

# Cryptographic Attestation Through Bitcoin's Taproot Activation Block: A Forensic Analysis of Cross-Chain Linkage in Zenon Network

Anonymous Community Investigation

December 26, 2025

## Abstract

*This paper presents a comprehensive forensic analysis of a cryptographic inscription discovered in Bitcoin block 709632, the first block following Taproot activation on November 14, 2021. Through systematic investigation of on-chain data and source code analysis, this research demonstrates that Base64-encoded strings embedded within ASCII art represent Zenon Network's genesis momentum identifiers, establishing a bidirectional cryptographic link between two independent blockchain systems. This work contributes to the understanding of cross-chain attestation mechanisms and demonstrates the use of Bitcoin's immutable ledger as a notarization service for external blockchain systems. The analysis further contextualizes the historical significance of this inscription by examining contemporaneous communications from the Zenon development team.*

## **1. Introduction**

On November 14, 2021, Bitcoin underwent one of its most significant protocol upgrades since the implementation of Segregated Witness (SegWit) in 2017. The Taproot soft fork, activated at block height 709632, introduced enhanced privacy and smart contract capabilities to the Bitcoin network. Coinciding with this activation, an elaborate ASCII art inscription was embedded in this historic block through multiple OP\_RETURN transactions, remaining cryptographically opaque for over three years until its complete decoding in December 2024.

This research presents a systematic investigation into the cryptographic significance of this inscription, revealing it as a sophisticated cross-chain attestation mechanism employed by Zenon Network. The findings demonstrate how one blockchain system can utilize another's immutable ledger as a timestamp and notarization service, establishing verifiable proof of existence at a specific point in blockchain history.

## **2. Background and Related Work**

### **2.1 Bitcoin Taproot Activation**

Taproot (BIP 340, 341, 342) represents a comprehensive upgrade to Bitcoin's scripting capabilities, introducing Schnorr signatures and enhanced privacy features. The activation occurred at block 709632, mined by F2Pool on November 14, 2021, at 05:15 UTC. This block height was deterministically established through Bitcoin Improvement Proposal (BIP) 341, making it a predictable and significant milestone in Bitcoin's history.

### **2.2 OP\_RETURN as a Data Storage Mechanism**

OP\_RETURN is a Bitcoin script opcode that marks transaction outputs as provably unspendable, allowing up to 80 bytes of arbitrary data to be embedded in a transaction. While primarily designed for metadata storage, OP\_RETURN has been utilized for various applications including digital asset issuance, timestamping services, and cross-chain proofs. The use of multiple OP\_RETURN transactions to store larger data structures predates the Ordinals protocol by 14 months, representing an early demonstration of creative data inscription on Bitcoin.

### **2.3 Cross-Chain Attestation**

Cross-chain attestation mechanisms allow one blockchain to make verifiable claims about events or states in another blockchain system. Traditional approaches include relay chains, hash locks, and bridge protocols. The mechanism described in this paper represents a unidirectional attestation model where Bitcoin serves as an immutable witness to the genesis of an external chain, without requiring ongoing synchronization or two-way communication.

### **3. Methodology**

#### **3.1 Data Collection**

Bitcoin block 709632 was examined through multiple blockchain explorers including blockchain.com and mempool.space. All transactions containing OP\_RETURN outputs were systematically identified and their payloads extracted. The ASCII art was reconstructed from 15-19 separate transactions, each containing a single line of the complete image.

#### **3.2 Cryptographic Analysis**

Three distinct Base64-encoded strings were identified within the ASCII art payload:

<b>String ID</b>	<b>Base64 Encoded Value</b>
String #1 (16 bytes)	vtv3f5aKY0jGQg1P9a1AGw==
String #2 (16 bytes)	BynQtpeUyWTXKGTrGhdV2Q==
String #3 (18 bytes)	tVMd3L1CKM4wFmyxEEEUV2bY

These strings were decoded to hexadecimal format and systematically compared against known cryptographic hashes, including Bitcoin block 709632's hash, transaction IDs, and Merkle root values. No matches were found within Bitcoin's blockchain data, suggesting an external reference.

#### **3.3 Source Code Analysis**

The Zenon Network's genesis momentum generation code (available in the public GitHub repository at [github.com/zenon-network/go-zenon](https://github.com/zenon-network/go-zenon)) was examined to identify potential matches for the decoded hexadecimal values. Particular attention was paid to the momentum.go file, which contains the logic for generating the blockchain's genesis block.

