Bootstrapping the Physical Layer of Web3

Attestima Whitepaper

• Cryptographically Secure Proof of Proximity

Version 0.1 (Draft) • July 2025

attestima.com

Contents

List of Figures

Acronyms

BLE Bluetooth Low Energy. 3

BLS Boneh–Lynn–Shacham. 10

CS Channel Sounding. 3, 7, 8, 9, 10, 15, 19, 23, 25

DAO Decentralized Autonomous Organization. 3, 23

dApp Decentralized Application. 24

DeFi Decentralized Finance. 3

DKG Distributed Key Generation. 10

DRBG Deterministic Random Bit Generator. 5

GPS Global Positioning System. 1, 2

IRL In Real Life. 1, 23

NFC Near-Field Communication. 2, 24

NFT Non-Fungible Token. v, 3

PBR Phase-Based Ranging. 3

POAP Proof of Attendance Protocol. 24

QR Quick-Response. v, 1, 2

RTT Round-Trip Timing. 3, 4

SIG Special Interest Group. 3

ZKP Zero-Knowledge Proof. 1, 14

Abstract

Attestima introduces a novel cryptographic infrastructure for verifying real-world proximity and presence without compromising privacy. Leveraging Bluetooth 6.0 Channel Sounding and tamper-resistant gateway devices, Attestima enables decentralized systems to cryptographically prove that users were physically co-located at a specific time and place. These proofs can be publicly verifiable, sybil-resistant, and optionally anonymous using zero-knowledge protocols or anonymous credentials. By transforming physical presence into a digital primitive, Attestima unlocks new possibilities for token-gated events, sybil-resistant airdrops, real-world NFT minting, decentralized ride access, and composable social graphs. It also lays the groundwork for future zero-knowledge-based reputation systems and off-chain interactions that anchor trust to real-world actions. Unlike legacy QR-code-based check-ins or GPS-based spoofable methods, Attestima provides relay-attack-resistant, cryptographically signed proximity proofs, with a flexible architecture compatible with both smart contract platforms and standalone networks.

1 Introduction

1.1 Background

As blockchain ecosystems evolve beyond purely digital interactions, the need to bridge real-world context with decentralized systems has become critical. Concepts such as sybil-resistant airdrops, token-gated IRL events, and real-world reputation increasingly demand trustworthy presence or proximity verification. However, existing approaches — such as QR code scans, GPS-based geofencing, or manual check-ins — suffer from critical limitations. They are either trivially spoofable, vulnerable to relay attacks, or require trusted third parties. These constraints make them unsuitable as cryptographic primitives in decentralized environments.

1.2 Problem Statement

There is no open, composable, and cryptographically secure infrastructure to verify physical co-presence and fine-grained proximity among participants. Without a tamper-resistant proximity layer, sybil attacks, fraudulent participation, and unverifiable claims remain unsolved in real-world Web3 applications.

The challenge is twofold:

- **Security:** Prove that devices were within a specific physical range, resistant to relay and spoofing attacks.
- **Privacy:** Allow users to prove presence and proximity without revealing identity, while still enabling event-level linkability or reputation building when desired.

1.3 Our Contribution

Attestima introduces a cryptographic proximity proof layer that enables verifiable, tamper-resistant, and optionally anonymous attestations of real-world co-presence. Our architecture combines:

- Bluetooth 6.0 Channel Sounding for fine-grained distance estimation
- Attestima Gateway Devices that serve as distributed trust anchors
- Smart contracts for token issuance and verification logic
- ZKPs / Anonymous Credentials (optional) for privacy-preserving linkability
- Composability for use in governance, airdrops, access control, and more

This whitepaper outlines the motivations, design, cryptographic properties, and potential applications of Attestima's system — laying the foundation for physical trust in decentralized networks.

2 Problem Motivation

As Web3 applications increasingly touch the physical world, proving that someone was present at a location or event has become a fundamental need. However, proving that two devices (or users) were within a specific physical distance — not just at the same general place — remains unsolved in a cryptographically secure way.

2.1 Existing "Presence" Methods Are Insecure

Today's presence verification systems rely on:

- QR codes (easily forwarded or scanned from afar)
- GPS coordinates (spoofable with off-the-shelf tools)
- Wi-Fi triangulation or NFC (low accuracy, still spoofable)
- Verbal or manual attestations (trust-based, unverifiable)

These approaches lack cryptographic rigor and are vulnerable to:

- Relay attacks: An attacker forwards presence signals remotely
- Sybil attacks: Bots simulate multiple identities "being there"
- Lack of granularity: No way to prove fine-grained proximity (e.g., who you stood near)

2.2 Presence $\neq$ Proximity

Importantly, presence alone isn't sufficient for many real-world applications. Use cases such as:

- Token distribution based on interaction density
- Building social graphs from physical co-presence
- Verifying co-riders, co-voters, or co-attendees require precise proximity evidence — not just being in the same venue.

There's currently no trustless infrastructure to:

- Cryptographically verify that two or more devices were within X meters
- Prevent spoofing, relaying, or misreporting
- Offer programmable logic based on co-proximity

2.3 A Missing Primitive for Web3

This creates a critical gap in Web3 tooling. Without cryptographically verifiable proximity:

- Sybil resistance in physical events remains weak
- Reputation systems built on attendance are easily gamed
- On-chain incentives for IRL activity are limited to heuristics

- Composability with DAOs, NFTs, and DeFi is fragmented and unverifiable

What's missing is a primitive — like a signature or a hash — but for co-location at the cryptographic level.

3 Background: Bluetooth Channel Sounding

Bluetooth and Bluetooth Low Energy (BLE) are wireless technologies that allow devices to communicate with each other over short distances. These technologies have evolved continuously for over 25 years. The Bluetooth Special Interest Group (SIG) manages the development of bluetooth standards.

By the end of 2024, the SIG published the new Bluetooth 6.0 standard, which introduced a new feature called Channel Sounding (CS). This feature enables devices to measure distances between each other accurately and securely [5, 8]. Although bluetooth radio-based distance measurements were already possible, the new channel sounding feature achieves significantly higher accuracy and includes explicit security mechanisms.

