Bitcoin Fiscal Protocol (BFP)

A Minimal Decentralized Framework for Spend-Based Voluntary Contributions

Joan Smith
jo-smith@gmx.us

Abstract.

Bitcoin defines an open, predictable monetary system secured by decentralized consensus. However, fiscal mechanisms—how resources are contributed and allocated—remain opaque, centralized, and incompatible across jurisdictions.

This paper introduces the **Bitcoin Fiscal Protocol (BFP)**:
a deterministic, transparent fiscal layer that records **voluntary spending-based contributions** and anchors their auditability to Bitcoin.
BFP does not modify Bitcoin or create a new currency.
It provides a global, permissionless method for encoding fiscal rules, recording contributions, producing verifiable logs, and distributing pooled funds through transparent voting.

The protocol records only **spending events**, applying a **minimum 10% voluntary contribution** (“fiscal tip”), with optional additional contribution.
All resulting data structures are periodically committed to the Bitcoin blockchain for immutability.

1. Introduction

Bitcoin established a trustless monetary system through consensus, fixed issuance, and publicly verifiable state.Fiscal systems today rely on:

- centralized intermediaries,
- opaque processes,
- discretionary policy changes,
- fragmented jurisdictional tax rules,
- and unverifiable accounting.

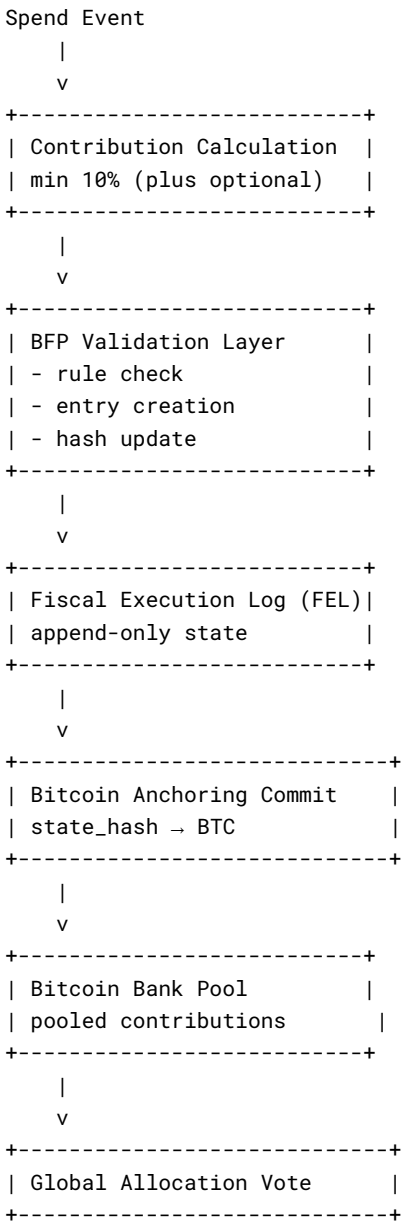
These systems create cost, friction, and lack of global coordination.

The Bitcoin Fiscal Protocol provides a minimal, interoperable solution:

- contributions are tied to **spending only**,
- users voluntarily add a **minimum 10% contribution**,
- entries are logged in an append-only structure,
- state hashes are periodically anchored to Bitcoin,
- pooled funds are allocated through global voting.

BFP is not a government system, not a taxation authority, and does not require identity.
It is a rule-execution protocol available for any voluntary institution.

2. System Model Overview



3. Contributions: Spending-Only Fiscal Model

BFP records only **spending**, not income.
Each spend event triggers a contribution:

```
contribution = max( amount * 0.10 , user_extra )
```

Users may increase their contribution above 10% at will.

This model ensures:

- simplicity,
- predictable contribution dynamics,
- privacy (income is never tracked),
- voluntary compliance,
- universal applicability across systems.

