GALXE Protocol

Preview

Current Landscape

- Galxe.com: witnessed the challenges firsthand
    - 100M+ credentials
    - 11M+ users
    - Acting as an intermediaries, with inherent privacy & security concerns.
    - Galxe ID SDK: OAuth protocol
    - Cross-platform verification is becoming……expensive?
        - Expensive Twitter (X) API
        - Reddit API
- Rise of Self-Sovereign Identity (SSI): The promise of empowerment.
    - An approach to digital identity that gives individuals control over the information they use to prove who they are.
    - Verifiable credential + zero-knowledge proof
    - Pioneers: Ethereum Attestation Service.
        - Lack of scalability and flexibility
        - Cannot completely get rid of intermediaries
        - Hard to implement data minimization

320k+

Daily active users

3100

Partners on
25 Blockchains

GALXE

The Goal of Galxe Protocol

- For Issuers
  - Scalability: handle vast numbers of issurances efficiently.
  - Flexibility
    - Versatile credential schema
    - Support revocable credentials
  - Ease-of-use: no ZKP knowledge required, support no-code service.
  - Everyone can be an issuer.
- For Users (credential holders)
  - Identity vault app for managing credentials
  - Anonymity: act under pseudonymous identity.
  - Data minimization: zero-knowledge proofs for selective info disclosure.
  - zkOAT mechanism: aggregation of revealed information in form of NFT for gas efficiency.

The Goal of Galxe Protocol

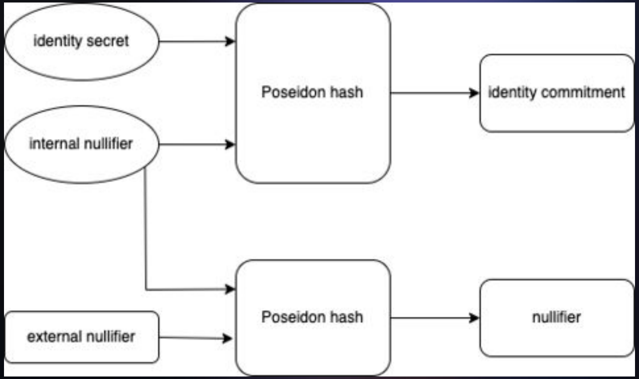
- For Verifiers
  - Double spending prevention: proofs with nullifiers.
  - Flexibility: on-chain & off-chain verification.
  - Socialized trust: find trustworthy issuers.
- As a protocol for SSI
  - Permissionless and fully decentralized
    - “At the end of the day, it’s all about signatures.”
  - Setting a new standard: Aiming to redefine digital identity verification for the better.
  - Future-proof: modular design, ready to adapt to the rapid evolution of ZKP.

Concept: Digital identity multiplicity

- Users have different identities across platforms, e.g., MightyKitty on Twitter, BraveBarbie on Discord.
- Credential Protocol Dilemma
  - Which identity should credentials be issued to? Need a solution without privacy leaks.
- Traditional Solutions:
  - Domain-specific IDs: Limits interoperability and can compromise privacy.
  - Global identifier schema: Risks of tracking and linking user activities.
- Galxe Protocol's Approach
  - Embeds identity commitments into credentials, enabling cross-platform use while ensuring privacy.

Concept: Identity commitment & Nullifier

- Identity Commitment:
  - Public value hiding two secrets
    i. Identity secret
    ii. Internal nullifier (unchangeable)
  - Constructed similarly to [Semaphore protocol](), Poseidon hash of two secrets
  - Use in Galxe protocol
    i. Proves ownership of credentials & generates deterministic nullifiers.
- Nullifier:
  - Prevents double-spending in a privacy-preserving manner.
  - Critical for practical applications of zero-knowledge proofs.
  - Analogy: Preventing multiple entries with a single concert ticket.



Concept: Credential Schema in Galxe Protocol

- Type: Structs specifying the list of typed claims.
  - Associated with on-chain zero-knowledge circuits and verification parameters.
- Context: Constructs a concrete instantiation from a credential type.
- Functionality:
  - Together, type and context form a credential schema with typed claims under a specific context.
  - Example: Using a 'scalar' type for loyalty points, game ranks, or UNIX timestamp birthdays.
- Advantages:
  - Flexibility: Different schemas can leverage the same type by linking different contexts.
  - Ease-of-use: All schemas can use pre-existing zero-knowledge circuits for their type.
  - User-Friendly: Enables issuers, holders, and verifiers to apply zero-knowledge proofs without coding.