Attestima leverages bluetooth channel sounding to generate tamper-resistant proximity proofs for cryptographically binding physical co-presence and proximity. This section describes the technical underpinnings of bluetooth channel sounding, which is central to the trust assumptions in Attestima.

3.1 Distance Measurement Methods

There are two commonly used methods to measure distance with bluetooth:

- Phase-Based Ranging (PBR)
- Round-Trip Timing (RTT)

3.1.1 Phase-Based Ranging

The distance measurement procedure with PBR [8] is illustrated in Figure 1. Device 1 refers to the device performing the measurement, and Device 2 refers to the device being measured.

1. Device 1 transmits a signal at a known frequency f_1 with a known initial phase.
2. Device 2 receives the signal and records its phase (`receivephase`).
3. Device 2 echoes the signal back at frequency f_1, ensuring that the transmit phase equals the received phase.
4. Device 1 receives the echoed signal and measures the phase P_{f_1}.

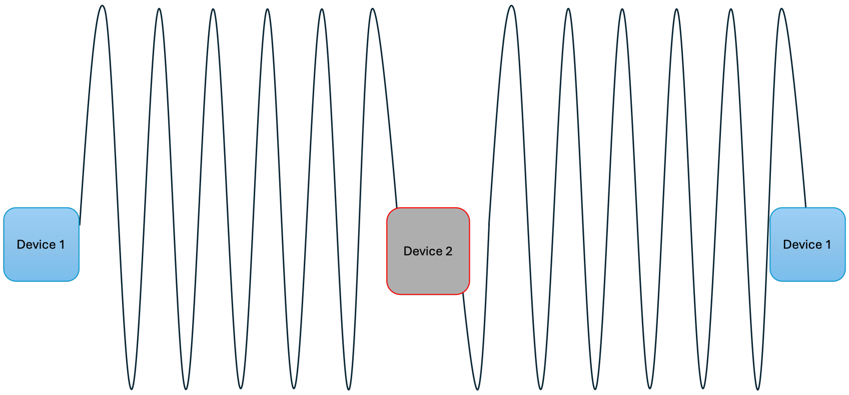

Figure 1: Ranging with Frequency using PBR [8].

Device 1 then selects another frequency f_2 and repeats the same process to obtain P_{f_2}. The distance r is computed as:

$$r = \left(\frac{c \cdot (P_{f_2} - P_{f_1})}{2\pi(f_2 - f_1)} \right) \mod \left(\frac{c}{f_2 - f_1} \right)$$

where c is the speed of light. This method is called two-way ranging since Device 2 reflects the signal back to Device 1.

3.1.2 Round-Trip Timing

The Round-Trip Timing (RTT) method calculates the time required for a signal to travel from Device 1 to Device 2 and back [8]. As radio signals travel at the speed of light, this time can be used to compute distance.

The variables used in RTT are:

- `ToD_1`: Time of departure from Device 1
- `ToA_2`: Time of arrival at Device 2
- `ToD_2`: Time of departure from Device 2
- `ToA_1`: Time of arrival at Device 1

The RTT is calculated as:

$$RTT = 2 \cdot ToF = \left[\frac{1}{1 + FFO_{RX} \cdot 10^{-6}} \cdot (ToA_1 - ToD_1) \right] - (ToD_2 - ToA_2)$$

where `FFO` is the fractional frequency offset, and `ToF` is the time-of-flight.

For Device 1 to compute RTT, it must know the turnaround time at Device 2, which is $(ToD_2 - ToA_2)$. A practical solution is to use a fixed turnaround time agreed in advance, ensuring Device 2 responds at a predefined interval.

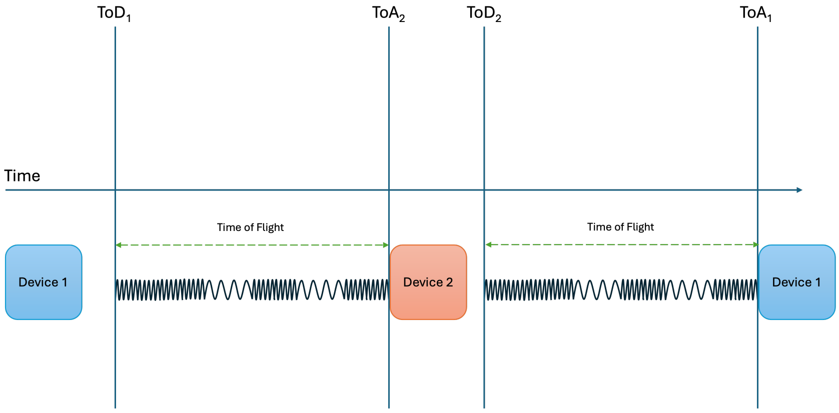

Figure 2: RTT-based distance measurement [8].

3.2 Sounding Procedure

Before initiating channel sounding, the Central device must establish a connection to the Peripheral device. The Central scans and connects, while the Peripheral advertises its presence. According to the Bluetooth 6.0 specification, the connection must be encrypted before channel sounding begins. Bluetooth uses AES in different modes internally for this purpose [5].

The full channel sounding procedure includes:

- **Security Start**
- **Capabilities Exchange**
- **Configuration**
- **Channel Sounding Start**

Security Start: Bluetooth channel sounding includes a dedicated internal security mechanism separate from connection encryption. In this stage, the Central generates:

- `CS_IV_C`: Initialization vector (64 bits)
- `CS_IN_C`: Instantiation nonce (32 bits)
- `CS_PV_C`: Personalization vector (64 bits)

Then the Peripheral generates:

- `CS_IV_P`, `CS_IN_P`, `CS_PV_P`

The vectors `CS_IV` and `CS_IN` are generated per FIPS PUB 140-2 [1]. `CS_PV` is implementation-defined. These values are used to seed a deterministic random bit generator (DRBG), which is compliant with NIST recommendations.

Capabilities Exchange: Devices exchange their optional and supported capabilities, such as number of antennas or supported roles.

Configuration: Devices agree on a configuration, including role assignment (Initiator, Reflector).

Channel Sounding Start: Once configured, devices exchange timing and structural parameters and begin sending CS_SYNC packets as shown in Figure 3.

