BGIN Block#12 Meeting Report

- BGIN is a multi-stakeholder discussion body / distributed think tank.

Wallet Governance / Accountable Wallet

bg in

blockchain
governance
initiative
network

The Global Network for Blockchain Stakeholders™

BGIN Block#12

Wallet Governance / Accountable Wallet

Date: Monday, March 3, 2025

Location: Tokyo, Japan

Duration: Approx. 90 minutes

Materials: BGIN_WD_SR00**_ Wallet Governance and Policy Study Report
IKP_Accountable Wallet Accountable Wallet - BGIN #12.pptx.pdf

Summary

1. Background and Motivation for the Accountable Wallet
    - Addressing the Problem Space
        - The speaker begins by setting the context for the problem the Accountable Wallet aims to address.
        - They cite recent high-profile incidents in the crypto space, particularly exchange hacks and DeFi exploits that have resulted in significant financial losses.
    - Types of Security Threats Identified
        - The speaker categorizes three major security concerns affecting decentralized transactions:
            - Exchange and platform vulnerabilities – Billions in losses due to exchange breaches.
            - DeFi attack vectors – Manipulation through flash loan exploits, sandwich attacks, and smart contract loopholes.
            - Illicit finance risks – Despite existing monitoring tools, money laundering remains a challenge.
    - The Growing Complexity of Transaction Tracking
        - The speaker highlights that Layer 2 solutions, rollups, and privacy-enhancing technologies are making transaction tracking increasingly complex.
        - They explain that as scaling solutions improve, transaction data is becoming more difficult to analyze, leading to concerns about compliance and transparency.
2. Philosophy Behind the Accountable Wallet
    - Acknowledging that a perfect solution does not exist, the speaker sets realistic expectations:
        - "We recognize that there is no single mechanism capable of completely eliminating illicit activity in decentralized transactions."

    - Instead of attempting to block every illicit transaction, the goal is to help legitimate users protect themselves from inadvertently engaging with illicit funds.

- Proposed Approach: A Practical Framework for Trust

    - The Accountable Wallet is framed as a proactive solution that helps users:
        - Prove their legitimacy before engaging in transactions.
        - Avoid exposure to illicit funds by filtering out interactions with suspicious sources.
        - Preserve privacy while still complying with legal and financial regulations.

    - The analogy of "building protective barriers" is used to describe how the system helps ensure compliance for honest actors rather than focusing on eliminating bad actors directly.

3. Discussion on Current Security Threats

The speaker outlines three main categories of illicit activities in decentralized finance:

(a) Security Breaches and Hacks on Crypto Platforms

- Large-scale exchange hacks have resulted in billions of dollars in losses over the past decade.
- Despite improvements in security infrastructure, audits, and operational safeguards, hackers continue to exploit vulnerabilities in both centralized and decentralized platforms.
- The speaker mentions notable DeFi exploits, stating that:
    - Some attackers directly exploit vulnerabilities in smart contract code.
    - Others use advanced financial strategies such as flash loan attacks to manipulate market prices and extract profits without technically breaking any rules.

(b) Money Laundering via Decentralized Networks

- The speaker highlights that illicit transactions are increasingly difficult to track as decentralized financial tools evolve.
- Privacy-enhancing technologies and Layer 2 solutions allow users to conduct transactions off-chain, making traditional forensic tracking methods less effective.
- The growing adoption of cross-chain asset transfers makes it even harder to trace the origins of funds, enabling bad actors to move funds across multiple blockchains.
- A key point made:
    - *“Despite having sophisticated on-chain monitoring tools, we still lack a foolproof way to detect and prevent illicit activities before they occur.”*

(c) Market Manipulation Through Algorithmic Exploits

- The speaker discusses how some financial exploits do not involve hacking but instead take advantage of market inefficiencies.
- Examples include:
    - Flash Loan Attacks: Where attackers borrow and repay large sums instantly to manipulate prices.
    - Sandwich Attacks: Where a bot front-runs a user's transaction by placing an order before and after it, manipulating the final execution price.

- These attacks do not technically break the rules but undermine the integrity of DeFi markets and harm retail users.

4. Why Current Regulatory and Compliance Approaches Are Insufficient

The speaker shifts to discussing existing compliance mechanisms and explains why they are ineffective or difficult to implement in a decentralized context.