4. Contribution Flow

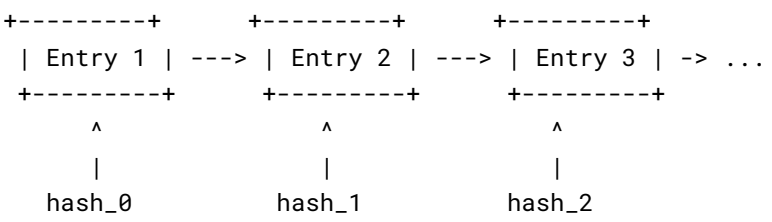
```
User Spends Money
      |
      v
10% Minimum Contribution
      |
      v
Optional Extra Contribution
      |
      v
Fiscal Entry Created → Logged in FEL
```

Each entry contains:

```
spend_tx_id
amount_spent
contribution_amount
signatures
timestamp
prev_state_hash
state_hash
```

5. Fiscal Execution Log (FEL)

The FEL is an append-only log similar in structure to a hash-chained ledger.



Properties:

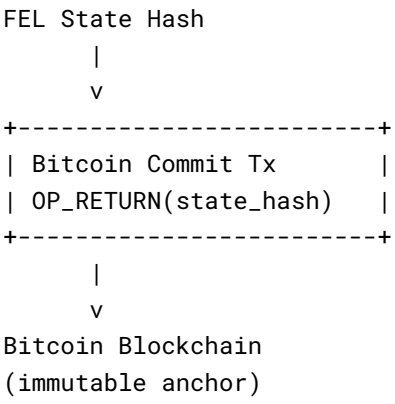
- retroactive modification invalidates all subsequent hash states,
- multiple FELs may exist across institutions,
- verification is possible without revealing sensitive details.

6. Anchoring to Bitcoin

At defined intervals:

```
state_hash(FEL) → OP_RETURN → Bitcoin Transaction
```

Diagram:



Anchoring provides:

- tamper-evidence
- global verifiability
- shared auditability
- long-term integrity

Anchoring is the only interaction with Bitcoin.

7. Bitcoin Bank: Global Contribution Pool

All contributions flow into a pooled treasury:

```
Contributions → Bitcoin Bank → Allocation
```

Properties:

- stored in Bitcoin
- balances publicly visible
- no single-actor control
- governed by rules + multi-signature approvals
- auditability ensured through anchoring

Bitcoin Bank is not an institution; it is a protocol-defined treasury mechanism.

8. Global Allocation Voting

Allocations occur through transparent, global voting.

```
+-------------------------------------+
| Public Goods Funding Priorities     |
|                                     |
| Education    | 22%                  |
| Healthcare   | 18%                  |
| Climate      | 14%                  |
| Poverty      | 33%                  |
| Innovation   | 13%                  |
+-------------------------------------+
```

Voting is:

- reputation-weighted
- verifiable
- logged in FEL
- deterministic in allocation rules

BFP does not assign political authority.
It assigns rule-defined influence through transparent mechanisms

9. Governance Model

BFP uses:

- multi-signature approval
- rule-based execution
- periodic anchoring
- transparent log structures

No central authority exists.
Any organization may adopt BFP voluntarily.
Rules govern behavior—not individuals.

10. Security Considerations

- hash-linked log structure prevents retroactive tampering
- Bitcoin anchoring provides immutability
- multi-signature approvals prevent unilateral changes
- optional zero-knowledge proofs maintain privacy
- protocol does not itself hold private keys for user funds
- no modification to Bitcoin consensus

Security depends on:

- the integrity of the FEL,
- anchoring regularity,
- multi-signature governance.

11. Applications

BFP can be adopted by:

- global NGOs
- DAOs
- charitable institutions
- fintech platforms
- cross-border project funding
- cooperatives
- voluntary global public-good systems

Its contribution model and transparency mechanisms are universal

12. Relationship to Bitcoin

BFP is not a fork or extension of Bitcoin.
It does not change issuance, consensus, or monetary policy.

It uses Bitcoin solely as:

- an immutable timestamp
- a state-hash commitment layer
- a globally verifiable integrity mechanism

Bitcoin remains the monetary layer.
BFP provides an optional fiscal layer.

