Overpass Channels on Bitcoin (B^2O): A Non-Invasive Layer 2 Solution for Privacy-Preserving, High-Volume Transactions with Instant Finality

Brandon "Cryptskii" Ramsay

November 14, 2024

Abstract

In response to the growing economic challenges faced by traditional financial systems, Bitcoin's significance as a decentralized, censorship-resistant store of value continues to rise. Building on the Overpass Channels architecture [Ramsay 2024], we propose a privacy-preserving, scalable Layer 2 solution that enables high-volume transactions on Bitcoin without altering its protocol or consensus model. This paper presents a comparative analysis of Overpass Channels and BitVM2, substantiating Overpass's superiority in privacy, economic neutrality, and scalability. We formalize the system's operational assumptions and provide rigorous theorems and proofs that validate Overpass's ability to maintain Bitcoin's security properties and monetary principles, setting a new benchmark for scalability on Bitcoin's blockchain.

1 Introduction

The escalating volatility within traditional financial systems underscores Bitcoin's foundational role as a decentralized store of value. As Bitcoin adoption grows, the need for scalable and private transaction mechanisms is evident. Leveraging the Overpass Channels architecture [Ramsay 2024], we introduce a solution specifically designed to scale Bitcoin transactions without altering its consensus or core protocol. By contrasting Overpass Channels with BitVM2, we elucidate the distinct advantages of our approach in maintaining privacy and network integrity while ensuring economic neutrality.

1.1 Motivation

Given the limitations of traditional Layer 2 solutions—often requiring protocol adjustments or trust-based assumptions—the Overpass Channels approach offers a uniquely adaptable, non-invasive solution that enables Bitcoin to scale without compromising its decentralized ethos. While recent advancements like BitVM2 have made strides in SNARK-based verification, Overpass Channels address these challenges through its established hierarchical structure [Section 9.1] and privacy-focused mechanisms [Section 3].

- **Distributed Storage**: Utilizes Overpass's distributed storage model [Section 10] for efficient transaction handling.
- **Optimized State Management**: Employs hierarchical sparse Merkle trees [Section 12] for lightweight Bitcoin state management.
- **Privacy-Enhanced zk-SNARKs**: Integrates Plonky2-based zk-SNARKs [Section 3.8] to preserve transaction privacy.
- **Compatibility with Bitcoin's HTLC**: Ensures seamless Bitcoin integration through HTLC adaptation [Section 8.2].

1.2 Core Principles

Our design prioritizes the following principles to ensure Overpass Channels aligns with Bitcoin's core properties:

1. **Protocol Integrity**: Achieves scalability without protocol modifications to Bitcoin.

2. **Economic Consistency**: Preserves Bitcoin's economic incentives and fee structure.

3. **Trustless Design**: Implements trustless operation based on Overpass's proven cryptographic assumptions [Section 6].

4. **Privacy Assurance**: Enhances transaction privacy by default, following Overpass's established privacy guarantees [Section 18].

5. **Decentralization Support**: Maintains economic neutrality to avoid concentration of network power.

1.3 Comparison Framework

To formalize the comparison between Overpass Channels and BitVM2, we establish a rigorous evaluation framework based on privacy, scalability, economic neutrality, and security. Each metric is substantiated through theorem-proof structures that quantify the systems' respective capabilities.

Definition 1 (Layer 2 Security Preservation)**.** *A Layer 2 solution S preserves Bitcoin's security model if and only if:*

$$\forall t \in T,\ P(attack \mid S) \leq P(attack \mid Bitcoin)$$

where T is the set of all transaction types, and $P(attack)$ represents the probability of a successful attack.

Theorem 1 (Security Preservation in Overpass Channels)**.** *Overpass Channels maintain Bitcoin's security properties with respect to consensus and decentralization by ensuring that no additional vulnerabilities are introduced in state management or transaction validation:*

$$P(attack \mid Overpass) = P(attack \mid Bitcoin).$$

Proof. Let A be an adversary aiming to compromise transactions in Overpass Channels. For any attack strategy σ:

1. The adversary must either:

(a) Break Bitcoin's security assumptions, or

(b) Exploit a flaw in Overpass's zk-SNARK verification or channel closure mechanism.

2. Overpass Channels enforce the following:

(a) zk-SNARK soundness guarantees transaction validity.