(a) The Travel Rule for Crypto Transactions

- The Travel Rule, modeled after traditional financial regulations, requires exchanges to share customer information when transferring assets above a certain threshold.
- While this approach works in centralized financial institutions, it faces major challenges in decentralized networks, including:
    - High operational costs for exchanges to comply.
    - No way to verify self-reported wallet ownership when receiving crypto from a self-custodial wallet.
    - Privacy concerns, as user data must be shared across multiple parties.
- The speaker argues that these issues create a huge vulnerability because exchanges have no way to independently verify the information provided by users.

(b) On-Chain Transaction Analysis (Blockchain Forensics)

- Companies specializing in blockchain forensics (e.g., chain analysis firms) use advanced tracking tools to trace illicit funds.
- However, these tools have limitations:
    - They require off-chain data (such as KYC information) to be fully effective.
    - Only a few private companies have access to comprehensive data, leading to a centralization problem.
    - They excel at investigating past incidents but are less effective at preventing illicit activity in real time.
- The speaker stresses that these forensic tools do not provide protection for regular self-custodial users, who have no direct way to check the legitimacy of incoming funds.

(c) Mining Pool-Level Censorship

- Some mining pools and validators have attempted to block transactions from addresses associated with illicit activities.
- The speaker notes that this approach has received significant backlash from the blockchain community because:
    - It contradicts the core principles of decentralization.
    - It introduces subjectivity—who decides which transactions to censor?
    - It could lead to political or regulatory overreach, where miners act as gatekeepers, undermining the neutrality of blockchain networks.

5. The Need for a Different Approach: The Accountable Wallet

After discussing the limitations of current methods, the speaker introduces the Accountable Wallet as an alternative framework.

- The approach shifts the burden of proof to users, allowing them to demonstrate compliance upfront rather than relying on after-the-fact detection.
- Instead of centralized monitoring, the system enables decentralized verification, preserving privacy and autonomy.
- The speaker emphasizes:
    - *"Rather than relying on centralized controls, we need a system where users can cryptographically prove their legitimacy without exposing unnecessary personal data."*

6. Defining the Accountable Wallet

- *The Accountable Wallet is introduced as a cryptographic proof system that allows users to:*
    - *Demonstrate the legitimacy of their transactions.*
    - *Verify counterparties before engaging in financial interactions.*
    - *Ensure compliance without disclosing sensitive personal information.*
- *The speaker explains that the core idea is similar to a digital passport, where users can present credentials that prove they meet certain requirements (e.g., not on a sanctions list) without revealing unnecessary details.*

- *Key characteristics of the Accountable Wallet:*
    - *Decentralized & User-Controlled: Users generate and manage their own proofs of legitimacy.*
    - *Privacy-Preserving: Uses cryptographic techniques to verify information without exposing personal data.*
    - *Interoperable: Works across multiple blockchains and jurisdictions, allowing seamless verification.*
    - *Flexible & Scalable: Can be adapted to various compliance and risk frameworks.*

7. The Four Core Components of the Accountable Wallet

The speaker introduces the technical building blocks of the system:

(a) Zero-Knowledge Proofs (ZKPs) for Privacy-Preserving Compliance

- *Users can cryptographically prove they meet requirements (e.g., not on a sanctions list) without revealing personal details.*
- *Example:*
    - *A person proves they are not on a blacklist without revealing their name, location, or other identity details.*
- *This ensures that regulatory requirements can be met without sacrificing user privacy.*

(b) Chain-Based Credentialing System

- *This system tracks the origin of digital assets across multiple transactions.*
- *It enables verifiable history, ensuring that assets are not tainted (e.g., proceeds from a hack or illicit activity).*
- *Instead of tracking individual coins (which could harm fungibility), the system assigns credibility scores to transactions.*

(c) Verifiable Credentials for Identity & Status Verification

- *A credentialing system allows trusted entities (such as exchanges, DeFi platforms, or regulatory bodies) to issue credentials that users can carry.*
- *Examples:*
    - *A verified investor credential could show that a user meets specific financial or regulatory requirements.*
    - *A jurisdictional credential could prove that a user is based in a compliant jurisdiction.*
- *Users can choose which credentials to share, maintaining self-sovereignty over their identity.*

(d) Trust Score Calculation

- *Transactions and credentials contribute to an ongoing "Trust Score".*
- *This score helps counterparties evaluate transaction risk before engaging.*
- *Trust Score Factors Include:*
    - *Quality of credentials attached to the wallet (e.g., verified investor status).*
    - *Transaction history (e.g., whether past transactions were with reputable entities).*
    - *Behavioral reputation (e.g., frequency of suspicious activity).*
- *The Trust Score is dynamic, meaning that bad behavior can lower it while responsible actions can improve it.*

