

Bitcoin Unlimited: Articles of Federation

Bitcoin is at a crossroads that will determine whether it becomes a worldwide public good, embodying a trustless ledger and currency for all people, companies, and financial institutions worldwide.

The Bitcoin Unlimited project seeks to provide a voice, in terms of code and hash power, to all stakeholders in the Bitcoin ecosystem. As a foundational principle, we assert that Bitcoin is and should be whatever its users define by the code they run and the rules they vote for with their hash power. This project seeks to remove existing practical barriers to stakeholders expressing their views in these ways.

We see in the Bitcoin ecosystem many companies, groups and economic actors that have made large investment decisions based on maintaining the current trajectory of growth – a growth that would naturally ensue if Bitcoin is available as a public good. These include payment processors, micro-payment solutions, exchanges, merchants, and more. We recognize the importance of the mining industry and the necessity to increase transaction revenue to support its growth as the block subsidy decreases. This growth is aligned with the interests of the Bitcoin network as a whole since it increases network security.

In the Bitcoin Core variant, we do NOT see a venue for these actors to formally express their desires in regards to the evolution of the network. Instead we see a project controlled by a small group of developers employed by finance-oriented for-profit startup companies, and the emergence of corporate products (Lightning network, Side-chains and permissioned ledgers) that would materially benefit from a Bitcoin network that is incapable of handling the transactional demand required for a worldwide public good.

Whether these corporate developers are intentionally acting against the long term success of Bitcoin is irrelevant. In cases of potential conflict of interest, the moral and socially accepted behavior is to recuse oneself from a position of determination. Instead these developers insist on a poorly defined consensus for determining the development of a MIT licensed code base which they did not initially create. This tactic has had the opposite effect of recusal, giving themselves veto power over any changes. This has stalled all improvements on the block size issue in the Bitcoin Core variant.

Bitcoin Unlimited perceives itself as an important element in the Bitcoin ecosystem. We believe our founding statutes are firmly based on Satoshi's original vision. However, we acknowledge that Bitcoin is fundamentally a decentralized system and thus we will not assert centralized ownership of the protocol.

Article 1: A Peer-to-Peer Electronic Cash System for Planet Earth

I. Satoshi's original vision--a scalable Bitcoin

Bitcoin Unlimited adheres to Satoshi Nakamoto's vision for a system that could scale up to a worldwide payment network and a decentralized monetary system. Transactions are grouped into blocks and recorded on an unforgeable global ledger known as the Bitcoin blockchain. The Blockchain is accessible to anyone in the world, secured by cryptography, and maintained by the most powerful single-purpose computing network ever created.

II. Governed by the code we run

The guiding principle for Bitcoin Unlimited is that the evolution of the network is decided by the code people freely choose to run. Consensus is therefore an emergent property, objectively represented by the longest proof-of-work chain. This fact is an unassailable property of Bitcoin and cannot be changed by fiat.

The final sentence of the Bitcoin white paper states:

They [nodes/miners] vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. *Any needed rules and incentives can be enforced with this consensus mechanism.*

It is this mechanism of "voting with their CPU power" that keeps Bitcoin permissionless and uncensorable. Were it possible to compel miners to run a specific application with a specific set of rules then it would be trivial for the owner of the codebase to, for example, invalidate transactions, modify the inflation schedule, block certain bitcoin addresses or IP ranges, limit the quantity of transactions in a block, or implement any other centralized policies.

In other words, Bitcoin only maintains its intrinsically valuable properties of being permissionless, uncensorable, trustless, and uninflatable, precisely because the software is not, and should not be, controlled by any single governance entity.

III. What makes a valid block?

From the Bitcoin white paper, "*nodes accept the block only if all transactions in it are valid and not already spent.*" A block cannot be invalid because of its size. Instead, excessively large blocks that would pose technical challenges to a node are dealt with in the transport layer, increasing the block's orphaning risk. Bitcoin Unlimited nodes can accept a chain with an excessive block, when needed, in order to track consensus.

IV. Values and beliefs: adoption is paramount

Bitcoin should freely scale with demand through a market-based process. The user's experience is important -- we seek to engage with all people. Therefore, low fees are desirable. As the block subsidy declines, miners can make money based on volume, not exclusivity. As the Bitcoin network grows, the limitations of the underlying transport and storage technologies will naturally create a fee market -- and this market will naturally fluctuate with supply and demand and properly track innovations in the underlying physical technologies.

