Master’s in Quantitative Economics - Digital Economics Track

Solidity and Smart Contract Development

Bitcoin and Open Source

Ibukun ADEBAYO & Andrés FIALLOS

January 2026

Dauphine | PSL
UNIVERSITÉ PARIS

01

The Past

Bitcoin’s Context

Digital Currencies Before Bitcoin

- **The "Trusted Third Party" Problem:** pre-Bitcoin systems failed because they relied on a central mint to prevent double-spending. If the mint was shut down or corrupted, the currency failed. **Specific Failures:**
  - **E-gold (1996):** Backed by gold but managed by a centralized entity (Gold & Silver Reserve Inc.). Shut down by the US DOJ in 2008 due to regulatory non-compliance.
  - **Liberty Reserve (2006):** A centralized digital currency service shut down for money laundering.
- Satoshi's Goal: A Peer-to-Peer Electronic Cash System.
  - **A trustless, decentralized ledger that removes the need for financial intermediaries.**

Bitcoin: A Peer-to-Peer Electronic Cash System

(Published Oct 31, 2008).

"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."

The Double-Spending Problem

Solution: A distributed timestamp server that publicly announces all transactions.

- Hashing transactions into an ongoing chain of Proof-of-Work, creating an immutable record
- "One-CPU-One-Vote"

The Longest Chain Rule

The longest chain is considered the correct one because it represents the greatest proof-of-work effort.

Incentives

- Block rewards
- Transaction fees

> An attacker should find it more profitable to play by the rules than to undermine the system and the validity of his own wealth
>
> **— Satoshi Nakamoto**

02

The Present

Bitcoin’s Open Source Governance

Bitcoin Improvement Proposals

- "A design document providing information to the Bitcoin community, or describing a new feature for Bitcoin or its processes or environment."
- Formal documents that propose changes or upgrades to the Bitcoin network.
- Heavily inspired by PEP-0001 (Python Enhancement Proposal).

Source: BIP 2, BIP 3

Types of BIPs

Specification

Describes any change that affects most or all Bitcoin implementations, like changes to the network protocol, block/transaction validity, or interoperability.

Informational

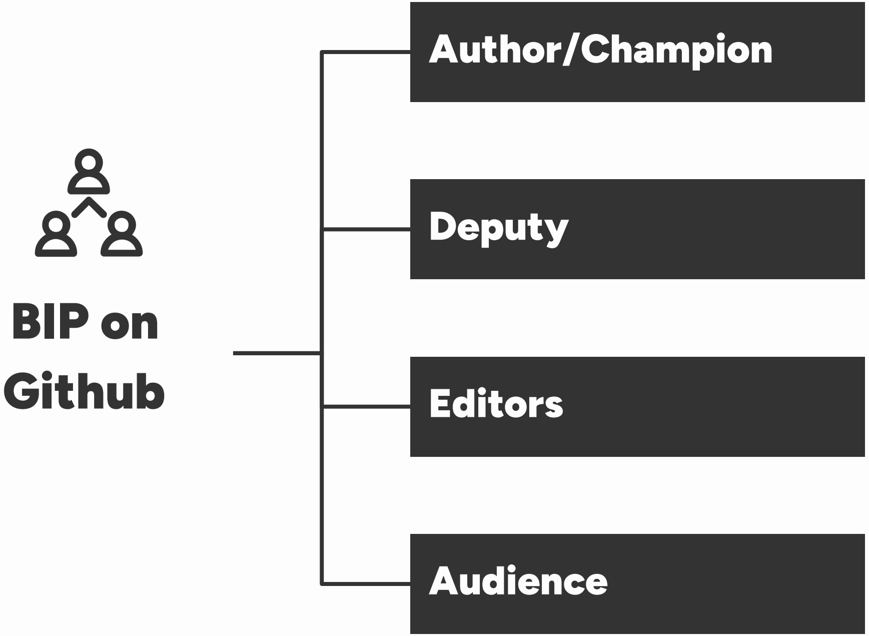
Addresses design issues or provides general guidelines, but doesn't propose new features.

