposes today: they protect scarce network resources without introducing centralized gatekeepers, and they incentivize desirable behavior in network participants. Bitcoin [9], the first and currently the largest blockchain network, has digital currency as the scarce network resource. Ethereum [10] has computing power and digital currency as the scarce network resources. Filecoin [11] incentivizes people to host files for other users and provides storage resources to the network.

On Blockstack, the scarce network resource is digital property like domain names and registered applications; users spend tokens to register digital property. Blockstack's new mining system, presented in this paper as the Stack protocol, incentivizes growth of the ecosystem of decentralized applications. Tokens on Blockstack, called *stacks*, protect the scarce network resource (digital property) and incentivize desirable behaviors (growth of the ecosystem of applications and keeping the network secure).

The new mining system introduced by Stack has three parts. With *proof-of-burn*

mining, miners destroy a proof-of-work-based cryptocurrency (currently Bitcoin) to get tokens; this enables the functionality where nodes can select between conflicting blockchain forks, as the blockchain fork with the most amount of cryptocurrency burned is considered to be the "correct" fork. *App-rewards mining* provides incentive mechanisms for application developers in the early stage (first four years) of the ecosystem and helps with bootstrapping the two-sided market. A set of independent entities, called *App Reviewers*, are elected for a 1-year term and curate eligible applications and assign them appropriate weights which are used in calculating mining rewards for apps. *Web-of-trust mining* provides incentive mechanisms for users where an initial trusted-set of unique users is curated in the genesis block and, in the future, the initial set of users can expand the web-of-trust after the network goes live. Avoiding Sybil attacks [12] is the key challenge for algorithmically expanding the initial trusted-set and is an area of ongoing research; we plan to fall back to a process involving gatekeepers, similar to curating the initial trusted-set, if the algorithmic approach does not lead to a reliable mechanism. Our goal is to have a wide distribution of tokens to real users and not bots.

Stack is a major upgrade to the Blockstack network and, like earlier major upgrades, e.g., the introduction of *virtualchains* [13], will be proposed as a network hard fork. Incentive mechanisms of Stack optimize for maximizing participation in the network and limit any single party, including the protocol developers, from having too much control. Further, the token distribution mechanism of Stack optimizes for getting a wide distribution without having any single party or category of participants, like developers or investors, having disproportionately large economic power on the network.

2 Design Goals

In this section, we present the design goals of the Stack protocol. These goals are informed by 3+ years of operational experience of the Blockstack network and numerous discussions with 7,500+ Blockstack community members and developers [3, 14, 15].

1. **Incentive Mechanisms for Ecosystem Growth:** In an app ecosystem, a developer's incentive to build an application is proportional to the number of daily active users in the application ecosystem, as well as the total size of the app economy (money exchanging hands across applications). However, a large active userbase and app economy cannot exist unless there are many useful applications. This is a classic two-sided market problem. Stack needs an explicit incentive mechanism that can address the two-sided market problem and ensure a sustainable growth of the decentralized app ecosystem in the long run. Moreover, it must do so without introducing centralized gatekeepers.
2. **Decentralized Governance:** Blockstack is an open-source project and a decentralized network. For the past four years, one company, Blockstack Public Benefit Corp (PBC), has taken the lead on protocol development. As the ecosystem grows, it becomes increasingly important that no single party has control over the net-

work and protocol development. Economic stakeholders in the network should be able to vote on protocol changes with a transparent and auditable mechanism.

3. **Preserve Economic Distribution through Migrations:** The fault-tolerant design of Blockstack's blockchain, and its use of virtualization, enables the network to survive failures of underlying blockchains (see [6] for details). However, the current implementation uses tokens of the underlying blockchain (layer-1 tokens) instead of tokens native to the Blockstack blockchain. The layer-1 tokens become irrelevant for the Blockstack network after a migration, as happened in our migration away from the Namecoin blockchain [16]. The Stack protocol needs a mechanism to preserve economic stakeholders through migrations, otherwise, a migration can completely disrupt/reset the economic distribution and incentives.
4. **Enable Support for Light Clients:** Blockstack users run full nodes to verify transactions and data mappings independently. However, running a full node is too resource intensive for mobile devices or may not be allowed by mobile platform vendors. Some users might not want to run a full node on end-user computers as it takes up significant disk space (∼1GB currently) and adds computing and network bandwidth overhead. Blockchains like Bitcoin support "light" clients that can independently validate the existence of transactions by downloading only block headers and not the entire blockchain [17]. The majority of end-user computing devices are mobile devices, and they account for the majority of internet usage [18]. A key challenge in supporting light clients, like mobile devices, is selecting the longest blockchain fork without running a full node. Stack should enable light clients to differentiate between conflicting blockchains and pick the correct fork.
5. **Enable Support for Advanced Namespace Operations:** The Blockstack open-source developer community has expressed interest [15] in certain advanced namespace operations, like namespace auctioning, atomic swaps, and more expressive payment structures. These features require programmatic interaction of digital assets and native tokens (which are also a type of digital asset) and the current implementation of Blockstack's blockchain does not support them. Stack needs support for programmatic interaction with a native token to enable advanced namespace operations like atomic swaps, advanced payments, etc.

3 Stack Protocol

In Blockstack's architecture, the blockchain occupies the lowest layer and is used as a secure base layer to provide consensus on data bindings. This gives global consensus on the state of digital assets like domain names. Blockstack follows a design principle to keep complexity and logic outside of the blockchain layer as much as possible (see [6] for details). Blockstack's blockchain, as of Blockstack Core v0.17 [19], uses *virtualchain* [13]; a virtualization mechanism that implements a blockchain on top of existing blockchains (just like virtual machines are constructed on top of physical hardware). The primary

benefit of the virtualchain (layer-2) implementation is better fault tolerance in case of a failure of the underlying blockchain.

