Set in Stone

prepared for

All users of the Bitcoin Protocol

by

The Metanet Membership Club,
with a conglomeration of its members, individuals, professionals,
businesses & other interested parties.

TABLE OF CONTENTS

Vigilantia Aeterna

Preface

Bitcoin does not fork. It has existed since 2008, though it has had its ticker symbol changed through forced necessity. BTC is not bitcoin, BTC is an altered bastardization of the protocol which does not work and never will serve the global world.

What occurs is that organized nefarious groups steal the ticker symbol and then proceed to illegally copy the database and then imitate the real bitcoin whilst fleecing the masses and passing off with their illegal imitation.

Users need to be aware of this ticker stealing tactic from organized nefarious groups.

Bitcoin exists under the ticker symbol BSV. The ticker BSV stands for Bitcoin Satoshi Vision.

This document describes the Bitcoin Protocol. There is no earlier edition of this, the text from this document draws its information from the Bitcoin White Paper, the Bitcoin Code and the writings of Dr Craig Steven Wright under the moniker of Satoshi Nakamoto and from under his real name within the Metanet Membership Club. It also draws upon the contributions of the Metanet Club members. This document will clarify a lot of details about bitcoin in an easy to read and digest format that is aimed at all users across the sector. With huge thanks to Craig for guidance, teaching and mentoring.

Joel Dalais
Editor
February 2022

1. INTRODUCTION

The Bitcoin Protocol is an information commodity. The first application was use as electronic cash, it has many other applications. The various potential applications can be measured in its utility. This document will not discuss the unmeasured utility as the totality is unknown and is down to human ingenuity over time.

This document covers the base bitcoin protocol. It defines what should never be changed and the aspects of what Set in Stone covers and means. The expectation is that readers research what they do not understand, as this document will attempt to explain itself to the majority of people but understands that it cannot reach all people.

A copy is uploaded to the blockchain with the relevant hash shown below.

Any newer versions will always reference the previous copy, so if ever needed a chain of this document can be followed.

We expect, and hope, that generations of the future will understand the work and efforts we had to go through to bring this to you and that you keep it (bitcoin) safe so that it may continue to serve you and the generations after you.

<< tx hash of the uploaded copy >>

<< previous version >>

1.1. Motivation

Base protocols should remain static so that software, individuals and businesses that rely upon on it need never worry about a shifting foundation. And if we are to expect bitcoin to last far into the future as the basis for many products and services, then we need to understand and accept the base protocol. It also needs to be done in such a way so that it can not be misinterpreted by accident or purposefully.

The initial ten years of Bitcoin's existence was met with a lot of tampering and manipulation to break and subvert the technology. Even to date there are those that attempt this. And it is expected that this trend will continue. We foresee that every generation will put forward individuals and groups that try to "fix bitcoin", and in the process will do their best to break and subvert it.

Bitcoin is a fixed protocol that has very few caveats for change, such as the spare op_code requirements which is discussed later in this document. Albeit from that, bitcoin continued throughout its first ten years through name changes the base protocol was saved and restored under the name of Bitcoin Satoshi Vision (BSV). Now there are no more repairing required.

There has however been some friction due to people not understanding the scope of the bitcoin protocol, as to what exactly is 'set in stone'. Because of this there are those who innocently, or maliciously, try to alter the base protocol. This document will lay out what is Set in Stone regarding the base protocol, what should not ever be changed.

1.2. Scope

This document does not cover in-depth technical analysis or code. It is not a discussion or debatable document. It defines the Bitcoin Protocol in a hopefully understandable format for the majority of users.

The uploaded blockchain document will be updated and this document will contain the new hash and the previous.

You are not meant to change the scope of this document, you are not meant to change the bitcoin protocol. Do not attempt to use later versions of this document to introduce changes to the base protocol. We are clearly stating this in this original 1st version of this document so that it may be a reference point into the future and as needed.

1.3. About this Document

This document coalesces information from the Bitcoin White Paper, the Bitcoin Code and the writings and words of Satoshi Nakamoto (Craig Steven Wright), the inventor of Bitcoin. The white paper is the unilateral contract, the code is the technical software and the writings and words of Craig Wright are akin to the complimentary footnote explanations attached to both the white paper and the code.

