

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

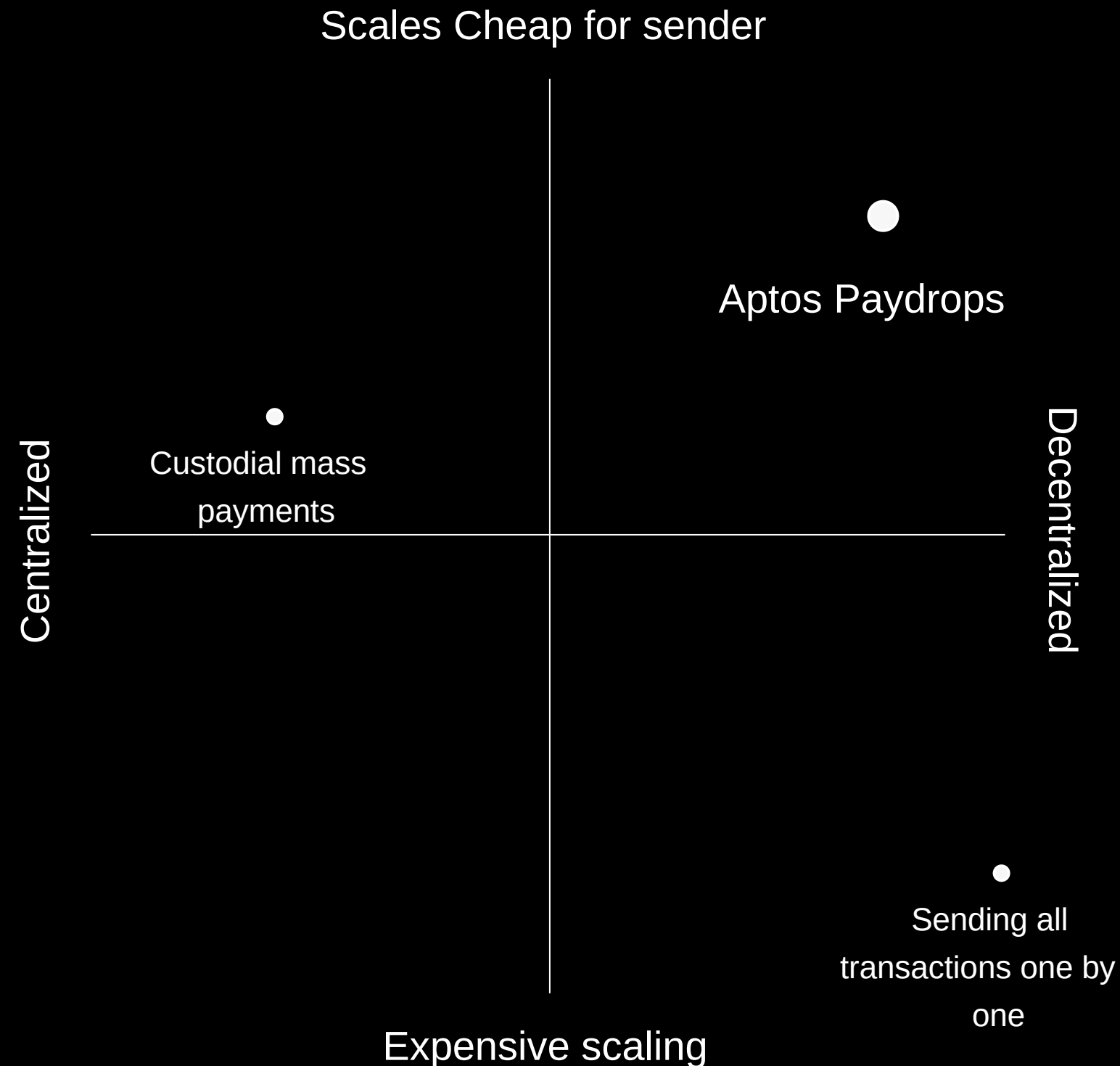
Aptos Paydrops

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

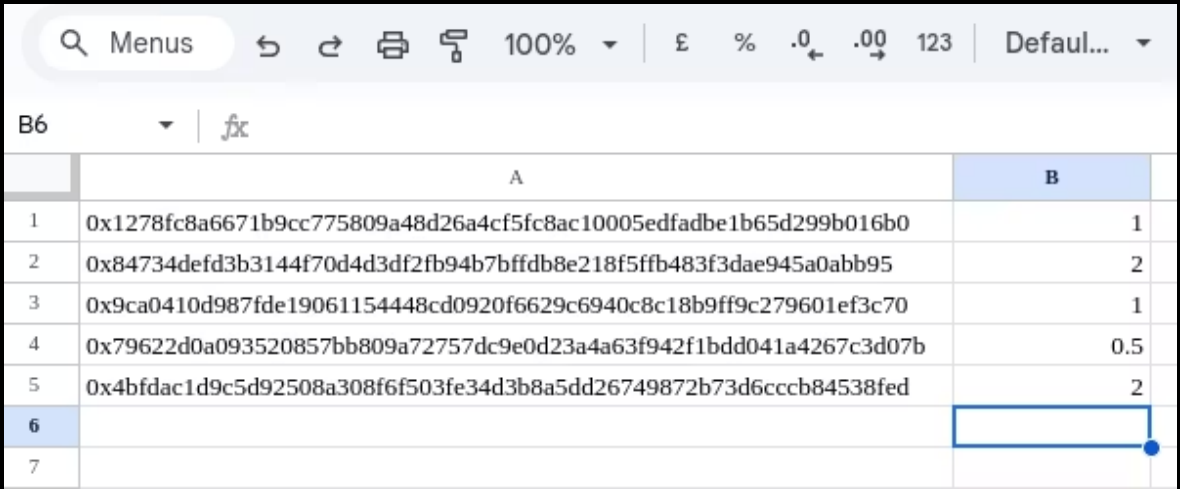
Import a CSV with the payment addresses and amounts and compute a Merkle Tree to upload to decentralized Storage

[Clear](#) Verified Entries: 20000/20000 [Mine Merkle Tree](#)

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



How it works?