The Stack protocol proposes modifications to the Blockstack blockchain. These modifications are a major upgrade of the Blockstack network and, like earlier major upgrades, require a network hard fork. Historically, the network has been undergoing a protocol upgrade through a hard fork every year, and the community and developers expect that pace to continue in the short-term [20]. The Stack protocol introduces the following modifications to the Blockstack blockchain to enable new functionality:

- **Blocks:** There is no real concept of blocks in the current Blockstack blockchain, the current design only requires total ordering of operations and is agnostic of categorizing operations into individual blocks. Stack introduces a concept of distinct blocks in the Blockstack blockchain. This is similar to how most other blockchains work [21]. A 1:1 correspondence between blocks in the Blockstack blockchain and the underlying blockchain is conceptually simpler.
- **Tokens:** The Stack protocol proposes to switch the protocol token from the underlying blockchain (layer-1 token) with a native (layer-2) protocol token, called *stacks*. This introduces new incentive mechanism for the growth of the ecosystem, establishes the economic stakeholders of the network, preserves the economic stakeholders through migrations, and enables support for mobile clients and advanced namespace operations.
- **Mining:** The Stack protocol introduces a new native mining system for the Blockstack blockchain. The mining system has three components: (a) a proof-of-burn mining mechanism to incentivize people to participate in building a longest blockchain, (b) an app-rewards mining mechanism to incentivize developers to build apps during the initial years, and (c) a web-of-trust mining mechanism to incentivize users to participate in an ecosystem of decentralized apps.

The Blockstack mining system is novel in that it allows traditional miners, developers, and users to mine the token, called *stacks*, in different ways. Traditional miners can use proof-of-burn mining to destroy tokens of the underlying blockchain (currently Bitcoin) to mint new stacks. Developers and users can mine stacks (also called *tokens* in this paper) by following the rules of the incentive mechanisms. Developers receive tokens by having a popular app on the network and users receive tokens simply by joining and verifying their account. The Blockstack blockchain, using its virtualization mechanism, benefits from the security of the underlying blockchain on which it operates.

3.1 Stacks: Blockstack Token

The Blockstack token, called *stacks*, will provide an access control mechanism for performing various operations on the Blockstack network. Protocol operations on the Blockstack network will "consume" tokens; network users will need to purchase tokens

to perform network operations. The tokens introduce a cost factor for performing operations, discouraging malicious users or spammers from performing too many operations on the network. The tokens are a scarce network resource and they're used to protect other scarce network resources like domain names.

The network operations on the Blockstack network are currently mostly around domain/username registrations and maintenance [6]. Every application and user identity registered on the Blockstack network has a record on the Blockstack blockchain and is logically registered in a particular namespace (namespaces are like top-level domains in the Domain Name System). The registration record has a human-readable domain name, a public key, and a hash of the data payload of associated resolution information (known as a *zone file*), and is owned by the associated public-private keypair.

For spam protection, registration of records on Blockstack requires a registration fee. The registration fee is sent to a "black hole" address and is equivalent to destroying money. The registration fee is currently payable in bitcoins (the token of the current underlying blockchain) but Stack proposes to change the default token used for registration fees to stacks. (See Section 4 for a detailed discussion of the proposed benefits of using stacks for this functionality.) To maintain backwards compatibility, all current namespaces will continue to work with bitcoins, as long as Bitcoin remains the underlying blockchain, and creators of future namespaces can choose to use the underlying blockchain token, instead of the native Blockstack token, for payments.

In addition to registration operations, Blockstack currently supports maintenance operations like *update*, *transfer*, and *revoke* on the name record. All network operations require a *transaction fee* on the underlying blockchain as well. This transaction fee is the price users pay to store Blockstack operations in the underlying blockchain [6]. Similar to registration operations for domains, Blockstack supports operations for creating namespaces. The tokens used to register namespaces are currently destroyed, but we are working on support for namespace auctions (discussed in Section 6). The Stack protocol proposes to add new operations, like *mint* and *transfer*, for mining and managing stacks, which are a new type of digital asset on the Blockstack network.

3.2 Preserve Economic Distribution through Migrations

We believe that the blockchain industry is still relatively young and evolving, and it is too early to pick a winning blockchain. It is hard to predict which blockchain will be operational and reliable five years from now. Individual blockchains might fail, but a new internet for decentralized apps built on top of blockchains needs to live for decades to come. Our early experience with moving away from Namecoin shows that a layer-1 token might become irrelevant for the Blockstack network after a migration [16].

In contrast to a layer-1 token, a native Blockstack token (implemented natively in the Blockstack blockchain) establishes the economic stakeholders of the Blockstack network and not the underlying blockchain. Migration of the underlying blockchain is possible without a native Blockstack token, but results in a loss of economic stakeholder state

and distribution; all of the previous stakeholders that bought into the earlier distribution now have to convert their holdings into the new token to continue their participation in the network. Further, their relative ownership of the token economy can drastically reduce after a migration. Therefore, preserving the distribution and relative ownership of economic stakeholders through migrations is important for the long-term success of the Blockstack ecosystem. The process of starting the genesis block and assigning early allocations optimize for getting a wide distribution of the Blockstack token (Section 5).

Establishing the economic stakeholders also enables better governance of the protocol. The stakeholders can vote, through a transparent voting mechanism, on whether or not a move should take place and if so when. Decentralized governance is discussed in more detail in Section 5.

3.3 Light-client Support

Blockstack users run *full nodes* to independently verify transactions and data mappings. However, running a full node is too resource intensive for mobile devices or may not be allowed by mobile platform vendors. We currently have a protocol that lets light clients (on mobile or desktop) to verify data fetched from untrusted nodes, given a trusted consensus hash [22]. However, this requires establishing a "trust channel" or getting a trusted consensus hash offline. With a native token, we can get rid of this limitation and enable independent verification of the longest Blockstack blockchain by light clients. This opens the door to bitcoin-like Simplified Payment Verification (SPV) [17] client support and truly decentralized apps on mobile devices (explained in Section 4.1). Mobile devices are the vast majority of end-user devices and supporting them is critical for the growth of the ecosystem. This also enables users with low-end computing devices to easily connect to the network.

3.4 Newly Enabled Features

The Stack protocol, with a native Blockstack token, enables the following new features:

Atomic Swaps

Currently domain names on Blockstack can be listed on commerce sites, like eBay and Sedo, and purchased by individuals who want to buy them. This is simple enough, but it often requires the domains to be put into an escrow service that has additional costs. In addition, the need for external services to list domains adds friction to the secondary market of selling domains and can leak personal data depending on the service used.

