

Wrapped Monero — ラプトモネロ

Mads — マッツ

Justus — ユストウス

azukitofu — あずきとうふ

ETHTokyo 2025 hackathon

Background — 背景

Issues:

- Almost zero privacy in Ethereum
- Lack of liquidity in Monero due to regulatory pressure

Existing solutions:

- Atomic swaps (2021; e.g. ETH-XMR)
- Railgun (2022)

Monero:

- Non-optional privacy
(payer, receiver, transaction amounts)

問題：

- イーサリアムのゼロに近いプライバシー
- 規制圧力によるモネロの流動性不足

従来のソリューション：

- Atomic Swaps (2021; 例： ETH-XMR)
- Railgun (2022)

モネロ：

- 強制的なプライバシー
(支払人、支払先、金額)

Proposal — 提案

Wrapped Monero:

- EVM ERC-20 contract
- XMR—EVM bridge

Use cases:

- Provides liquidity to Monero users
- Provides privacy to Ethereum users

Properties:

- Asynchronousness: XMR party and ETH party need not be online simultaneously
- No new wallets are created in the process

Limitations/:

- If centralized, bridge is prone to attack
- Proof of liquidity?

ラプトモノロ：

- EVM ERC-20 コントラクト
- XMR—EVM ブリッジ

使用事例：

- モネロユーザに流動性を提供
- イーサリウムユーザにプライバシーを提供

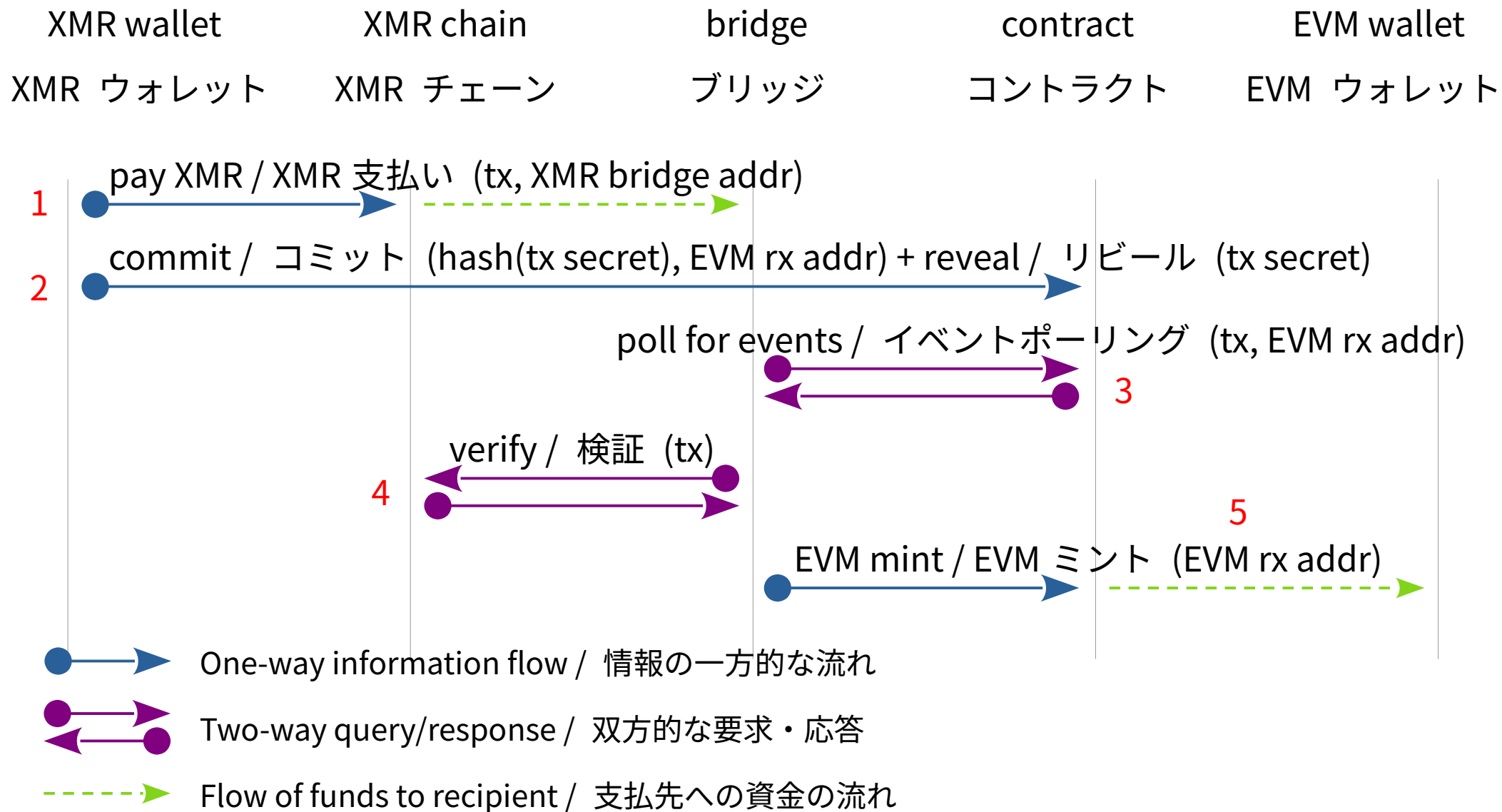
特徴：

- 非同期性： XMR 側と ETH 側が同時にオンラインではなくても使用可能
- プロセスには新規ウォレットの作成が不要

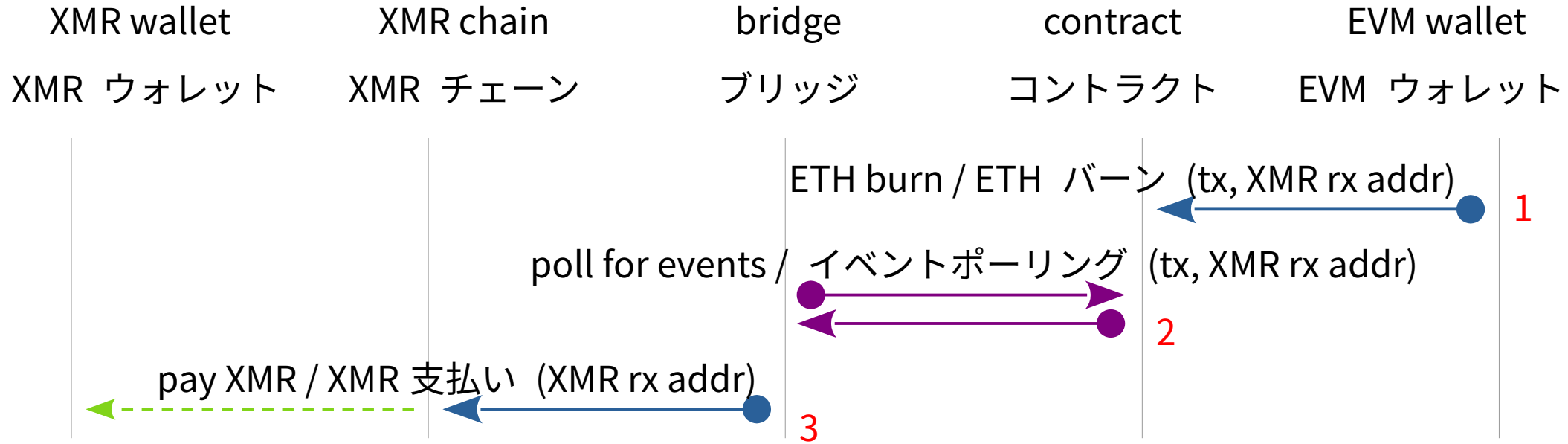
限界：

- ブリッジが中央型ならば攻撃されやすい
- 流通性の証明？

Process (EVM mint) — プロセス (EVM ミント)



Process (EVM burn) — プロセス (EVM バーン)



- One-way information flow / 情報の一方的な流れ
- Two-way query/response / 双方向的な要求・応答
- Flow of funds to recipient / 支払先への資金の流れ

User interface proposal — ユーザインタフェースの提案

ETH mint / ETH ミント


Transaction type:

XMR > ETH ▼

Amount:

1337 XMR ▼

ETH address: Scan QR

0x0123456789abcd... 

Send

Cancel

ETH burn / ETH バーン


Transaction type:

ETH > XMR ▼

Amount:

1337 ETH ▼

XMR address: Scan QR

888tNkZrPN6JsEge... 

Send

Cancel