8. Addressing Privacy & Fungibility Concerns

- *A participant asks whether this system could unintentionally harm the fungibility of cryptocurrencies.*
- *The speaker clarifies that the Accountable Wallet does NOT track individual coins.*
    - *Instead, it assesses the legitimacy of transactions and wallet behavior over time.*
- *Example given:*
    - *If a wallet receives both "clean" and "suspicious" funds, its Trust Score is calculated based on a weighted average, rather than marking specific assets as "tainted."*

9. Incentives for Adoption

- *The speaker addresses a common concern:*
    - *"If the Accountable Wallet is voluntary, why would people use it?"*
- *Answer: Economic Incentives Drive Adoption*
    - *Exchanges and DeFi platforms may require a minimum Trust Score to deposit/withdraw funds easily.*
    - *Users with higher Trust Scores could receive better trading conditions, lower fees, or faster transaction processing.*
    - *Institutional investors may only transact with verified accountable wallets, increasing demand for compliant participants.*

10. Audience Engagement: Addressing the Trust Score Calculation Concern

- *A participant raises a critical question:*

    - *"You mentioned a Trust Score. Can you explain how it is calculated?"*
    - *"Wouldn't some users try to avoid the system altogether? How do you make them use it?"*
- *The speaker acknowledges that Trust Score calculation is complex and that it is one of the most debated aspects of the Accountable Wallet framework.*

11. Trust Score: Key Principles

The speaker explains that the Trust Score is designed to be a market-driven, incentive-based system rather than a centralized compliance tool.

(a) Trust Score is Based on Three Factors:

1. *Credentials Attached to the Wallet*
    - *If a wallet has verifiable credentials (e.g., proof of KYC, regulated entity status, or jurisdictional compliance), it gains a higher baseline trust level.*
    - *Example:*
        - *A self-custodial wallet with a verified financial institution credential has a higher trust level than an anonymous, newly created wallet.*
2. *Transaction History & Provenance*
    - *The system analyzes transaction history to determine if funds come from trusted sources.*
    - *If a wallet has only received funds from reputable exchanges and high-trust-score wallets, its Trust Score remains high.*
    - *If a wallet interacts frequently with high-risk or unverified addresses, its Trust Score may decrease over time.*
3. *Behavioral Patterns & On-Chain Reputation*
    - *Trust Score can decay if a wallet interacts with suspicious or flagged transactions.*
    - *The system takes into account long-term activity rather than just one-off interactions.*
    - *Example:*
        - *If a DeFi trader interacts with a high-risk protocol associated with fraud, their Trust Score might drop slightly.*
        - *However, if they consistently engage in transparent transactions, their score stabilizes.*

12. How Trust Score Influences User Behavior

The speaker explains that users will not be "forced" to use the Accountable Wallet, but market incentives will encourage adoption.

- *Why would users care about their Trust Score?*
    - *Many DeFi platforms, exchanges, and institutional investors may start requiring a minimum Trust Score for users to access better financial services.*
    - *A higher Trust Score could mean:*
        - *Faster processing times for deposits & withdrawals.*
        - *Lower trading fees.*
        - *Better borrowing rates on DeFi lending platforms.*

        - *Access to exclusive financial services.*
- *Example:*
    - *A crypto exchange could prioritize withdrawals from wallets with high Trust Scores, reducing compliance burdens.*
    - *DeFi lending platforms could offer better collateral ratios to users with higher Trust Scores, similar to how traditional finance assesses creditworthiness.*

13. Addressing Concerns: Fungibility & Regulatory Compliance

A participant asks:

- *"If my wallet receives funds from an unknown or illicit source, does that permanently lower my Trust Score?"*

The speaker clarifies:

1. *Trust Score is not a permanent blacklist.*
    - *It can recover over time if the wallet engages in legitimate activity.*
    - *Users can prove that funds were received unintentionally and take corrective action.*
2. *Funds themselves are not "tainted"; the system evaluates wallet behavior.*
    - *Unlike traditional banking, where some funds can be "frozen", the Trust Score system avoids marking specific tokens as illicit.*
    - *Instead, it assesses wallet activity over time to provide a dynamic, reputation-based evaluation.*
3. *Different jurisdictions have different rules.*
    - *Trust Scores do not create a single global standard but instead allow users to select compliance frameworks based on their needs.*