Preamble (1 or 2 octets)	CS Access Address (4 octets)	Trailer (4 bits)	Sounding Sequence (32 or 96 bits) or Random Sequence (32, 64, 96, or 128 bits)

Figure 3: CS_SYNC packet structure used during RTT [8].

3.3 Security Mechanisms

Channel sounding incorporates several security mechanisms based on cryptographically controlled randomness. These defenses significantly increase resistance against replay, relay, and spoofing attacks [8]:

- **Secure Access Addresses:** The 32-bit access address changes for each step, derived from the DRBG state. This prevents packet tracking and spoofing.
- **Random/Sounding Sequences:** Sounding packets use random sequences, generated by DRBG, and sounding sequences into which 4-bit marker signals are randomly inserted.
- **Tone Extension Slots:** In PBR, tone slot usage is randomized. The receiver knows whether to expect a tone or silence.
- **Antenna Path Selection:** Up to 4 antennas and 8 paths may be used. The antenna configuration order is randomized by the DRBG.
- **Channel Selection:** Transmissions span 79 RF channels in the 2.4 GHz ISM band, and the sequence is DRBG-randomized.
- **SNR Control:** Devices agree to inject known noise into their signals. Since both devices know the noise pattern, they can cancel it. Attackers cannot.

These mechanisms ensure only mutually authenticated and synchronized devices can complete a valid channel sounding session. They form the basis for Attestima's proximity proofs, enabling cryptographically secure, verifiable, and Sybil-resistant IRL interaction attestations.

4 Protocol Design

4.1 System Architecture

Attestima's architecture consists of Bluetooth CS-capable end-user devices, gateway nodes with trusted execution, and optional relayer or backend components depending on the deployment context.

User Devices. Each participant device must support Bluetooth 6.0 with Channel Sounding capabilities. These devices engage in proximity measurement sessions either with Attestima gateways or, in some configurations, with each other. Devices are provisioned with public/private keys and optionally configured for biometric association, enabling both anonymous and person-linked proofs.

Gateways. Gateways are stationary devices deployed at events, venues, or public/retail spaces. They coordinate channel sounding exchanges with nearby devices and act as secure anchors for proof generation. Gateways:

- Execute CS rounds with all devices that want to join Attestima network
- Collect and optionally aggregate distance measurements
- Sign and timestamp interaction data
- Submit proofs on-chain or to off-chain endpoints

Gateways are trusted to execute channel sounding securely and attest to proximity measurements. In event-based scenarios, they coordinate proximity rounds on a fixed schedule. In ambient/passive deployments, they collect distance data opportunistically without requiring an explicit round structure.

Relayers and APIs. Depending on the integration model, gateways can transmit proofs directly to smart contracts or use intermediate relayers. Relayers can batch, filter, or reformat proofs, and provide external APIs for retrieval, analytics, or business logic integration.

Smart Contracts. When used in minting or governance scenarios, smart contracts on-chain validate proximity proofs and trigger token distribution, NFT minting, or reputation updates. The contracts verify cryptographic signatures and evaluate distance thresholds and time constraints.

This modular design supports both Attestima-native applications (e.g., $TIMA rounds, IRL NFTs) and external systems using proximity data as a verifiable input. Figure 4 illustrates the architecture of Attestima, highlighting key system components and the flow of proximity proofs across both on-chain and off-chain pathways.

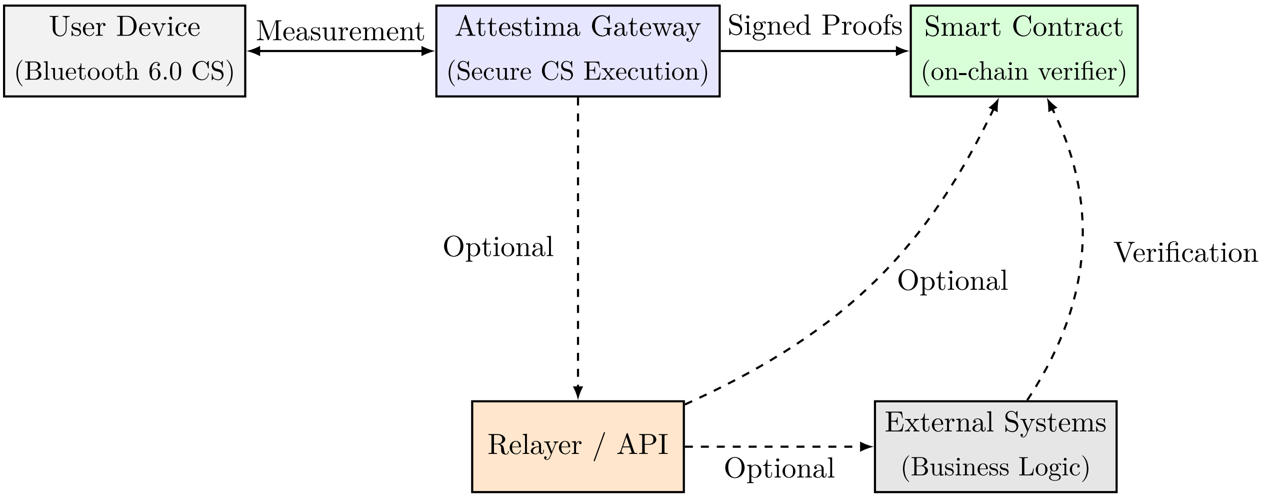

Figure 4: Attestima system architecture showing proximity measurement, proof flow, and optional integration paths.

4.2 Proximity Round Mode

Attestima provides a structured "proximity round" mode designed primarily for event-based or periodic scenarios, where proximity proofs need to be generated, validated, and optionally associated with on-chain rewards, reputation metrics, or governance mechanisms.

A proximity round is a time-bounded interval during which Attestima gateways initiate and coordinate proximity measurements between themselves and participant devices. These rounds start at predefined intervals (e.g., every 10 minutes) and follow a consistent, secure workflow:

Round Initialization. At the beginning of each round, gateways announce their readiness to conduct Bluetooth CS sessions. Participant devices discover these announcements via standard bluetooth advertising methods and become ready to join the round.