Concept: zkOAT

- zkOAT Defined:
  - A soul-bound NFT caching revealed facts for on-chain verifications.
  - Properties represent owner's facts, aggregated from past on-chain verifications.
  - Owner: the pseudonymous identity
- Functionality & Benefits:
  - Type-aware aggregation: e.g., height field
    i. lower_bound: 101
    ii. upper_bound: 122
  - Efficient future verification: Reduced computational cost compared to traditional methods.
  - Privacy vs. Efficiency: zkOAT allows users to choose between maximum privacy and gas efficiency.
- Cost Efficiency:
  - Traditional ZK-SNARK verification: ~300k gas on Ethereum.
  - Querying an NFT property: Only a few thousand units.
- Flexibility:
  - zkOAT allows for public activities under the same pseudonym, offering a balance between privacy and efficiency.

GALXE

Roles

- Holder
  - Central to the ecosystem, possessing verifiable credentials.
  - Uses Galxe identity vault for managing identity commitments.
  - Employs ZKP to reveal only necessary data.
- Issuer
  - Endorses claims about the holder using digital signatures.
  - Registers on-chain for revocable credentials and public key management.
  - Enhances trustworthiness via DNSSEC verification and GAL staking.
  - Keep 1-to-1 mapping for identity commitment (internal nullifier).
- Verifier
  - Verifies if identities meet specific requirements.
  - Chooses trustworthy issuers via a programmable trust schema.
  - Uses unique external nullifiers for each verification.
  - Correctly use nullifiers to prevent double-spending.
- Credential Type Designer
  - Proposes new credential types to the community.
  - Provides detailed specifications for each credential type.

CASE STUDY

On-chain NFT Drop for Early Users

- Senario:
  - Project Alpha NFT drops for their early supporters.
  - They built a DEX on EVM chains.
  - Cares about user privacy and decentralization.
    1. Avoid linking EVM address, Twitter, and KYC.
    2. Everything, public and on-chain.
- Angel User NFT Criteria:
  - Cross-platform identity-based ACL
    1. Followed Project Alpha's Twitter by 01/31/2021.
    2. Nationality not on the disallowed list.
  - Every $1000 trading volume earns one NFT.

Streamlining it with Galxe Protocol (3 steps)

1. Prepare and select credentials
    a. Trading Volume Credentials
        i. Alpha issues scalar-typed credentials. Users submit identity commitments either on-chain or off-chain.
    b. Collaboration with 3rd-Party Credential Issuers
        i. deSocial (Twitter)
        ii. DeKYC (nationality)
2. Decide an external nullifier: 0x18d.... (a hash of string: *Alpha angel user NFT drop*)
3. Deploy NFT Drop Smart Contract
    a. Allow mint NFTs based on trading volume and valid zero-knowledge proofs.
    b. Requirements of proofs?

On-chain proof check

1. General requirements of proofs:
   a. Identity Verification: Revealed identity in proof must match *msg.sender*.
   b. External Nullifier: Must be 0x18d....
   c. Nullifier Integrity: Either unused or binded to the same addresses.
2. Twitter Follow:
   a. Confirm account followed is Alpha.
   b. Verification date before 01/31/2021.
3. Passport:
   a. List countries not matching user's nationality.
   b. Countries should be a super set of Alpha’s disallow list.
4. Trading Volume:
   a. Reveal the lower bound of trading volume.
   b. Linked to EVM address for future updates, not voided.

Credential-Specific Requirements

- Twitter Follow
  - Type: custom, with two typed claims
    1. Property: Followed account ID
    2. Scalar: Verification date.
  - Context: Simple non-revocable twitter follow credentials with verification date by DeSocial.
  - Public inputs
    1. Equality of followed account ID v.s. “Alpha”.
    2. Upper bound of verification date.
    3. External nullifier and nullifier A
  - On-chain verification
    1. Equality is true.
    2. Upper bound is before 01/31/2021.
    3. A has not been marked as used.
  - Post-verification actions
    1. Mark nullifier A as used for passport credentials.

