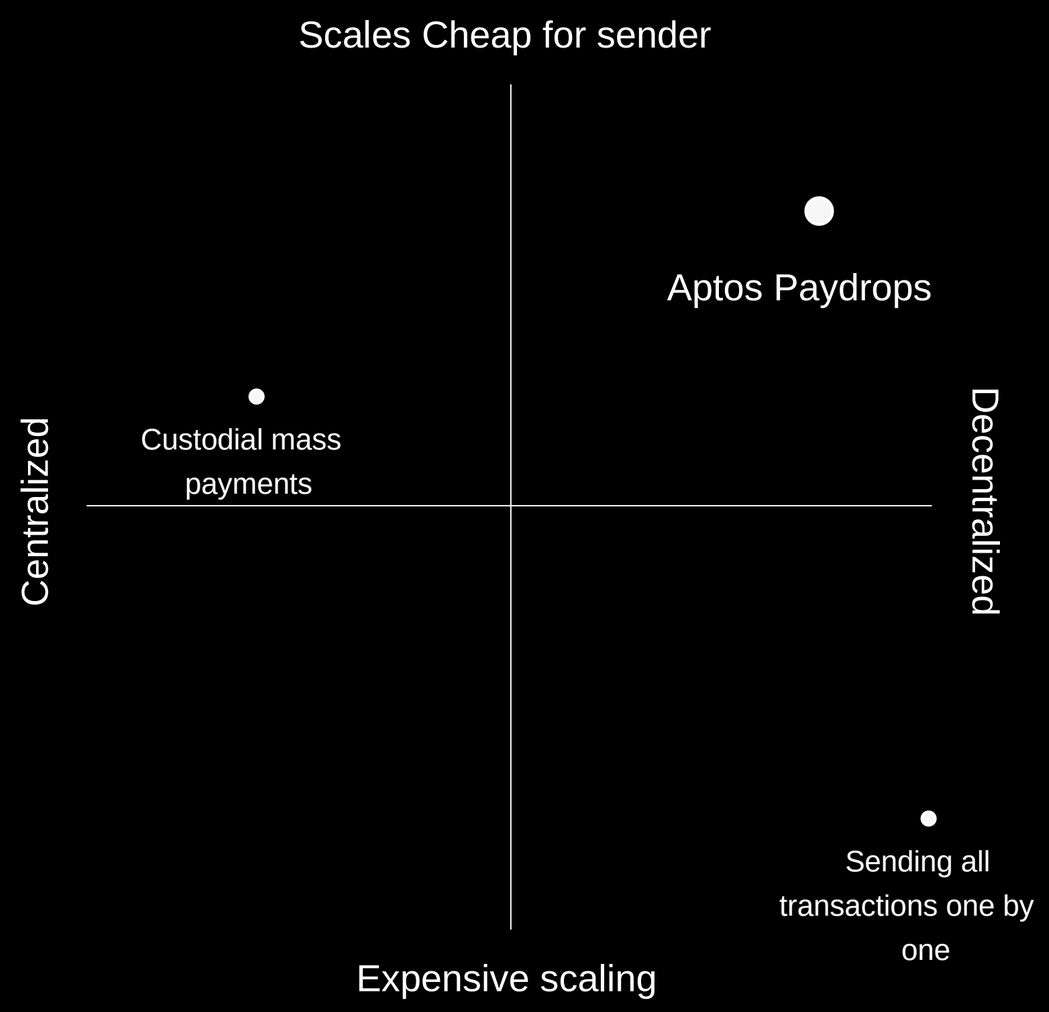
AirDrops, Quadratic Funding, Payrolls and Mass Payouts scaled with Zero-knowledge cryptography

Aptos Paydrops

aptospaydrops.com

February 2025

The landscape



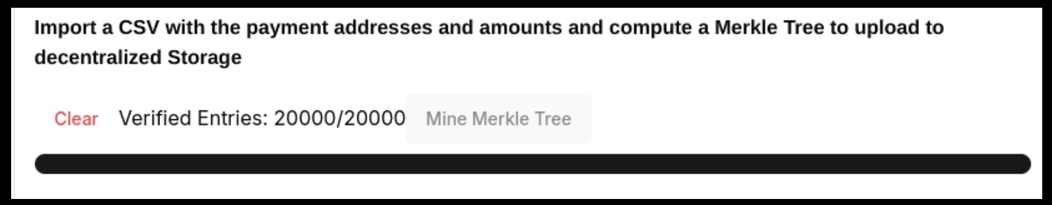
Finding balance between cheap and decentralized

A unique solution that replaces custodial mass payments found on the current market

The problem:

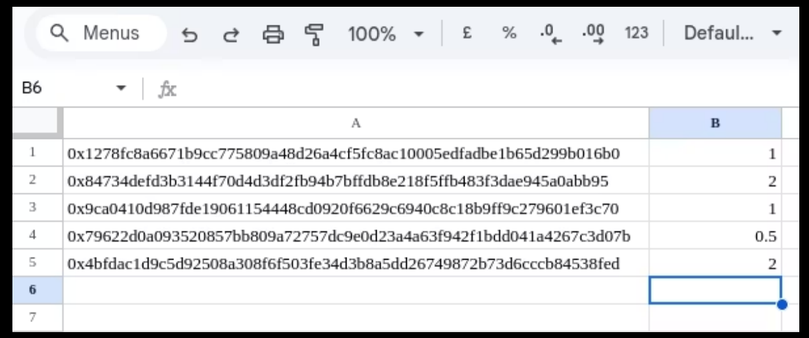
1. Creating thousands of transactions have high gas cost for the sender
2. Payments are non-refundable
3. Test transactions are a chore
4. Current offerings on the market only scale to a thousand transactions max

Scaling Pull Payments with ZKP

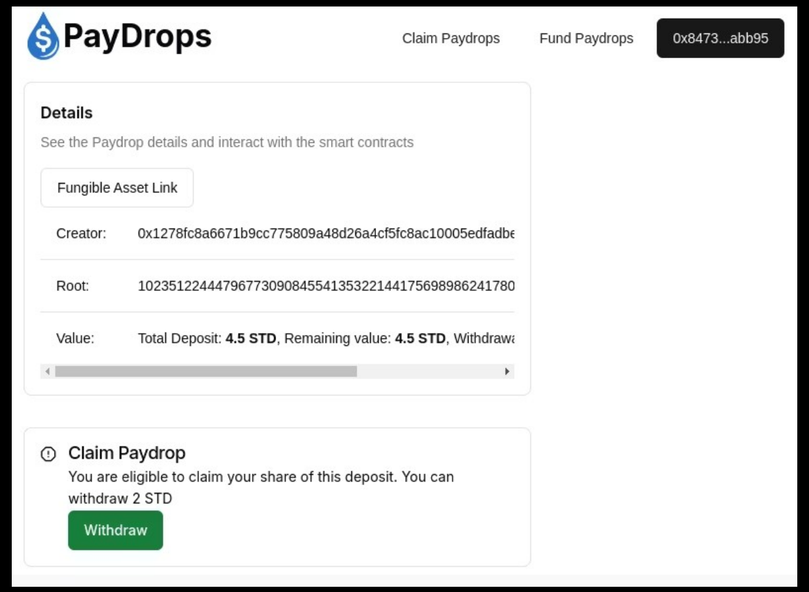


The tech unlocks mass payments on a never before seen scale. Single deposit → tens of thousands of withdrawals.

How it works?



	A	B
1	0x1278fc8a6671b9cc775809a48d26a4cf5fc8ac10005edfadbe1b65d299b016b0	1
2	0x84734defd3b3144f70d4d3df2fb94b7bffdb8e218f5ffb483f3dae945a0abb95	2
3	0x9ca0410d987fde19061154448cd0920f6629c6940c8c18b9ff9c279601ef3c70	1
4	0x79622d0a093520857bb809a72757dc9e0d23a4a63f942f1bdd041a4267c3d07b	0.5
5	0x4bfdac1d9c5d92508a308f6f503fe34d3b8a5dd26749872b73d6cccb84538fed	2
6		
7		



Compose a list of addresses and amounts

Use excel or other tools to create a CSV, the DApp will compose a Merkle Tree from the withdraw information and you will be prompted to upload the tree to Irys, decentralized storage.

Deposit and Claim

Transfer any fungible asset on the Aptos blockchain to a known address, after making a deposit once.
Send payments for Quadratic Funding or to your employees easily. The unclaimed deposits can be refunded any time.

