Remintooor

Pleb.fi Miami 2023

Jonathan Harvey-Buschel

17 May 2023

Why?

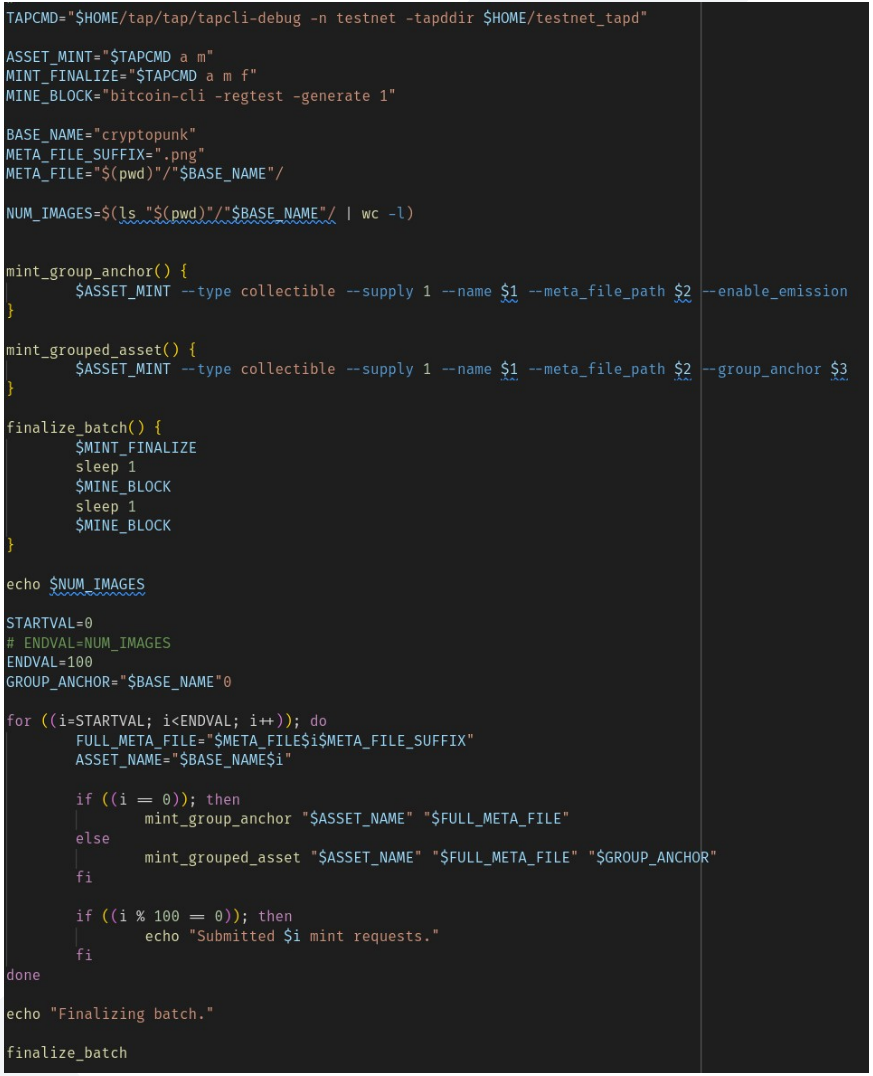
- Keep collectible data off-chain

-Create collectibles in batches, in a simple TX

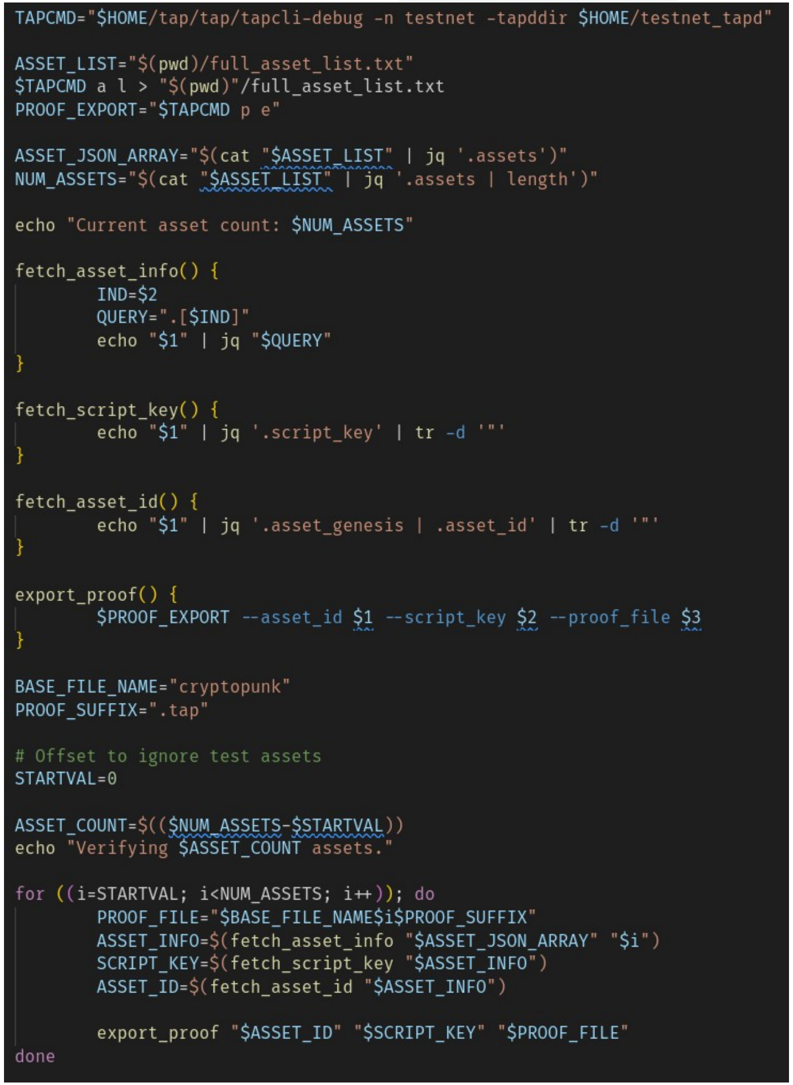
