Bitcoin Israel: A National Bitcoin Clone

Eli Sklar
eli.sklar@gmail.com
bitcoinil.org

Final v1.2

Abstract. Bitcoin [1] as an electronic, unbiased, financial system has been in operation for over a decade, with minimal error rate and downtime. It exists without any governing body, despite the many groups who steer its development and maintenance. It's a proven technology that can manage large sums of wealth securely and efficiently with impunity, which no other technology or product has been able to reproduce since. Bitcoin Israel (BitcoinIL, BTCIL) is a simple clone of the entirety of the existing Bitcoin Core source code and an attempt to scale the existing Bitcoin Core consensus sideways. Instead of investing in larger blocks, shorter block intervals, or alternatives to proof of work (PoW), BitcoinIL simply implements the existing consensus of the BTC network as an entirely new network using the same code, restrictions, and abilities of the Bitcoin Core code base.

1. Introduction

At this early stage of Bitcoin's existence, it is entirely possible to completely underestimate the effect that the Bitcoin technology has on the human species. Bitcoin has shown that it is possible to have computer systems that are different from the coupled server-client model developed in the last 40 years. Bitcoin has shown that the most coveted human concept, money, can be managed securely and effectively without any governing body and allows all to participate in its development, usage, and maintenance, without limitations or restrictions, regardless of their place of origin, chosen language, age, gender, or political outlook.

2. Motivation

Consensus and Governance

Bitcoin's main attribute that draws value to its currency is the public knowledge and agreement that bitcoin has limits. It has limits in the functions it can perform technically, limited to a very small number of said functions, and each new functionality added or removed is heavily discussed and all aspects are investigated before a change is implemented. Bitcoin has a limited quantity, and this makes it valuable, because there's only a finite number of these tokens to ever be created, effectively behaving as a finite resource, much like natural gas, wood, or land. But unlike natural gas, wood, or land, Bitcoin is entirely digital and manmade, a human creation that behaves like a natural law. The first of its kind.

These limits are not a natural law, but instead, a consensus agreed upon by all its users, maintainers, miners, and developers, which is expressed in the form of computer code freely available. This is unlike the existing human consensus, where we rely upon the written word to describe the agreements made between given parties. When there's a dispute in the existing human consensus, it is resolved by a court of law with litigators whose purpose is to evaluate and articulate the details of such agreements that have been agreed upon prior and signed by all parties. Bitcoin, however, does not rely on such agreements; its code cannot be interpreted differently by different jurisdictions or appear to have different meanings in different cultures like all written and spoken languages do. Bitcoin's consensus stems from the consensus of computer systems, of programming languages, and mainly basic logic.

Logic is not necessarily the ultimate tool for all decision making, but it's a great tool for most of our interpersonal interactions in ways that our legal systems no longer are. In its current form, the legal system is inefficient, hard to modify, hard to learn, and there are no absolutes within it. This makes the legal system vulnerable to attacks by popular opinion and vulnerable to manipulation by human bias.

Legacy

Bitcoin's innovation is such a radical departure from existing systems that it is expressed by the desire of many to get a hold of Bitcoin, as it can be used as a globally accepted medium of exchange. This attribute of Bitcoin, combined with its limited capacity for transactions volume, makes Bitcoin expensive for daily use, as the volume of transactions stays constant but the number of incoming transactions that are waiting to be included in the blockchain keeps increasing. The result is a simple rise in transaction cost, which correlates back to its value and the trust it engenders. The limits imposed on the network are the very reason the network and its tokens are so highly desirable.

One of the key advantages that makes Bitcoin so desirable is its legacy, its code, and the developer community around the codebase, which on one hand, guard the code from malicious or unintentional modifications that might harm the existing blockchain in one way or another, and on the other hand, they are responsible for keeping bitcoin's code current and up to date, both with newly discovered exploits and proposed technological changes and modifications. Everyone can inspect the Bitcoin Core code, propose modifications, fixes, or adaptations, but only a small group of people who are considered the Bitcoin Core developers are the ultimate decision makers regarding the modifications that the codebase receives, along with the signaling mechanism that allows the users to either adopt the change—by upgrading their software to incorporate the new change and hence signaling to the network its acceptance, or reject the change—and not upgrade the required software, and hence signal the network of its rejection.

