BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2026
http://excel.fit.vutbr.cz

Balthazar Wallet: Making Password Authentication Practical on Web3 via OPAQUE and Privacy-Preserving Smart Contracts

Tomas Krajci

Abstract

What is the problem? Passwords cannot be used securely on public blockchains: all contract state is public, and there are no server-enforced rate limits, making offline brute-force attacks against password-derived keys trivial. **How is it solved?** We adapt the OPAQUE protocol to run inside a confidential smart contract on a TEE-backed Privacy-Preserving smart contract Platform (PPP), protecting per-user OPRF keys inside the enclave while enforcing on-chain rate limits on authentication attempts. **What are the results?** A prototype on Oasis Sapphire securely manages secp256k1 key pairs and authenticates users in under 4.2 s, costing approximately 496k gas (2048-bit OPRF) or 300k gas (1024-bit OPRF) per login, with one-time registration at approximately 275k gas. **So what?** Password-based Web3 wallets, long considered infeasible on public blockchains, are now both secure and practical, therefore opening decentralized applications to users who cannot manage raw private keys or seed phrases.

*xkrajc25@stud.fit.vut.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

[Motivation] Passwords remain the dominant authentication method across digital services due to their ease of use. Yet existing Web3 wallet solutions are complex for ordinary users: software wallets require managing raw private keys or 12-word seed phrases, while hardware wallets require a dedicated physical device, all of this is a well-documented usability barrier [1] that excludes non-technical users. Bringing 'username and password ' login to blockchain wallets would meaningfully lower the barrier to adoption.

[Problem definition] Public blockchains expose all contract storage, transaction calldata, and execution traces to every participant. Storing password verifiers on-chain immediately leaks them, and without server-enforced rate limits, an attacker can brute-force password-derived keys offline. The challenge is a password-authenticated wallet with strong guarantees, resistance to offline dictionary attacks, and protection against server compromise without a centralized trusted server.

[Existing solutions] OPAQUE [2, 3], a modern asymmetric PAKE, prevents the server from learning the password and resists offline attacks even upon server compromise. It requires a confidential long-term server-side OPRF key, which is impossible on a transparent blockchain. The closest prior work, PDID [4], combined OPAQUE with Hyperledger Fabric Private Chaincode (FPC) on a *permissioned* chain. Its permissioned nature and C/C++ enclave dependency limit public accessibility and EVM interoperability.

[Our solution] We deploy the OPAQUE OPRF server inside a confidential smart contract on *Oasis Sapphire* [5], a PPP backed by Intel SGX enclaves. The enclave protects per-user OPRF keys; the blockchain enforces rate limits. A relay verifies email identifiers and sponsors gas via ephemeral wallets, enabling fully gasless onboarding.

[Contributions] To the best of our knowledge, Balthazar is the first password-based wallet deployed on a **public, permissionless, EVM-compatible** confidential blockchain. We implement the OPAQUE OPRF directly in Solidity using the EVM modular exponentiation precompile (`0x05`), and introduce a relay-assisted architecture that enables **gasless onboarding** via ephemeral wallets. A prototype on Oasis Sapphire confirms practical gas costs and sub-4.2 s latency per authenti-

cation.

2. Background

TEEs and Oasis Sapphire A Trusted Execution Environment, such as Intel SGX, provides an isolated, remotely-attestable boundary where code and data remain confidential even from the host OS [6]. Oasis Sapphire [5] integrates SGX into an Ethereum-compatible runtime: storage encrypted at rest, state transitions encrypted in transit, computations hidden from observers, and fully compatible with Solidity and EVM bytecode.

OPAQUE OPRF OPAQUE [2] resists offline guessing even upon server compromise. The client blinds its password as $\alpha = (H'(pwd))^r \bmod p$; the server evaluates $\beta = \alpha^{k_s} \bmod p$ and returns β; the client unblinds as $k = H(\beta^{1/r} \bmod p)$ therefore the password is never revealed. Key k encrypts the *credential envelope* $c = \mathrm{AEnc}_k(p_u, P_u)$ at registration and decrypts it at login.