Credential-Specific Requirements

- Passport
  - Type: Custom, at least containing a claim of
    1. Property: nationality
  - Context: DeKYC's AI-power KYC solution.
  - Public inputs
    1. Equalities of nationality v.s. a list of countries.
    2. External nullifier and nullifier B
  - On-chain verification
    1. Equalities are all false, and the list of countries is a superset of the disallow list.
    2. B has not been marked as used.
  - Post-verification actions
    1. Mark nullifier B as used for passport credentials.

GALXE

Credential-Specific Requirements

- Trading volume
  - Type: Scalar (a basic credential type shipped)
  - Context: Project Alpha trading volume
  - Public inputs
    1. Lower bound of trading volume.
    2. External nullifier and nullifier C
  - On-chain verification
    1. C has not been binded yet, or binded with msg.sender
  - Post-verification actions
    1. Bind C with ***msg.sender,*** as used for trading volume credentials, and set the number of available NFTs to mint to be *volume_lower_bound / 1000*

User Experience with Galxe Identity Vault

- User Workflow Overview:
    - Collect credentials from issuers & generate proofs via Galxe Identity Vault.
    - Send proofs to Alpha’s contract to mint NFTs.
- Credential Collection:
    - Twitter Follow
        1. Use DeSocial’s platform, connect with Galxe Identity Vault, verify Twitter follow status.
    - Passport
        1. Access DeKYC, undergo KYC verification, and receive credentials.
    - Trading Volume
        1. Request trading volume credential directly within Project Alpha's application.
- Proof Generation:
    - Use Galxe Identity Vault to produce zero-knowledge proofs.
    - Project Alpha provides statements for verification.
    - User **confirms** information disclosure.
    - Proofs sent to smart contract for NFT minting.

Alternative: zkOAT

- Mint zkOAT under the pseudonym for
    - Twitter Follow
    - Passport
    - Trading Volume
- Project Alpha
    - Check NFT holdings of the address
        1. Own a Twitter Follow credential that has traits of:
            - Followed account ID = Alpha's twitter account
            - Verification date <= 01/31/2021
        2. Similar for passport.
    - On-chain query of trading volume, and mint NFTs based on the value.

Security and Privacy Analysis

- Identity Linkage Protection:
    - Conceals users' identities across platforms.
    - Colluded issuers can't correlate a user's identity, given best practices are followed (it will be mandatory for Galxe Identity Vault).
- Pseudonymous Claims:
    - Users claim NFTs under pseudonyms.
    - Separates DEX trading address from NFT ownership. Allows selling NFTs on KYC-mandated platforms without linking to DEX trading activities.
- Double-spending Prevention:
    - Nullifiers ensure credentials aren't reused.
    - Angel users can only claim their rightful NFTs, while allowing the volume to be updated.

Security and Privacy Analysis

- Minimal Data Exposure:
  - Only essential data is disclosed.
- Examples:
  - Twitter Follow Date: Users disclose an upper bound, standardizing to 01/31/2021.
  - Nationality: Doesn't reveal direct country. Provides a list of non-matching countries.
  - Trading Volume: Uses a lower bound instead of exact volume. Adjusts based on NFTs a user can and intends to mint.

galxe.com/protocol

Use cases

- Sybil Prevention, Reputation score:
  - Run local zero-knowledge proof circuits to compute user’s score.
  - New paradigm: Sybil prevention solution providers can directly issue credential to users, from 2B to 2C.
- Identity Verification:
  - Digital verifiable credentials combat identity fraud.
  - Tamper-proof and easily verifiable by relying parties.
  - No compromise on sensitive information.
- User-centric achievement System:
  - Own their achievements, permanently.
  - Enhances the value of achievements across platforms.
  - Incentivizes users to pursue and showcase achievements.
- Decentralized Review System:
  - Aggregated reviews for entities within the network.
  - Weighted review aggregations for robust results.
- Personal Data Market:
  - Monetize personal data by proving to be a high-value customer.

Galxe.com upgrades

- “Credential”
    - Support issuers other than Galxe itself.
        - Web3 Score
        - On-chain data: NFT holding, token balance..
        - Real-World Asset
        - Web2 data
    - Submit proof, get verified for campaigns.
- Galxe ID & Passport (KYC)
    - Upgrade to Galxe protocol verifiable credential.
    - ZKP-powered
    - Support exporting Galxe-signed verifiable credentials to Galxe identity vault
        - Social login with credentials.
        - KYC
            - Age > 21
            - Nationality check

Q&A