P1nch — Its Cute

Claudia + Lev + Rodney
With help from Pseudotheos, Philogy, Viktor from Boosty Labs
See code @ https://github.com/laudiacay/p1nch

Private ___: Adding Actions to ZCash's Model

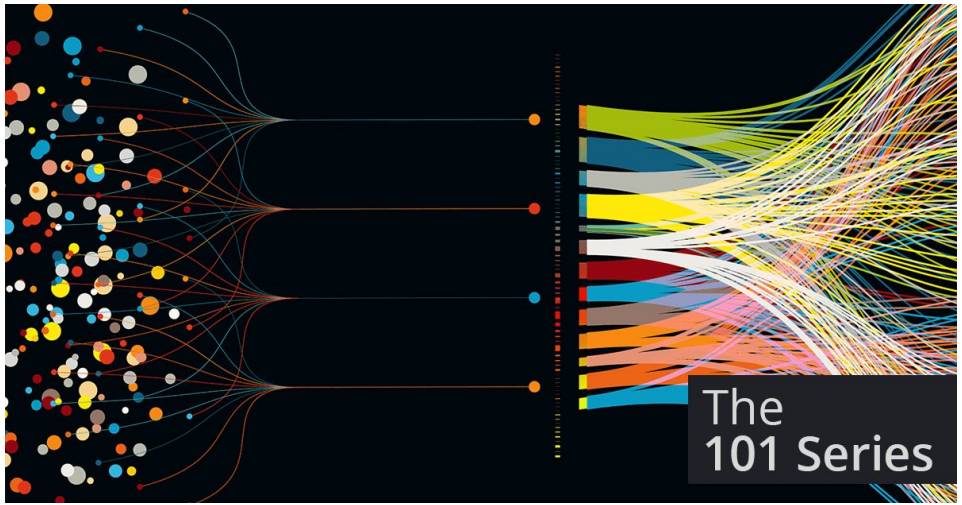
- Want to do a swap and preserve privacy?
- Want to do private governance voting?
- We introduce a generalized framework for "mixed/ private" computation
- Think along the lines of Zexe/ Aleo et.
- Allows for public aggregation
- Layer 2 like gas with batching

DeFi Privacy? But with What Liquidity?

- Aggregate Swapping over **Uniswap** (1inch, Sushi, etc.)
- Mixing within the *swap itself*
- Mixing *over time*

Ex. Dog ⟶ Eth.