Measurement and Interaction. Once devices join, they engage in secure channel sounding exchanges both with gateways and among themselves. This multi-party simultaneous measurement ensures a highly reliable proximity graph. Specifically:

- Devices perform distance measurements simultaneously with gateways and peer devices using Bluetooth Channel Sounding (CS), as described in Section 3.
- Each participant (gateways and user devices) securely measures distances to as many reachable participants as they can within the round, creating a comprehensive interaction graph.
- Measurements are executed in synchronized intervals, ensuring consistency and verifiability of proximity data across multiple independent measurements.

For instance, if Device 1 and Device 2 both join proximity measurements coordinated by Gateway X, all three participants (Device 1, Device 2, and Gateway X) simultaneously measure distances to each other. This mutual and simultaneous measurement provides strong cryptographic assurances of physical co-presence.

Proof Aggregation and Signing. Upon completion of simultaneous measurements, gateways aggregate proximity data and generate cryptographic signatures. This ensures:

- Authenticity, timeliness, and integrity of proximity data.
- Inclusion of metadata (timestamps, session identifiers, or additional context) to uniquely identify each round.
- Verifiable multi-party attestations: signatures from gateways reinforce proof validity, allowing independent on-chain verification of simultaneous measurements.

Proof Submission and Processing. Aggregated and signed proximity proofs are submitted directly to blockchain smart contracts as well as to designated off-chain endpoints:

- **On-chain submission:** Proximity proofs are publicly verifiable, supporting token distributions, NFT minting, or on-chain reputation management.
- **Off-chain submission:** Proofs can be delivered through APIs to external business logic, analytics services, or customer-defined systems without involving blockchain operations.

Proximity rounds thus provide a structured, secure, and comprehensive mechanism for verifying simultaneous physical co-presence in scenarios such as conferences, festivals, governance meetings, and other Web3-aligned physical events. This mode supports Attestima-native incentives (such as $TIMA token minting), while offering rich cryptographic guarantees and flexibility for various external business use cases.

4.3 On-Demand Passive Mode

Besides the periodic round mode designed for event-driven scenarios, Attestima also offers an on-demand, passive proximity verification mode. This mode allows customers to continuously measure and utilize proximity information without scheduling explicit rounds or minting tokens.

In passive mode, Attestima gateways continuously perform Bluetooth CS distance measurements with nearby user devices. Unlike proximity rounds, this mode does not require synchronized start intervals.

Use-Case Example. Consider a retail shop equipped with Attestima gateways. The shop owner might want to reward customers based on their presence or behavior in certain areas. Without the need to initiate explicit rounds, the gateways passively measure the proximity of devices carried by shoppers moving around the store. This allows the retailer to:

- Identify customer engagement zones (e.g., specific aisles, promotional displays).
- Trigger targeted real-time promotions or random rewards based on proximity data.
- Analyze aggregated shopper behavior to optimize store layout or merchandising strategies.

Measurement and Data Collection. Gateways continuously gather proximity values by securely measuring distances to devices within range. Collected proximity information can be timestamped and cryptographically signed, ensuring authenticity and tamper-resistance.

Data Delivery and Usage. Proximity data collected in passive mode can be provided directly through Attestima's APIs to customer systems for integration into their proprietary analytics, CRM, or reward management platforms. This data is typically delivered off-chain, enabling flexible, real-time use cases without the complexity or latency associated with blockchain transactions. However, customers may optionally choose to commit selected proximity proofs on-chain if verifiable public auditability is required.

On-demand passive mode thus provides businesses with continuous, verifiable, and actionable proximity data, enabling flexible integration into diverse operational contexts without necessarily interacting with blockchain components or minting new tokens.

4.4 Multi-Party Signature Mode

Attestima also offers a specialized Multi-Party Signature Mode, specifically designed for scenarios requiring cryptographically secure, proximity-based multi-party signatures. This mode ensures that a specified threshold of participants must be physically present together in a designated location to generate valid signatures or authorize sensitive blockchain transactions.

This mode leverages the Boneh–Lynn–Shacham (BLS) signature scheme [2, 3], which supports aggregation of multiple individual signatures into one concise, verifiable signature. Additionally, Attestima integrates a secure Distributed Key Generation (DKG) protocol, managed by the gateways, allowing participant devices to securely generate and distribute cryptographic keys among themselves without relying on a single trusted authority. The integrated DKG protocol follows the secure construction presented in [7].

Devices supporting Bluetooth 6.0 Channel Sounding—whether off-the-shelf smartphones with the Attestima application or dedicated Attestima hardware—execute this distributed key generation protocol and subsequently generate proximity proofs to cryptographically bind physical co-location with multi-party signatures.

Use-Case Example. Consider a company's board of directors consisting of five members, each authorized to sign blockchain transactions. Company policies require at least three board members to physically meet in a secure room at the corporate headquarters to authorize transactions. The company's smart contract validates transactions only if it receives signatures from at least three members and verifies that these signatures were generated simultaneously from the same physical location.

In this scenario:

- Board members' devices conduct simultaneous Bluetooth CS measurements among each other and with the gateway installed in the secure room.

- Each device participates in the distributed key generation process, establishing shared cryptographic keys without any single point of failure or trust (anytime before the signing process).
- During transaction signing, devices simultaneously generate proximity proofs and cryptographic signatures.
- The gateway aggregates and signs these proofs, attesting to the authenticity, simultaneous presence, and physical co-location of signatories.
- Finally, the smart contract verifies the threshold BLS aggregated signature and associated proximity proofs before executing the transaction.

This mode effectively combines multi-party cryptography, threshold signatures, and Bluetooth 6.0 Channel Sounding to offer a secure, verifiable, and auditable mechanism for physically constrained multi-party blockchain transactions.

4.5 Proximity Proof Generation

The details of Attestima's proximity proof generation involve novel, cryptographically secure processes that represent critical intellectual property and significant competitive advantage. At the current pre-seed stage, these core mechanisms are intentionally omitted from this whitepaper. Additional information can be disclosed to investors upon mutual agreement under appropriate confidentiality arrangements.

4.6 Proof Consumption

Attestima provides flexible options for clients and integrators to consume and leverage proximity proofs generated by the system. Proofs can be utilized through on-chain smart contracts or off-chain integration points, allowing businesses and organizations to choose the most suitable approach for their use cases.