-Receiver still is guaranteed to have the data

How?

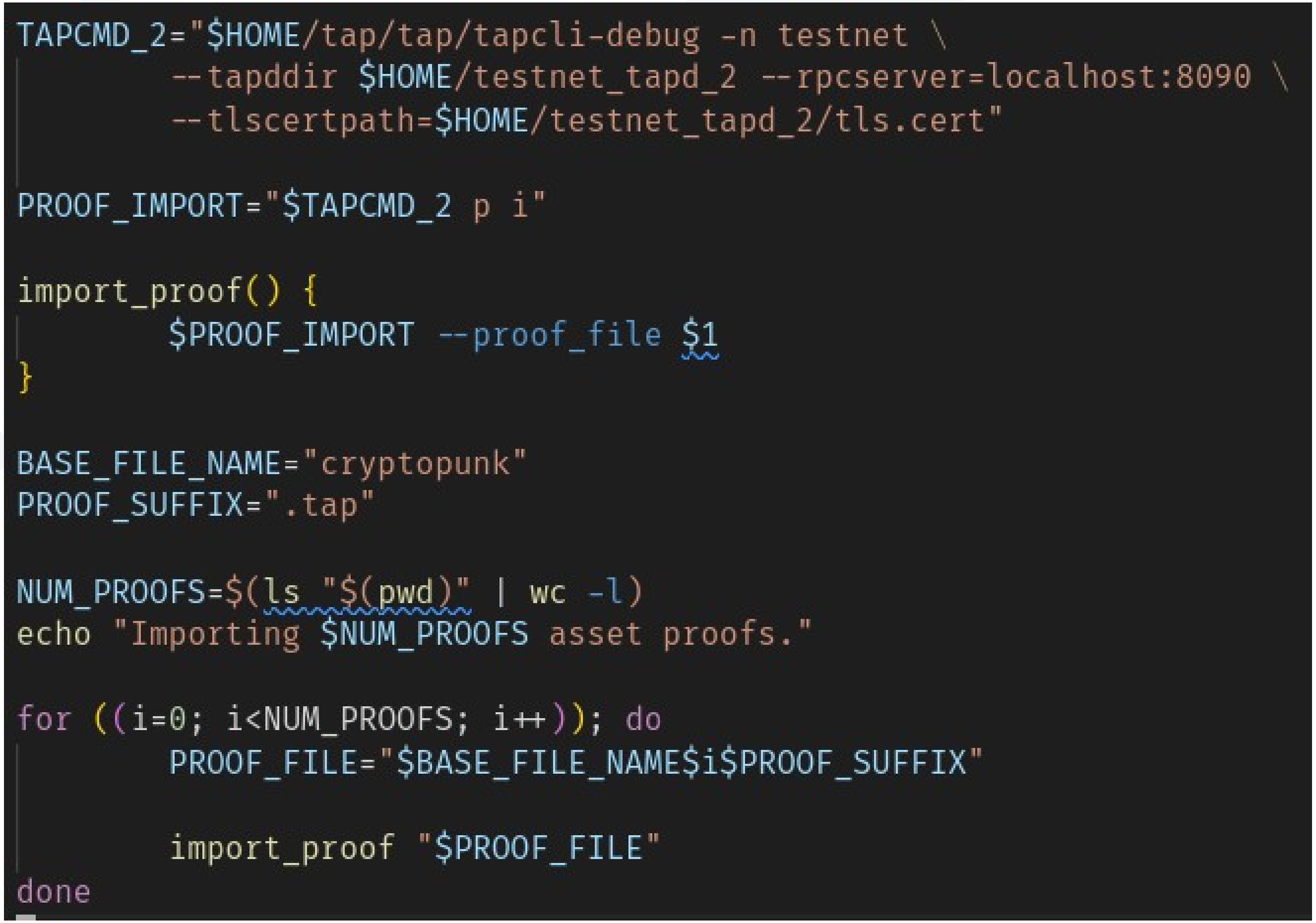
- Collect a batch of data (images)
- Create an asset group, build a minting batch
- Submit the TX
- Export and import proofs
- Can extract metadata