1. Deposit
2. Declare Swap (wait for aggregation)
3. Withdraw



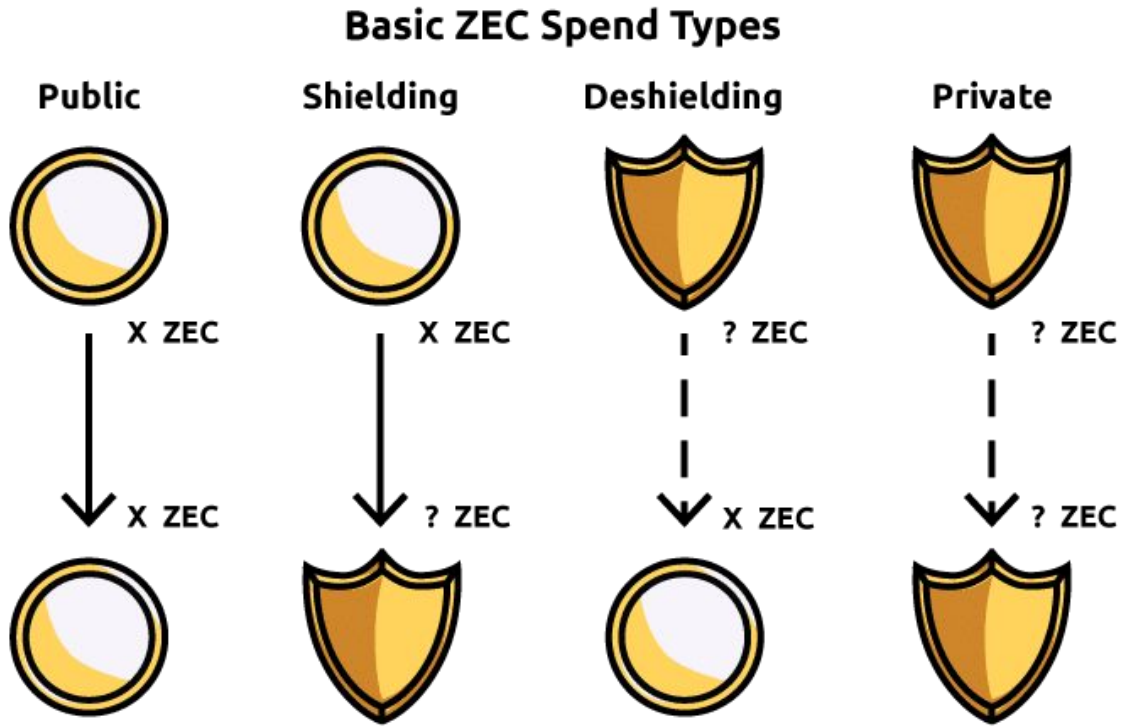
Prior Work

- Penumbra
  - private batched swap on Cosmos
  - has their own liquidity / shielded LP
  - threshold decryption of FHE sum of swap batch parts
  - Liquidity hard…
- Nocturne (hi friends!)
  - Generalized actions on ethereum
  - Wallet integration
  - No batching
- Aztec (hi friends again!)
  - Private/public hybrid L2
  - Can “shell out” to eth L1
- Zexe — its sexy

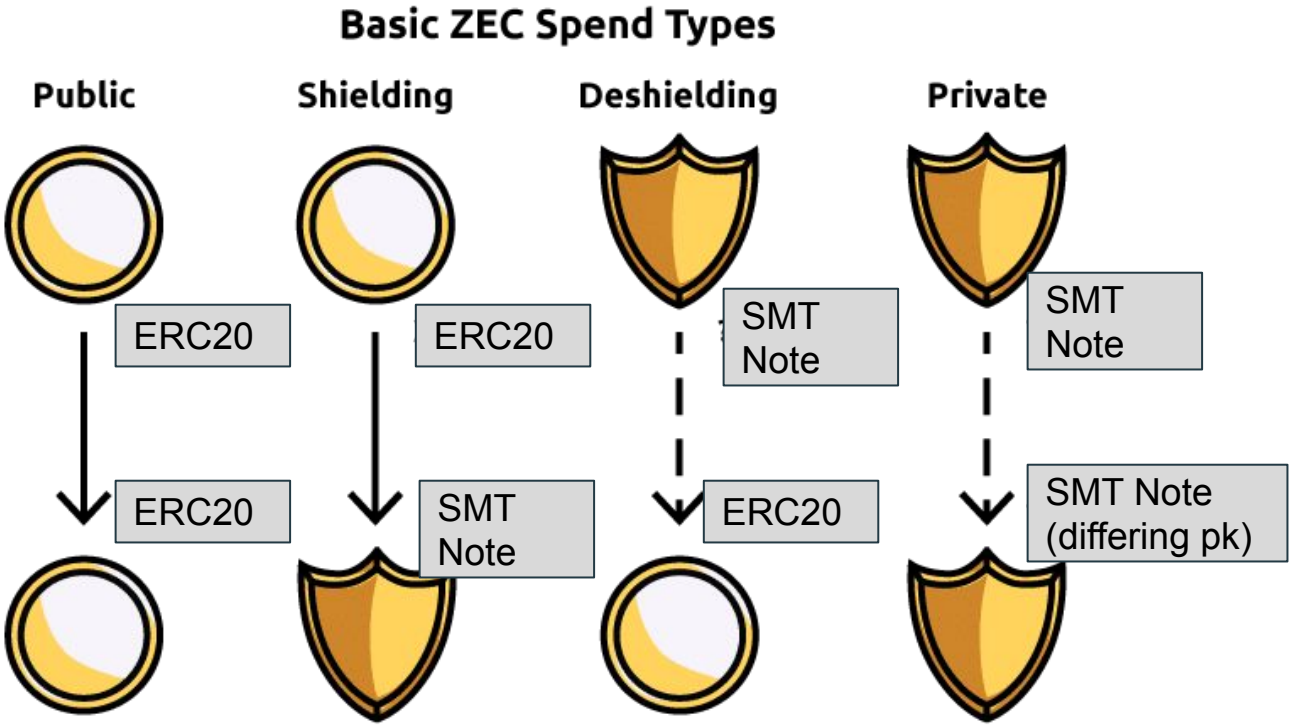
Sparse Merkle Trees

- Merkle trees but really big (256 layers deep!)
- Actually it is a trie on the key value
- Fast proofs of non-inclusion
- Updates are 256 hashes long
- Track state privately (just enter the hash of the “ticket”, which is basically a BTC UTXO)