## 4. Results and Analysis

### 4.1 Identification of Zenon Network Genesis Identifiers

Analysis of Zenon Network's genesis momentum code revealed exact matches for all three hexadecimal values:

Hexadecimal Value	Zenon Network Identifier
bedbf77f...401b	ChainIdentifier
0729d0b6...55d9	Momentum #1 Hash (first 16 bytes)
b5531ddc...66d8	Momentum #2 Hash (18 bytes)

The ChainIdentifier serves as a unique identifier for the Zenon blockchain instance, while the momentum hashes represent cryptographic fingerprints of the first two blocks in Zenon's ledger structure.

### 4.2 Bidirectional Cryptographic Linkage

The inscription establishes a bidirectional cryptographic relationship:

1. Bitcoin block 709632 contains Zenon's genesis identifiers embedded in OP\_RETURN transactions.
2. Zenon's genesis momentum (verifiable through RPC queries to Zenon nodes) references Bitcoin block 709632 in its ExtraData field.
3. This creates a closed cryptographic loop, establishing immutable linkage between the two chains.

This bidirectional reference is verifiable by any party with access to both blockchains, requiring no trusted intermediaries or bridge protocols.

### 4.3 Historical Context: The "Already Made History" Statement

On November 14, 2021, contemporaneous with the Taproot inscription, a member of the Zenon core development team posted the following message in official project communications: "We already made history." This statement, cryptic at the time, takes on significant meaning in light of the discovered inscription.

The phrase "made history" operates on multiple levels:

4. **Literal Historical Record:** The team had successfully inscribed Zenon's cryptographic identity into Bitcoin's most significant block in years, ensuring permanent historical preservation of their project's genesis.
5. **Technical Achievement:** The successful execution of a complex multi-transaction inscription at a precise, predetermined block height represented a significant technical accomplishment requiring deep Bitcoin protocol knowledge and precise timing.
6. **Strategic Positioning:** By inscribing in the Taproot activation block, Zenon established itself as present at a pivotal moment in Bitcoin's evolution, positioning the project within Bitcoin's historical narrative.
7. **Cryptographic Proof of Concept:** The inscription demonstrated a novel approach to cross-chain attestation 14 months before the Ordinals protocol popularized Bitcoin data inscription, potentially influencing subsequent developments in the space.

The statement's ambiguity was likely intentional, serving as a breadcrumb for future investigation while maintaining operational security for the core team. The three-year gap between inscription and full public understanding suggests the team anticipated that the full significance would only be appreciated through community-driven forensic analysis.



## 5. Discussion

### 5.1 Technical Implications

This inscription demonstrates several important technical capabilities:

8. **Precise Block Targeting:** The ability to reliably include transactions in a specific, predetermined block requires sophisticated fee estimation and network timing analysis.
9. **Multi-Transaction Coordination:** Coordinating 15-19 separate transactions to form a coherent message demonstrates advanced Bitcoin transaction construction and management.
10. **Cross-Chain Attestation:** The mechanism provides a template for how blockchain projects can establish verifiable proof of existence using Bitcoin as a timestamp service.

### 5.2 Economic Considerations

The estimated cost of approximately \$50-200 in Bitcoin transaction fees represents a remarkably cost-effective method for achieving permanent, global, and censorship-resistant data storage. This compares favorably with traditional notarization services and demonstrates Bitcoin's utility as a timestamping infrastructure layer.

### 5.3 Relationship to Ordinals Protocol

The Zenon inscription predates the Ordinals protocol (launched December 2022) by 14 months. While Ordinals utilize witness data rather than OP\_RETURN transactions, both approaches demonstrate Bitcoin's capability as a data inscription layer. The Zenon inscription may have contributed to the conceptual groundwork for subsequent inscription protocols, though direct influence remains speculative without documentary evidence.

### 5.4 Limitations and Future Work

While this analysis establishes the cryptographic linkage between Bitcoin block 709632 and Zenon Network's genesis, several questions remain for future investigation:

11. What specific technical mechanisms, if any, does Zenon Network employ to verify Bitcoin block references?
12. Could this attestation model be generalized into a formal protocol for blockchain timestamp verification?
13. What cryptographic guarantees does this linkage provide for light clients or simplified payment verification?