These mechanisms are not perfect in themselves and are open to various attacks, but in combination with other architectural advantages that Bitcoin possesses, it seems that overall, the Bitcoin network is advancing slowly but surely, even if not all parties agree on all changes and modifications as they arise. This mechanism ensures the resiliency of the network, and as a result, people trust the network more as the network keeps growing and amassing larger audiences and followers. However, this mechanism creates a simple deadlock in regards to the accessibility of Bitcoin: the Bitcoin Core users and developers chose the slow-and-steady method of progress at the price of increasing the cost of using Bitcoin for the promise of a stable and reliable codebase that maintains the assurances given earlier on in its development process.

The existence of a plethora of altcoins—some derived directly from the Bitcoin Core codebase, others invented from scratch—only enhances and enables the slow progress of Bitcoin itself, by allowing Bitcoin to behave as an expensive backbone to the entirety of the crypto economy, a reserve currency so to speak. The altcoins experiment with new and potentially risky technologies that the Bitcoin

Core has either chosen not to adopt or simply is in the progress of researching and implementing such advances via its robust BIP (Bitcoin Improvement Proposal) protocol. Those who seek larger transaction volume, sophisticated smart-contracts, or advanced functions can find these in several flavors throughout the crypto-sphere, and their risk of attempting to use the new technologies does not risk the existing Bitcoin infrastructure, as those networks and their respective codebases are entirely decoupled. Individuals or organizations who wish to utilize advanced features in any of the network are free to do so, exposing only themselves and their assets to the potential risks, not the entirety of the crypto economy.

Clean Slate

Bitcoin's cost of usage has become prohibitive for almost every application apart from being the ultimate store of value. This in itself poses a fundamental shift in how people perceive Bitcoin and its potential uses, and as a result the developers of the codebase are naturally biased towards preserving the codebase functions that amplify the use of Bitcoin as a store of value, and reduce focus on developments to the core codebase that would increase its uses as a form of exchange, and opting to develop second and third layers or entirely redirect users to alternative coins for use cases that are less suitable for bitcoin at this point in time.

While many altcoins have chosen to enhance their codebase, their blockchain, with new or different features and capabilities as a way of improving the bitcoin technology or coping with its limitations of scale, a simple clone of the network's codebase has not yet been attempted. Despite the hundreds of blockchains and thousands of tokens that exist, no proposal has ever been provided for a simple sideways scaling solution, where the entirety of the Bitcoin Core codebase is used as-is, without any changes or modifications, to simply utilize the existing Bitcoin technology as-is, on a new and legacy-free, blockchain.

The effectiveness of Bitcoin stems from its open-source nature, which enables altcoins to modify and improve upon bitcoin without affecting it. Bitcoin enables altcoins users to verify, on their own, the validity of the code and its functions. This open-source nature is what drives trust in this system, drives innovation, and exemplifies to our culture that open and fully transparent systems can host and enable large-scale human cooperation on a system that is based on absolute code. This translates to the most fundamental logic that eventually drives the progress of human civilization.

With BitcoinIL, we are attempting to exercise this open-source nature to tap into the power and ability of the existing Bitcoin Core codebase and scale it by copying the existing codebase as-is, starting the blockchain from block 1, and as a result, having no pre-existing value or the congestion associated with it, effectively doubling the capacity of the Bitcoin Core blockchain and its consensus without actually modifying the existing Bitcoin Core code.

Glocality

Israelis were one of the earliest adopters of Bitcoin specifically and blockchain technologies in general. As such, Israel became an epicenter of the crypto economy in the past decade. This enabled Israeli developers to learn these technologies, while others still debated whether it was worth teaching, and launching countless projects and products, introducing new technologies both to the general crypto ecosystem and specifically to Bitcoin's codebase. Israeli blockchain tech is currently regarded as one of the strongest communities in this space, rivaling distant communities and able economies such as the USA or China in these regards.

The Israeli community attempted several times to create local cryptocurrencies, as far back as 2014, and while the local authorities and regulators are still unsure as to how to tax these technologies and

currencies, or even how to define them, Israeli entrepreneurs are helping governments across the planet form their own cryptocurrencies in all shapes, forms, and sizes.