14. Who Calculates the Trust Score?

- *A key concern is:*
    - *“Who decides what my Trust Score should be? Could this system be manipulated?”*
- *The speaker emphasizes that:*
    - *Trust Scores will be determined by an open-source algorithm, ensuring transparency and fairness.*
    - *No single entity controls the calculation, reducing centralized risk.*
    - *Users can verify their own Trust Score using cryptographic proofs, maintaining auditability.*
- *Example Given:*
    - *The Trust Score algorithm could be maintained by a decentralized governance system, ensuring that bias is minimized and the system remains fair.*

15. Incentives for Institutional & Regulatory Adoption

The speaker explains that many financial institutions and regulators are interested in the Accountable Wallet concept because it:

- *Reduces compliance costs for exchanges and DeFi platforms.*
- *Provides a market-based approach to financial integrity rather than strict enforcement.*
- *Gives regulators a tool to encourage compliance without requiring full identity disclosure.*
- *Example Given:*
    - *A crypto exchange operating in multiple jurisdictions could require a minimum Trust Score to comply with regulations without revealing private user data.*

16. What Are Zero-Knowledge Proofs (ZKPs)?

The discussion shifts from the Trust Score mechanism to the technical details of how Zero-Knowledge Proofs (ZKPs) enable privacy-preserving compliance.

- *The speaker introduces the challenge:*
    - *"How do we ensure a user is legitimate without revealing personal details?"*
    - *"How do we verify compliance without requiring centralized oversight?"*
- *Solution: Use ZKPs to allow users to prove legitimacy without disclosing private data.*
- *The speaker provides a brief explanation of ZKPs:*
    - *A cryptographic method that allows one party to prove a statement is true without revealing any details.*
    - *Example:*
        - *A user can prove they are not on a sanctions list without revealing their identity or location.*
        - *A DeFi trader can prove they meet investor qualifications without sharing personal documents.*

17. How ZKPs Are Used in the Accountable Wallet

The speaker outlines three key areas where ZKPs enable compliance:

(a) Proving Non-Membership in a Sanctions List

- *Problem:*
    - *If a wallet holder is asked to prove they are NOT on a sanctions list, they shouldn't have to reveal their identity.*
- *ZKP Solution:*
    - *A user can generate a "non-membership proof" using ZKPs.*
    - *This proves that their identity hash is NOT in a sanctions database without revealing any actual data.*
- *Example:*
    - *A trader in a DeFi protocol proves they are not sanctioned by showing a cryptographic proof instead of sharing their name.*

(b) Verifying Credentials Without Revealing Information

- *Problem:*
    - *A DeFi lending platform wants to offer better rates to verified investors but doesn't want to handle personal documents.*
- *ZKP Solution:*
    - *Users can present a ZKP proving they hold a "qualified investor" credential without revealing their name, ID, or jurisdiction.*
- *Example:*
    - *A decentralized exchange (DEX) offers higher withdrawal limits for wallets that can prove they are compliant investors.*

(c) Ensuring Transaction Legitimacy Without Disclosing Transaction History

- *Problem:*
    - *How can we track whether funds are legitimate without exposing full transaction details?*
- *ZKP Solution:*
    - *A ZKP-enabled provenance system allows a wallet to prove that its funds have not passed through illicit sources.*
- *Example:*
    - *A user can prove their funds were sourced from regulated exchanges without showing their transaction history.*

18. Addressing Potential Challenges

A participant asks:

- *"If a user can prove they are NOT on a sanctions list, what prevents them from generating a new wallet if they get sanctioned later?"*

The speaker acknowledges this as a valid concern and explains:

1. *Wallets must periodically refresh their compliance proofs.*
    - *If a user is sanctioned in the future, their wallet will lose its verifiable credentials over time.*
    - *This prevents users from using an old ZKP indefinitely to avoid detection.*
2. *Users must generate new ZKPs for each transaction.*
    - *This prevents them from using outdated proofs if circumstances change.*

19. The Role of Decentralized Identity & Verifiable Credentials

- *The speaker introduces how ZKPs work alongside decentralized identity (DID) frameworks.*
- *Decentralized identity (DID) systems allow users to:*
    - *Store credentials off-chain and prove them on-chain using ZKPs.*
    - *Control which credentials they disclose based on counterparties' requirements.*
- *Example:*
    - *A user proves they are a resident of an approved jurisdiction without revealing their country.*

20. Scaling ZKPs for Mass Adoption

- *A participant asks:*
  - *"Aren't ZKPs computationally expensive? Can this system scale?"*
- *The speaker explains:*
  - *Recent advancements in ZKP technology (e.g., zk-SNARKs, zk-STARKs) are making proofs faster and more efficient.*
  - *Batch verification techniques can reduce on-chain computational costs.*
  - *Off-chain computation with on-chain verification is a key design choice.*

21. The Role of Governance in the Accountable Wallet System

The speaker explains that governance will play a critical role in ensuring fairness, neutrality, and sustainability.

