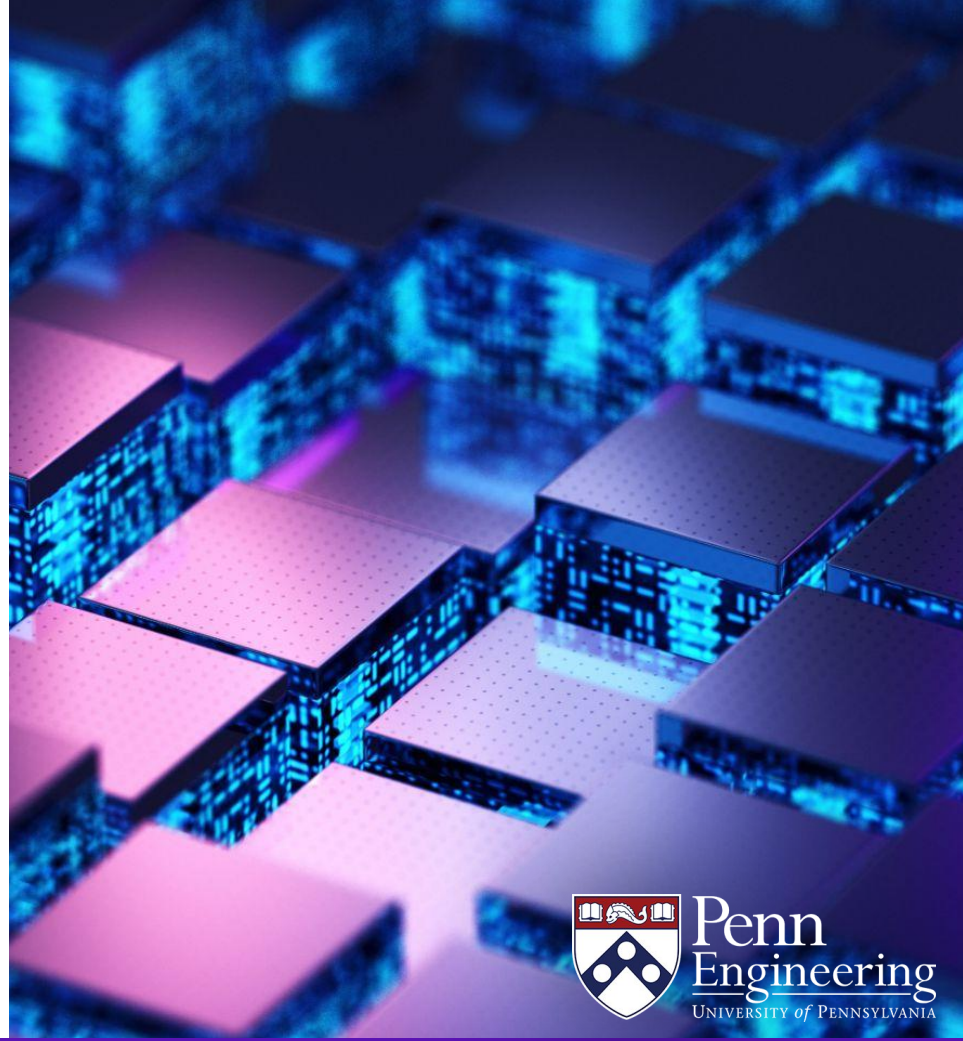
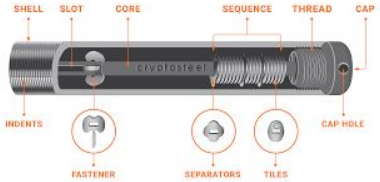
EAS 5830: BLOCKCHAINS

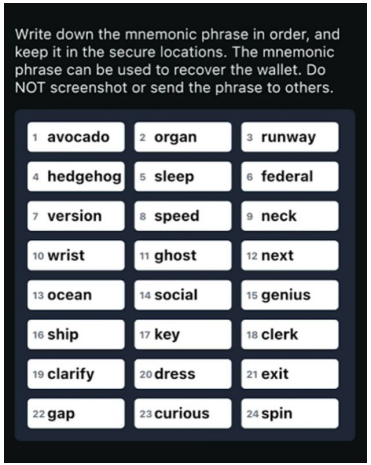
Account Abstraction

Professor Brett Hemenway Falk



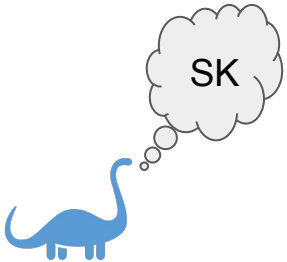
Key Management





Accounts

- Externally owned accounts (EOAs)
  - Controlled by digital signatures (ECDSA)
- Contract Accounts
  - Cannot initiate transactions
  - Can execute arbitrary logic



