BUIP166: Launch a Chain for Proving Next Generation Features

Submitted by: Andrew Stone
Date 19 May 2021

Abstract

This proposal calls for the creation of a new blockchain, initially supported by Bitcoin Unlimited with its direction determined by its membership. The principal goal of the new blockchain is to Prove Features, i.e. demonstrating new functionality on a real-world blockchain with some unit coin monetary value. These additional software features will be theoretically deployable in Bitcoin Cash, however, because of the conservatism required in rollout on BCH (now worth $20 billion) there is a major benefit in first seeing major changes piloted separately. BU support for BCH and its regular upgrades remains unchanged. A modest budget is required for launch and maintenance of the new blockchain with its principal characteristics outlined.

Background

Every cryptocurrency must choose a path that embodies its fundamental philosophy. Often this path navigates a compromise between conflicting requirements, and this philosophy may deviate between the cryptocurrency as a whole, and individual or group participants. In particular, I have always believed that to be competitive against the first mover advantage of Bitcoin and against the versatility of Ethereum, the blockchain architecture Satoshi left us requires a phase of dramatic innovation followed by continuous improvement. This philosophy causes greater risk and uses blockchain space differently, and so is inherently in conflict with Bitcoin Cash's vision of a stable, massively scalable, universal currency.

Over the last few years the Bitcoin Unlimited members have emphatically agreed with and supported a focus on innovative research. I am not aware of a single BUIP that was defeated on the grounds of being "too innovative". The result of this is a series of technologies, many of them requiring consensus changes, that are both envisioned and completed. For example, some of these technologies are deployed on the "NextChain" testnet located at (www.nextchain.cash).

Motivation

However, it should be completely obvious to all that there is minimal to zero use of and interest in testnet features that have no roadmap to deployment. Investing the time and effort to deliver even a simple "minimum-viable-product" based on these technologies will not happen. The most obvious barrier to such an effort is finding the venture capitalist willing to risk such an uncertain deployment. But the second is probably more important: displaying such a product on a testnet simply invites competition that can be fully ready by the time the required consensus changes are deployed in BCH. This defeats the first mover advantage that is essential to the success of most startups.

Without such products it is impossible to effectively communicate the value of consensus changes to the general public, and it is impossible to achieve the levels of use (and black-hat interest) that give individuals confidence in the underlying implementation. And even for those who can understand the proposed change at a technical level, any assessment of value is simply guessing at the future. So technology assessment remains a "crystal-ball gazing exercise" – some people will see value and some will not. In fact, some of the features will have value and some will end up as useless "cruft" complicating the blockchain. It's very difficult if not impossible to determine a priori which category a particular feature will fall into.

Proposal

Therefore, I propose that Bitcoin Unlimited create its own blockchain containing these features and allow it to gain whatever value the market gives it. This blockchain will NOT be a fork of Bitcoin Cash and it will follow a very different philosophy of dramatic innovation. To begin with, we will use a "white ball" approach to feature inclusion – if I, Andrew Stone, OR you the voters pass a BUIP, then the feature will go in (subject to the normal BUIP rules of providing an implementation, undergoing code review and security analysis, etc). So this blockchain will fill a different niche than Bitcoin Cash.

Despite being forward-looking, this new blockchain will maintain the same high standards expected of Bitcoin Unlimited. In particular, we will continue to take great care in implementation with regards to security and usability. But since the underlying token has value, it will allow startups to build products and services with the certainty of deployment on a blockchain with value. This will allow these companies to gain revenue, users, and the first-mover advantage before a possible transition to the more-broadly-adopted BCH blockchain. And this will allow the BCH blockchain to prove the value of a feature before making consensus changes.

Some of the initial deployment features will likely be:

A different POW algorithm (to prevent the chain from competing for ASIC capacity with BCH)
Smart contracting features: transaction introspection, OP_EXEC, OP_TEMPLATE (see the nextchain work around these) etc.
Tokens
A different block header
A different UTXO database structure which will allow UTXO commitments
Sound money
Fair launch – no premined coins go to Bitcoin Unlimited, the blockchain's creator, or its developers, and there will be no coinbase tax.
2 minute average block interval
Specifically, this BUIP authorizes Bitcoin Unlimited to "officially" create, develop, and support such a blockchain, with the genesis block happening within a year, with a minimum of a 1 month advance notice.

All such development activities will occur within and as part of existing BUIP budgets. All prior BUIPs (such as Group Tokenization) can be satisfied by being initially deployed on this new blockchain and being proposed for BCH via the CHIP system and supported throughout the BCH evaluation.

Budget

Furthermore, this BUIP allocates 10000 USD annually to acquire and deploy hardware associated with this new blockchain – full nodes, explorers, web properties, and mining nodes. This money shall be provided solely from BTC donated prior to the creation of BCH. No funds donated after the creation of BCH and by implication no BCH will be spent on this new cryptocurrency.

This BUIP further creates a consulting position within BU with the task of sheparding new features through the CHIP process and into BCH, and allocates 30000 USD annually towards the payment of this individual's time. The goal of this position is to engage with key BCH stakeholders to increase the likelihood of BU developed features becoming part of the BCH protocol.

Any additional funds requested for additional activities around this blockchain will require a separate BUIP, following normal Bitcoin Unlimited processes.

Precedent
Since the introduction of this BUIP, individuals have brought to my attention other coins that appear to benefit from similar system of a fast-moving experimental chain and a more stable high value chain. Here is a (possibly incomplete) list:

Polkadot and Kusama
From Kusama's description:

Kusama is a scalable network of specialized blockchains built using Substrate and nearly the same codebase as Polkadot. The network is an experimental development environment for teams who want to move fast and innovate on Kusama, or prepare for deployment on Polkadot.

Polkadot has a serendipitous interaction with us in that it was announced and presented in the same BU Arnhem Conference as Bitcoin Cash. In the interim, Polkadot has moved from a nascent (0 value) coin to exceeding Bitcoin Cash in market cap (according to coinmarketcap.com) and doubling Bitcoin Cash in exchange volume (according to cryptowat.ch). At the same time, Bitcoin Cash has dropped in market cap rankings from #3 to #13, and its price has dropped from a trading range of .2 to .1 BTC (I am including a range to be conservative – to ignore the new coin "pop") to a recent trading range of .0088 to .018 BTC.

Bitcoin and Groestlcoin
Groestlcoin has preceded the delivery of Bitcoin features throughout its history. It deployed segwit first, and and it launched Taproot first on its testnet. It uses a different POW algorithm and a 1 minute block time, which is a mirror of my choices. If you've developed in crypto, you'll have realized that a shorter block time is great for experimental services since it reduces the time a developer needs to wait around. Sure there is regtest and testnets where blocks can be produced faster, but at some time you still need to move to something with real money and it is essential to watch those initial transactions to make sure they are correct. This happens not once, but every time a new release or bug fix goes live on a value-carrying network.

Reddit r/groestlcoin - Groestlcoin Dec 2020 Release
https://www.reddit.com/r/groestlcoin/comments/kics9f/groestlcoin_dec_2020_release/

Bitcoin and Litecoin

Any long time BCHer should know very well how Litecoin was used competitively against BCH as the Bitcoiner's temporary answer to scalability. "Just use LTC for your daily use now and BTC will deliver lightning soon." Although unquantifiable, I feel that this argument was extremely damaging to BCH since our story centered on scalability. Why is this relevant to this BUIP? Because we can use a similar argument for various forward looking features such as miner validated tokens and smart contracts: "deploy on this new chain now, while waiting for BCH to complete its integration".