On-chain Proof Consumption. Attestima proximity proofs can be directly submitted and validated on blockchain platforms. This approach provides transparency, immutability, and public auditability, which are valuable for decentralized applications or scenarios that benefit from public verifiability. Typical on-chain use cases include:

- **Token Distribution and Rewards**: Automatically distribute tokens (e.g., $TIMA) based on verified physical proximity or interaction metrics.
- **NFT Minting**: Mint NFTs as proof-of-attendance or verifiable IRL experiences, ensuring only physically present participants receive these unique digital assets.
- **Governance and DAO Roles**: Enhance decentralized governance systems by weighting voting rights or assigning specific roles based on verifiable physical co-presence.
- **Reputation and Identity Management**: Establish verifiable proximity-based reputations, trust metrics, or anonymous credentials integrated with decentralized identity (DID)

frameworks.

Importantly, clients can also utilize these on-chain proofs to support their specific business logic, extending Attestima's trust infrastructure into custom blockchain-enabled applications.

Off-chain Proof Consumption. Attestima also supports traditional off-chain integrations through APIs and data streams, enabling businesses to seamlessly incorporate proximity data into their existing infrastructure. Common off-chain applications include:

- **Business Analytics**: Real-time or historical proximity data analytics for retail stores, event organizers, or venue management systems.
- **Loyalty and Reward Systems**: Customer engagement programs triggered by proximity events (e.g., random or targeted gifts based on verified location).
- **Custom Integrations**: Flexible integration into CRM systems, marketing automation, IoT-based services, or proprietary business applications.
- **Real-time Triggers**: Real-time proximity-driven interactions or responses (e.g., targeted advertising, promotions, or operational alerts).

By supporting both on-chain and off-chain proof consumption, Attestima enables clients to freely choose or combine these options, facilitating integration with diverse business scenarios and technological infrastructures. This flexibility allows Attestima clients to fully leverage proximity proofs according to their operational, security, and business needs.

5 Security & Privacy

Attestima is designed with strong security and privacy principles at its core, ensuring that proximity proofs are trustworthy, tamper-resistant, and privacy-preserving. Given the sensitive nature of physical location data and identity-linked interactions, the system incorporates multiple cryptographic and architectural safeguards to protect both integrity and confidentiality.

5.1 Threat Model

Attestima defends against a broad set of threats common to proximity and presence protocols:

- **Spoofing**: Devices attempting to falsely claim proximity to other users or gateways.
- **Relay Attacks**: Adversaries relaying signals to simulate closeness between distant devices.
- **Replay Attacks**: Previously recorded measurements being reused to fake new proximity proofs.
- **Collusion**: Coordinated attacks by compromised participants to forge co-presence.
- **Tracking**: Linking proximity data across rounds or locations to infer user movement.

5.2 Security Mechanisms

Attestima integrates the following countermeasures:

- **Bluetooth Channel Sounding**: As detailed in Section 3, Bluetooth 6.0 CS provides high-resolution physical-layer measurements that are extremely difficult to relay or spoof due to time-bound round-trip timing constraints and directional measurements.
- **Cryptographic Binding**: All distance measurements are signed and timestamped by trusted gateways, ensuring the authenticity and temporal validity of the data. Signatures include metadata (e.g., round identifiers, block hashes) to prevent replay or injection attacks.
- **Multi-party Verification**: In proximity rounds and multi-party signature modes, participants verify proximity not just to the gateway but to each other. This mutual measurement increases resistance to manipulation and enforces decentralized validation.
- **Distributed Key Generation**: For multi-party settings, cryptographic keys are distributed securely among participants without relying on a central trusted authority, preventing single-point compromise (see Section 4.4).

5.3 Privacy Guarantees

Attestima is built to minimize unnecessary data exposure and offer users control over identity linking. Key privacy-preserving properties include:

- **Optional Identity Binding**: Users may choose to associate their device with a persistent identity (e.g., for token rewards), or remain pseudonymous, depending on the use case.

- **Minimal Data Collection**: Gateways only record proximity metadata required to verify proofs. No continuous tracking, GPS, or external identifiers are required by design.
- **Selective Disclosure**: Proofs are composable and scoped to individual events or rounds, preventing long-term correlation or behavioral profiling.
- **Anonymous Credentials (Roadmap)**: In future deployments, Attestima will support anonymous credential systems. When enabled, these allow users to obtain and prove possession of attributes (e.g., “early adopter,” “attended 3 events,” “employee tier 1”) without revealing their identity or enabling linkability across events. This ensures that while users’ activities remain fully unlinkable, clients can still derive meaningful, privacy-preserving insights about user behavior and engagement patterns.

5.4 ZK Proof Roadmap

To further enhance user anonymity and unlinkability, Attestima plans to integrate Zero-Knowledge Proof (ZKP)-based proximity attestations. These mechanisms will allow users to:

- Prove participation in proximity events without revealing specific devices or times.
- Link event participation to reputation or eligibility without disclosing identities.
- Perform threshold attestations (e.g., "I was in proximity with at least 5 attendees") without exposing raw distance data.

Our privacy roadmap aligns with emerging best practices in decentralized identity and verifiable credential systems, making Attestima a long-term enabler of privacy-preserving physical presence protocols.

6 Token Economics

6.1 Token Overview

$TIMA is the native utility token of the Attestima ecosystem. It underpins the economic incentives and trust mechanisms behind cryptographically verifiable physical proximity. Unlike generic presence tokens, $TIMA is explicitly tied to high-integrity proofs of co-presence and proximity derived from Bluetooth Channel Sounding (CS), making it uniquely resistant to spoofing and manipulation.

6.2 Token Utility

The $TIMA token serves several core functions:

- **Proximity Incentives**: Users who participate in proximity rounds and generate verifiable proofs receive $TIMA as a reward.
- **On-chain Integration**: Third-party smart contracts can require $TIMA as a verifiable currency for services contingent on physical proximity (e.g., gated access, exclusive drops, IRL role validation).
- **Governance (Roadmap)**: Token holders will eventually participate in protocol governance, including rule updates, reward structures, and integration policies.
- **Sybil Resistance and Staking (Optional)**: Applications may require staking or token bonding to prevent spam, incentivize honesty, or prioritize premium proximity relationships.