It is understood that instant (0-conf) transactions intrinsically less secure than confirmed transactions. 1-conf transactions are less secure than 2-conf, etc along the continuum. Since 0-conf transactions are practically useful to people, we encourage innovations that enhance their security without undermining the other key properties of the Bitcoin network.

Resistance to censorship and security improves with adoption -- the more actors in a peer-2-peer network, the harder it is to gain control of an influential percentage.

V. Technical: put the user in control

Any software can join the Bitcoin network because it is a permissionless decentralized ledger. If adding code that allows users to easily change the behavior of their node puts the entire network at risk, then the network is at risk today. But we reject this idea. Instead we believe that the free market and dynamic network will eliminate bad actors, that differing implementations and behavior make the network more robust against attackers, and that a heterogeneous network will allow "good actors" to discover and fix potential problems before the bad actors do.

VI. Politics: Bitcoin is interdisciplinary

The voices of scientists, developers, entrepreneurs, investors and users should all be heard and respected.

Article 2: Confederation

I. All Bitcoin Unlimited (henceforth BU) activities shall be recorded and be publicly accessible.

II. BU roles shall consist of:

President: a publicly identified (real-life identity is known) BU Member who is responsible for the ongoing activities of the confederation. The president shall assign BUIP numbers, organize BUIP discussion, and voting.

Secretary: a publicly identified BU Member who is responsible for recording activities and vote results, and making this information publicly available. The Secretary is responsible for creating, maintaining and moderating a public forum where discussion can be held. Moderation is exclusively limited to moving content with an indication of it being moved – no content may be deleted.

Developer: a publicly identified BU Member who is responsible for maintaining the BU code repository, choosing which committers have access to the software repository, reviewing and merging patches, and periodically releasing BU software. The Developer is an outreach position – s/he must actively work to encourage others to work on submissions, and to convert one-time submitters into regular committers.

Pool Operator: a publicly identified BU member who is responsible for running the BU Mining pool as specified in Article 4. The position of pool operator might be vacant and pool operation is optional, as resources permit.

Member: an individual who is invited (by BUIP) to join the Confederation, signs this document, and has voted within the last 1 year. Non-publicly identified members may have restricted voting or other restrictions as determined by subsequent BUIPs – this measure may be needed to restrict duplicate accounts.

Officer term is for two years. For continuity, elections shall be staggered by 6 months and take place 1 week prior to responsibility transfer. Beginning with the President on Jan 15, 2018, then Secretary, Developer, and Pool Operator. This means that the initial officer term may exceed 2 years. Voting for all the initial officers shall occur on Jan 15, 2016.

III. Formal interaction between members, including but not limited to BUIP submission and voting must occur via cryptographically verified identities. Members shall supply a Bitcoin public key when applying for membership and sign all formal communications with the corresponding private key.

IV. Decisions shall be made via the following procedure:

Any member can propose a “Bitcoin Unlimited Improvement Proposal” (the Proposer). The Proposer can submit a proposal on behalf of another non-member. The president or secretary shall assign this Proposal a number and make it publicly accessible. The President, Secretary, or Developer has a 2 week opportunity to review the proposal and suggest modifications, within their own domain. That is, the President reviews proposals related to the operation of the Bitcoin Unlimited Confederation, the Secretary reviews proposals for adherence to BUIP standards, and the Developer reviews proposals related the the Bitcoin Unlimited code. The Proposer may choose to extend this 2 week period as long as desired.

After this period, the officers may attach an opinion or counter BUIP to this BUIP. This package shall be presented to all members and opened for discussion for a minimum of a 2 week period. The Proposer may choose to extend this period for a maximum of 6 months. At the end of the public discussion period, members shall vote whether to adopt the BUIP. A BUIP is adopted if accepted by a majority of voters (51%) with at least 50% of members voting, unless otherwise indicated in this document (BUIPs that change these articles or remove officers).

If a counter-BUIP is proposed, voting occurs in a twofold manner: first each member votes his preference, BUIP, counter, or none, with a 33% majority. Then if the BUIP or counter-BUIP wins, each member votes to accept it or not with the normal majority requirement. Note that members could make both votes simultaneously (I vote for the counter, but if BUIP wins I vote to accept it), depending on the Secretary's implementation of this process.