(a) Decentralized Governance vs. Centralized Control

- Option 1: Centralized Governance
  - A single authority (e.g., regulators, financial institutions) decides the rules for Trust Score calculation, credential issuance, and risk assessments.
  - Issue: This approach creates centralization risks and contradicts blockchain's decentralized ethos.
  - Risk: Could lead to subjective enforcement, censorship, and exclusion of certain users.
- Option 2: Decentralized Governance
  - A DAO (Decentralized Autonomous Organization) or similar model could manage rules and updates transparently.
  - Credential providers and stakeholders could vote on updates to the system.
  - Benefit: Ensures no single entity has control over Trust Scores or verification rules.
- The preferred model is a hybrid:
  - Regulatory input is considered, but algorithmic and community-based decision-making governs the system.
  - Similar to Ethereum Improvement Proposals (EIPs), updates to the Accountable Wallet framework could be proposed, discussed, and voted on.

22. Preventing Manipulation of Trust Scores

- A participant raises a key concern:
  - *"If Trust Scores determine access to financial services, what prevents bad actors from gaming the system?"*
- The speaker outlines three protection mechanisms:

(a) Reputation Decay & Continuous Verification

- Trust Scores are NOT permanent.
  - They decay over time to prevent users from accumulating a high score and then acting maliciously.

    - Users must regularly verify their credentials to maintain a high Trust Score.
- Example:
    - A wallet with a high Trust Score must periodically prove ongoing compliance, or its score will naturally decline.

(b) Cross-Verification of Credentials

- Credential issuers are incentivized to remain neutral and trustworthy because they are also being rated.
- If an issuer grants fake credentials, its own reputation declines, reducing the value of its credentials.
- Example:
    - A credential issuer that falsely verifies a sanctioned entity risks losing credibility, making its credentials unusable in the system.

(c) AI & Blockchain Analytics for Fraud Detection

- Advanced machine learning models and on-chain analytics can flag suspicious behavior.
- If wallets interact with known high-risk entities, their Trust Score automatically adjusts.
- Example:
    - If a DeFi wallet suddenly starts interacting with previously flagged addresses, the system detects and evaluates this change in real time.

23. Addressing Privacy Concerns in Governance

- Another participant asks:
    - *"Could this system be used for mass surveillance?"*
- The speaker acknowledges the risk and explains privacy-preserving safeguards:

(a) Verifiable but Anonymous Compliance

- ZKPs ensure that users prove legitimacy without exposing sensitive data.
- Example:
    - A wallet can prove compliance with KYC regulations without revealing name, passport details, or transaction history.

(b) Opt-In Participation & Self-Sovereign Identity

- Users can choose whether to participate in the Accountable Wallet system.
- If a wallet does not engage with compliant platforms, it remains outside the Trust Score system.
- Example:
    - A user engaging only in peer-to-peer transactions may never need to use Trust Scores.

(c) Governance Transparency & Open-Source Verification

- The Trust Score calculation algorithm and governance rules will be open-source for auditability.
- Community members can review and propose changes, ensuring fairness and adaptability.
- Example:
    - If a governance update negatively impacts a group of users, it can be challenged before enforcement.

24. Institutional & Regulatory Adoption Pathways

The speaker highlights potential adoption strategies for regulators, financial institutions, and DeFi platforms:

(a) Compliance Without Full KYC

- Regulators can enforce compliance without requiring centralized data collection.
- Example:
    - A DeFi lending platform could require Trust Scores for loans without collecting passport or social security numbers.

(b) Lowering Compliance Costs for Crypto Businesses

- Exchanges and DeFi protocols can automate risk assessment, reducing manual review costs.
- Example:
    - A DEX could automatically block flagged wallets without needing human intervention.