This document combines all of the above in a format that is agreeable to most. It offers a brief explanation of some of the protocol technical purposes and some of the philosophical basis for functions and workings of bitcoin. If the reader wishes a more in-depth understanding of either the contract, the code, or the philosophy, then the reader is advised to conduct research through readings, videos and interactions with professionals within the sector.

2. PHILOSOPHY

2.1. Bitcoin and Law

Bitcoin is friendly and complimentary to law and the legal process.

One of the key principles of bitcoin is that it works under the legal umbrella. It is a pseudonymous system that provides privacy which adheres to GDPR laws. It is the duty of businesses and software providers that utilize PII (personal identifiable information) to run their business or software in conjunction with bitcoin in a way that does not reveal their customers PII.

With regard to international money tracing laws, there is nothing better than bitcoin, which as a public ledger, does not require court orders to trace. Though in many cases old fashioned police work will certainly still be required, the weight of difficulty is lifted somewhat and the potential of following criminal or corrupt endeavours is raised significantly.

Recovery and restitution is also significantly increased, though in many cases individuals or businesses will still require a court order for recovery, the fact is that freezing and recovery can still be instigated no matter the country criminals might try to move the bitcoin capital into. Businesses and projects that seek to assist criminal endeavours are strongly advised not to, that they should follow AML and KYC practices for their own protection.

Over time criminals and corrupt practices will see that bitcoin is not a good tool to operate within. And it will be left for the more honest and transparent individuals, businesses and governments who will be able to capitalize on its efficiency-boosting utility and methods to better serve their people and their legal framework.

2.2. Bitcoin and Economics

The Bitcoin fee market is meant to be many small transactions that accumulate into blocks and are rewarded alongside the subsidy. The subsidy, otherwise known as the block reward, is halved constantly with the intention of being replaced by the transaction fees.

It is not meant to be a few transactions at a high value. The fee market is many transactions at very low value that will replace the subsidy as the primary revenue for miners processing transactions and blocks.

Miners can mine whatever fee rate they want. There is no obligation or contractual statement that dictates that they must mine all transactions at any given fee rate. Miners decide what is best for themselves depending on the number of transactions available and their own hardware and software capabilities.

The 21 million coins were issued at the outset of bitcoin, the distribution is what is known as the mining subsidy.

Do not try creating more decimal places. This will break the contract and break the economics of bitcoin. If you require more lower value denominations you can capitalize on payment channels and fiat denominations built as tokens.

2.3 Bitcoin and Software

The software and technical code is the last part of importance, behind the need to be lawfully compliant and to have a working economic system. It is still an important part that no one should tinker with. There is an unbounded space for creating protocols, new languages and software on top of the base protocol.

The op_codes form a type of script language, the Bitcoin Script Language (BSL). This language functions as a predicate system. There can be many other languages built on top, this is done by compiling the script code (op_codes) to execute in the manner that you require. These languages built from the script are known as Higher Programming Languages, built on Bitcoin, or simply HPL.

You can code directly with the BSL, or you can use a HPL. A HPL can be read easier by a majority of programmers and are the primary source of what most bitcoin software development will use.

All the op_codes required already exist, there does not need to be any more. If you cannot build what you want it is because no one has discovered how, not that it is not possible.

If you wish to see the documentation of the code you can use the reference client's documentation [3].

2.4 Capitalism

Bitcoin is a capitalist system. Not an anarchist, or anarcho-capitalist, or crony capitalist, or anything else. It is a capitalist system.

Individuals and businesses can use bitcoin to increase efficiency and thereby increase profit, productivity and social effectiveness, depending upon their requirements and application of the technology.

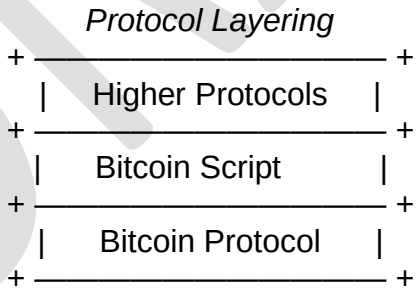
Bitcoin is not a tool that will automatically get rid of crony capitalistm and corruption, it still needs to be wielded by those with good morals and the intention to bring about better and more efficient services and products.