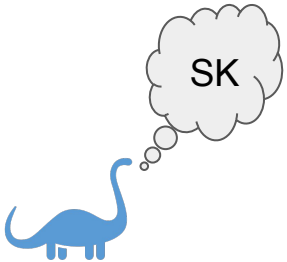
Spender

Contract wallet

Spending Key

PK

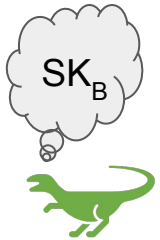
(Social) Recovery



Spender

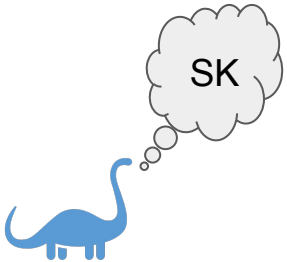
Contract wallet

Spending Key	Recovery Keys
PK	PK_A
	PK_B

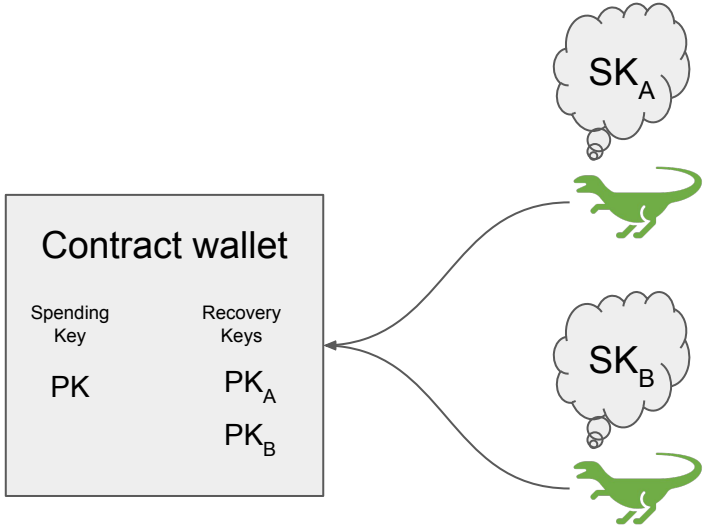


Recovery Partners

(Social) Recovery

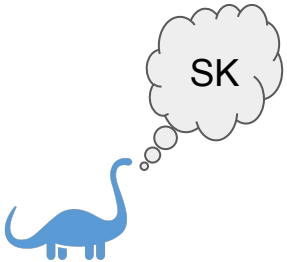


Spender

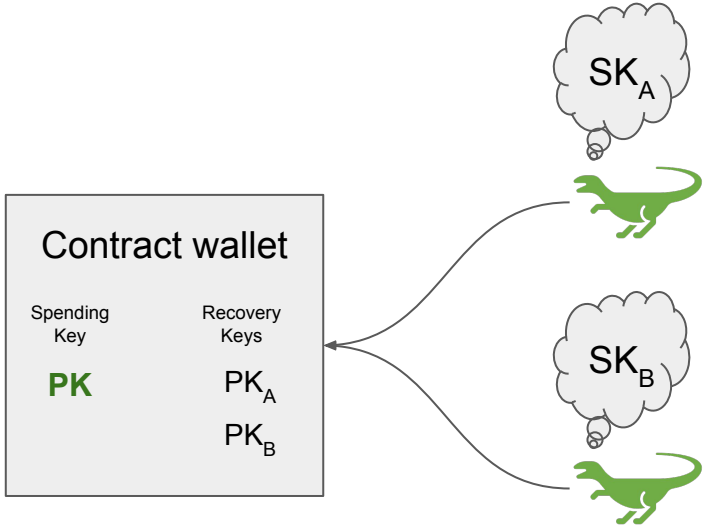


Recovery Partners

(Social) Recovery



Spender



Recovery Partners

Fraud protection

- Multi-sig
  - Adaptive
    - Larger transfers require approval from more signers
- Spending limits
- Allow / Deny lists
  - Example: No transfers to members of the OFAC SDN list
    - Provided by Chainlink oracle
- Arbitrary logic to prevent fraud and money-laundering