(c) Enabling Cross-Border Financial Services

- Because the Accountable Wallet system works across jurisdictions, it allows regulated financial access for users in multiple countries.
- Example:
    - A European DeFi protocol could recognize US-issued credentials without extra verification steps.

25. Transition to Implementation Challenges

- The discussion shifts from governance models to practical barriers in deploying the Accountable Wallet system.
- The speaker outlines key implementation concerns:
    - *“How do we ensure scalability without overloading blockchain networks?”*
    - *“What are the risks of centralization creeping into a decentralized system?”*
    - *“How can we encourage adoption by exchanges, DeFi platforms, and regulators?”*

26. Scalability Challenges in Zero-Knowledge Proofs (ZKPs)

A participant raises a concern:

- *"ZKPs sound great, but aren’t they computationally expensive? How do we scale this to millions of users?"*

The speaker explains two key scalability issues:

(a) High Computational Costs of ZKPs

- Problem:
    - Generating a ZKP requires significant computational power, making on-chain verification slow.
- Solution:

    - Move most ZKP computations off-chain, submitting only small proofs on-chain.
    - Use zk-SNARKs and zk-STARKs to compress proof sizes.

(b) On-Chain Data Bottlenecks

- Problem:
    - Storing verifiable credentials and proof history directly on the blockchain would be costly.
- Solution:
    - Use off-chain storage with cryptographic commitments.
    - Store only minimal verification data on-chain.
- Example:
    - A user's Trust Score and credential proofs could be stored off-chain, with only hashes of these credentials on-chain.

27. Addressing Risks of Centralization

- Another participant raises a key concern:
    - *"Won't this system give too much power to credential issuers? Could they control access to financial services?"*
- The speaker acknowledges this as a valid risk and presents three solutions:

(a) Decentralized Credential Issuers

- Instead of a single authority issuing credentials, multiple trusted issuers can exist.
- Users can choose from different credential providers, reducing single points of failure.

(b) User-Controlled Credentials

- Users can hold their credentials in self-sovereign identity (SSI) wallets.
- This prevents issuers from revoking credentials without justification.

(c) Transparent Credential Verification Rules

- The Trust Score formula and credential verification rules should be open-source and auditable.
- If an issuer is found to be unfairly restricting users, the community can challenge it.

28. Overcoming Adoption Barriers

The discussion shifts to real-world adoption challenges:

- *"Even if this system is great, how do we get people to actually use it?"*
- The speaker outlines three key adoption strategies:

(a) Incentives for Crypto Exchanges & DeFi Platforms

- Problem:
    - Exchanges and DeFi platforms may hesitate to adopt a new compliance system.
- Solution:
    - Offer compliance cost savings and risk reduction incentives:
        - Lower fraud risk → Lower regulatory scrutiny.

        - Faster compliance checks → Lower operational costs.
- Example:
    - A DEX offering lower fees to wallets with high Trust Scores.

(b) User Adoption Through Financial Benefits

- Problem:
    - Users may not see an immediate benefit in using the Accountable Wallet.
- Solution:
    - Offer better financial terms for verified users:
        - Lower lending rates on DeFi platforms.
        - Faster transaction approvals on exchanges.
- Example:
    - A user with a high Trust Score gets a 0.5% lower interest rate on a crypto loan.

(c) Regulatory Endorsement & Compliance Recognition

- Problem:
    - Some regulators might be skeptical of decentralized compliance systems.
- Solution:
    - Engage regulatory bodies early and demonstrate privacy-preserving compliance.
- Example:
    - A pilot program with a crypto-friendly regulator to test self-sovereign KYC.

29. Ensuring Security & Preventing Abuse

A participant asks:

- *"Could bad actors find a way to fake their credentials or manipulate Trust Scores?"*

The speaker outlines three security measures:

(a) Multi-Signature Verification

- Credential issuance requires signatures from multiple independent issuers, preventing single-point fraud.
- Example:
    - A user's KYC verification comes from three independent identity providers.

(b) AI-Powered Anomaly Detection

- Machine learning models analyze wallet behavior patterns to detect fraudulent activity.
- Example:
    - If a wallet suddenly moves large amounts of assets through privacy tools, its Trust Score is flagged for review.

(c) Revocation & Reputation Mechanisms

- If a credential issuer is caught issuing fake credentials, its reputation drops, making its credentials worthless.