Voting shall be open for a 24 hour period. Members who will not be available during that period may submit an early vote in a manner described by the Secretary. Members may not change their vote. All votes are publicly recorded.

V. Additional BUIP requirements on patches.

If a BUIP contains a patch, the Developer may review the patch for acceptability (including but not limited to bugs, tests, coding standards) AFTER BUIP acceptance. The developer may work with the Proposer or other party for as long as necessary to ensure the patch is acceptable. After 2 months, if the Proposer believes that this process is taking too long, the President, Secretary, or Proposer may propose that the patch be included “as is”, via the same BUIP proposal channel and schedule a vote (normal BUIP majority rules). This vote may not occur within one 1 week of the formal “commit as is” proposal.

If the BUIP does NOT contain a patch but suggests technical changes, it is the responsibility of the Proposer or any other party to produce this patch. After the patch is produced, the Developer reviews it as suggested in the preceding paragraph, except in the “as is” case, the normal BUIP schedule and process must be followed. In the unfortunate situation where a

patch is deliberately accepted which does not agree with the Proposer's BUIP, the Proposer's recourse is to resubmit the BUIP with a patch.

VI. This document can be modified via a greater than 66% majority vote on a BUIP with at least 75% of the members voting.

VII. Elections occur via the following procedure. The Secretary (or President then Developer if the Secretary/President is vacated) announces vacancy or impending vacancy of a position to the BU public forum and an election date not earlier than 4 weeks subsequent to the announcement. Interested members submit a BUIP announcing their candidacy, real-life identity, and including any other desired information. Submissions can happen at any time. Public discussion of the candidates is allowed and follows the same mechanism as other BUIPs.

During the election, a modified BUIP voting process occurs where members vote for the candidate of their choice. If there are > 2 candidates, a second round of voting occurs solely between the 2 candidates with the most votes. Largest number of votes wins. Note that for expediency purposes, the Secretary may choose to collapse the voting operation into a single phase (where voters make multiple choices in a manner similar to the BUIP/counter-BUIP system) if the number of candidates is small enough to reasonably do so.

VIII. The President, Secretary, Developer or Pool Operator may voluntarily resign before term completion, via a signed public message posted to the BU public forum. In this situation, elections occur prematurely via the process outlined in VII starting from the date of resignation. In the case of abrupt departure, an interim person may be appointed by the President, including someone currently holding another role. In that case s/he will not vacate the originally elected role.

IX. An officer can be removed via a "no confidence" BUIP. This BUIP follows the normal schedule, however it must pass with a 75% majority of voters, with at least 33% of members voting. A BUIP advocating for the removal of a particular officer may not occur within 4 months of a prior unsuccessful proposal advocating for the removal of that officer. Removal proposals will be managed by an officer who is not affected by the BUIP. Multiple officer removal BUIPs are not allowed. Submit them separately.

X. If actions of the President, Secretary, Developer, Pool Operator, or Member is in violation of these rules, that is grounds for removal. Any member may submit a "no confidence" BUIP as per section IX. Members are exhorted to vote based on their belief as to whether the individual broke these rules rather than their personal opinion of the individual's fitness for the office. A removed officer may re-run for any position.

Article 3: Operations and Resources

This article provides guidelines for operations assuming that Bitcoin Unlimited becomes a non-profit corporation. Yet it also provides instructions for operations before that event occurs.

I. Any unallocated funds raised shall be held in a 2-of-3 multi-signature account with the President, Secretary, and Developer holding the keys. Fiat currency holdings shall only occur to ensure that commitments can be paid regardless of Bitcoin's volatility and shall be held either by the President or in a Bitcoin Unlimited non-profit corporation account.

Allocated funds may be held temporarily by the person who will employ them.

II. Funds donated to Bitcoin Unlimited may be applied to any purpose (including the Bitcoin Unlimited Pool) that furthers the project's goals and is authorized by majority vote via line items in a President's "Operational BUIP". Donations may not be used to pay salaries, bonuses, etc. for the President, Secretary, Developer or Pool Operator. These volunteer roles are unpaid, with the expectation that these individuals will benefit from Bitcoin's success.

However, the people fulfilling these roles may be paid upon completion of particular tasks that exceed their stated role. For example, the Developer may be paid to implement a particular feature -- however the time required to review and merge the feature is unpaid.