(b) Channel closure requires a valid Bitcoin transaction, preserving the network's security model.

(c) No additional cryptographic assumptions beyond standard zk-SNARK soundness are introduced.

3. Consequently, the security of Overpass Channels is bounded by Bitcoin's own security assumptions and the integrity of zk-SNARK proofs:

$$P(\text{attack} \mid \text{Overpass}) = P(\text{attack} \mid \text{Bitcoin}).$$

This completes the proof, showing that Overpass Channels do not degrade Bitcoin's security guarantees. ■

2 Technical Architecture

The integration of Overpass Channels with Bitcoin leverages several technical mechanisms to achieve scalability and privacy while preserving security. We provide a structured comparison with BitVM2 to highlight Overpass's unique advantages.

2.1 Unilateral Payment Channels

Overpass Channels introduce a unilateral payment channel structure specifically optimized for Bitcoin, distinct from BitVM2's state model.

Definition 2 (Bitcoin-Compatible Unilateral Channel)**.** *A Bitcoin-compatible unilateral channel C is defined as a tuple $(pk_s, pk_r, v, t, \sigma)$ where:*

- pk_s*: Sender's public key.*
- pk_r*: Receiver's public key.*
- v*: Channel value in satoshis.*
- t*: Timelock value.*
- σ*: Channel signature.*

satisfying the following property:

$$\mathit{ValidChannel}(C) \iff \mathit{VerifyBitcoinSig}(\sigma, (pk_s, pk_r, v, t)) = \mathit{true}.$$

2.2 Cryptographic Constructions for Bitcoin Channels

Overpass Channels ensure privacy and security through cryptographic constructions designed to operate efficiently on Bitcoin's existing infrastructure. This approach contrasts with BitVM2's focus on sequential verification, yielding distinct privacy and efficiency advantages.

Theorem 2 (Channel State Privacy)**.** *Given a channel state S and its corresponding zk-SNARK proof π, no adversary A can determine the transaction history or current balances with probability greater than negligible, while still being able to verify the validity of the state.*

Proof. Let S be a channel state and π its corresponding zk-SNARK proof. Privacy is ensured through a series of games:

1. **Game 0**: The real privacy game, where an adversary A attempts to learn information about the channel state S.

2. **Game 1**: Modify Game 0 by replacing the real zk-SNARK proof with a simulated proof.

By the zero-knowledge property of zk-SNARKs:

$$|\Pr[A \text{ wins Game 0}] - \Pr[A \text{ wins Game 1}]| \leq \text{negl}(\lambda),$$

where $\text{negl}(\lambda)$ is a negligible function in the security parameter λ.

3. **Game 2**: Replace the real channel state S with a random, valid state.

By the hiding property of the commitment scheme:

$$|\Pr[A \text{ wins Game 1}] - \Pr[A \text{ wins Game 2}]| \leq \text{negl}(\lambda).$$

In Game 2, the adversary receives no information about the actual channel state S, resulting in:

$$\Pr[A \text{ wins Game 2}] = \frac{1}{2}.$$

Through this sequence of games, we conclude that A's advantage in the real game (Game 0) is negligible, establishing privacy for the Overpass Channels. ■

2.3 Channel Operations and Bitcoin Script Integration

Overpass Channels implement functionality through Bitcoin-compatible scripts, enabling secure channel operations without modifying Bitcoin's protocol. This approach differs from BitVM2, which requires sequential verification stages, by focusing on privacy preservation and operational efficiency.

Algorithm 1 Channel Opening on Bitcoin

Require: Sender keys $(\text{sk}_s, \text{pk}_s)$, Receiver public key pk_r, Channel value v

Generate funding transaction T_f with the following script:
  `OP_IF`
    `OP_SHA256` $\langle H(\text{revocation\_key})\rangle$
    `OP_EQUALVERIFY`
    $\langle \text{pk}_r \rangle$ `OP_CHECKSIG`
  `OP_ELSE`
    $\langle \text{timeout} \rangle$ `OP_CHECKLOCKTIMEVERIFY`
    `OP_DROP`
    $\langle \text{pk}_s \rangle$ `OP_CHECKSIG`
  `OP_ENDIF`
Broadcast T_f to the Bitcoin network
Generate zk-SNARK proof π of the channel state validity

Ensure: (T_f, π)

3 Comparison with BitVM2

Overpass Channels and BitVM2 both utilize zk-SNARKs to enable advanced transaction verification on Bitcoin. However, their approaches to state management, privacy, and scalability vary significantly. This section provides a detailed comparison to illustrate the advantages of Overpass Channels over BitVM2.