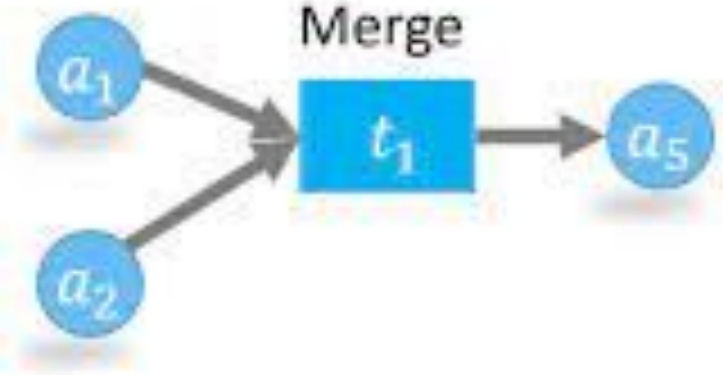
ZCash: Shielded Pools UTXO 101



ZCash (modified): Shielded Pools UTXO 101

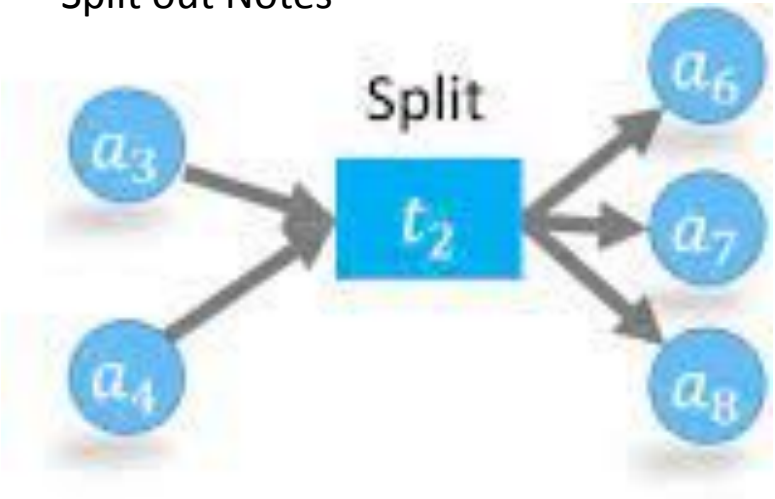


Merge Split: Shielded Pools UTXO 101

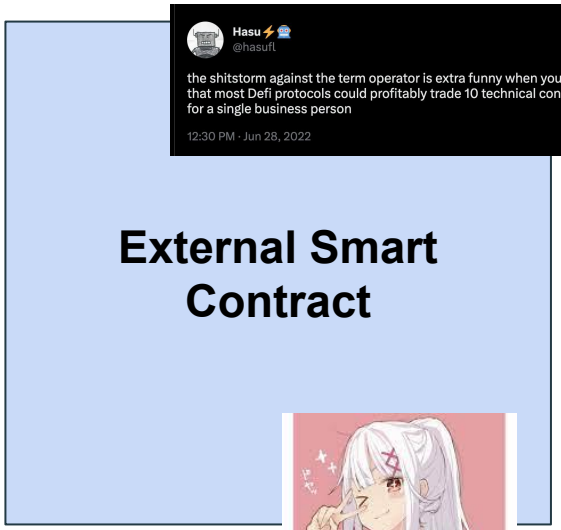


Combine Notes

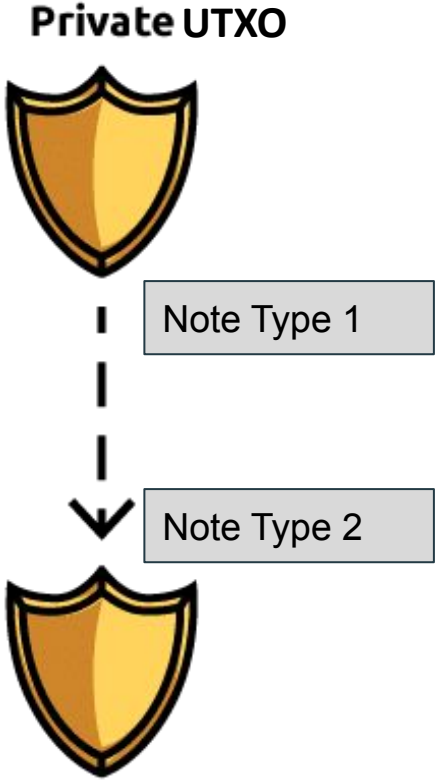