Atomic swaps of assets on the Blockstack network can enable a truly decentralized exchange of domain names that preserves privacy of both parties in a transaction. With atomic swaps, one person can send a new transaction that lists a domain for sale and another person can send a transaction to claim the domain with tokens that references the first transaction. This would trigger the simultaneous release of the

domain and tokens; no trusted exchanges, escrow services, or middlemen are needed for this functionality. Atomic swaps with a layer-1 token can be implemented by using Hashed Timelock Contracts (HTLC) [23], but would require a third-party service to learn the address of the recipient. Atomic swaps with a native Blockstack token do not require third-party services and can more expressive conditions for exchange of assets.

Advanced Payments

A native Blockstack token implemented as an accounts-based token vs. a UTXO-based token like Bitcoin [5] enables more expressive payment transactions. The Blockstack Core v0.17 hard fork [20] enables namespace creators to specify an address to collect name registration proceeds (instead of burning the registration fees). With an accounts-based native Blockstack token, this feature can be expanded upon so that the proceeds from domain registrations payments can be distributed amongst a set of namespace owners. This can allow a group of users to collectively purchase and maintain a namespace. In this case, the creators would have an incentive to build a community of users around their namespace and each get a fraction of the rewards.

Namespace Auctioning

Currently in Blockstack, users can create namespaces by burning a certain amount of tokens, based on the length of the namespace name [6]. This mechanism is fairly simple, but (a) if the namespace prices are too high then not many namespaces will get created, and (b) if namespace prices are too low, then spammers can end up registering a bunch of namespaces without actively using them. Enabling namespace auctioning can establish a better price for namespaces based on market demand. A native accounts-based Blockstack token can enable this feature. This feature is a future work and is not part of the currently proposed changes of the Stack protocol hard fork. See Section 6 for details on our ongoing work on namespace auctioning.

4 Mining Incentives

The Stack protocol introduces the concept of discrete blocks in the Blockstack blockchain, instead of just having totally ordered operations; the first block after Stack is activated on the network will be the *genesis block* of the protocol. New tokens released in the genesis block are created by a company, Blockstack Token LLC, and the details of the token allocations in the genesis block are out of the scope of this paper. Readers are encouraged to see the Blockstack Token LLC website [24] for details.

After the *genesis block* is released and the new network goes live, the Stack protocol releases new tokens into the system through a *mining* process. New tokens can be mined by three methods: (a) proof-of-burn mining, (b) app-rewards mining, and (c) web-of-trust mining.

4.1 Proof-of-burn Mining

In the Stack protocol, the main mechanism for mining is proof-of-burn mining. A layer-1 blockchain token can be destroyed or "burned" by sending it to an owner address from which it can never be retrieved. Such "black hole" burn addresses are already used in cryptocurrencies like Bitcoin [25] e.g., the burn address used by Counterparty [26]:

1CounterpartyXXXXXXXXXXXXXXXUWLpVr

Burning a proof-of-work cryptocurrency, like Bitcoin, to mine another token is functionally equivalent to proof-of-work [5] mining. In proof-of-work, computing power and electricity is converted into tokens and in proof-of-burn the same resource is further converted into another token.

The proof-of-burn mining in the Stack protocol establishes the longest blockchain fork where "longest" is defined as the blockchain fork with the most amount of cryptocurrency burnt and the state on the longest fork is considered the correct state of the network. Establishing the longest blockchain fork without processing the blockchain from the genesis block is important for **supporting light clients**, such as mobile devices. Our goal is to support truly independent light clients that don't need to trust a third party. With Stack, light clients like mobile devices can ask public Blockstack nodes for the latest consensus hash, set of all *mine* transactions, and Merkle proof that the set of *mine* transactions is included in the consensus hash. Light clients can independently validate if the *mine* transactions were included in the underlying blockchain, for example by using the Bitcoin SPV protocol [17], and independently calculate the total money burned. Light clients can repeat this process for a set of public Blockstack nodes and pick the state view with the most amount of money burned as the "correct" one. In this mechanism, you only need one honest public node in the set of queried public nodes to converge on the longest/correct blockchain and state view. An attacker who wants to present an alternate blockchain history to a light client will need to destroy a lot of money to present an alternate history on a fork longer than the current blockchain; such attacks become prohibitively expensive and impractical for tampering with data that is several days or weeks old. Light clients can also cache data, e.g., hash of transaction and tokens burned, for each transaction that they've seen for scalability. They don't need to issue new SPV queries [17] to check transactions that they've already seen.

In the Stack protocol, a new mining reward is released every new layer-2 block. The mining reward per block is defined by the Stack protocol at the time of the genesis block and the mining reward reduces over time following a step function. The initial mining reward is 8000 tokens per block and it reduces annually by 500 tokens until it reaches 2000 tokens per block after which it stays constant forever. The mining reward rate per block and the new tokens released in the genesis block imply that there will be 4,702,500,000 tokens after ∼10 years, assuming 144 blocks per day (average in Bitcoin [9]). The economic distribution of mining rewards and the rationale for our distribution model is discussed in Section 5.

The mining reward for each *mine* operations in a given block is calculated by looking

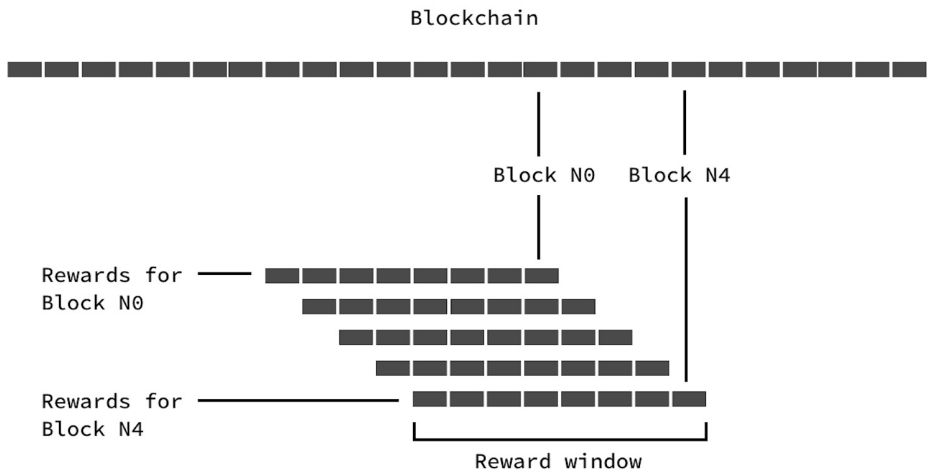

Figure 1: *Proof of burn mining.*

at the last N blocks. For any given block, all of the burns of the last N blocks are added up. For all of the *mine* transactions in the last N blocks, the total money destroyed over the time period is calculated and the mining reward for the current block is divided proportionally based on the fraction of the total amount burned. This implements a *rolling mining window* (described in Figure 1) where a *mine* operation in a given block receives a small reward in that block and rewards over the next $N - 1$ blocks.