3.1 Architectural Differences

The core architectural design of each system impacts their performance and scalability. Overpass Channels leverage distributed state management and privacy-preserving mechanisms, while BitVM2 emphasizes sequential verification stages.

3.2 Economic Implications

The economic implications of each approach significantly affect Bitcoin's fee market and miner incentives. While both systems maintain Bitcoin's security model, their respective costs and operational overhead differ.

Theorem 3 (Incentive Compatibility)**.** *Let M represent Bitcoin miners, and let $I(m)$ be the expected income of a miner m. Under both Overpass Channels and*

Feature	Overpass Channels	BitVM2
State Model	Privacy-preserving off-chain	Off-chain with on-chain verification
Privacy	Full transaction privacy	Basic transaction privacy
Scalability	$O(n)$ horizontal scaling	$O(n)$ with verification overhead
Trust Model	Bitcoin-equivalent	Bitcoin-equivalent with setup
Impact on Miners	Neutral	Neutral with verification cost
Verification Method	Optimized SNARK proofs	Sequential SNARK-based verification

Table 1: Comparison of Key Features

BitVM2:

$$\forall m \in M : E[I(m) \mid L2] \geq E[I(m) \mid Bitcoin],$$

with system-specific overhead distributions as follows:

$$O_{Overpass} = O_{constant},$$

$$O_{BitVM2} = O_{verification} + O_{setup}.$$

Proof. For Overpass Channels: 1. Channel operations rely on standard Bitcoin transactions. 2. Verification burden remains constant due to optimized SNARK proofs. 3. Mining decentralization and fee structures remain unaffected.

For BitVM2: 1. Similar reliance on standard Bitcoin transactions. 2. Initial setup and verification costs introduced. 3. Verification overhead potentially impacts miner fees due to increased computational requirements.

Therefore, both systems preserve Bitcoin's incentive model, although Overpass offers a more consistent and lower overhead for miners. ■

3.3 Network Effects and Liquidity

The liquidity distribution and network effects of each system are crucial for Bitcoin's economic stability. Overpass Channels achieve liquidity efficiency with minimized operational costs, offering an advantage over BitVM2's verification overhead.

Theorem 4 (Liquidity Preservation)**.** *In a network with total liquidity L, both systems preserve Bitcoin's liquidity pool:*

$$L_{effective} = L_{total} - O_{system},$$

where:

$$O_{Overpass} < O_{BitVM2}$$

due to Overpass's optimized state management and lack of setup costs.

4 Security Considerations and Risk Analysis

Layer 2 solutions must be carefully analyzed for security implications to ensure they do not compromise Bitcoin's core properties. This section provides a comprehensive examination of the security models for Overpass Channels and BitVM2, focusing on privacy, attack surface, and resistance to double-spend attacks.

4.1 Attack Surface Analysis

The attack surface of each system represents the potential vulnerability points that could be exploited by adversaries. Overpass Channels and BitVM2 both introduce minimal attack surfaces, but their structural differences affect the composition of these surfaces.

Definition 3 (Attack Surface Extension)**.** *For a Layer 2 solution L, the attack surface extension $E(L)$ is defined as:*

$$E(L) = \{(v, p) \mid v \in V(L) \setminus V(Bitcoin), p > 0\},$$

where $V(L)$ is the set of potential vulnerability points in L and p is the probability of successful exploitation.

Theorem 5 (Equivalent Base Extension)**.** *Both systems maintain minimal attack surface extension:*

$$|E(Overpass)| = O(1),$$
$$|E(BitVM2)| = O(1),$$

with different vulnerability classes:

$$V_{Overpass} = \{V_{privacy}, V_{state}\},$$
$$V_{BitVM2} = \{V_{setup}, V_{verify}\}.$$

Proof. For both Overpass Channels and BitVM2:

1. State transitions and transaction validity are secured by zk-SNARKs. 2. Channel operations rely on standard Bitcoin transaction security. 3. No additional consensus requirements are introduced.