Split out Notes



Our modifications: Adding UTXOs + Contracts



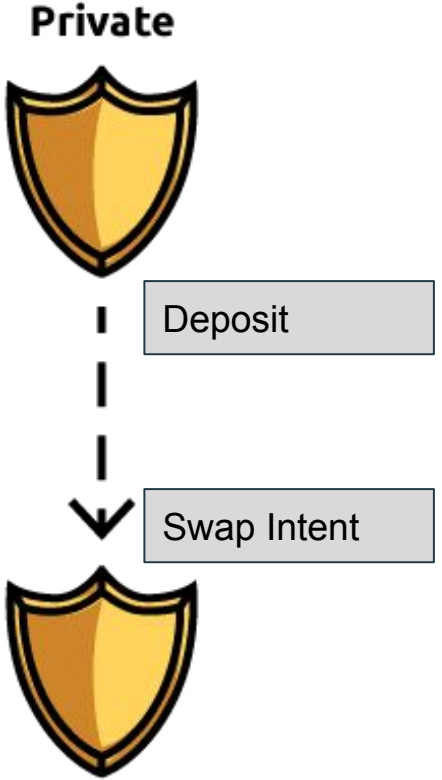
+



Adding UTXOs + Contracts (Uniswap), Before Swap

Smart Contract: Aggregate across swap pair. Verify ZK proofs

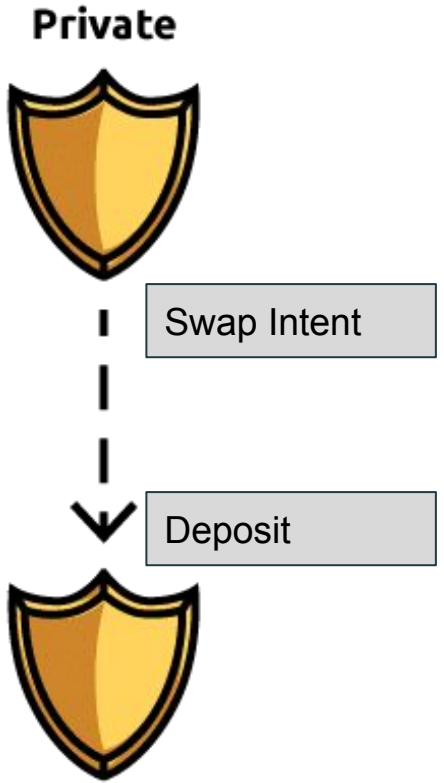
+



Adding UTXOs + Contracts (Uniswap), After Swap