III. The source repository administrative account shall be held by the President. But the President may only add and remove committers on the recommendation of the Developer. Additionally, the President may not use his administrative account to directly commit software to the source repository. Instead, these contributions must be submitted as a fork or patch and be reviewed and merged by the Developer or another committer.

IV. All domain name registrations shall be controlled by the Developer.

V. Public Forum infrastructure shall be controlled by the Secretary.

VI. Source repository committers may commit to the master branch repository without explicit BUIP approval during the course of their day-to-day work. Commits that implement a particular BUIP should reference that document in the checkin comments. However committers have the responsibility to implement any large or potentially controversial change on a fork or branch and

bring it to Member attention via the BUIP process. Committers have the responsibility to respect the efforts of independent submissions by ensuring that authorship attribution is correct in the final commit to the BU repository. Committers must work respectfully with independent submitters to ensure coding, testing, documentation, and formatting standards are met as defined by the Developer.

VII. A Member that feels a commit needs BUIP approval can submit a BUIP referencing the commit arguing against the change. This change may remain in the repository until the issue is determined but the Developer may not issue (non-experimental) binary releases containing any commit that is under BUIP debate.

VIII. The Developer may release experimental features under the Bitcoin Unlimited brand, and develop them in Bitcoin Unlimited repository branches. However these releases must be named and advertised as distinctly separate from the primary Bitcoin Unlimited release. Additional flavors of release may also be recommended to be created by members through the BUIP process.

IX. Administrators of resources (source repository account, domain name, public forum, and any others) are responsible for paying for the resource for the duration of the administrator's term. However, these administrators should be compensated or pre-compensated out of BU funds if available, via an Operational BUIP.

X. The President may periodically issue a special BUIP called an "Operational BUIP" that details proposed payments and other organizational activities. This BUIP follows the same voting methodology as any other (detailed in 2.IV).

XI. The President, Secretary, Developer, or Pool Operator can issue (or issue on behalf of another member) a special BUIP called an "informative BUIP" which allows members to vote on a non-binding issue or question. These BUIPs allow the community to formally give feedback on future directions for the project. For example, an informative BUIP could be "Should we look into and then propose partnerships with hardware wallets?" Issuance is restricted to reduce BUIP spam.

Article 4: The Bitcoin Unlimited Mining Pool

I. Overview

Increasingly, users who have a strong vested interest in the success of Bitcoin control proportionally little hash power. The Bitcoin Unlimited Mining Pool seeks to provide companies and users a transparently run, not-for-profit, high payout, mining pool which explicitly supports global bitcoin adoption through Bitcoin Unlimited block creation.

II. Operation

The Pool will be run by the Bitcoin Unlimited Pool Operator and other real-identity-known Bitcoin Unlimited members as designated by the Pool Operator, with operational and mission transparency as key priorities. The Bitcoin Unlimited Pool will run Bitcoin Unlimited full node software.

III. Donator Incentives

Users, companies, and other ecosystem stakeholders will be incentivized to contribute to this pool as long as it supports their values. As has always been the case, hash power speaks loudest, and stakeholders ultimately exercise their vote via hashing.

IV. User Incentives

In the ideal case, donations will exceed operational cost, and therefore the Bitcoin Unlimited Pool will offer an overlay payout to participant miners, specifics to be decided by BUIP. This should build a strong base of hash power for the pool. Donations can be made for the specific purpose of supporting the Pool, as opposed to donations to the general Bitcoin Unlimited fund, and will be managed in a 2 of 3 (President, Secretary, Pool Operator) multi-sig account separate from Bitcoin Unlimited general purpose funds.

V. 51% Risk

To alleviate real or perceived risk of this pool gaining more than 50% of total network hash power, if the pool's hash power exceeds an average of 30% for more than 30 consecutive days, it must disband into two completely separate entities with no personnel overlap.

I, the undersigned, substantially agree with the Bitcoin Unlimited Vision as defined in Article 1 and agree to work towards the success of Bitcoin as defined by Article 1. I agree to follow the rules outlined in Articles 2,3, and 4 for all matters pertaining to Bitcoin Unlimited. I further recognize that becoming a member of the Bitcoin Unlimited Federation and simultaneously working to undermine the Bitcoin Unlimited Vision will inflict substantial harm on the other members of the Bitcoin Unlimited Confederation, including but not limited to, loss of Member's time quantified by the average hourly wage of a principal engineer in the USA, loss of member monetary donations, and loss of opportunity.