13. Conclusion

Bitcoin established a decentralized monetary foundation.
The Bitcoin Fiscal Protocol extends this clarity to fiscal processes by providing a minimal, deterministic, spending-based contribution model anchored to Bitcoin's security.

The protocol introduces:

- voluntary 10%+ spending contributions,
- an append-only fiscal log,
- Bitcoin anchoring for integrity,
- a global pooled treasury,
- transparent allocation voting.

The result is a simple, auditable fiscal mechanism compatible with any voluntary institution worldwide.

Appendix: Full Diagram Set

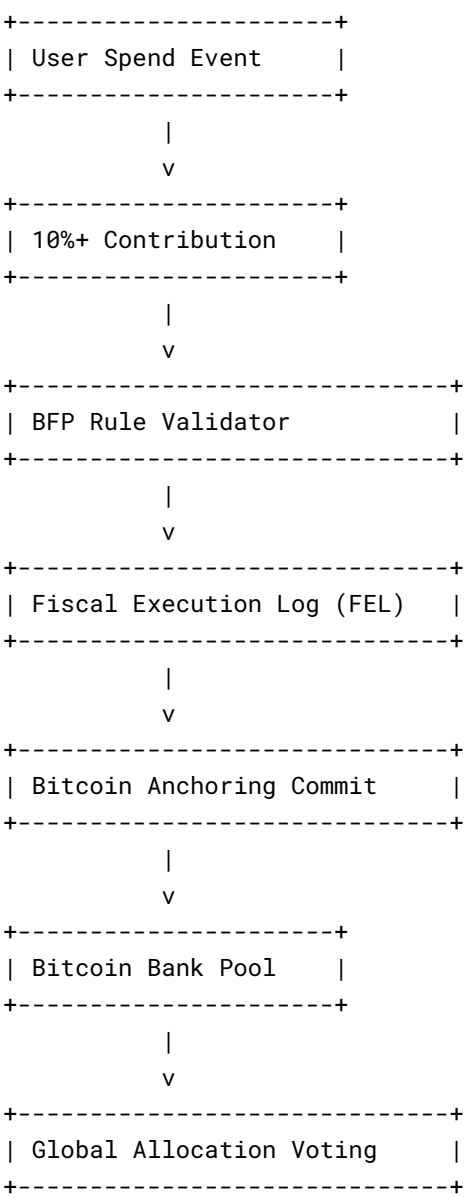
A1. End-to-End Protocol Flow

```
Spend → Contribution → Validation → FEL → BTC Anchor → Pool → Vote → Allocation
```

A2. Compact Pipeline

```
[S] → [C] → [BFP] → [FEL] → [BTC] → [POOL] → [VOTE] → [ALLOC]
```

A3. Overview Architecture



References

[1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. https://bitcoin.org/bitcoin.pdf

[2] W. Diffie and M. Hellman, “New Directions in Cryptography,” *IEEE Trans. Info. Theory*, vol. 22, no. 6, 1976.

[3] R. C. Merkle, “Protocols for Public Key Cryptosystems,” *Proc. IEEE Symposium on Security and Privacy*, 1980.

[4] L. Lamport, “Password Authentication with Insecure Communication,” *Communications of the ACM*, vol. 24, no. 11, 1981.

[5] D. Chaum, “Blind Signatures for Untraceable Payments,” *Advances in Cryptology*, Springer, 1983.

[6] S. Haber, W. S. Stornetta, “How to Timestamp a Digital Document,” *Journal of Cryptology*, 1991.

[7] R. Anderson, *Security Engineering*, Wiley, 2001.

[8] M. Castro, B. Liskov, “Practical Byzantine Fault Tolerance,” *OSDI ’99*, USENIX, 1999.

[9] A. Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016.

[10] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” Ethereum Yellow Paper, 2014.

[11] S. Goldwasser, S. Micali, “Probabilistic Encryption,” *J. Comput. Syst. Sci.*, 1984.

[12] E. Ben-Sasson et al., “Zerocash: Decentralized Anonymous Payments,” *IEEE S&P*, 2014.