Process

Describes a process surrounding Bitcoin, or proposes changes to procedures, decision-making process, or development tools.

Source: BIP 1, BIP 2, BIP 3

The Community



Author/Champion

Writes the BIP and is responsible for its progress.

Deputy

Assigned by the author to to act as a stand-in owner to help advance the proposal.

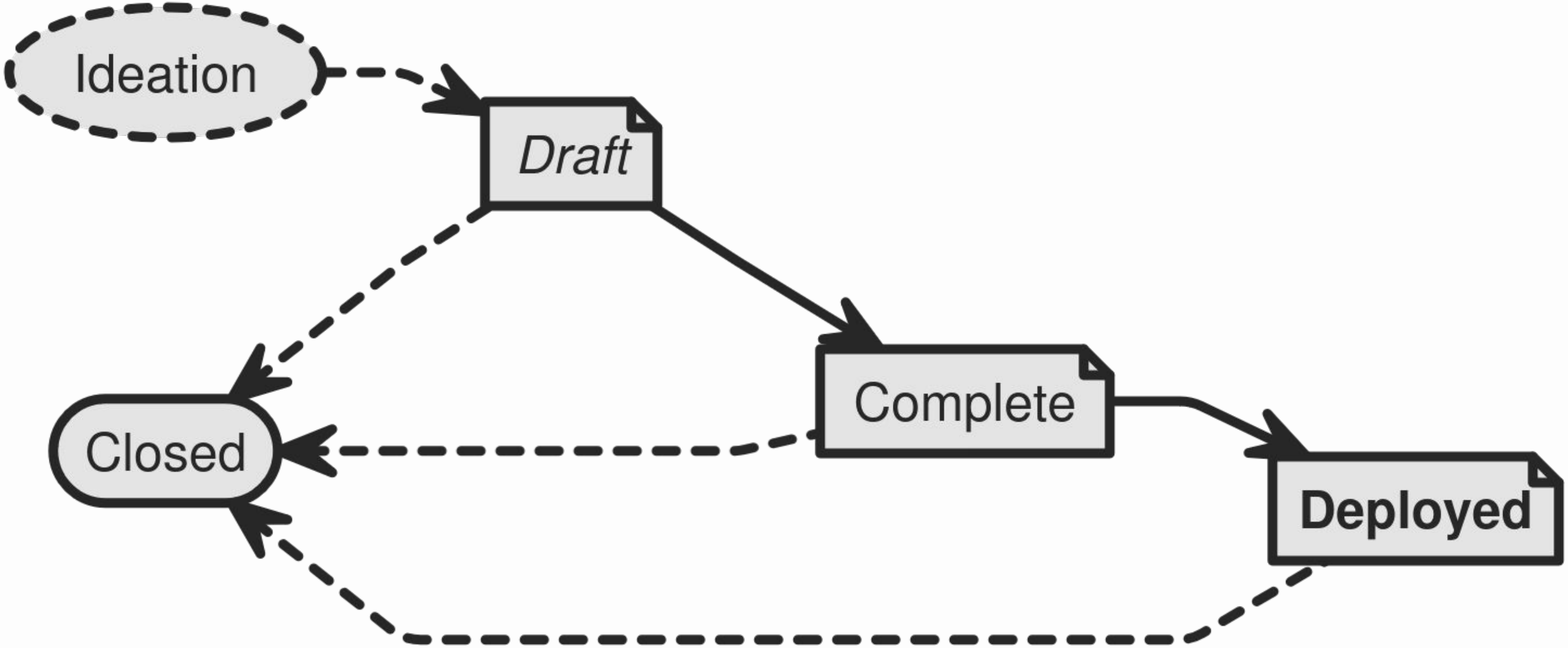
Editors

Assign BIP numbers, verify that proposals meet minimum formal criteria, and manage the status flow.

Audience

The peer-review engine. Composed of developers, researchers, and the Bitcoin-Dev Mailing List.

Source: BIP 2, BIP 3



Source: BIP 3

03

The Future

What's Next?