6.3 Minting Policy

$TIMA tokens are minted only in conjunction with verified proximity events. The system ensures that all minting activity is backed by cryptographically signed interaction graphs, authenticated by trusted gateways.

Each proximity round produces a limited number of $TIMA tokens, which are distributed between participants and gateway operators. This scarcity model aligns token issuance with real-world activity and event intensity, not arbitrary emissions.

6.4 Use Cases and Value Accrual

$TIMA gains utility and value from its role in a growing set of physical-world and Web3-integrated applications, including:

- **IRL Engagement Campaigns**: Events and venues can sponsor $TIMA-backed proximity rewards to boost participation or reward long-term supporters.
- **Loyalty Systems and Access Control**: Brands or communities may distribute $TIMA or require it for proof-backed memberships or access tiers.
- **Trust and Reputation Signals**: Applications using Attestima data can rely on $TIMA-backed proofs for roles, voting power, or IRL-based Sybil resistance.

6.5 Future Extensions

As part of the Attestima roadmap, we plan to launch a dedicated L2 rollup or custom chain purpose-built for proximity applications. All existing $TIMA tokens on the current deployment chain will be redeemable or migrated to this native environment. This ensures continuity and cross-chain utility, while enabling scalability, low-latency settlement, and native interoperability for proximity-driven smart contracts.

Future mechanisms under consideration include:

- **ZK-based Airdrops**: Token drops targeted at users with specific proximity histories, without disclosing identities.
- **Burn-and-Mint Cycles**: Reward models where proximity participation affects future token minting ceilings.
- **Staking and Vesting**: Long-term lock-in models for governance or infrastructure participants.

7 Roadmap

Attestima is being developed through clearly defined phases that align technical, product, and go-to-market strategies. From early-stage proximity verification to full protocol-level infrastructure, the roadmap focuses on delivering value to users while evolving toward a native blockchain environment.

7.1 Q4 2025 – Q1 2026: Alpha Rollout

- BLE gateway hardware development, certification, and production
- Initial real-world deployments at selected IRL events
- Smart contract deployment for $TIMA minting and proximity graph access
- Begin $TIMA token operations and gateway monetization (sales/rentals)

7.2 Q2 2026: Ecosystem Launch

- Onboard early customers: DAOs, NFT platforms, event organizers
- Release SDKs and APIs for proximity-based applications
- Launch linkable reputation mechanisms (non-ZK)
- Introduce staking/burning models for $TIMA usage

7.3 Q3 – Q4 2026: Privacy & ZK Layer

- Add optional zero-knowledge presence and proximity proofs
- Launch anonymous credentials and KYC-compatible private identity layer
- Enable private linking of event attendance and participation history

7.4 2027: Proximity as a Protocol

- Launch Attestima-native Layer-2 rollup or standalone chain
- Enable composable on-chain proximity queries and ZK access control
- Support third-party adoption of Attestima as a verifiable physical layer for Web3

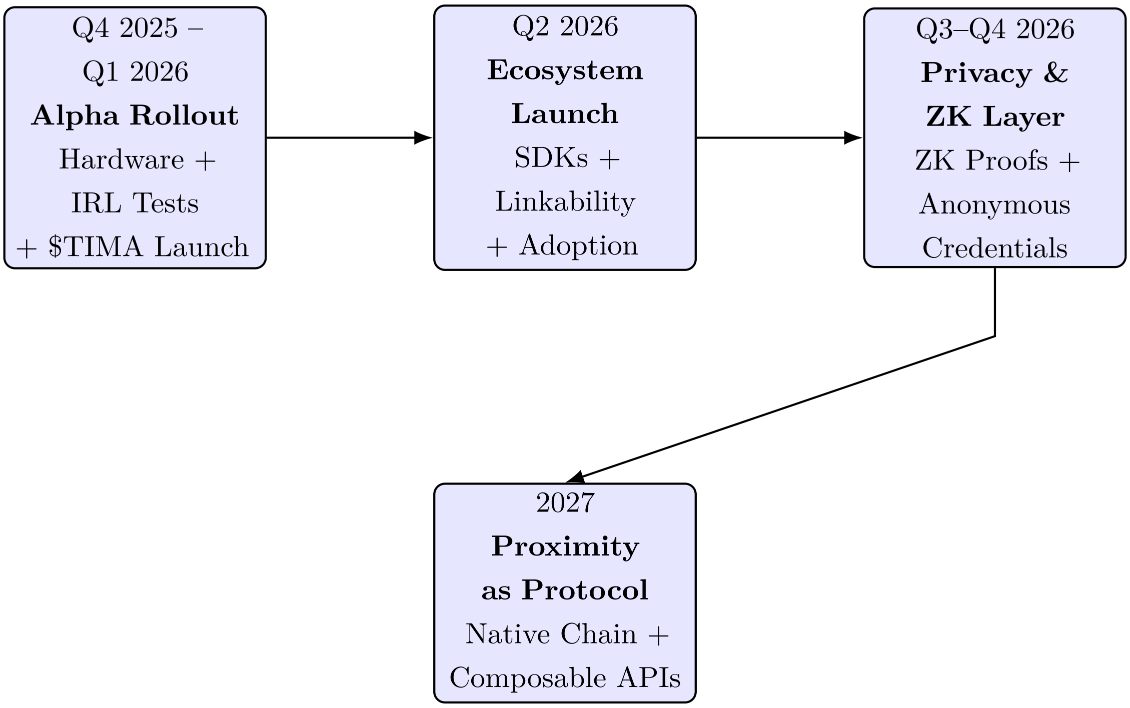

Figure 5: Attestima roadmap overview

8 Use Cases

Attestima transforms verifiable physical proximity into a programmable primitive, enabling a broad range of applications across Web3, enterprise, and public infrastructure domains. Unlike location-based or QR-based solutions, Attestima provides tamper-resistant cryptographic proximity proofs with optional biometric or anonymous credentials. Below we highlight key use cases grouped by context.