The screenshot shows an Excel spreadsheet with two columns, A and B. Column A contains five hexadecimal addresses, and column B contains corresponding numerical values. The interface includes a search bar, navigation icons, and a status bar at the bottom.

	A	B
1	0x1278fc8a6671b9cc775809a48d26a4cf5fc8ac10005edfadbe1b65d299b016b0	1
2	0x84734defd3b3144f70d4d3df2fb94b7bffd8e218f5ffb483f3dae945a0abb95	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

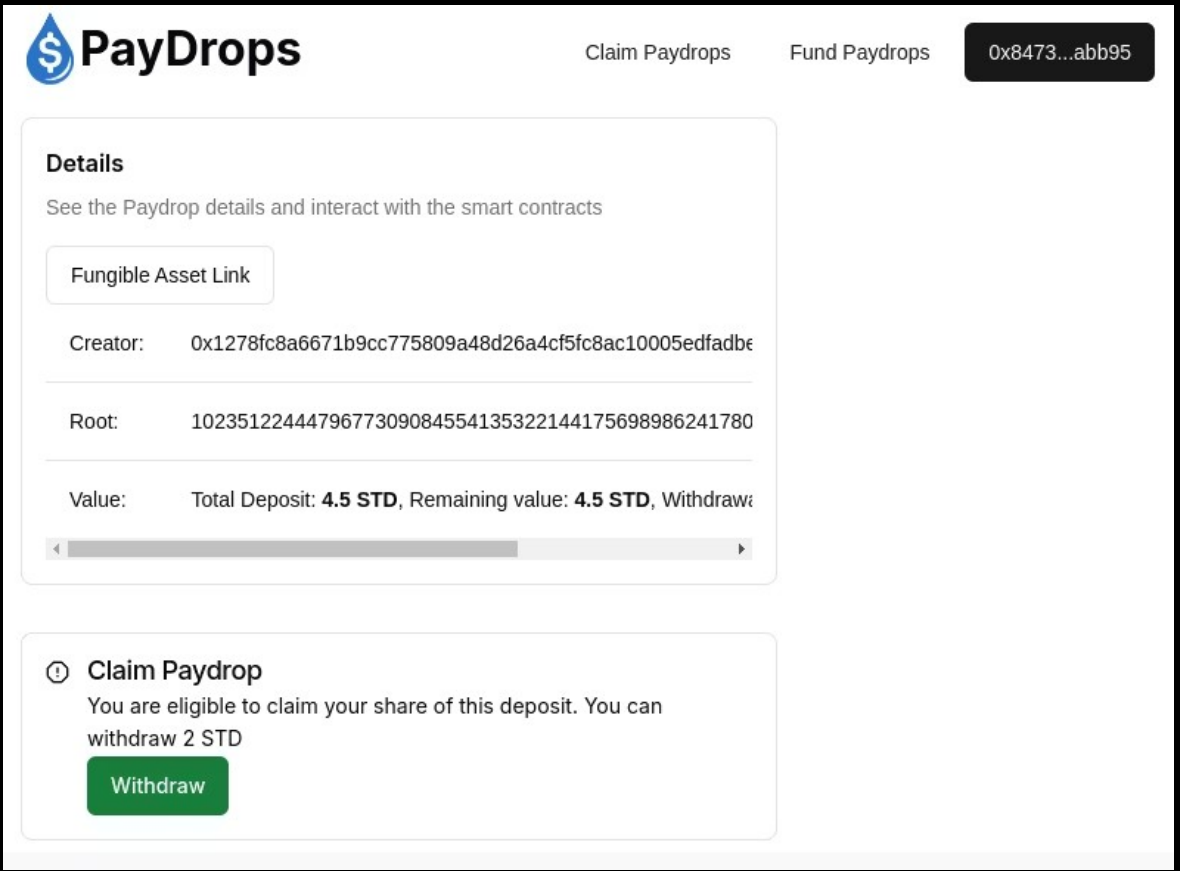
Transfer any fungible asset on the Aptos blockchain to a known address, after making a deposit once.

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.



The screenshot shows the PayDrops web interface. It has a header with the PayDrops logo and navigation tabs for 'Claim Paydrops' and 'Fund Paydrops'. A dark button shows the address '0x8473...abb95'. The 'Details' section includes a 'Fungible Asset Link' and fields for 'Creator', 'Root', and 'Value'. The 'Value' field shows 'Total Deposit: 4.5 STD, Remaining value: 4.5 STD, Withdraw:'. A 'Claim Paydrop' section at the bottom states 'You are eligible to claim your share of this deposit. You can withdraw 2 STD' and features a green 'Withdraw' button.

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


Fund Paydrops

[Claim Paydrops](#)[Fund Paydrops](#)

0x1278...016b0

Payment Details

Go to History

Fungible Asset Address 

Fetch Asset Metadata

name	decimals	symbol
------	----------	--------

Import a CSV with the payment addresses and amounts and compute a Merkle Tree to upload to decentralized Storage


Choose CSV file

Make sure your CSV has the following first two columns:

address	amount
0x....	...

Each address will be able to withdraw only the specified amount. Duplicate addresses won't be able to withdraw twice.

Amount to deposit: 0

Enable withdrawals: ☒ 

Upload and Deposit Assets

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](#)
[0x629a9a226a53badad0e3a18bb81408c1b2bf5072363dfef603d8af](#)
[559f2755e3](#)

