Module #2.4

There’s no innovation happening in Bitcoin

There’s no innovation happening in Bitcoin

2.4 There’s no innovation happening in Bitcoin

> **The creation of a thousand forests is in one acorn.**
>
> Ralph Waldo Emerson,
> American essayist

Critics often attempt to claim that Bitcoin is 'old' or 'dead' technology because it does not change the base layer protocol as often as competing blockchains. This claim ignores both the reasons why changes to Bitcoin are adopted slowly and the amount of innovation happening to scale the network on higher layers, such as the Lightning Network. It also ignores that many of our most flexible and durable technologies also do not scale quickly on the base layer.

For example, there's also no innovation happening in Transmission Control Protocol (TCP), which underlies the internet. TCP was first created in 1974. The last time TCP was updated was in 1982. It does what it needs to do. It’s not perfect, and there are debates about whether we need to upgrade IPv4 to support future internet developments. However, to say that there has been no innovation in the internet since 1982 would be a remarkable claim. All this innovation has been ‘on’ TCP, rather than ‘in’ it.

The vast majority of innovation that’s happening is not ‘in’ Bitcoin but ‘on’ Bitcoin. One day there will likely be no innovation ‘in’ Bitcoin, and that should be a target and not a criticism, as it will be a reflection of how fundamental it has become in supporting the global economy by providing the foundations for global, neutral and permissionless sound money. Money that is sound both in the economic sense that there is fixed supply and an immutable ledger, but also sound in technological terms as it doesn’t change and what’s running has had years of uninterrupted uptime. Bitcoin has already achieved 100% uptime over the last 10 years.

However, it would be a concern if no innovation were happening ‘on’ Bitcoin.
Let’s take a look at that over the last 10 years:

'In' Bitcoin

Segregated Witness (SegWIt) was implemented in 2017 to protect against transaction malleability and to increase block capacity. SegWit was also a necessary precursor for lightning and some side chains to work efficiently.

Taproot was implemented in 2021 to allow batching and validating of multiple signatures by incorporating Schnorr signatures, introducing a scripting language to allow for more complex functionality and increasing the privacy and censorship resistance of transactions.

'On' Bitcoin

Liquid Sidechain

The Liquid sidechain was implemented in 2018. Liquid, like other sidechains, is a separate blockchain ledger that is linked to the main Bitcoin blockchain, according to a predefined set of rules. These rules are flexible enough to allow the Liquid chain to develop and incorporate design and scalability enhancements over time. However, the link to the Bitcoin blockchain ensures the total 21 million supply cap of bitcoin is consistent across both chains.

The asset in Liquid, L-BTC, is two-way pegged to bitcoin on the main chain. There are cost, speed, privacy and security trade offs which make L-BTC ideal for some applications. Cost, speed and privacy are all improved with L-BTC, at the expense of placing some trust in the organisations making up the Liquid Federation, who between them control an 11 of 15 multisig process to peg in and peg out L-BTC to bitcoin and vice versa.

Lightning Network

The Lightning network was implemented in 2018. Lightning is designed to be a peer to peer payments network in the form of a graph of nodes connected via channels; it is not a blockchain. Bitcoin is locked by a node runner on the main blockchain in order to make it available for use on the Lightning Network, this ensures that only 'real' bitcoin is used. Nodes can then open liquidity channels via multisig smart contracts with each other. Payments find routes through the network from source to destination, optimising for cost against the requirement that sufficient liquidity exists in the right direction between each node step in the route. The Lightning Network massively improves cost, speed and privacy in return for a loss in security (or increase in trust required) and increase in complexity. However, it is intended for high volume, low value day-to-day payments, so this is considered a very reasonable trade off for its millions of daily transactions (source: River, 2023).

Chaumian eCash Mints (David Chaum, 1983)

Fedimints can be thought of as a community-bounded lightning network. They are designed to leverage the inherent trust that exists within certain communities (eg. families, villages, friendship groups) in return for simplifying the complexity and enhancing privacy for users. They are modular, open source protocols to custody and transact bitcoin in a community context. They are interoperable with the Lightning Network itself.