Development Trajectory and Open Questions

Evaluation of the BIP GitHub Community: Still Relevant?

- **Repository Health:** The repository is highly active but deliberately slow-moving to ensure security. It currently holds over 10,500 stars and 5,900 forks, with approximately 455 total contributors.

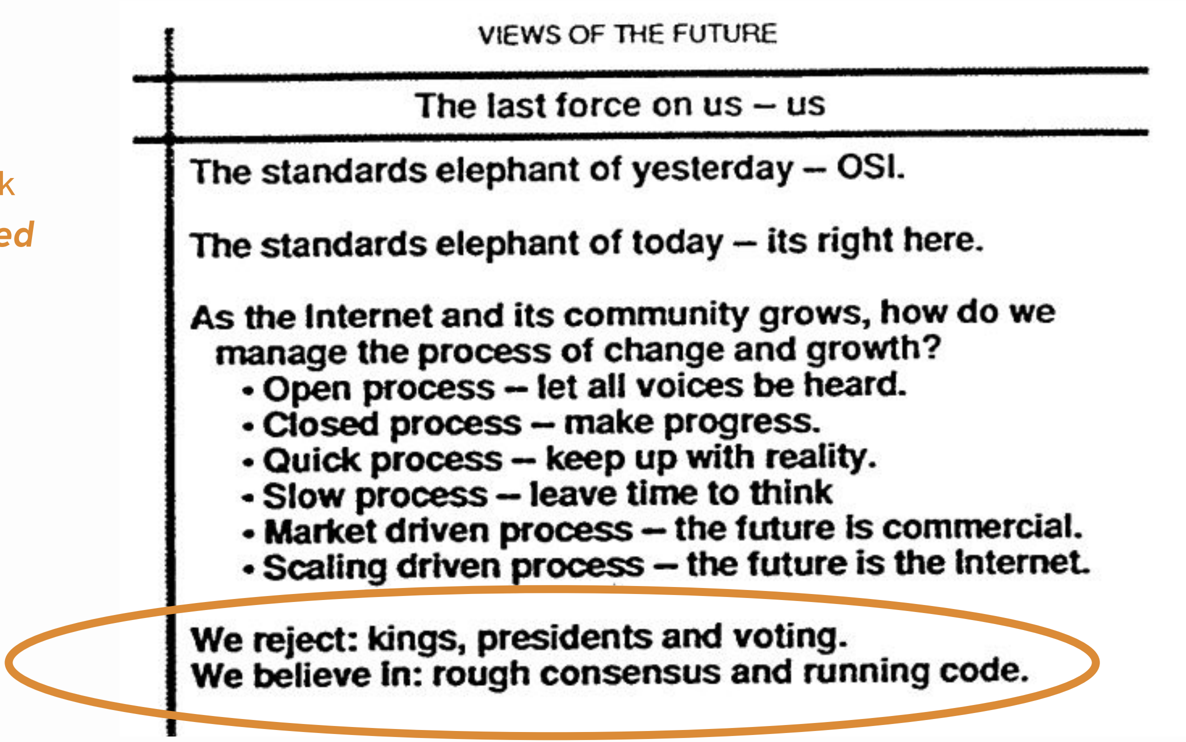
- **Culture**: The community prioritizes "rough consensus" over voting. Proposals often sit in the "Draft" stage for years (e.g., BIP 119: covenants) while technical debates occur on the Bitcoin-Dev mailing list rather than just GitHub issues.

Evaluation of the BIP GitHub Community: Still Relevant?

Rough Consensus:

The (**Internet Engineering Task Force**) IETF principle adopted by Bitcoin

You don't ask for permission to build on Bitcoin; you just write the code. If your code is useful, people will run it. If it is bad, they won't.



VIEWS OF THE FUTURE

The last force on us – us

The standards elephant of yesterday – OSI.

The standards elephant of today – its right here.

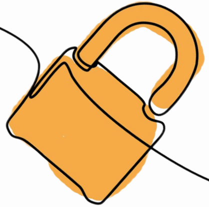
As the Internet and its community grows, how do we manage the process of change and growth?