Smart Contract: After Swap Aggregated Pair. Verify ZK Proofs

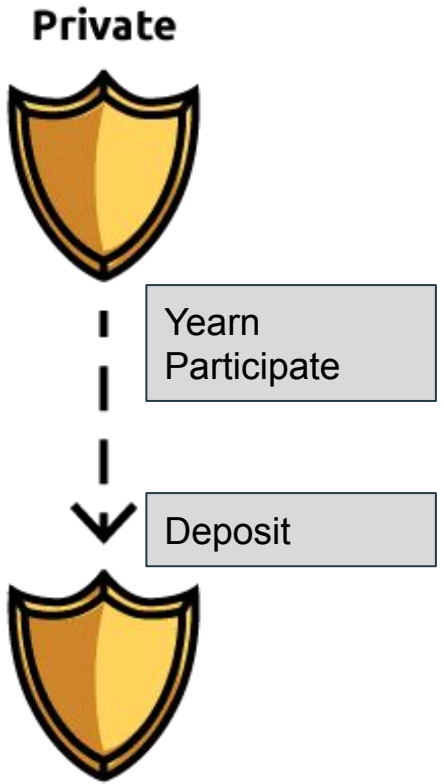
+



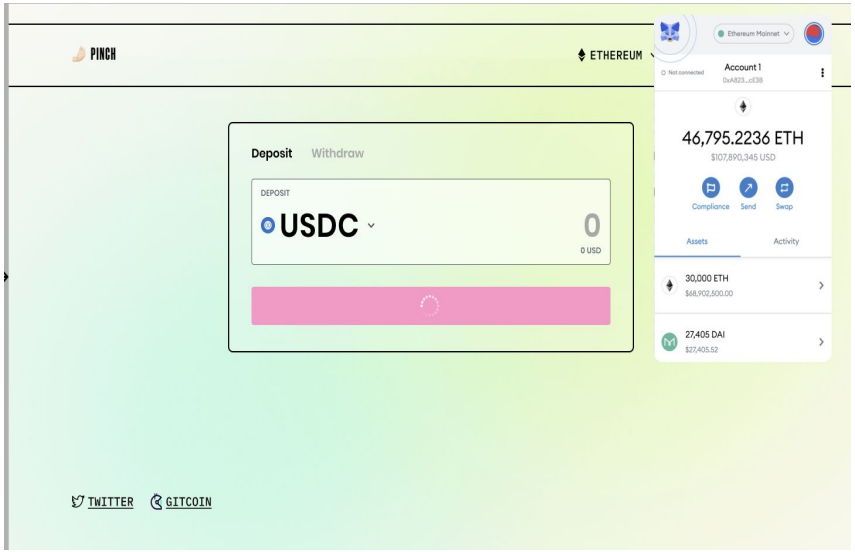
Adding UTXOs + Contracts (Uniswap), Yearn

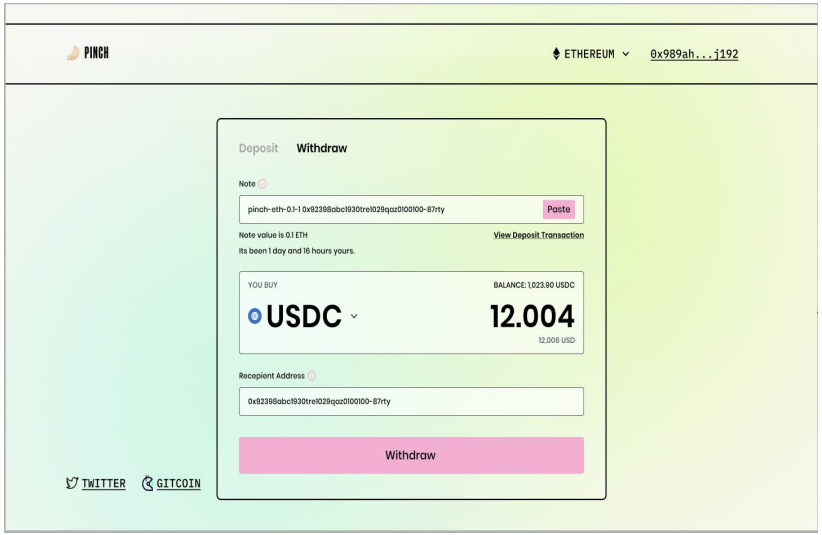
Smart Contract: Batch is a day. Aggregate daily pool size and earning