Figure 1 gives an example of how the proof-of-burn mining system releases rewards. At any given block, a single reward R, containing a predefined number of new tokens, is released that is distributed amongst all of the miners of the last N blocks (including the current block). At block M, the reward R is distributed amongst all burns in the blocks from block M to block $M-N$. For example, let's say we choose our N to be 4032 (a long rolling window of rewards smooths out any short term fluctuations in rewards). That means that a *mine* operation ("burn") in block 5000 will receive rewards in block 5000 and will also receive rewards from the next 4031 blocks. Similarly, the mining reward of block 5000 will go to *mine* operations in blockstack 5000 and *mine* operations in the previous 4031 blocks. Mining rewards for a given reward window are handed out only after the reward distribution is clear and is not likely to change because of underlying blockchain reorgs [27].

4.2 App-rewards Mining

The second type of mining in the Stack protocol, called *app-rewards mining*, has incentive mechanisms for incentivizing developers to participate in the ecosystem by developing high-quality applications. App-rewards mining distributes rewards to developers periodically in the form of tokens. App rewards per block are defined in the Stack protocol. App-rewards mining targets the bootstrapping problem of the two-sided market

of developers and users and will distribute rewards for only the initial four years, called the *bootstrapping period*.

Determining what applications on Blockstack are eligible for these rewards and how the rewards should be distributed amongst eligible applications is a hard problem to solve algorithmically. Developers can try to game any automated algorithmic distribution of rewards and covering for all potential corner cases there is impractical. Instead, we propose a mechanism involving a federation of independent entities, called *App Reviewers*, that participate in the curation process of selecting eligible applications and assigning appropriate weights to each application. The goal of the curation process is to produce a set of "top applications" similar to how applications get featured on application stores like the Apple App Store or the Google Play Store. App Reviewers are elected for a 1-year term and the reviewer set membership is updated during the annual hard fork. App Reviewers are selected by the following process:

1. App Reviewers for the first year term, after the network goes live, need to be part of the genesis block i.e., they need to become economic stakeholders of the ecosystem as the first step. They must use the associated private key of their ownership address in the genesis block to perform curation operations.
2. Every ownership address in the genesis block will get one vote for selecting App Reviewers, regardless of the number of tokens owned by the address. The reason is that Blockstack Token LLC, the company starting the genesis block, plans to perform checks to ensure only unique individuals and entities can get allocation in the genesis block and Sybils are not possible (Section 5). Our goal is to have a wide distribution of tokens in the genesis block and give each unique entity equal say in the selection of App Reviewers for the first year.
3. App Reviewers will publicly submit their statements for why they should be selected as App Reviewers. The statements should include how they've contributed to the Blockstack ecosystem in the past and how they plan to contribute in the future.
4. In the time between genesis block allocations are finalized and before the network goes live, Blockstack Token LLC will conduct a vote in which genesis block owner addresses will publicly submit their votes for selecting App Reviewers. The votes must be signed by the respective keypairs.
5. After the first year term, the second year term App Reviewers will be selected before a planned hard fork of the network. Genesis block owner addresses will be given 50% weight in the second voting process and the token holders will get 50% weight. Unlike genesis block addresses, the votes from token holder addresses are weighted based on how many tokens are owned by each address. The reason for this is that (a) we don't want the genesis block participants to have control over App Reviewers selection for all the 4 years and other economic stakeholders should also get a representation and (b) after the genesis block, tokens are likely to be mined and traded freely and we cannot ensure that owner addresses represent unique

entities; number of tokens owned by addresses becomes a better representation of voter participation in that situation (otherwise a malicious user can create hundreds of Sybil addresses with small token balances to influence the voting process).

6. App Reviewers will publicly submit their statements for the second year term similar to the first year term. Voters will have visibility into past performance of App Reviewers who wish to get re-elected since all of their previous curation actions will be publicly auditable on the blockchain.
7. The App Reviewers selection process will repeat for the third year term and fourth year term with 50% voting power going to the genesis block owner address (one vote per address) and 50% voting power going to token holders (one vote per token including tokens that were originally released in the genesis block since they might have changed owners by now). Rules for App Reviewers selection remain the same for year 2, 3, and 4.
8. The app-rewards mining will stop at the end of the fourth term as it's meant to provide incentives to developers only in the initial bootstrapping stage of the ecosystem and can get overly complicated and political in the long-run.

The app-rewards per block are distributed proportionally, based on respective weights, to all applications that end up getting selected as eligible for a reward. If there are R tokens in a given block and there are a total of W weights across all eligible apps, then the number of tokens rewarded in a given block to application A would be the weight assigned to application A times the number of tokens in the block reward R divided by the total weight assigned to all eligible apps W_N:

$$R_A = \frac{(W_A * R_{block})}{W_N} \tag{1}$$

The reward mechanism is easy to implement once the set of eligible applications and their respective weights can be defined; defining the set of applications and their weights is the real challenge. In the Stack protocol, we propose using a set of independent legal entities as App Reviewers. The App Reviewers should have an incentive to (a) do the work of evaluating various applications and curating them, and (b) remain honest and neutral during the curation process. Further, the App Reviewers themselves should not become a point of centralization in the ecosystem. To incentivize App Reviewers to stay honest we propose using legal entities, for example top venture capital firms or prominent non-profits, that have reputational risk of being publicly dishonest. We propose to start with a set of at least seven App Reviewers and increase the set members over the coming years. The numbers of App Reviewers from a particular category, like venture capital or technology non-profit, should be limited; our goal is to have a diverse set of App Reviewers. The Blockstack network traditionally goes through a hard fork every year [20] and the set membership can be updated based on the vote of economic stakeholders (Section 3.2). The Blockstack ecosystem already has 6 venture capital

firms that set up a USD $25 million fund for applications developed on Blockstack [28]. Some of these venture capital firms can be good candidates for serving as App Reviewers for the first year. Developing the detailed charter for App Reviewers is ongoing work and out of the scope of this paper. In this paper, we focus on the incentive mechanisms for developers and App Reviewers:

- Developers have an incentive to participate in the ecosystem because they are explicitly getting tokens as rewards for developing applications. These rewards are in addition to the respective business models of their applications. The higher the proceeds from app-rewards mining, the more developers are likely to participate.
- App Reviewers get 2% of the rewards allocated for app-rewards mining, per block, as compensation for their time and effort. The fee gives App Reviewers an incentive to do the curation work during their 1-year term.
- Some App Reviewers, like venture capital firms, might have an additional incentive to do the curation work as they can use their own funds to invest in the applications as well. The curation work is very similar to the work they already do for finding high quality startups to invest in. The App Reviewers will be required to disclose any conflicts of interests, like existing investments, with the apps under consideration.

4.3 Web-of-trust Mining

The third type of mining in the Stack protocol, called *web-of-trust mining*, has incentive mechanisms for incentivizing real users to participate in the ecosystem, register a unique identity, and use applications. Ideally, users should be able to receive mining rewards simply by being on the platform and going through a process to prove that they are a unique real person. However, doing this algorithmically is challenging since a single user can create many accounts, each appearing to be a unique user but in reality all controlled by the same person. A malicious user can use such bots to trick the protocol into giving her more rewards. This is known as the classic Sybil attack problem [12]. Differentiating between real users and bots, known as detecting Sybils, is the key challenge here, and is generally considered a hard computer science problem to solve [29]. Our goal is to have a broad distribution of rewards and get Blockstack tokens in the hands of a large number of real users (and not bots).

We divide the incentive mechanisms for web-of-trust mining into two parts:

- **Initial trusted-set:** In the first part, Blockstack Token LLC – the company responsible for creating the genesis block, runs a process where any user can register to be a part of the genesis block allocation. The company will require the users to verify control of accounts on well-known social media properties on their Blockstack ID [30] and will perform standard Know Your Customer (KYC) checks on the users during the registration process to ensure that they are real users. These users will be offered a discount on the initial token price to incentivize

them to participate in the registration process. The registration process will result in an initial trusted set of users who passed the KYC checks and are real users.

- **Expanding the trusted-set:** In the second part, after the network goes live, we will introduce mechanisms for how the initial trusted-set can be expanded to include more users similar to how the traditional web of trust protocols [31] work. This part of the web-of-trust mining mechanism is under active development and we will release more details on it in a future version of this paper. We plan to fall back to a process with gatekeepers, similar to how the initial trusted-set is curated, if the algorithmic approach does not lead to a reliable mechanism. We discuss our ongoing work on algorithmic expansion of the trusted-set in Section 6.

4.4 Potential Attack Vectors

In this section, we consider some potential attack vectors for the mining system. The attack vectors presented here are only a small set of potential attack vectors. We discuss future work on incentive mechanisms and security of the protocol in Section 6.

Miner Consolidation

There is a possibility that miners of the underlying blockchain, currently Bitcoin, start blocking all *mine* transactions from other Blockstack miners and only allow their own *mine* transactions to go through. Since the mining rewards for Blockstack are distributed over a large number of blocks, the underlying blockchain miners will need to carry out such a transaction censorship attack for a very long time, such as a period of 4032 blocks, to be able to block other miners. This is extremely hard to do in practice since even a single honest miner of the underlying blockchain can let *mine* transactions in. Further, even small transaction fees can incentivize underlying blockchain miners to include Blockstack *mine* transactions in their block. In the worst case, the system devolves into a situation where underlying blockchain miners block out all other burners. This means that the set of underlying blockchain miners also form the total set of miners of the Blockstack blockchain, and new Blockstack tokens will go to the same set of miners as the underlying blockchain which is not a bad outcome.

Changes of the Underlying Blockchain

The underlying blockchain can have blockchain *reorgs* where miners change the order of blocks or change which transaction got included in which block [27]. Such reorgs are often short-lived and do not impact data written earlier in time e.g., in Bitcoin, data written in blocks with more than 6 confirmations is highly unlikely to change in a reorg. However, there can be long-lived reorgs of the blockchain where data written in earlier blocks can change as well. We avoid short-term reorgs by requiring > 6 confirmations between Blockstack operations where strict ordering is important. We have a mechanism to detect long-lived forks [13] and nodes reprocess transactions from blocks earlier than

the fork point to resolve conflicts. In the case of a permanent fork of the underlying blockchain, we use the default policy of picking the blockchain with the most proof-of-work. If the underlying blockchain fails completely or becomes insecure or miners of the underlying blockchain become non-cooperative, we can move away from that particular blockchain (see our migration away from Namecoin after discovering security issues [16]). The migration can potentially be to a dedicated underlying blockchain for Blockstack as well (see Future Work in Section 6).

Key Compromise Attacks

The app-rewards mining mechanism requires a use of App Reviewers which are elected for at least one year. These App Reviewers attest to data and write it to the blockchain. The App Reviewers can have their data-signing keys compromised. Since it's impossible to distinguish between an honest reviewers with a compromised key and a rogue reviewer, we can treat each of these scenarios as equivalent and refer to them simply as a "key compromise attack". We plan to use "key revocation certificates" for such attacks where revocation keys are shared with the reviewer and with a separate foundation. In the event of a key compromise, anyone with a revocation key can effectively stop the compromised reviewer from participating. Further, the community can remove App Reviewers from the system in a future hard fork of the network.

5 Decentralized Governance

The Blockstack network needs to be governed in a way that there are no central points of failure or control and various stakeholders can have a representation in protocol development and direction.

Protocol Forks and Upgrades

The Blockstack network undergoes periodic hard forks to upgrade core functionality and to add or update protocol operations. Not all software updates are consensus breaking and therefore don't require a hard fork. Upgrades that do need a hard fork, however, are harder to deploy and require (a) community agreement over protocol changes, and (b) software updates of all deployed nodes. The nodes that don't upgrade get disconnected from the main network and end up on a forked network. If the community has a disagreement over protocol changes then the network usually forks into separate networks, as with the case of Bitcoin and Bitcoin Cash [32].