3. System Architecture

Client Computes the blinded OPRF input α with a fresh exponent r, generates an ephemeral key pair to sign transactions, then unblinds β and decrypts the envelope locally. The password *never leaves the device*.

Relay Verifies user identifiers (e.g., via email OTP) and funds ephemeral wallets with no prior cryptocurrency balance needed. Considered *fully untrusted*: blinded OPRF inputs reveal nothing about the password even to a compromised relay.

PPP Smart Contract Stores $users[U] = (k_s, P_u, c)$ in TEE-encrypted enclave storage. During login evaluates $\beta = \alpha^{k_s} \bmod p$ via precompile `0x05` and returns (β, c) over Sapphire's encrypted channel. All sensitive values are sealed inside the TEE, invisible to node operators or blockchain observers.

4. Protocols

Registration The client generates k_s, derives $k = H((H'(pwd))^{k_s} \bmod p)$, and forms $c = \mathrm{AEnc}_k(p_u, P_u)$. The relay calls `startRegistration`$(U,\ X_u)$ to bind the identifier. The client finalizes via `finalizeRegistration`$(U,\ k_s,\ P_u,\ c)$; the contract verifies the sender matches X_u and writes the record to enclave storage. No password-derived value reaches the relay or the chain.

Authentication The client sends $\alpha = (H'(pwd))^r \bmod p$ with nonce N via `startAuth`$(U,\ \alpha,\ N,\ X_u)$. The contract evaluates $\beta = \alpha^{k_s} \bmod p$ and returns (β, c). The client unblinds to recover k and decrypts $(p_u, P_u) = \mathrm{ADec}_k(c)$. Every attempt requires an on-chain transaction, imposes rate limits, charges fees per guess, and makes brute-force attempts publicly visible.

5. Evaluation

All experiments ran on a local Oasis Sapphire testnet using a TypeScript client and Solidity contract with Hardhat.

Operation	2048-bit	1024-bit	Latency
startRegistration	∼111k	∼111k	<4,023 ms
finalizeRegistration	∼164k	∼164k	<4,102 ms
startAuth	∼338k	∼213k	<4,059 ms
evaluateAuthOPRF	∼158k	∼87k	<4,115 ms
Full auth	∼496k	∼300k	<4,200 ms

The dominant cost is `startAuth`, which stores the blinded OPRF input and commits the on-chain rate-limit record. The OPRF modular exponentiation in `evaluateAuthOPRF` is efficient thanks to the EVM precompile. Latency below 4.2 s is acceptable for real-world login flows.

6. Conclusions

We presented **Balthazar**, a password-based blockchain wallet securing private keys via a PPP. Placing the OPAQUE OPRF server inside a TEE-backed confidential EVM demonstrates that password authentication, once considered long incompatible with public blockchains, is now both secure and practical. The system inherits OPAQUE's guarantees (resistance to offline attacks and server compromise) and remains fully compatible with standard Ethereum tooling. Evaluation on Oasis Sapphire confirms approximately 500k gas and under 4.2 s per authentication. Future work includes elliptic-curve OPRF variants to reduce gas costs and deploy on the Sapphire public mainnet.

Acknowledgements

I want to thank my senior, Samuel Oleksak, for his help with the finishing touches.

References

[1] Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012.

[2] Stanislaw Jarecki, Hugo Krawczyk, and Jiayu Xu. OPAQUE: An asymmetric PAKE protocol secure against pre-computation attacks. In *Annual International Conference on the Theory and Applications of*

Cryptographic Techniques (EUROCRYPT). Springer, 2018.

[3] Daniel Bourdrez, Hugo Krawczyk, Kevin Lewi, and Christopher A. Wood. The OPAQUE augmented password-authenticated key exchange (aPAKE) protocol. Technical Report RFC 9807, IRTF Crypto Forum Research Group (CFRG), July 2025. Informational.

[4] Pawel Szalachowski. Password-authenticated decentralized identities, 2020.

[5] Oasis Protocol Foundation. Oasis sapphire: Confidential EVM. https://docs.oasis.io/dapp/sapphire/, 2022. Accessed: 2025-01-01.

[6] Victor Costan and Srinivas Devadas. Intel SGX explained, 2016. IACR Cryptology ePrint Archive, 2016/086.