It lowers the trading threshold, for national and specially for international trade.

2.5 Relation to other Protocols

There can be many other protocols built on top of the main base bitcoin protocol, for example the Paymail protocol. These other protocols can also be patented to protect the inventor and bitcoin at large.

Creating and running these protocols will have no effect on the base protocol. If any of these protocols require a change in the base bitcoin protocol, they should be reconsidered by their inventors and constructed in a way that does not require any base protocol changes as no base protocol changes will occur to accommodate such protocols.



3. FUNCTIONAL SPECIFICATIONS

3.1 OP_Codes

There is no need to add new op_codes. The codes that exist form a type of script language, the Bitcoin Script Language. All other programming is possible through the use of this script language.

If you feel like you need more op_codes, then you should consider your methodology and that you just have not figured out how to do what you want to do with what is available.

The spare op_codes are left as an important requirement in case sha256 is ever compromised, which has the potential to occur sometime in the distant future. The spare op_codes are not there for you to add in your own specific op_codes because you can not figure out how to do the things you want with the current op_codes.

Do not add more op_codes.

3.2 Difficulty Algorithm

The medium for block solving is 10 minutes. It is not meant to be lower, or higher. The target for adjustment is meant to be every 2016 blocks, which equates to roughly two weeks with a median of 10 minutes.

3.3 Total Units

The total amount of bitcoin is approximately 21 million.

Each bitcoin is dividable to 8 decimal places.

This makes for a total amount of 2.1 quadrillion units.

The smallest unit is known as a Satoshi, which is 0.00000001 of a bitcoin.

If you require smaller denominations you are expected to use tokens built on top of bitcoin that can be used as fiat denominations or other similar instruments.

Do not create more satoshi or bitcoin, this will destroy the economic model and break the unilateral contract. Do not create more decimal places, this will destroy the economic model and break the unilateral contract.

The subsidy halves every four years until it disappears.

3.4 Transaction Processing

New transactions are broadcast to all nodes. If a node gets a transaction, it sends it.

If it has zero fees – it sends it.

The node can choose to include a transaction in a block or not if there are no fees.

Miners are not obligated to accept your transaction. They can process as many, or as few transactions as they want. This may differ from miner to miner depending upon their software, hardware, and any specialisation they might be offering.

Miners are not obligated to accept transactions at any specific fee rate. They can set their own fee rate for acceptable transactions and will have to compete with other miners who are willing to accept lower or higher minimum transaction fee thresholds.

Miners can prune data if they want to.

Transactions can be sent straight to a specific miner if so chosen.

It is expected that miners will offer competitively lower rates so that they can capture more of the transaction fees.

3.5 Bitcoin Nodes

Bitcoin nodes are Mining nodes.

If you are not producing a block within the space of every 2016 blocks period you are not a node. Blocks should generally include transactions, they do not have to, but they should as otherwise the miner is not properly competing and would be losing the fee revenue.

Developers, businesses and similar can use the node software for their own means, for running their projects or businesses, but if they are not producing blocks, they are not a node.

Nodes enforce rules, they do not create them. They accept the unilateral contract that is the white paper, that is to process transactions and produce blocks, and in turn, be rewarded with the subsidy and fee revenue as a reward.

There are two races, block creation and block propagation.

The subsidy from block creation will not mature until 100 blocks have passed.

You can specialize mining nodes.

3.6 Block Size

Bitcoin blocks are unbounded in size.

A specific limit (like 1mb) is not part of the protocol.

Miners can set themselves limits, this is a deterministic choice for themselves. The Bitcoin code can enable an unbounded size of blocks.

Miners are expected to determine the number of transactions to include and when to propagate a solved block based upon their own metrics.

REFERENCES

[1] Craig S Wright (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
https://craigwright.net/bitcoin-white-paper.pdf

[2] Craig S Wright (2022). A rational Argument around Nodes.
https://craigwright.net/blog/bitcoin-blockchain-tech/a-rational-argument-around-nodes

[3] Documentation for Miners.
https://bitcoinsv.io/documentation/miners/introduction-miners/

[4] OP_Codes used in Bitcoin Script
https://wiki.bitcoinsv.io/index.php/Opcodes_used_in_Bitcoin_Script