+

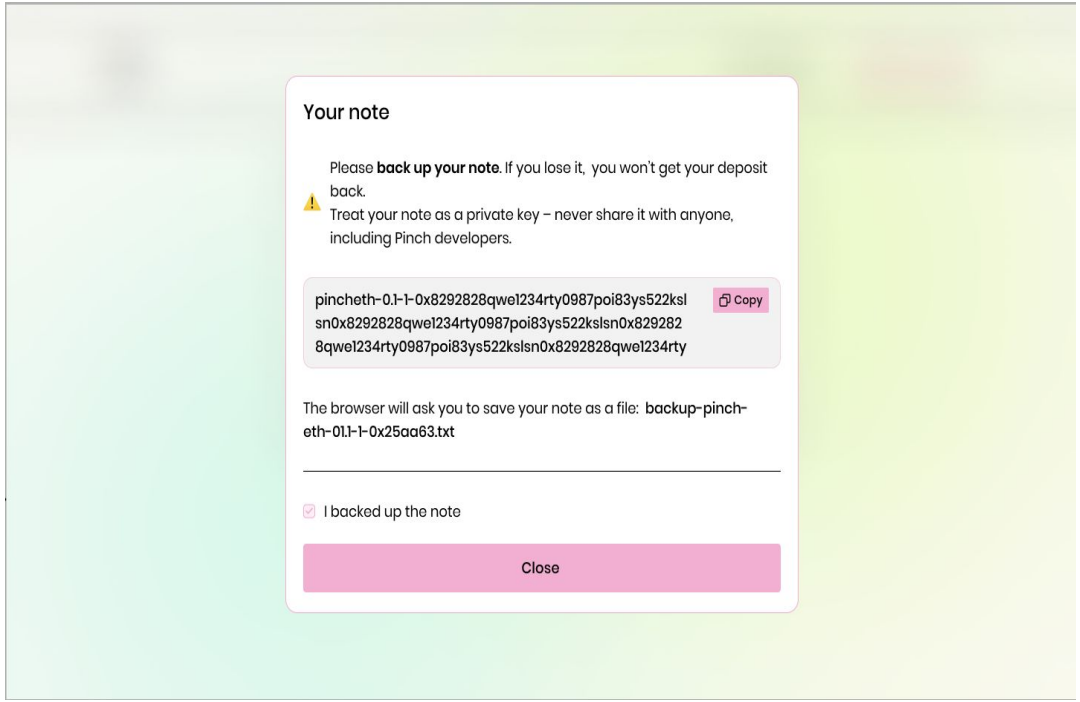


Frontend mockups for swap (thanks @yasya from Boosty Labs)





More frontend mockup from yasya



State of the repo (child up for adoption)

- Positives: very modular architecture for Solidity/ Circom: very extensible system with simple contracts and circuits
- Needs a cleanup and some love and a trusted setup ceremony
    - But the way we architected it is future-improvement-friendly
- Circom/Solidity work!
    - 5s prover time on Lev's laptop
    - Gas is $50 per verification, and some txns have multiple verifications
    - Swap bot will literally be $100 per pair participating in batch…
    - Hello @ the Nova on-chain verifier boys (save us from ourselves)
- Javascript (sequencer/swap bot)
    - Swap bot is centralized, doesn't quite work, needs to use the sequencer
        - uuuugh: should be a mevbot and have its own SMT for state independence from sequencer
    - Sequencer works but…
        - forgets state when rebooted (entire historical state in memory 😇)
        - each proof and transaction happens within the request-serving express.js thread 😇💅
            - can take a bit before returning a response
        - Both these issues are very easily fixed by using redis to make the sequencer less dumb
    - Generalized devops and key management, sequencer decentralization
        - neither of these can do anything REALLY evil, but can freeze or DoS withdrawals

Future Vision

- looking 4 a founder- he is going to grad school and i have a company
  - We can do pretty hands-on advising for a relatively small token share
  - Claudia can probably help u raise if u want that
- Repo @ https://github.com/laudiacay/p1nch
- A pseudo (shout out to @Pseudotheos)-layer 2 focused on privacy which plugs into layer 1 DeFi and Governance
  - Yearn, Aave, Voting Systems
  - Gas Amortization (Nova helps with this a LOT) (nova PLZ)
  - Internal order matching to get better swap prices
  - Add MEV-bot for aggregation
  - #decentralized #sequencer @ScrollResearchers #yolo
  - Friendly and usable — should be as easy normal crypto transactions
  - Compliance Blacklisting
  - State Channel esque?
  - ~~Conquer Mongolia and use it as a home base~~