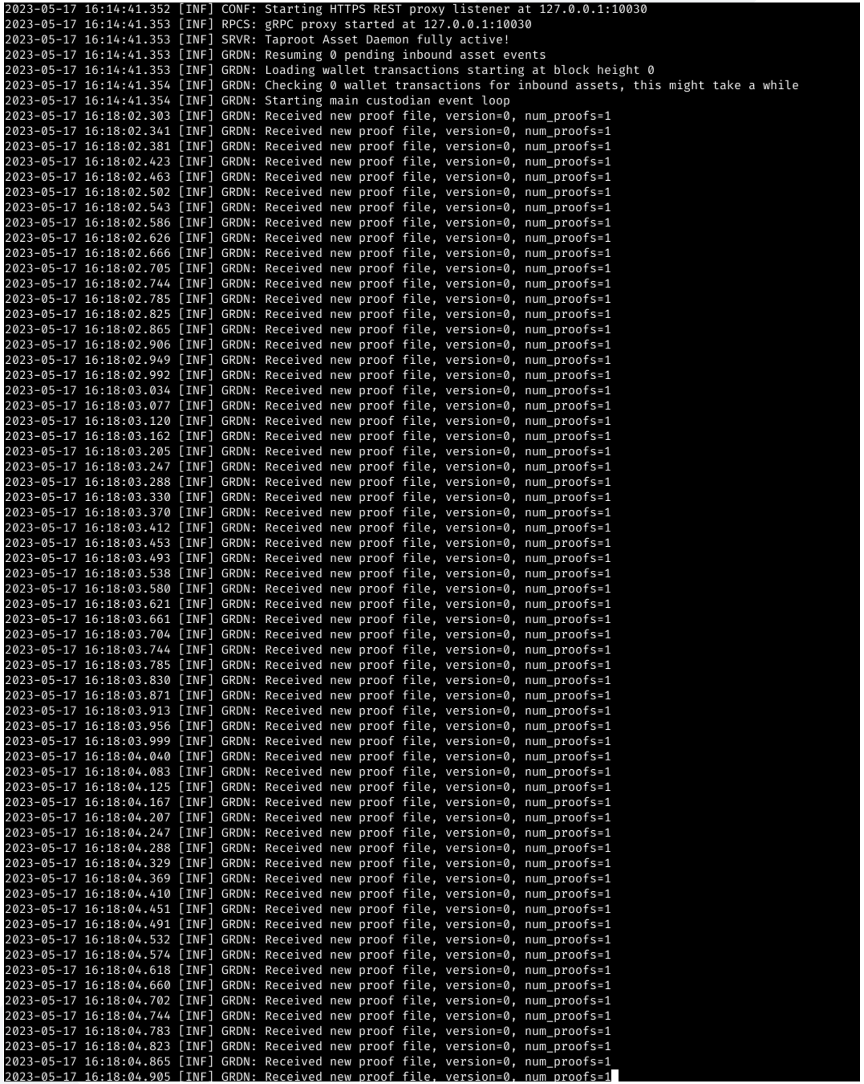
```
TAPCMD="$HOME/tap/tap/tapcli-debug -n testnet -tapddir $HOME/testnet_tapd"

ASSET_MINT="$TAPCMD a m"
MINT_FINALIZE="$TAPCMD a m f"
MINE_BLOCK="bitcoin-cli -regtest -generate 1"

BASE_NAME="cryptopunk"
META_FILE_SUFFIX=".png"
META_FILE="$(pwd)"/"$BASE_NAME"/

NUM_IMAGES=$(ls "$(pwd)"/"$BASE_NAME"/ | wc -l)


mint_group_anchor() {
        $ASSET_MINT --type collectible --supply 1 --name $1 --meta_file_path $2 --enable_emission
}

mint_grouped_asset() {
        $ASSET_MINT --type collectible --supply 1 --name $1 --meta_file_path $2 --group_anchor $3
}

finalize_batch() {
        $MINT_FINALIZE
        sleep 1
        $MINE_BLOCK
        sleep 1
        $MINE_BLOCK
}

echo $NUM_IMAGES

STARTVAL=0
# ENDVAL=NUM_IMAGES
ENDVAL=100
GROUP_ANCHOR="$BASE_NAME"0

for ((i=STARTVAL; i<ENDVAL; i++)); do
        FULL_META_FILE="$META_FILE$i$META_FILE_SUFFIX"
        ASSET_NAME="$BASE_NAME$i"

        if ((i == 0)); then
                mint_group_anchor "$ASSET_NAME" "$FULL_META_FILE"
        else
                mint_grouped_asset "$ASSET_NAME" "$FULL_META_FILE" "$GROUP_ANCHOR"
        fi

        if ((i % 100 == 0)); then
                echo "Submitted $i mint requests."
        fi
done

echo "Finalizing batch."

finalize_batch
```