- Open process – let all voices be heard.
- Closed process – make progress.
- Quick process – keep up with reality.
- Slow process – leave time to think
- Market driven process – the future is commercial.
- Scaling driven process – the future is the Internet.

We reject: kings, presidents and voting.
We believe in: rough consensus and running code.

***Source:** David Clark (1992). 'A Cloudy Crystal Ball- Visions of the Future'. MIT*

Future Development Outlook



The primary focus of Bitcoin development has shifted from "fixing malleability" (SegWit era) to **Covenants and Programmability.**

- **The Covenant Wars**

  The biggest upcoming battle is over which "Covenant" proposal to soft-fork into the protocol. Covenants would allow transactions to control how their outputs are spent in the future (e.g., "these coins can only be sent to this specific address"). **BIP 119 enables Covenants, the ability to put strict conditions on where bitcoins can be sent in the future, not just who can sign for them.**

Programmable money: *"This transaction requires Alice's signature to move, AND she can only send it to these specific addresses (or this specific transaction structure)."*

SCALABILITY + SECURITY

Open Questions and Outlook

Fee Security Model:

As block rewards vanish, the network must prove transaction fees alone can incentivize miners.

Quantum Resistance:

The community faces a time-sensitive race to upgrade to post-quantum cryptography before ECDSA keys are compromised **(Future UTXOs are safe due to Pay to Quantum Resistant Hash (P2QRH) , but all existing UTXOs are vulnerable)**

Upgrade Consensus:

Soft forks (backward compatible) are prioritized over hard forks to prevent network splits.

The Ossification Debate:

A growing ideological divide.

- Ossifiers: Keep the base layer unchanged for stability. **Ossify: slow down in the rate of change.**
- Reformers: Implement updates (e.g., Covenants) to ensure competitiveness. Does ossification freeze progress?

Conclusion

Thanks to Open Source Bitcoin is a Living Organism

- It is not static code. It evolves through a distinct lifecycle:

  Idea → BIP → Review → Consensus → Deployment

- The "open source engine" relies on a delicate balance of power between Developers, Miners, and Nodes.

Friction is a Feature, Not a Bug

- The difficulty of passing a BIP (like the Covenant debates) protects the network's immutability.
- Slow governance prevents the "corruption" that destroyed previous digital currencies.

The Unsolved Challenges

- **Scalability:** Scale without compromising the base layer?
- **Security:** Will transaction fees alone pay for security when the block reward hits zero?
- **Quantum Resistance:** Can the ship turn fast enough if encryption is threatened?

References

- Nakamoto, Satoshi. “Bitcoin: A Peer-To-Peer Electronic Cash System.” 2008.
- Bitcoin. (2020, December 3). *Bitcoin/Bips*. GitHub. https://github.com/bitcoin/bips
- Utxos.org. (n.d.). *BIP-119*. Retrieved January 21, 2026, from https://utxos.org/
- Bitbo. (2026). *What is a Bitcoin improvement proposal (BIP)?* https://bitbo.io/glossary/bip/
- Internet Engineering Task Force. (1992, July 13–17). *Proceedings of the Twenty-Fourth Internet Engineering Task Force*. Massachusetts Institute of Technology, Cambridge, MA. https://www.ietf.org/proceedings/24.pdf (See here David Clark (1992). *A Cloudy Crystal Ball- Visions of the Future*).
- Lopp, J. (2024, November 3). *On Ossification*. Jameson Lopp. https://blog.lopp.net/on-ossification/
- O'Beirne, J., & Sanders, G. (2023). *BIP 345: OP_VAULT*. Bitcoin Improvement Proposals. https://bips.dev/345/
- Parker, G. (2025, March 14). *Bitcoin's Next Major Upgrade? An Assessment of OP_CAT & OP_CTV*. Galaxy Research. https://www.galaxy.com/insights/research/bitcoins-next-major-upgrade-op-cat-and-op-ctv
- Westerbaan, B. (2025, October 28). *State of the post-quantum Internet in 2025*. The Cloudflare Blog. https://blog.cloudflare.com/pq-2025/