Currently, the Blockstack network does not have an algorithmic metric for community consensus and protocol changes are discussed on community forums before they're activated [15]. The Stack protocol introduces an algorithmic metric for community consensus based on the economic distribution of the Blockstack token. Token owners can sign messages from their respective owner addresses to participate in a voting mechanism. Different proposed protocol changes can have different thresholds for activation.

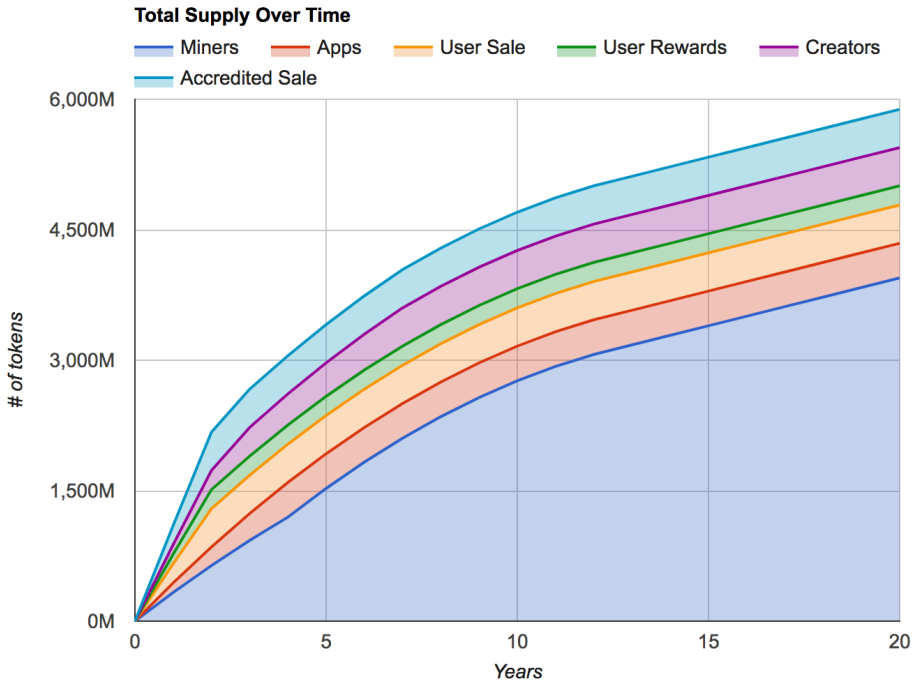

Figure 2: *Blockstack token distribution to different categories over 20 years.*

For example, a change can require 75% of the economic stakeholders to agree before the change is activated. Initially the stakeholder votes will be used as *signaling* and will not automatically activate protocol features. Fully-automated voting on protocol upgrades is an area of active research (Section 6). Further, getting users to consistently participate in voting is usually challenging and we discuss a delegated voting mechanism in Future Work (Section 6) that will improve upon the simple stakeholder majority vote mechanism.

Economic Distribution

Voting on protocol changes needs to represent all the different parties participating in the ecosystem and no single party or category should have too much control over protocol development. It's critical to ensure that the economic distribution of the Blockstack token reflects the various stakeholders and all stakeholders are given access to the token regardless of their financial status. Figure 2 shows the proposed Blockstack token distribution over 20 years with the following categories:

- **Miners:** The majority of the tokens are released through the proof-of-burn mining process (Section 4.1) and anyone can participate in that process.
- **App-rewards:** During the bootstrapping period (first four years) app developers can get tokens by developing high quality applications (Section 4.2) instead of

participating in the proof-of-burn mining. They can effectively use their time and skills to get tokens instead of burning cryptocurrency.

- **User-rewards:** Users can get tokens by either purchasing them at a discounted price (details are on the Blockstack Token LLC website [24]) or by participating in the web-of-trust mining (Section 4.3) where real users get tokens for creating verified unique accounts. These categories are listed as "User Sale" and "User Rewards" in Figure 2 respectively.
- **Investors:** Qualified investors can fund protocol development and participate in the token sale to Accredited Investors and Qualified Purchasers. Details are on the Blockstack Token LLC website [24].
- **Protocol Developers:** Protocol developers and creators get tokens for their contributions to building and maintaining the network and the software.

There is a predefined amount of Blockstack tokens that exist in any given year. The mining system starts by releasing 8000 new tokens into the system per block. This rate slows down over time (by 500 tokens per year where a year is defined in terms of number of blocks) until it reaches 2000 new tokens per block and then continues to release 2000 new tokens per block forever. This gives a $\sim$2% annual inflation rate after year 13. The reason for constant inflation is that there needs to be room for the ecosystem to grow, and register new users and applications, even after decades of operation. Tokens are also destroyed during registration operations which decreases the supply.

For decentralized governance, it is important to ensure that no single party – including the protocol developers and maintainers – do not have too much economic power in the system in any given year. Figure 3 shows the creator ownership of the Blockstack token as compared to other major networks/projects like Bitcoin [9], Ethereum [10], Zcash [33], Tezos [34], and Filecoin [11]. Our protocol allocates less tokens to the protocol creators and developers than other major projects; we believe that limiting the relative economic power of the creators helps the long-term success of the ecosystem.

Genesis Block and Protocol Development

Protocol development can be divided into two phases. The initial development phase in which the core software is developed and the first block, called the *genesis block*, is launched on the live main network. The genesis block contains initial token allocations for different parties. Mining starts at block 2 and protocol rules start releasing new tokens to the three types of miners (Section 4).