Quantum resistance

- ECDSA is vulnerable to quantum attacks
- Wallet can validate requests using any logic it wants
  - Post-Quantum signature scheme
- Not a long-term solution
  - Transactions still need to be signed by EOA using ECDSA
  - Block-producers use BLS

Alternative authentication

- Contract wallets can authenticate requests any way they want
  - Arbitrary signature schemes
  - ZK proofs

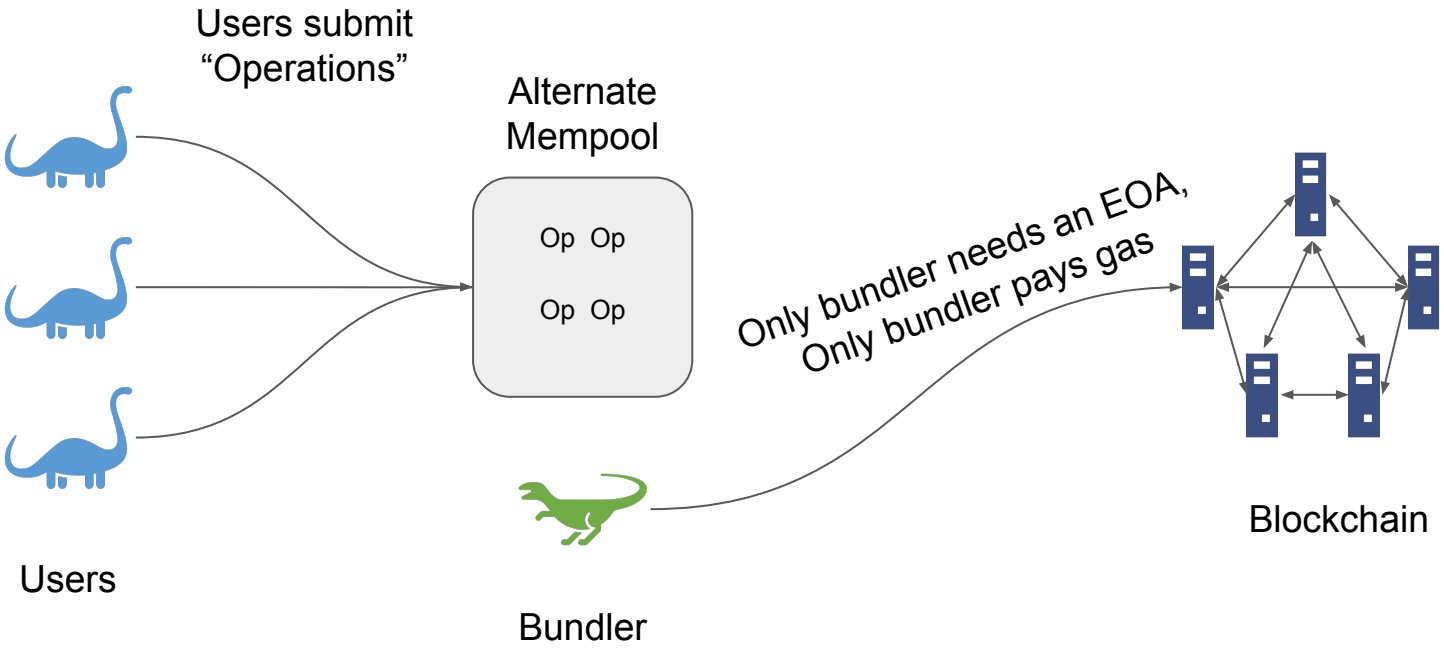
Gas abstraction

- With EOAs single signature
  - Authorizes operations
  - Authorizes transaction fees
- Account abstraction allows you to separate the authorization of the on-chain actions, from the gas payments
  - Chain validates transaction using the same signature as before
  - Contract authorizes operations based on its own internal logic
    - Probably also by verifying a signature

EIP-4337

- More benefits from account abstraction if we have standards
- Standardized format for user operations
- Single “EntryPoint” contract to distribute operations

EIP-4337


Users submit
“Operations”
Alternate
Mempool
Op Op
Op Op
Only bundler needs an EOA,
Only bundler pays gas
Users
Bundler
Blockchain