8.1 IRL Events and Conferences

Events and festivals represent a natural fit for Attestima's periodic proximity rounds. Attendees equipped with BLE CS-enabled devices can participate in scheduled rounds to prove their co-location with peers or booths.

- **Token-Gated Participation:** Access to exclusive zones, meetups, or voting rights is granted only to those physically present.
- **Proof-Based NFT Minting:** Mint verifiable "I Was There" NFTs without QR codes, GPS spoofing, or manual check-ins.
- **Sybil-Resistant Airdrops:** Reward real-world participation with $TIMA or partner tokens, ensuring one-human-one-proof.
- **Reputation Systems:** Build persistent IRL participation records, optionally linked via anonymous credentials.

8.2 Retail and Ambient Campaigns

Attestima's passive mode supports business use cases where proximity is measured continuously without rounds:

- **Presence-Based Loyalty:** Customers earn rewards or coupons by spending time in specific zones (e.g., an alley near a shop).
- **Randomized Gifting:** Businesses can trigger surprise gifts based on verifiable presence windows.
- **Dwell Time Analytics:** Track foot traffic near stores, installations, or city zones in a privacy-preserving way.

8.3 Workplace and Institutional Applications

Gateways deployed in secure buildings or offices can verify physical co-presence of employees, students, or visitors.

- **Workplace Attendance:** Employees earn $TIMA or custom enterprise tokens based on presence proofs.
- **University Classes:** Instructors receive verifiable attendance data without QR roll-calls.

- **Secure Room Entry:** Combine proximity with biometric keys to control entry to sensitive rooms.

8.4 Governance and Multi-Signature Authorization

Attestima supports proximity-constrained multi-party authorization:

- **Boardroom Multisig:** Enforce smart contracts that require t-of-n co-signers to be present in the same room.
- **DAO Governance Anchoring:** Weight voting or proposal access by physical meeting participation.

8.5 Mobility and Logistics

Proximity proofs can be used to verify co-presence in decentralized mobility and logistics contexts.

- **Decentralized Ridesharing:** Verify passengers and drivers are co-located before triggering payments.
- **Trusted Package Delivery:** Require physical proximity of recipient and courier to confirm handoff.
- **AV Unlock Conditions:** Enforce IRL access control to autonomous vehicles based on proximity attestations.

8.6 Social, Gaming, and Experience Design

Attestima makes physical interaction composable into games and social logic.

- **IRL XP Systems:** Users gain experience points or tokens by attending quests, missions, or events.
- **Fan Campaigns:** Artists or brands reward physical presence during tours, product launches, or flash mobs.
- **Friend Graph Construction:** Build verifiable proximity-based friend graphs without revealing identities.

8.7 Public Sector and Identity Systems (Future)

With optional ZK-based anonymous credentials, Attestima enables strong identity primitives:

- **ZK-Proof of Presence:** Prove you were present at event X and Y without revealing you are the same person.
- **GovTech Applications:** Municipal services or voting mechanisms requiring physical presence can leverage Attestima.
- **IRL Whitelisting:** Enable verified anonymous access to events, subsidies, or checkpoints.

9 Business Model

Attestima operates as a proximity verification infrastructure provider, enabling cryptographically verifiable proofs of co-presence to be consumed by diverse applications. Its business model combines infrastructure deployment, token-based incentives, and enterprise integrations.

9.1 Revenue Streams

Infrastructure-as-a-Service (IaaS). Attestima gateways can be deployed by customers (e.g., event organizers, retailers, enterprises) under a licensing or subscription model. This enables:

- **Self-hosted gateways:** Customers purchase or lease Attestima gateways and run their own proximity logic.
- **Managed service:** Attestima provides hosted backend and gateway orchestration.
- **Hybrid deployment:** Gateways operate on customer premises while submitting proofs to Attestima APIs or smart contracts.

Proof API Access. Customers can query and verify proximity proofs through Attestima APIs for:

- Attendance validation and audits
- IRL gating of services or digital content
- Loyalty, rewards, and consumer analytics

Tiered API pricing supports volume-based billing.

On-Chain Proof Monetization. Proximity proofs submitted on-chain can trigger:

- $TIMA token minting and burning
- NFT issuance and royalties
- Governance weight updates in dApps

Attestima can take protocol fees or share revenue from proof-triggered assets.

9.2 Token Utility and Economy

$TIMA Token. $TIMA is the native token of the Attestima protocol. Its primary utilities include:

- Rewarding users for verifiable presence and proximity
- Staking or bonding to operate gateways
- Settling on-chain proof validations and gas fees

Clients can build custom applications using $TIMA or integrate it into their reward and access systems.

Future Chain Migration. Attestima is designed to evolve toward a dedicated rollup or custom chain. Prior $TIMA tokens will be convertible and usable on the native chain, preserving early utility and aligning incentives across migration.

9.3 Integration Models

Attestima supports multiple integration pathways:

- **Smart Contract Consumers:** dApps ingest proximity proofs directly to gate functionality (e.g., vote eligibility, claim rights, mint conditions).
- **Off-Chain Business Logic:** External systems (e.g., HR tools, CRMs, analytics engines) consume signed proofs via API.
- **SDKs and White-label Solutions:** Partners can embed Attestima into their mobile or IoT platforms.

9.4 Network Growth and Flywheel

- More gateways deployed → more coverage and utility.
- More users generating proofs → higher value for customers.
- More customer integrations → higher token velocity and revenue.
- Token incentives → bootstrap supply and encourage honest participation.

Attestima builds a decentralized and privacy-preserving physical layer for Web3, with value capture at both infrastructure and application layers.

10 Market Opportunity

The convergence of physical presence and digital interaction is opening a new frontier for cryptographic infrastructure. Attestima is positioned at the intersection of this emerging domain, enabling secure proofs of proximity that serve as a foundational primitive for real-world Web3 applications.

10.1 The Physical-Digital Convergence

As digital systems increasingly integrate with real-world environments, demand is growing for technologies that bridge physical presence with verifiable, privacy-preserving computation. Existing methods such as QR codes, GPS, NFC, and camera-based scanning fall short in either security, precision, or usability. Attestima addresses this gap with a novel cryptographic proximity protocol built on Bluetooth CS.