Scale

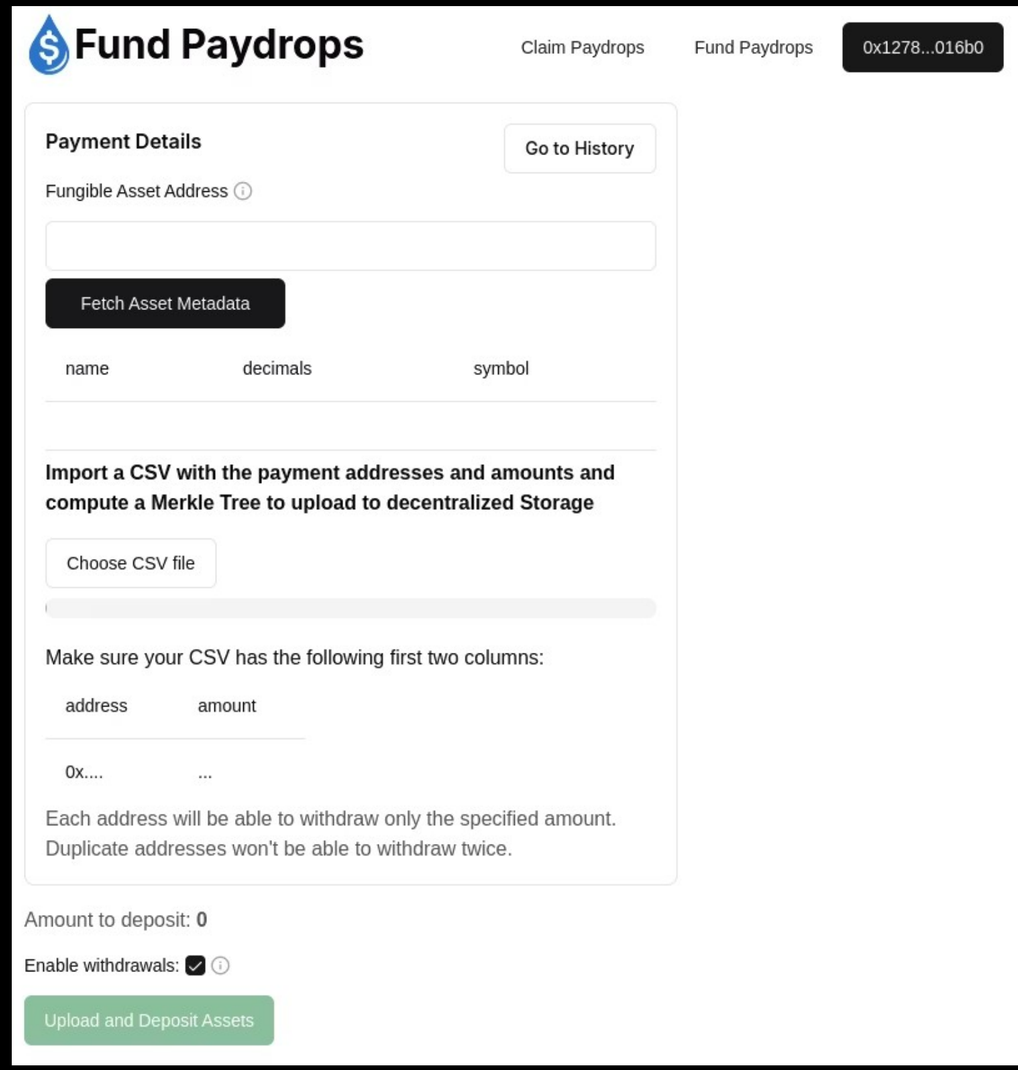
The underlying technology allows massive amounts of transfers.
The merkle tree must be mined which is time intensive so
20k-50k transactions are the recommended max.

But it scales to up to 500k withdrawals from a single deposit.

Use Cases

Scaling transactions with Zero-knowledge proofs and Merkle Trees will allow you to simply send Fungible Assets to a lot of addresses

- AirDrops
- Quadratic Funding
- Payrolls
- Mass Payouts



Current status & use of funds

Current status

The MVP is deployed on Aptos Testnet and you can try it out using any Fungible Asset you own.

- February
  MVP On Testnet
- March
  Phase-2 ceremony
  for Groth-16 proving system
- April
  Mainnet Launch

Open Source

Developed a full featured application. Circom circuits, Move Contracts and DApp Front End.

- 1.
  A ZKP DApp implementation for the Aptos Ecosystem
- 2.
  Simplifies ZKP usage and best practices.
- 3.
  Working on a Move Package to help to reproduce ZKP features without rewriting them every time

Use of funds

Funds are spent on further development of Aptos Paydrops, mainnet deployment and research into more ZKP implementations on Aptos

- 1.
  Paydrops are marketed via free token AirDrops
- 2.
  Publishing a Move Package to help use ZKP
- 3.
  Further research into ZKP apps on Aptos to explore more possibilities

Source Code and Links

The application is fully open source and available on github.

- https://github.com/Aptos-PayDrop/Aptos-Paydrops-DApp
- https://aptospaydrops.com
- Aptos explorer: Object 0x629a9a226a53badad0e3a18bb81408c1b2bf5072363dfef603d8af559f2755e3