30. Preparing for the Next Topic: Future Roadmap & Research Priorities

- The speaker summarizes the discussion:
    - Scalability concerns can be addressed through off-chain ZKPs and minimal on-chain data storage.
    - Centralization risks can be mitigated using decentralized credential issuers and transparent governance.
    - Adoption strategies include economic incentives, regulatory engagement, and cost savings for DeFi platforms.
    - Security concerns are managed through multi-signature verification, AI-based risk detection, and revocation mechanisms.
- Next topic:
    - The future roadmap and next research priorities for improving the Accountable Wallet framework.

31. Transition to the Roadmap Discussion

- The conversation shifts to the next steps in developing the Accountable Wallet framework.
- A speaker introduces the three major focus areas for future research and implementation:
    - *“How can we improve the efficiency and accuracy of Trust Scores?”*
    - *“What additional privacy-preserving techniques should be integrated?”*
    - *“How do we ensure real-world usability while maintaining decentralization?”*

32. Enhancing the Trust Score System

A participant asks:

- *"Can you clarify how Trust Scores will evolve over time?"*

The speaker outlines three improvements planned for the Trust Score model:

(a) Dynamic Trust Scores with More Granular Risk Assessments

- Instead of a fixed Trust Score, the system will adjust based on:
    - Transaction frequency and counterparties.
    - Type of credentials provided.
    - Interaction with high-risk wallets.
- Example:
    - A wallet that consistently interacts with low-risk, verified entities sees gradual Trust Score improvements.
    - A wallet that frequently uses privacy-enhancing tools without justification may receive additional scrutiny.

(b) Context-Aware Trust Scores

- Rather than a one-size-fits-all Trust Score, users could have different scores for different use cases.

- Example:
    - A DeFi lending protocol might use a creditworthiness-based score, while a DEX might use a transaction-risk score.

(c) Incorporating Verifiable Off-Chain Reputation Data

- The system may integrate off-chain reputation sources, such as:
    - Business credentials from financial institutions.
    - Transaction history with verified payment services.
- Example:
    - A crypto wallet linked to an established financial institution could receive a higher initial Trust Score.

33. Advancing Privacy-Preserving Techniques

A participant raises a privacy concern:

- *"If Trust Scores are public, doesn't that reveal too much information about users?"*

The speaker explains three new privacy-focused enhancements:

(a) Selective Disclosure with Zero-Knowledge Proofs (ZKPs)

- Users will be able to prove compliance without revealing full transaction details.
- Example:
    - A user can prove they meet KYC standards without sharing passport details.

(b) Multi-Layered Verification to Reduce Data Exposure

- Instead of sharing a single Trust Score, users can present only the minimum required proof for each interaction.
- Example:
    - A DEX might only require proof that a user is not on a sanctions list, rather than the full Trust Score.

(c) Time-Limited Credentials to Prevent Data Hoarding

- Credentials will expire periodically, requiring users to revalidate their information.
- Example:
    - A Proof of Clean Transaction History might only be valid for 6 months, after which it must be reissued.

34. Usability & Adoption Strategies

A key challenge is ensuring that the system is user-friendly while maintaining strong security.

(a) Simplifying User Experience (UX) for Non-Technical Users

- Problem:

    - Most blockchain users do not understand cryptographic proofs or complex compliance frameworks.
- Solution:
    - Develop intuitive wallet interfaces that automate compliance processes in the background.
- Example:
    - A wallet app could show a simple “Verified” badge, rather than exposing raw cryptographic proofs.

(b) Seamless Integration with DeFi & Exchanges

- Problem:
    - If exchanges and DeFi platforms do not integrate with the Accountable Wallet system, adoption will be slow.
- Solution:
    - Develop APIs and SDKs to allow easy integration with existing platforms.
- Example:
    - A crypto exchange could use the Accountable Wallet framework to streamline its compliance checks.

(c) Regulatory & Institutional Engagement

- Problem:
    - Regulators may resist decentralized compliance solutions if they do not understand them.
- Solution:
    - Conduct pilot programs with financial regulators to showcase the effectiveness of privacy-preserving compliance.
- Example:
    - A sandbox program with a central bank to test self-sovereign KYC solutions.

35. Research Priorities for the Next 6 Months

The speaker summarizes the top research areas that need further work before Block 13 (the next BGIN conference):

(a) Improving the Scalability of ZKP-Based Compliance Proofs

- Investigating zk-SNARKs vs. zk-STARKs for faster, more efficient proofs.
- Exploring layer 2 solutions to offload computationally expensive verification steps.