Key distinctions include:

1. **Privacy Mechanism**: - Overpass: Full privacy achieved through state channels. - BitVM2: Basic privacy limited by sequential verification.

2. **Setup Requirements**: - Overpass: Direct channel initialization without additional setup. - BitVM2: Requires an initial verification setup phase.

Thus, both systems achieve minimal and comparable attack surface extensions, though the structure of vulnerability classes differs. ■

4.2 Double-Spend Prevention

Double-spend prevention is essential for maintaining Bitcoin's integrity as a monetary system. Both Overpass Channels and BitVM2 implement robust mechanisms to prevent double-spend attacks.

Theorem 6 (Double-Spend Prevention)**.** *For both systems, the probability of a successful double-spend attack $P(DS)$ is bounded by:*

$$P(DS) \leq \min(P(\textit{Bitcoin\_DS}), P(\textit{zk\_break})),$$

where $P(\textit{Bitcoin\_DS})$ represents the probability of a double-spend on Bitcoin and $P(\textit{zk\_break})$ represents the probability of breaking the zk-SNARK system.

Proof. Let A be an adversary attempting a double-spend attack. For success, A must either:

1. Compromise Bitcoin's underlying security model with probability $P(\text{Bitcoin\_DS})$.
2. Generate a false zk-SNARK proof with probability $P(\text{zk\_break})$.

Additionally, both systems enforce a channel closure mechanism that ensures:

$$\forall s_1, s_2 \in \text{States} : \text{Close}(s_1) \land \text{Close}(s_2) \implies s_1 = s_2.$$

Thus, the probability of a successful double-spend attack is bounded by the minimum probability of either compromising Bitcoin's security or breaking the zk-SNARK proof system, regardless of system-specific differences. ■

4.3 Impact on Bitcoin's Security Model

Each Layer 2 solution must be assessed for its impact on Bitcoin's core security properties, such as decentralization, censorship resistance, and immutability. Overpass Channels and BitVM2 maintain these properties, though their verification and state management differ.

Definition 4 (Security Model Preservation)**.** *A Layer 2 solution S preserves Bitcoin's security model if:*

$$\forall p \in \textit{Properties(Bitcoin)} : \textit{Guarantee}(p \mid S) \geq \textit{Guarantee}(p \mid \textit{Bitcoin}),$$

where Properties(Bitcoin) includes decentralization, censorship resistance, and immutability.

Theorem 7 (Security Model Impact)**.** *Both Overpass Channels and BitVM2 maintain Bitcoin's security model with distinct architectural trade-offs:*

$$\Delta_{security}(Overpass) = \Delta_{security}(BitVM2) = 0,$$

though they follow different verification pathways:

$$Path_{Overpass} = \{Privacy, StateManagement\},$$

$$Path_{BitVM2} = \{Setup, VerificationFlow\}.$$

Proof. To assess security preservation, consider the following for both systems:

1. **Consensus Requirements**: - Both systems operate without modifying Bitcoin's consensus.

2. **Cryptographic Assumptions**: - Each system relies on zk-SNARKs, ensuring equivalent cryptographic strength.

3. **State and Transaction Management**: - Overpass: Employs integrated, privacy-preserving state channels, minimizing exposure. - BitVM2: Utilizes a sequential verification process that introduces verification layers but maintains on-chain compatibility.

4. **Implementation Distinctions**: - Overpass prioritizes direct state transitions, reducing operational overhead. - BitVM2 requires setup and verification sequences, increasing complexity.

Therefore, both systems preserve Bitcoin's security model while following distinct approaches to verification and state management. ■

4.4 Liveness and Availability Analysis

The liveness and availability of transactions are critical for user experience and adoption. Overpass Channels and BitVM2 achieve comparable liveness guarantees through different transaction handling mechanisms.

Theorem 8 (Liveness Guarantee)**.** *Under both systems, transaction liveness $L(t)$ for a transaction t is guaranteed with probability:*

$$P(L(t)) \geq 1 - (1 - p)^k,$$

where p is the probability of successful Bitcoin transaction inclusion and k is the number of confirmation attempts.

Proof. For both systems:

1. **Channel Operations**: - Rely on standard Bitcoin transactions for channel creation and closure.