By tapping into this treasure trove of capabilities, knowledge, and know-how BitcoinIL aims both to empower the local community and provide value to the global community. BitcoinIL, as Bitcoin Core itself, is an open system, based on open-source code, and its network is not biased towards users of a given country. The locality of this network is a testament to our desire to improve upon the existing codebase and ideas that Bitcoin itself introduced in the past decade and our commitment to groom and garner this network for all to use and benefit from.

3. Implementation

Our goal with the new network is to create a network that adheres to the general consensus created by the Bitcoin Core network. The new network is designed with minimal modifications [2] to the new network, enabling existing and legacy software designed to work with the Bitcoin network to work almost seamlessly with the new BitcoinIL network.

Mining Hash Function

Bitcoin originally used the SHA256 hashing algorithm to hash newly minted blocks. As the SHA256 algorithm was easy to implement, it was intended by Satoshi Nakamoto that anyone could participate in securing the network, and as a reward, receive generated bitcoins. Later in bitcoin's development, the mining industry adopted the *Application Specific Integrated Chip* (ASIC) model, and the mining industry has evolved to massive ASIC mining farms spanning the globe.

BitcoinIL hopes to achieve a similar path with mining. Early users are able to mine with their personal computers, and as the network strengthens and evolves, new ASIC developments might be created to mine and secure the BitcoinIL network in more efficient ways.

Furthermore, adopting the Bitcoin Core SHA256 mining algorithm would result in a potential security risk, as the cost of high-quality SHA256 ASIC miners is exorbitant and unattainable for the general population and would make purchasing dedicated miners a costly burden on the community and still be potentially risky, as any large-scale miner with existing SHA256 ASICs could, in theory, use it to rewrite BitcoinIL blockchain at will.

BitcoinIL chose to adopt a less-popular hashing function from the X family of functions, particularly X17[3]. This choice addresses both the desire to allow early users to mine the new coin with their personal computers, and later, to potentially develop locally designed and produced ASIC miners for the chosen hashing function.

Address Format

BitcoinIL modifies the standard Bitcoin addresses by simply changing the prefix of the public key addresses without introducing any actual modification to the format algorithm itself or the private key. This enables utilizing any and all existing bitcoin infrastructure—such as mining software, wallets, block explorers—while avoiding potential confusion and human errors.

Name	**Legacy** **Pubkey hash (P2PKH address)**

Network	BitcoinIL	Bitcoin
Leading characters	1	1
Example address	154aQbLJDhHU9kTRmBXtDbGmVLW5JxSnd6	17VZNX1SN5NtKa8UQFxwQbFeFc3iqRYhem

Name	**Script hash (P2SH address)** **SegWit Pay 2 Witness Public Key Hash (P2SH-P2WPKH)**	
Network	BitcoinIL	Bitcoin
Leading characters	v	3
Example address	vTNhKhojqCXrqcHNJtAFFuJt4pKM45EPvN	38PuaMPme2vxcXPJrsHrkuYHcaQSWVwMz6

Name	**SegWit mainnet (P2WPKH address)**	
Network	BitcoinIL	Bitcoin
Leading characters	il1q	bc1q
Example address	il1qc0u38hxd88ats8xwag23gssfywgmk4agupzhu2	bc1qtqzuwe0mcyxgdvd68y3942yymn7ya6rhqkhl6j

Genesis

Bitcoin Israel chose to create a new genesis block to achieve the goal of eliminating the historical weight of the main Bitcoin Core network, and by this, enabling a cheap and easier-to-access bitcoin network, with the same properties advantages but with fewer disadvantages of the original network.

The network established the genesis block with the hash:

0x00000d53b2d551fa1638333b80ca694fbfa021643d00f2e237f4021652cc61ea

Markel root:

e698eae92b0d33208ab3e087450fed7be77e4d12d232d7b4463edd889b0cd380

Which is a result of the timestamp hash of the string:

"כלכליסט 31/מרץ/2021 בנק ישראל: ייתכן שיהיה צורך להעלות מסים כדי לצאת מהמשבר"

The network went live on April 1, 2021, at 20:00 Israeli Standard Time, with block mining starting from block 1.

References

[1] S. Nakamoto, “Bitcoin”, https://bitcoin.org/bitcoin.pdf

[2] Bitcoin commit hash which BitcoinIL cloned from, https://github.com/bitcoin/bitcoin/commit/95ea54ba089610019a74c1176a2c7c0dba144b1c

[3] X17 Mining Algorithm, https://en.bitcoinwiki.org/wiki/X17