Intention Project

Recovery of Lost Bitcoin Private Keys without Brute Force or Discrete Logarithm

Introduction

For over five years, the Intention Project team has been developing a novel approach to one of the most challenging issues in the cryptocurrency world: the loss of private keys. Unlike traditional methods that rely on the discrete logarithm problem or brute-force attacks, our algorithm — named “Intention” — follows an entirely different logic based on distributed scalar geometry, pattern detection, and digital intention.

Current Status of the Project

The project has successfully completed its theoretical foundation and has been tested in a testnet environment that simulates real-world Bitcoin network conditions. In this environment, the algorithm has demonstrated:

The identification of private keys within a controlled test range.

The effective functionality of the “dimensional scalar map,” drastically reducing the search space.

The ability to analyze simulated blockchain data and detect cryptographic patterns.

Interaction with known cryptographic “blind spots” in a controlled and safe environment.

The system does not use linear or exponential searching. It does not iterate through every possible private key. Instead, it simultaneously analyzes multiple intention-based routes mathematically and geometrically.

Why hasn't the algorithm been tested on the mainnet yet?

This is a critical and very valid question. The answer must be honest, transparent, and focused on the logic behind our development and our controlled risk approach.

Official Response:

“We fully understand the concern about demonstrating the algorithm on a real wallet in the Bitcoin mainnet. At this stage, it would be neither prudent nor ethical to run direct tests on the live network without full validation of the final phase. Attempting to recover a real private key on the mainnet without absolute certainty of the algorithm's functionality could have unpredictable consequences and may harm the network or the project’s public perception.

That’s why we’ve spent the past five years conducting rigorous theoretical development and safe experimentation in a controlled environment. We built a testnet simulation that replicates the key conditions of the Bitcoin network relevant to our algorithm.

Within this simulated testnet, we’ve successfully demonstrated:

The algorithm’s ability to analyze and process blockchain-like data.

The successful identification of ‘lost’ private keys within defined test parameters.

The functionality of the ‘dimensional scalar map’ to reduce the search domain.

How the algorithm interacts with cryptographic ‘blind spots.’

The $50,000 investment is crucial for the final development stage, which includes:

Optimization and adaptation of the algorithm to handle mainnet complexity, transaction volume, and real-time latency.

Implementation of robust security measures to prevent exploitation and ensure all sensitive data remains protected.

Controlled and highly monitored testing on the mainnet using wallets with no real funds.

Development of the user interface and infrastructure for the recovery and auto-locking service.

Our strategy is to minimize risk. We will not expose real-value wallets until we reach very high confidence in the algorithm's performance and security.

In summary, our testnet validation demonstrates strong theoretical support and basic functional proof. The requested funding is what allows us to safely transition this strong base into a fully operational and secure tool for the real Bitcoin network."

The Next Stage: "Vuelta"

Once the mainnet adaptation is complete, the project will advance to its next evolutionary phase called Vuelta, which will:

Embed the algorithm inside a legitimate, user-facing wallet application.

Activate an automatic recovery protocol in the event of a confirmed hack or theft.

Guarantee the secure return of assets to a new address controlled by the original wallet owner, using a mathematically verified system.

This phase transforms Intention into not just a recovery tool, but a new layer of proactive defense within the Bitcoin ecosystem.

Call for Investors and Supporters

We are opening the project to select early investors and supporters. Your participation includes:

Priority access to real-world results and final prototype.

Optional inclusion in a private audit and advisory group.

Percentage-based participation in future earnings or licensed implementations.

Contact & Support

?? Website: https://intentionproject.github.io

?? Email: intentionproject@proton.me

Donation / Investment Addresses

Bitcoin (BTC):

bc1qyapqu6q38zc5w0zk74jz0nvhwfk2wzx2kznsa6

Ethereum / BNB / USDT (ERC-20):

0x04664e23e20536cc734b5db5ac653c2c19c84f68

Why hasn't a real wallet demonstration on the Bitcoin mainnet been conducted yet?