## 6. Conclusion

This research presents definitive evidence that the Base64-encoded strings embedded in Bitcoin's Taproot activation block (709632) represent Zenon Network's genesis momentum identifiers, establishing a sophisticated cross-chain attestation mechanism. The bidirectional cryptographic linkage demonstrates how blockchain systems can utilize Bitcoin's immutable ledger as a notarization and timestamping service without requiring ongoing coordination or trust assumptions.

The inscription represents a significant achievement in blockchain archaeology and cryptographic engineering, combining precise technical execution with strategic positioning at a historic moment in Bitcoin's evolution. The core team's contemporaneous statement "We already made history" is now revealed as a reference to this permanent inscription in Bitcoin's historical record, encompassing both literal historical preservation and technical accomplishment.

The three-year gap between inscription and full community understanding demonstrates the value of persistent forensic investigation in blockchain research. This work contributes to the broader understanding of how independent blockchain systems can establish cryptographic proofs of existence and temporal ordering through creative use of established protocols.

## **7. Verification Procedures**

All findings presented in this paper are independently verifiable through the following procedures:

### **7.1 Bitcoin Block Verification**

14. Navigate to [blockchain.com/explorer/blocks/btc/709632](https://blockchain.com/explorer/blocks/btc/709632) or equivalent block explorer
15. Identify transaction 71d9187cbb...f1fb6315 (or search for transactions with OP\_RETURN outputs)
16. Extract OP\_RETURN payload data from each transaction
17. Decode Base64 strings to hexadecimal format

### **7.2 Zenon Network Verification**

18. Access Zenon Network RPC endpoint
19. Query genesis momentum data
20. Compare ChainIdentifier field against decoded Bitcoin inscription data
21. Alternatively, visit [explorer.zenon.network](https://explorer.zenon.network) and examine momentum #1 and #2 hash values

### **7.3 Source Code Verification**

22. Clone repository: `git clone github.com/zenon-network/go-zenon`
23. Examine file: `chain/genesis/momentun.go`
24. Search for hexadecimal values in genesis configuration

## 8. References

- [1] Wuille, P., Nick, J., & Ruffing, T. (2020). Schnorr Signatures for secp256k1. Bitcoin Improvement Proposal 340.
- [2] Towns, A. J. (2020). Taproot: SegWit version 1 spending rules. Bitcoin Improvement Proposal 341.
- [3] Nick, J., Wuille, P., & Towns, A. J. (2020). Validation of Taproot Scripts. Bitcoin Improvement Proposal 342.
- [4] Bitcoin Block Explorer. [blockchain.com/explorer/blocks/btc/709632](https://blockchain.com/explorer/blocks/btc/709632). Accessed December 2024.
- [5] Zenon Network. (2021). Go-Zenon: Official implementation of the Zenon Network protocol. [github.com/zenon-network/go-zенон](https://github.com/zenon-network/go-zенон)
- [6] Zenon Network Explorer. [explorer.zenon.network](https://explorer.zenon.network). Accessed December 2024.
- [7] Santilli, C. (2024). Bitcoin Taproot ASCII Art. [cirosantilli.com](https://cirosantilli.com). Documentation of initial discovery.
- [8] Casey, R. (2022). Ordinals: Digital Artifacts on Bitcoin. [docs.ordinals.com](https://docs.ordinals.com). Protocol specification.

## **9. Acknowledgments**

This research builds upon initial observations by Ciro Santilli ([cirosantilli.com](http://cirosantilli.com)) regarding the ASCII art inscription in block 709632. Community contributions from Reddit users brando2131 and sroose provided valuable context. Social media discussions by @Zyler9985, @coinselor, @BagfootOP446, @Shazz, and other community members helped establish the investigation's direction. This investigation represents a collective effort by the Zenon Network community to understand the cryptographic significance of the Taproot block inscription.

## **Community Investigation Note**

This document represents the collective findings of community-driven forensic analysis conducted in December 2024. The investigation was performed through open-source intelligence gathering, public blockchain data analysis, and systematic examination of publicly available source code repositories.

The research methodology and findings are presented in an academically rigorous format to facilitate peer review and independent verification by the broader cryptocurrency research community.

### **License and Distribution**

This document may be freely distributed within the Zenon Network and Bitcoin communities. Citation of this work in derivative research is encouraged.