Blockstack is an open-source project and decentralized network. For the past years, one company, Blockstack Public Benefit Corp (PBC) [3], has taken the lead on protocol development and employs the protocol creators. Blockstack PBC will play a significant role in the software development of the new mining system and token protocol. A separate legal entity, Blockstack Token LLC [24], will manage the creation of the genesis block and selling tokens to various parties to help fund protocol development

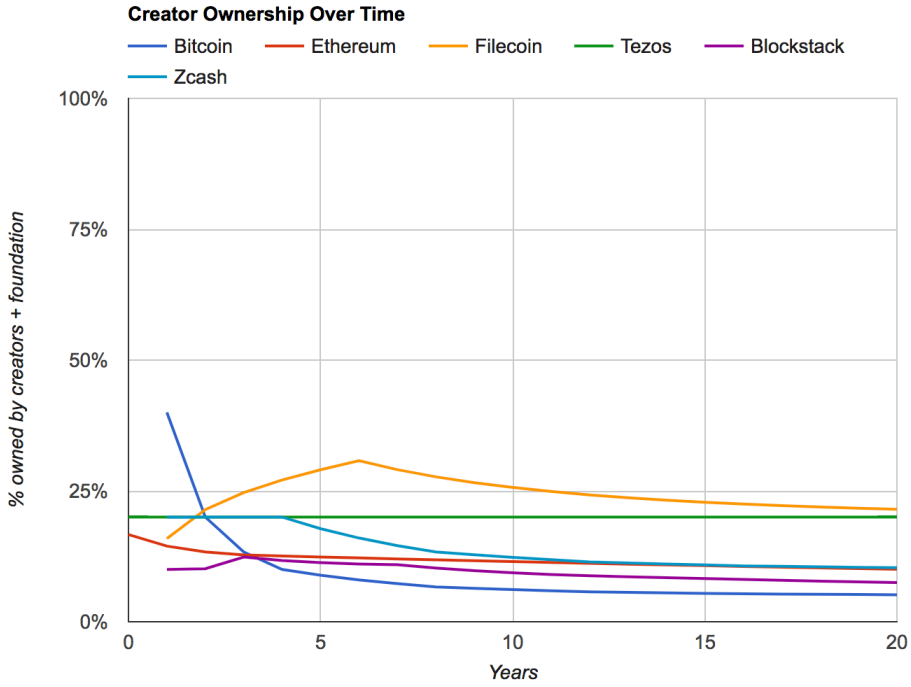

Figure 3: *Creator ownership of the Blockstack token vs. other major projects.*

in the coming years. A detailed discussion of the Blockstack token sale is out of the scope of this paper and token sale details are available at [24]. An important point to note about the Blockstack token sale is that there are concrete milestones in place for protocol developers and funds are released to protocol developers only if they meet these milestones (details of this process are at [24]). We believe that such checks and balances are important governance mechanisms and give developers incentives to work on protocol development and successfully deploy the new system. Over the coming years, we plan to have many independent individuals and companies operating on the network and taking on greater roles in the protocol's development. The app-rewards incentives play an important role in attracting independent developers to the open-source project.

6 Implementation & Future Work

The Stack protocol will be introduced to the Blockstack network as a major upgrade requiring a hard fork. The Blockstack network, historically, implements a hard fork with major upgrades once every year [20]. The genesis block of the new Blockstack blockchain was started in September 2017 and the process of assigning initial allocations in the genesis block has started. The software itself is expected to take a year of development and the network is expected to go live by early 2019.

Each Blockstack token is called a *stack*. Each stack is made up of one thousand

milli-stacks and one million micro-stacks. The token will have 6 decimal places. The token will be implemented as an accounts-based token like Ethereum [10]. The token implementation will introduce new operations on the Blockstack network for token mining, token transfers, etc. The software will be released as open source as a new version of Blockstack Core [19].

Some components of the Stack protocol are under active development. Most notably:

- **Namespace Auctions:** It's desirable to register namespaces using auctions instead of a fixed price as it's hard to predict the market demand of a namespace and price it accordingly without auctions. We're actively researching various auction mechanisms for namespaces and plan to implement them in a future release of the Blockstack software.
- **Voting Mechanisms:** The decentralized governance mechanism presented in this paper follows a simple economic majority vote for protocol changes. These votes are separate from the mining process and can be used to get stakeholder input on various things. Getting ecosystem users to regularly participate in voting is challenging though. We're exploring a delegated voting system (not to be confused with proof-of-stake blockchains [35]) where token holders can appoint a representative, out of 10-20 options, who can vote on the behalf of themselves on governance and open-source protocol development issues. Economic stakeholder can replace their representative at any time.
- **Algorithmic Web-of-Trust Mining:** The current Stack protocol presents a mechanism for building an initial trusted-set of real users (Section 4.3). The initial trusted-set requires a single gatekeeper to perform identity checks. Expanding the trusted-set in an algorithmic manner, after the network goes live, while staying resilient to Sybil attacks is challenging and an area of ongoing research. We are currently exploring mechanisms where users in the initial trusted-set select a limited number of new users and are incentivized to include real users and not bots; the protocol gives web-of-trust mining rewards only if the user they included passes identity proof checks. An identity proof verifier checks for attestations posted on a user account and if the attestations pass a threshold the user is classified as a real user. There are several challenges with this general approach involving use of external data sources ("Oracles"), maintaining network consensus, and making the classifier Sybil resistant to name a few.
- **Better Support for Mobile Clients:** Blockstack implements a trust-to-trust internet architecture [36] where end-users don't trust any node or infrastructure not in their explicit "trust zone". Mobile devices have inherent resource limitations and cannot have long-running processes or keep full copies of blockchains. Stack enables mobile clients to independently verify the longest Blockstack blockchain without running a full node. However, there are several other Blockstack components like decentralized storage [6] that need further work before they can be deployed on mobile devices. Seamless integration of the Stack protocol and the

Blockstack infrastructure from mobile devices remains an area of future work.

- **Dedicated Underlying Blockchain:** Transactions of layer-2 systems like the Blockstack blockchain can be considered as a non-traditional use case of the underlying blockchain, and in some extreme cases, users and miners of the underlying blockchain might consider them as "spam" [37]. On blockchains like Bitcoin, there has been a tension between the original use/purpose of the blockchain and any new use cases that develop on top. Further, a UTXO-based blockchain like Bitcoin might not be best way to implement the accounts-based token used in Stack. We're exploring the design of a dedicated underlying blockchain that is optimized for Blockstack operations and uses a combination of proof-of-work [38] and proof-of-replication [11]. Our use of virtualization means that we can seamlessly migrate to any blockchain and maintain the economic distribution of stacks.