2. **Verification Methodology**: - Both systems use zk-SNARK proofs for verification, enabling off-chain transaction finality.

3. **Channel Closure Attempts**: - With k attempts, the probability of successful closure is given by:

$$P(\text{closure\_success}) = 1 - (1 - p)^k.$$

Since each system relies on Bitcoin's underlying liveness properties for final settlement, they both achieve equivalent liveness guarantees. ■

4.5 Long-term Security Implications

Both Overpass Channels and BitVM2 must be evaluated for their long-term security impacts, especially in terms of protocol longevity and resistance to future attack vectors.

Theorem 9 (Security Model Evolution)**.** *The long-term security impact $I(t)$ of both Layer 2 solutions at time t satisfies:*

$$\lim_{t \to \infty} I(t) = 0,$$

with differing composition vectors:

$$V_{Overpass}(t) = \{v_{privacy}(t), v_{state}(t)\},$$

$$V_{BitVM2}(t) = \{v_{setup}(t), v_{verify}(t)\}.$$

Proof. Consider the following security properties for both systems:

1. **Longevity of Cryptographic Assumptions**: - Both rely on zk-SNARKs with long-term security guarantees, ensuring consistency over time.

2. **System-Specific Implications**: - Overpass: Long-term stability due to privacy-preserving channels and minimal setup requirements. - BitVM2: Security preserved through on-chain verification, though with added complexity in setup and verification stages.

3. **Impact on Bitcoin's Security**: - Neither system requires alterations to Bitcoin's protocol, preserving the core security properties indefinitely.

Thus, the long-term security impact remains neutral for both systems, with each maintaining minimal additional risk over time. ■

5 Privacy Guarantees and Economic Implications

The privacy and economic characteristics of a Layer 2 solution significantly affect Bitcoin's fungibility and monetary stability. Overpass Channels and BitVM2 both employ zk-SNARKs, yet their approaches to privacy and economic neutrality are fundamentally different.

5.1 Privacy Model

Privacy within a Layer 2 solution is critical for ensuring that transactions are indistinguishable, preserving Bitcoin's fungibility. Overpass Channels provide enhanced privacy over BitVM2 due to its integrated, privacy-preserving state channels.

Definition 5 (Transaction Privacy)**.** *A transaction T in a Layer 2 system provides δ-privacy if for any adversary A:*

$$|\Pr[A(T) = 1] - \Pr[A(T') = 1]| \leq \delta,$$

where T' is any other valid transaction with identical public parameters.

Theorem 10 (Privacy Guarantees)**.** *Overpass Channels achieve an enhanced level of privacy, denoted ε-privacy:*

$$\varepsilon_{Overpass} \leq \frac{1}{2^\lambda},$$

compared to BitVM2's basic transaction privacy:

$$\varepsilon_{BitVM2} \leq \frac{1}{2^\lambda} + \delta_{state},$$

where δ_{state} represents additional information leakage due to BitVM2's state verification.

Proof. Let A be an adversary attempting to distinguish between transactions:

1. **Base zk-SNARK Privacy**: - By the zero-knowledge property of zk-SNARKs, for any input x and witness w:

$$\{\text{Prove}(x, w)\} \approx_c \{\text{Sim}(x)\}.$$

2. **System-Specific Privacy Distinctions**: - Overpass: Full state privacy, leading to negligible information leakage:

$$|\Pr[A(\pi, P, U) = 1] - \Pr[A(\text{Sim}(\pi), P, U) = 1]| \leq \frac{1}{2^\lambda}.$$

- BitVM2: State verification introduces potential leakage:

$$|\Pr[A(\pi, P, U) = 1] - \Pr[A(\text{Sim}(\pi), P, U) = 1]| \leq \frac{1}{2^\lambda} + \delta_{\text{state}}.$$

3. **Conclusion**: While both systems provide robust privacy through zk-SNARKs, Overpass achieves stronger privacy guarantees due to its privacy-preserving state channels, resulting in reduced leakage. ■

5.2 Economic Impact Analysis

The economic implications of each system on Bitcoin's fee market and miner incentives are essential to maintaining a balanced ecosystem.