Cashu is a bearer token that can be stored on a device such as a mobile phone; the design is aimed at reproducing the benefits of physical cash but in a digital form. Cashu is an example of Chaumian eCash built on Bitcoin and increases privacy and censorship resistance and reduces complexity in return for trusting the eCash mint being used. Cashu mints issue eCash tokens, representing bitcoin, that can be spent by users without revealing their identity. Cashu is interoperable with the Lightning Network.

There are likely to be many more layer 2 applications built in the future, with many layer 3 applications in turn built on top of each of those.

As an example of the incredible number of applications being built on top of Lightning, below is an extract from a Lightning Network Research Report by River, 2023:

The Lightning Network Industry Market Map 2023

WALLETS & EXCHANGES

Non-custodial wallets

Phoenix, Breez, Zeus, Blixt Wallet, muun, LNbits, ELECTRUM, Mutiny, Bitkit, NAYUTA, lipa

Lightning top-up

Azteco, POCKET

Neobanks

Cash App, strike, bitnob, Bipa, belo, Chivo, XAPO BANK, NOAH.

Custodial wallets

Wallet of Satoshi, blink, Cashu, Satoshi, Machankura, coinos, AmberApp, VIPSats, Current, LifPay, SPARK WALLET, WALLETANO

Exchanges supporting Lightning deposits/withdrawals

RIVER, Buda.com, BITAROO, BITFINEX, okcoin, CoinCorner, OKEX, BULL BITCOIN, vbtc, SIMPLEFX, kraken, BL3P, PrimeBit, BINANCE, osmo, BitcoinVN, Mt Pelerin, Rain, coinfinity, UNOCOIN, ripio, Pouch.ph

Wallet interface

Alby, Joule, Lightsats

Non-fiat exchanges supporting Lightning

SIDESHIFT.AI, southXchange, FIXED FLOAT, ZIGZAG

USE CASES

Gaming

THNDR, ZEBEDEE, Pnk frg

Rewards and Earnings

Apollo, sMiles, Mash, FOLD, Slice, opentip, The Bitcoin Company, Crypto Parrot, joltz REWARDS, VIDN, Satsback.com

Marketplaces with Lightning deposits/withdrawals

Bitrefill, Civkit, niceHash

Crowdfunding

GEYSER, >_OpenSats

P2P Marketplaces

OSHI, Gigsats, BitEscrow, Scarce City, microlancer.io

Lightning native finance

LN markets, Boltz, Kollider, ROBOSATS, STROOM, Loft

Lightning native browser

IMPERVIOUS

Podcast and Streaming

Fountain, PODCAST INDEX, podfans, SHOCKNET, Conshax, WAVLAKE

Social apps

damus, Amethyst, SPHINX, primal, JUGGERNAUT, ZION

Community tech

Fedi, Orange Pill App

Smart contracts

RGB

Communities

PLEB NET, PlebLab_, bitcoin lake, Diamond Hands

INFRASTRUCTURE

Implementations

LIGHTNING LABS, Blockstream, ACINQ, ELECTRUM, LIGHTNING DEV KIT

Development

Spiral, chaincode, Polar, Talaia Labs

Lightning API

RIVER LIGHTNING, opennode, LIGHTSPARK, IBEX, Breez, Alby

Node infrastructure

Galoy, VOLTAGE, BLOCKDAEMON, GREENLIGHT, Bitnoder

Node management software

VLS, Torq, MYNODE, Umbrel, START9, RIDE THE LIGHTNING, RASPIBLITZ, ThunderHub, Citadel, PYBLOCK, bolt.observer

Merchant payment processing

BTCPAY, Speed, bitpay, flexa, BitKassa, synota, MUSQET, LNPAY, ElenPAY, coingate, neutronpay, The Bolt Card, CRYPTOCONVERT, Satimoto, Swiss Bitcoin Pay, MOON, Bolt Ring, zaprite, Scrib, Coincards

Liquidity services

Loop, Deezy, FLOW, Blocktank, LQwD, THOR CHANNELS, LNBIG, lightning network+, AFRICA FREE ROUTING, In2me.com, Lightning Pool

EMPOWERMENT

Startup accelerator

Wolf

Data & Analytics

AMBOSS, mempool, BTCMap.org, Roylio, 1ML, BITCOIN VISUALS, SparkSeer, LnRouter

Created by RIVER