7 Conclusion

The traditional internet is a 40-year-old technology that was originally meant to be a decentralized network. Even though the lower layers of the internet remain fairly decentralized, the application layer of the internet has several centralized points of control and failure. Blockstack is a new internet for decentralized applications that replaces points of centralization from the application layer of the internet; these include DNS root servers, certificate authorities, and centralized data stores. This paper presents *Stack*, a blockchain token protocol that upgrades the Blockstack blockchain and introduces decentralized governance and incentive mechanisms for a decentralized app ecosystem. Stack enables several new features like atomic swaps, support for light clients and it introduces a novel mining mechanism. The protocol is a major upgrade to the existing Blockstack network and focuses on the long-term sustainable growth of the entire ecosystem. The system is designed with decades of operation in mind and introduces several incentive mechanisms for developers and users to participate in a two-sided market of decentralized apps.

Acknowledgements

The people acknowledged in this section do not endorse the Blockstack token or the Blockstack token sale, and do not recommend any purchase of the Blockstack tokens or any related instruments, such as a simple agreement for future tokens or an interest in a fund sponsored by Blockstack Token LLC and its affiliates.

We'd like to thank Aaron Blankstein, Andrew Miller, Gina Abrams, Guy Lepage, Jack Zampolin, Jude Nelson, Ken Liao, Larry Salibra, Matt Weinberg, Mike Freedman, Patrick Stanley, and Phil Daian for their feedback on early drafts, helpful suggestions, or contributions to ideas presented in this paper.

References

[1] N. Perlroth, "Yahoo says hackers stole data on 500 million users in 2014," Sept. 2016. http://nyti.ms/2oAqn0G.

[2] C. Timberg, E. Dwoskin, and B. Fung, "Data of 143 million americans exposed in hack of credit reporting agency equifax," Sept. 2017. http://wapo.st/2ymtZIc.

[3] "Blockstack website," 2017. https://blockstack.org.

[4] "Gotenna mesh networking." https://www.gotenna.com.

[5] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21, 2015*, pp. 104–121, 2015.

[6] M. Ali, R. Shea, J. Nelson, and M. J. Freedman, "Blockstack: A new decentralized internet," Whitepaper, May 2017. https://blockstack.org/whitepaper.pdf.

[7] "Casa, open-source home sharing protocol." https://casa.cash.

[8] "Guild, decentralized blogging." http://www.guildblog.com.

[9] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," tech report, 2009. https://bitcoin.org/bitcoin.pdf.

[10] V. Buterin, "A next-generation smart contract and decentralized application platform," tech. rep., 2017. https://github.com/ethereum/wiki/wiki/White-Paper.

[11] Protocol Labs, "Filecoin: A Decentralized Storage Network," tech report, 2017. http://filecoin.io/filecoin.pdf.

[12] J. R. Douceur, "The sybil attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, IPTPS '01, (London, UK), pp. 251–260, Springer-Verlag, 2002.

[13] J. Nelson, M. Ali, R. Shea, and M. J. Freedman, "Extending existing blockchains with virtualchain," in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16)*, (Chicago, IL), June 2016.

[14] "Blockstack meetup groups." Retrieved from https://www.meetup.com/topics/blockstack/ in May 2017.

[15] "Blockstack community forum." https://forum.blockstack.org.

[16] "Why Blockstack is migrating to the Bitcoin blockchain." https://blockstack.org/blog/why-blockstack-is-migrating-to-the-bitcoin-blockchain.

[17] "Simplified payment verification (spv)." https://bitcoin.org/en/developer-guide#simplified-payment-verification-spv.

[18] J. Titcomb, "Mobile web usage overtakes desktop for first time," Nov 2016. http://bit.ly/2fbVqMw.

[19] "Blockstack core source code release v0.17," 2017. http://github.com/blockstack/blockstack-core.

[20] J. Nelson, "Blockstack annual hard fork 2017." https://forum.blockstack.org/t/annual-hard-fork-2017/1618/9.

[21] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ, USA: Princeton University Press, 2016.

[22] M. Ali, J. Nelson, R. Shea, and M. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in *Proc. USENIX Annual Technical Conference (ATC '16)*, June 2016.

[23] "Hashed timelock contracts." https://en.bitcoin.it/wiki/Hashed_Timelock_Contracts.

[24] "Blockstack Token LLC." https://blockstack.com.

[25] "Proof of burn." https://en.bitcoin.it/wiki/Proof_of_burn.

[26] "Counterparty: Why proof-of-burn." https://counterparty.io/news/why-proof-of-burn/.

[27] "List of Bitcoin CVEs." https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures.

[28] T. Geron, "Blockstack launches $25 million fund for blockchain startups," Aug 2017. http://on.wsj.com/2y68eiH.

[29] C. Lesniewski-Laas and M. F. Kaashoek, "Whānau: A Sybil-proof distributed hash table," in *Proceedings of the 7th USENIX Symposium on Networked Systems Design and Implementation (NSDI '10)*, (San Jose, CA), Apr. 2010.

[30] "Blockstack ID format, version 2." https://blockstack.org/docs/blockstack-profiles.

[31] N. Ferguson and B. Schneier, *Practical Cryptography*. New York, NY, USA: John Wiley & Sons, Inc., 1 ed., 2003.

[32] J. Titcomb, "Bitcoin cash: Price of new currency rises after bitcoin's 'hard fork'," Aug 2017. http://bit.ly/2hlEtUk.

[33] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin.," in *IEEE Symposium on Security and Privacy*, pp. 459–474, IEEE Computer Society, 2014.

[34] L.M Goodman, "Tezos a self-amending crypto-ledger," whitepaper, 2014. https://www.tezos.com/static/papers/white_paper.pdf.

[35] P. Daian, R. Pass, and E. Shi, "Snow white: Robustly reconfigurable consensus and applications to provably secure proofs of stake," 2016. https://eprint.iacr.org/2016/919.pdf.

[36] M. Ali, *Trust-to-Trust Design of a New Internet*. PhD thesis, Princeton University, June 2017. https://muneebali.com/thesis.

[37] J. Redman, "Tension rises around bitcoin's fees, unspendable addresses and spam," Mar 2017. http://bit.ly/2neJWdO.

[38] M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols," in *Secure Information Networks*, pp. 258–272, Springer, 1999.