Theorem 11 (Fee Market Preservation)**.** *Under both systems, Bitcoin's fee market equilibrium E remains stable:*

$$|E_{L2} - E_{Bitcoin}| \leq \epsilon,$$

where ϵ is a negligible factor, with differing overhead distributions:

$$\epsilon_{Overpass} = O_{channel} + O_{privacy},$$

$$\epsilon_{BitVM2} = O_{setup} + O_{verify}.$$

Proof. For a transaction t, the fee function $F(t)$ can be expressed as:

$$F(t) = \alpha \cdot s(t) + \beta \cdot p(t),$$

where $s(t)$ is the transaction size, and $p(t)$ is the priority.

1. **Overpass Channels**: - Operations incur minimal overhead due to privacy-preserving channels. - Fee structure remains consistent with Bitcoin's standard model.

2. **BitVM2**: - Additional setup and verification phases introduce operational overhead. - The fee model remains consistent but with added verification costs.

Thus, while both systems preserve the equilibrium of Bitcoin's fee market, Overpass offers a more efficient fee structure by minimizing extraneous costs. ■

5.3 Liquidity Efficiency

Efficient liquidity utilization is essential for a Layer 2 solution to scale while maintaining user accessibility and network sustainability. Overpass Channels provide a more optimized liquidity model than BitVM2 due to minimized verification and operational overhead.

Theorem 12 (Liquidity Utilization)**.** *Both systems achieve efficient liquidity utilization U, with different optimization paths:*

For Overpass Channels:

$$U_{Overpass} = \frac{L_{active}}{L_{total}} \cdot \prod_{i=1}^{n} r_i,$$

For BitVM2:

$$U_{BitVM2} = \frac{L_{active}}{L_{total}} \cdot \prod_{i=1}^{n} (r_i - \sigma_i),$$

where L_{active} is the active channel liquidity, L_{total} is the total liquidity, r_i represents rebalancing factors, and σ_i indicates verification overhead in BitVM2.

Proof. Consider the set C of all channels in the system. For each channel $c \in C$:

1. **Liquidity Utilization**:

$$u(c) = \frac{v(c)}{V(c)} \cdot r(c),$$

where $v(c)$ is the value utilized and $V(c)$ is the channel capacity.

2. **System-Specific Utilization Factors**: - Overpass Channels:

$$U_{\text{Overpass}} = \frac{\sum_{c \in C} u(c) \cdot V(c)}{\sum_{c \in C} V(c)},$$

indicating minimal operational costs and high liquidity efficiency.

- BitVM2:

$$U_{\text{BitVM2}} = \frac{\sum_{c \in C} (u(c) - \sigma(c)) \cdot V(c)}{\sum_{c \in C} V(c)},$$

where $\sigma(c)$ reflects verification overhead, reducing effective liquidity.

3. **Conclusion**: Overpass Channels exhibit greater liquidity efficiency as they avoid the additional verification overhead imposed by BitVM2. ■

5.4 Economic Centralization Resistance

Preserving decentralization within the economic model is crucial to avoid power concentration in a Layer 2 solution. Overpass Channels and BitVM2 maintain Bitcoin's decentralization, but Overpass's structure is inherently more resistant to centralization.

Definition 6 (Centralization Resistance)**.** *A system S is ρ-centralization resistant if no entity e can control more than ρ fraction of the system's economic activity:*

$$\forall e : \frac{Control(e)}{Total} \leq \rho.$$

Theorem 13 (Decentralization Maintenance)**.** *Both systems maintain Bitcoin's centralization resistance bound ρ:*

$$\rho_{L2} \leq \rho_{Bitcoin},$$

though they differ in their resistance mechanisms:

$$R_{Overpass} = \{R_{privacy}, R_{state}\},$$

$$R_{BitVM2} = \{R_{setup}, R_{verify}\}.$$

Proof. For both systems, we examine centralization resistance as follows:

1. **Architectural Aspects**: - Overpass Channels: - Privacy-preserving channels reduce reliance on trusted parties. - Distributed state management minimizes central control.

- BitVM2: - Initial setup and verification dependencies may centralize certain operations.

2. **Economic Distribution**: - Both systems employ decentralized transaction processing and verification to avoid reliance on centralized entities. - Dynamic rebalancing mechanisms distribute control across network participants.