10.2 TAM/SAM/SOM Estimates

We estimate Attestima's market opportunity through a conservative analysis of overlapping sectors:

- **Total Addressable Market (TAM):** The global market for location-based services (LBS), real-time location systems (RTLS), and event technology collectively exceeds $100 billion. According to MarketsandMarkets, the LBS and RTLS sector is projected to grow from $24.7 billion in 2023 to $60.4 billion by 2028 at a CAGR of 19.6% [6]. Simultaneously, the event management software market is projected to grow from $8.4 billion in 2024 to $17.3 billion by 2030 [4]. When we also consider adjacent segments such as access control, identity verification, and location-aware enterprise tooling, a combined TAM of over $100 billion is well justified.

- **Serviceable Available Market (SAM):** Focusing on sectors most directly aligned with Attestima's capabilities—such as physical ticketing, DAO governance tooling, workplace attendance verification, and IRL NFT minting—we estimate a SAM of $5–10 billion. These are areas where secure proximity verification is both immediately valuable and currently underserved by cryptographic infrastructure.

- **Serviceable Obtainable Market (SOM):** By targeting Web3-native early adopters, decentralized organizations, and event-based ecosystems, Attestima can credibly capture $50–100 million in its first adoption cycles. This projection corresponds to capturing 1–2% of the estimated SAM, based on comparable adoption trajectories of Web3 infrastructure protocols.

10.3 Emerging Adoption Trends

Attestima aligns with macro trends accelerating demand for verifiable co-presence:

- Growth of token-gated IRL experiences (festivals, DAOs, conferences)
- Enterprise demand for verifiable attendance (e.g., hybrid workplaces, shift validation)

- Rise of SocialFi and location-aware dApps
- Decentralized reputation systems that incorporate physical presence

10.4 First-Mover Advantage

While "proof of presence" systems exist (e.g., NFC badges, POAPs), they lack:

- Cryptographic guarantees of proximity
- Decentralized attestation
- Privacy-preserving credentials
- Multi-party composability

Attestima is the first platform to offer a cryptographically secure physical proximity protocol. This enables use cases previously unachievable with legacy or Web2 tools.

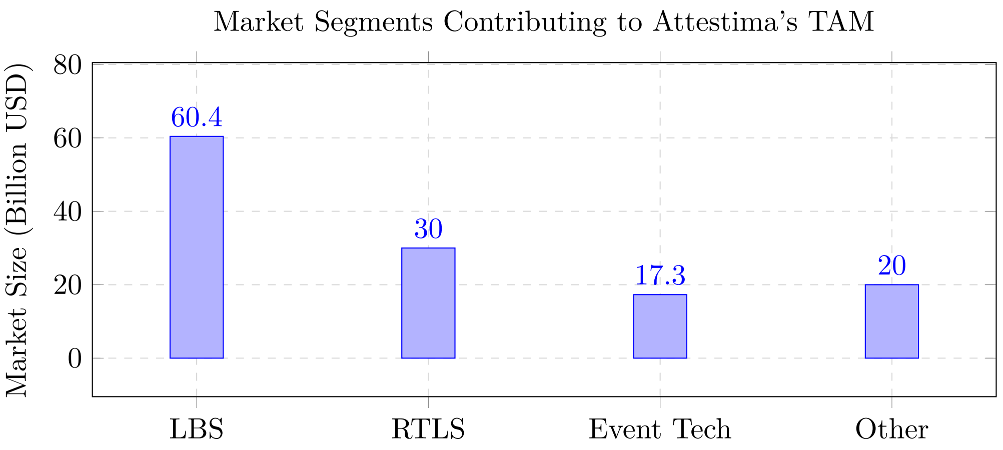

Figure 6: Estimated contributions of market segments to Attestima's Total Addressable Market.

11 Closing Remarks and Call to Action

Attestima introduces the first cryptographically secure physical proximity protocol, enabling a new class of decentralized applications that bridge physical presence and digital trust. By leveraging Bluetooth CS, trusted gateways, and privacy-preserving primitives, Attestima empowers event organizers, enterprises, decentralized communities, and builders with composable, verifiable, and privacy-aware proximity proofs.

This whitepaper outlines the foundational architecture, key use cases, and roadmap for Attestima. As the protocol matures, future phases will introduce anonymous credentials, multi-party signature schemes, and a native blockchain environment to further decentralize and scale Attestima's capabilities.

We are currently seeking aligned investors and partners who share our vision for a cryptographically secure physical layer of Web3. Attestima is an opportunity to shape this layer from the ground up — one that not only ensures trust at the edge, but also opens the door to entirely new primitives in digital coordination, governance, and reputation.

Join us in bootstrapping the physical layer of Web3.

To get in touch: `contact@attestima.com`

References

[1] E. B. Barker and J. M. Kelsey, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2015.

[2] D. Boneh, B. Lynn, and H. Shacham, Short signatures from the weil pairing, in *International conference on the theory and application of cryptology and information security*, pp. 514–532, Springer, 2001.

[3] D. Boneh and V. Shoup, *A graduate course in applied cryptography*, 2023.

[4] Grand View Research, Event management software market size, share & trends analysis report by component (software, services), by deployment, by organization, by application, by end-use, by region, and segment forecasts, 2024 - 2030, `https://www.grandviewresearch.com/industry-analysis/event-management-software-market-report`, 2024.

[5] B. S. I. Group, Bluetooth core specification v6.0, `https://www.bluetooth.com/specifications/specs/core-specification-6-0/`, 2024.

[6] MarketsandMarkets, Location-based service (lbs) and real-time location systems (rtls) market worth $60.4 billion by 2028, https://www.prnewswire.com/news-releases/location-based-service-lbs-and-real-time-location-systems-rtls-market-worth-60-4-billion-by-2028—exclusive-report-by-marketsandmarkets-302051809.html, 2024.

[7] W. Neji, K. Blibech, and N. Ben Rajeb, Distributed key generation protocol with a new complaint management strategy, Security and communication networks, 9(17), pp. 4585–4595, 2016.

[8] M. Woolley, Bluetooth channel sounding technical overview, Technical report, Bluetooth Special Interest Group, 2024.