This is a crucial and completely valid question. The answer must be honest, transparent, and focused on the logic of our development process and the controlled risks we've carefully taken.

Main Answer:

We fully understand the concern about demonstrating the algorithm on a real wallet within the Bitcoin mainnet. At this stage, it would be neither prudent nor ethical to conduct direct tests on the mainnet without the complete validation of our final development phase.

Attempting to recover a real private key on the mainnet without absolute certainty about the algorithm's behavior could lead to unpredictable consequences. This could compromise not only the public perception of the project but also the integrity of the Bitcoin network itself.

That is why we have dedicated the last five years to rigorous theoretical research and deep technical development in a controlled environment. During this period, we built a simulated testnet environment that replicates critical conditions of the Bitcoin network, allowing us to test the core features of our algorithm with precision.

How does the Intention algorithm work?

The core innovation behind the algorithm lies in not attacking the discrete logarithm directly, but rather neutralizing it through a combination of advanced mathematical structures. This is not brute-force, and it's not based on luck. It's a completely new model grounded in high-level logic and geometry.

Its essential components include:

Dimensional Scalar Mapping: A structure that allows us to represent all possible scalar multipliers over the Bitcoin base point G simultaneously, using a multidimensional framework. This drastically reduces the search space through symmetries that are invisible to traditional methods.

Mathematical Superposition: Borrowing from structured logical entanglement concepts, the algorithm overlays multiple possible states in a governed way, eliminating invalid paths while amplifying valid convergence patterns.

Natural Computational Distribution: Without relying on mining or artificial compute power, the algorithm can extend its scanning across distributed nodes and observational agents, covering specific regions of the keyspace without linear traversal.

Discrete Logarithm Neutralization: Rather than solving the classical discrete logarithm (which remains computationally infeasible), the algorithm nullifies it mathematically by mapping it onto a plane where it no longer poses a barrier. This becomes possible through a discovery we call the blind spot.

What is the Blind Spot?

The blind spot is a mathematical coordinate within the system that behaves as a region where the private-to-public key relation becomes transparently reversible under specific geometric and computational conditions. It is not a magic flaw, nor a network weakness. In fact, it only activates when multiple alignment factors converge under strict internal rules.

This can be compared to a transformation inspired by Shor-type methods—not in their quantum implementation, but in their logical restructuring of the problem. Instead of directly chasing a result, the system builds a geometric-mathematical landscape in which the result emerges naturally.

It is essential to note that this blind spot does not weaken the Bitcoin network, nor does it break elliptic curve cryptography. It works only within our defined dimensional mapping and exclusively with keys that satisfy certain isolated structural criteria.

What have we already demonstrated?

Within our controlled testnet environment, we have successfully shown:

The algorithm's ability to analyze and process blockchain-like data.

The successful recovery of ‘lost’ private keys within defined parameters.

The functionality of the scalar dimensional mapping to reduce the search domain.

The blind spot acting as a predictable and mathematically governed construct.

Why is the $50,000 investment critical?

This investment is fundamental to executing the final phase of the project, which includes:

Optimization of the algorithm for real-world mainnet conditions.

Implementation of advanced security measures to prevent exploitation.

Controlled testing on the Bitcoin mainnet using valueless trial wallets.

Development of the user interface and recovery/blocking infrastructure.

Strategy: Zero exposure until full operational certainty

We will never expose real wallets with value until we have extremely high certainty that the algorithm operates correctly and securely on the mainnet. Our technical and ethical responsibility is absolute.

Summary:

The algorithm is already theoretically validated and functionally proven in a high-fidelity test environment.

It is based on strong mathematical foundations that redefine the approach to the discrete logarithm problem.

It does not compromise Bitcoin’s security and only acts on lost keys within a controlled domain.

The required investment will allow us to bring this foundation into a real-world operational phase—safely, ethically, and professionally.