(b) Enhancing the Trust Score Calculation Model

- Refining criteria for score adjustments based on real-world risk assessments.
- Preventing Trust Score manipulation and unfair downgrades.

(c) Strengthening Governance & Decentralization Strategies

- Defining rules for credential issuance & revocation.
- Determining who governs updates to the Trust Score algorithm.

36. Addressing Remaining Questions from Participants

The session moves into an open discussion, allowing participants to raise final questions and comments.

(a) Handling Malicious Attacks on Trust Scores

A participant asks:

- *"Could an attacker manipulate the Trust Score system by sending illicit funds to innocent wallets?"*

The speaker acknowledges this as a valid attack vector and explains two possible countermeasures:

1. "Tainted Coins Don't Immediately Reduce Trust Score"
    - A wallet does not automatically get penalized for receiving funds it did not request.
    - Instead, the verification process records whether the recipient signed the transaction.
    - Example:
        - If a sanctioned wallet randomly sends crypto to an innocent user, but that user does not interact with those funds, their Trust Score remains unaffected.
2. "Funds Can Be Purged via Official Channels"
    - Users accidentally receiving illicit funds can send them to an "authorized disposal address" (such as a law enforcement-controlled address or charity fund).
    - Example:
        - If a wallet receives hacked funds, it can immediately send them to a verified recovery address to restore its Trust Score.

(b) Can Credentials Be Revoked?

Another question is raised:

- *"What happens if a user's credentials change or are revoked? Will the Trust Score reflect this?"*

The speaker outlines how credential revocation will be handled:

1. "Revoked Credentials Automatically Reduce Trust Scores"
    - If a credential (e.g., Proof of Compliance) is revoked by an issuer, the Trust Score recalculates in real-time.
2. "Verifiable Credentials Have Expiry Dates"
    - Many credentials (such as Proof of Residency or Proof of Investor Status) expire periodically.
    - Users must renew them to maintain a high Trust Score.
3. "Credential Issuers Can Flag Suspicious Users"
    - If an issuer detects fraud, they can flag the credential and prevent it from contributing to the Trust Score.

(c) Handling New Wallets with No Transaction History

A concern is raised about new wallets:

- *"How do we handle users who create a new wallet with no history? Will they start with a low Trust Score?"*

The speaker provides two solutions:

1. "Trust Score Can Be Transferred from Old Wallets"
    - A user can transfer reputation proofs from an old wallet to a new wallet using zero-knowledge proofs.
    - This allows them to maintain their credibility while using new keys for security reasons.
2. "Verifiable Credentials Can Provide an Initial Score"
    - Even if a new wallet has no transaction history, it can present credentials (such as government-issued KYC or DeFi reputation records) to start with a higher Trust Score.

37. Final Thoughts on Privacy vs. Compliance

A debate arises on balancing privacy with regulatory compliance.

- Some participants argue that requiring credentials moves too close to centralized identity systems.
- Others argue that a completely anonymous system will never gain adoption by regulators or financial institutions.

The discussion highlights three key takeaways:

1. "Users Should Control Their Own Data"
    - Users should choose which credentials to disclose based on who they are transacting with.
    - Example:
        - A DEX might only require proof of non-sanctioned status, while a DeFi lender might require additional financial credentials.
2. "Zero-Knowledge Proofs Allow Compliance Without Exposing Identity"
    - Users can prove compliance without revealing unnecessary details (e.g., proving they are over 18 without showing their exact birthdate).
3. "Compliance is a Tool, Not a Restriction"
    - A properly designed system should empower honest users rather than punish them with unnecessary bureaucracy.

38. Next Steps for the Accountable Wallet Initiative

As the session concludes, the speaker outlines the next milestones for the project:

(a) Further Research & Refinements

- The Trust Score model will be refined with more data-driven risk assessment techniques.
- Additional privacy-preserving methods will be explored to minimize data exposure.

(b) Development of a Prototype

- A technical prototype of the Accountable Wallet will be built to demonstrate real-world functionality.
- The team will collaborate with wallet providers, exchanges, and DeFi projects to test integration.

(c) Engagement with Industry Stakeholders

- The project will continue discussions with regulators, crypto businesses, and researchers.
- A proposal will be presented at Block 13 in Washington, D.C. to gather further feedback.

39. Closing Remarks & Future Collaboration

- The session moderator thanks all participants for their contributions.
- Attendees are encouraged to join bi-weekly working group meetings to stay involved.
- The session ends with a reminder to continue discussions in upcoming industry forums.