Thus, Overpass Channels provide a higher resistance to centralization due to minimized setup dependencies and enhanced privacy, while BitVM2 maintains resistance but with increased operational complexity. ■

5.5 Long-term Economic Stability

Ensuring economic stability over time is critical for the viability of a Layer 2 solution on Bitcoin. Both Overpass Channels and BitVM2 aim to preserve Bitcoin's economic model; however, Overpass offers more consistent long-term stability due to its minimal operational overhead and direct transaction management.

Theorem 14 (Economic Model Preservation)**.** *Both systems preserve Bitcoin's long-term economic stability:*

$$\lim_{t\to\infty} |M_{L2}(t) - M_{Bitcoin}(t)| = 0,$$

where $M(t)$ represents the economic model at time t. Each system has different stability vectors:

$$S_{Overpass}(t) = \{S_{privacy}(t), S_{channel}(t)\},$$
$$S_{BitVM2}(t) = \{S_{verify}(t), S_{setup}(t)\}.$$

Proof. To examine economic stability, we consider the following for each system:

1. **Monetary Properties**: - Both Overpass Channels and BitVM2: - Preserve Bitcoin's fixed supply. - Maintain its issuance schedule. - Do not alter mining incentives or economic dynamics.

2. **System-Specific Characteristics**: - **Overpass Channels**: - The privacy-focused, channel-based structure ensures consistent fee and operational costs. - Direct state management minimizes fluctuations in transaction handling fees.

- **BitVM2**: - Additional setup and verification stages introduce occasional cost spikes, which may lead to minor fee market adjustments over time. - The sequential verification process results in varying operational expenses.

3. **Network Effects**: - Both systems are designed to maintain decentralization and support censorship resistance, ensuring long-term usability and user accessibility.

As $t \to \infty$, both systems converge towards stable economic models with minor fluctuations for BitVM2 due to its additional verification overhead. Overpass Channels, however, offer a smoother economic trajectory with fewer cost variations. ■

6 Comparative Analysis of Trustless Mechanisms

A fundamental requirement for Layer 2 solutions on Bitcoin is the minimization of trust assumptions. Overpass Channels and BitVM2 each establish distinct trust models, yet Overpass achieves stronger trust minimization due to its direct channel structure and privacy integration.

6.1 Trust Model Foundations

The level of trust required by a Layer 2 system impacts its alignment with Bitcoin's trustless design. We formalize the trust minimization for each system.

Theorem 15 (Trust Minimization)**.** *For both Layer 2 systems B, the trust requirement $T(B)$ can be defined as:*

$$T(B) = \sum_{i=1}^{n} w_i \cdot t_i,$$

where w_i represents trust weights and t_i represents individual trust assumptions. Each system has unique trust vectors:

$$T_{Overpass} = \{t_{privacy}, t_{state}\},$$

$$T_{BitVM2} = \{t_{setup}, t_{verify}\}.$$

6.2 Bridge Trust Models

Layer 2 solutions require secure bridging mechanisms with Bitcoin's Layer 1 to facilitate interoperability while preserving trust assumptions.

Definition 7 (Bridge Security)**.** *A bridge transaction maintains Bitcoin's trust assumptions if:*

$$\forall tx \in Transactions : Trust(tx) \subseteq Trust(Bitcoin),$$

where Trust(Bitcoin) encompasses Bitcoin's base security assumptions.

Theorem 16 (Trust Preservation)**.** *Both systems preserve Bitcoin's trust model through different bridging mechanisms:*

$$T(L2) = T(Bitcoin) + T(SNARK),$$

where $T(SNARK)$ represents the trust assumption introduced by zk-SNARKs. Distinct implementation paths are followed:

$$Path_{Overpass} = \{Privacy, StateTransition\},$$

$$Path_{BitVM2} = \{Setup, VerificationFlow\}.$$

Proof. The preservation of trust assumptions is achieved by both systems through:

1. **zk-SNARK Trust Requirement**: - Both systems introduce SNARK-based proofs, which assume soundness and non-interactivity.

2. **System-Specific Mechanisms**: - **Overpass Channels**: - Direct channel state transitions ensure trust minimization. - Integrated privacy reduces the reliance on trusted setups.

- **BitVM2**: - Requires an initial setup phase, adding a layer of trust for configuration integrity. - Sequential verification process may introduce dependencies on verification nodes.

In summary, both systems maintain Bitcoin's trust model, but Overpass achieves a higher degree of trust minimization by avoiding setup requirements and emphasizing privacy-preserving operations. ■

7 Conclusion

This paper has provided a detailed comparative analysis of Overpass Channels and BitVM2 as Layer 2 solutions for Bitcoin, focusing on scalability, privacy, security, and economic neutrality. Through rigorous theorem-proof structures, we have demonstrated Overpass Channels' unique advantages in privacy preservation, efficient liquidity utilization, and trust minimization, establishing it as a leading solution for scaling Bitcoin without altering its core protocol.

7.1 Summary of Key Findings

Overpass Channels emerge as a compelling choice for high-volume, privacy-preserving transactions on Bitcoin, offering the following distinct advantages:

- **Enhanced Privacy**: Through integrated privacy-preserving state channels, Overpass ensures stronger privacy guarantees, minimizing information leakage compared to BitVM2.
- **Scalability and Efficiency**: Achieving $O(n)$ horizontal scaling with minimal verification overhead, Overpass efficiently supports high transaction throughput, whereas BitVM2 incurs higher verification and setup costs.
- **Economic Neutrality and Stability**: Closely aligned with Bitcoin's fee market structure, Overpass preserves Bitcoin's economic neutrality without introducing additional cost burdens.
- **Trustless Design**: Overpass Channels eliminate the need for trusted setups and emphasize zk-SNARK-based verification, achieving stronger trust minimization than BitVM2's setup-dependent model.

7.2 Overpass Channels as the Cash Layer for Layer 1 Blockchains

While Bitcoin serves as an optimal reserve asset and "gold layer" of a decentralized financial network, Overpass Channels have the potential to become the "cash layer" not only for Bitcoin but for any Layer 1 blockchain that integrates with its architecture. By extending Overpass Channels as a universal Layer 2 solution, any compatible blockchain can benefit from instant, privacy-preserving transactions with high scalability, thus providing a cash layer capable of supporting everyday transactional demands across various blockchain ecosystems.

This analysis specifically highlights Overpass Channels in the context of Bitcoin as an extension of the original Overpass Channels research. However, the modular design of Overpass allows seamless integration with multiple blockchains, enhancing each one with Overpass's advanced privacy and scalability benefits. This interoperability offers a transformative vision: a decentralized, multi-chain economy where Bitcoin and Overpass work symbiotically, with Bitcoin as the global reserve and Overpass as the universal, privacy-preserving cash layer.

7.3 Future Directions

Several areas of future research and development can help realize the full potential of Overpass Channels across multiple blockchain networks:

1. **zk-SNARK Optimization**: Further research into zk-SNARK efficiency can reduce computational overhead, making verification faster and more accessible across diverse Layer 1 blockchains.

2. **Expanding Integration Capabilities**: Developing tools and protocols for seamless Overpass integration with other blockchains will extend its applicability as a cash layer beyond Bitcoin.

3. **Real-world Deployment and Audits**: Comprehensive security audits and real-world testing will validate Overpass's privacy and scalability claims, ensuring robust performance across different blockchain networks.

7.4 Final Remarks

In conclusion, Overpass Channels represent a groundbreaking Layer 2 solution that enhances the scalability and privacy of Bitcoin and has the potential to serve as a universal cash layer across various Layer 1 blockchains. By offering a scalable,

privacy-focused transaction layer, Overpass can redefine the usability and accessibility of decentralized finance. This cash layer for the Internet enables a flexible, interoperable financial system that respects user privacy and decentralization principles, positioning Bitcoin and Overpass as essential building blocks in the future of a decentralized global economy.

Bibliography

[1] Ramsay, B., "Overpass Channels: Horizontally Scalable, Privacy-Enhanced, with Independent Verification, Fluid Liquidity, and Robust Censorship Proof Payments," Cryptology ePrint Archive, Paper 2024/1526, 2024. Available: `https://eprint.iacr.org/2024/1526`

[2] Linus, R., Aumayr, L., Zamyatin, A., Pelosi, A., Avarikioti, Z., Maffei, M., "BitVM2: Bridging Bitcoin to Second Layers," presented by ZeroSync, TU Wien, BOB, University of Pisa, University of Camerino, and Common Prefix, 2024.

[3] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin.org, 2008.