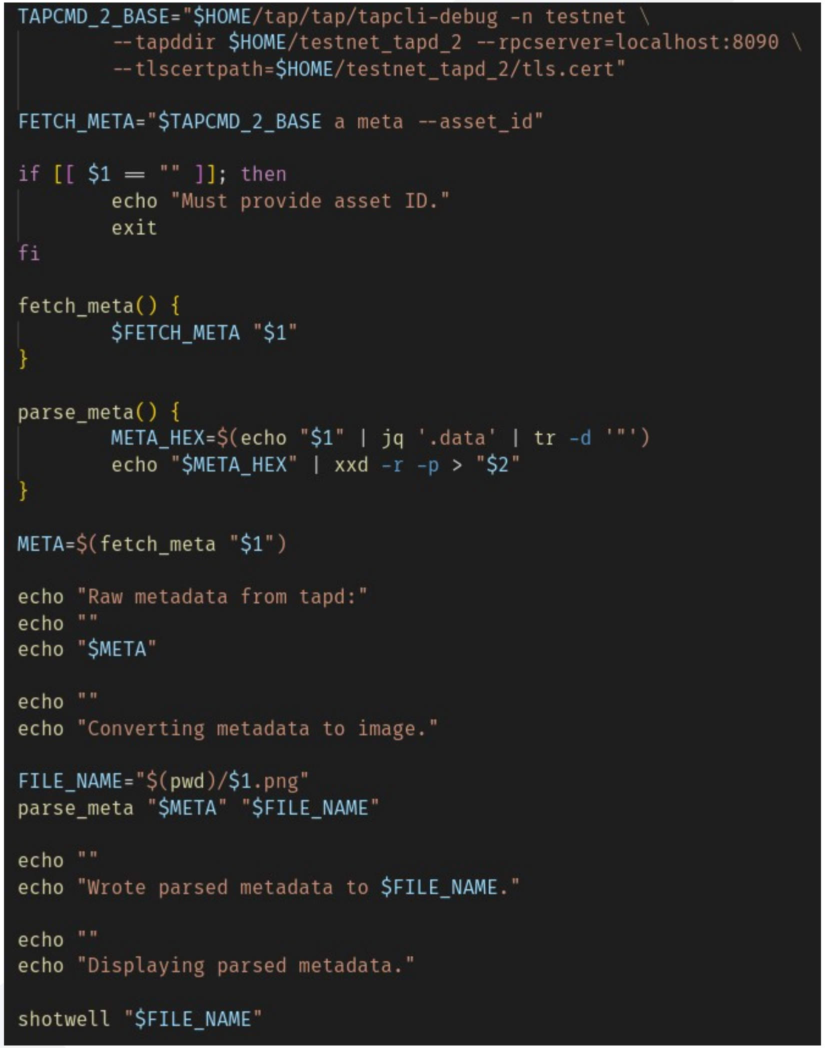
```
TAPCMD="$HOME/tap/tap/tapcli-debug -n testnet -tapddir $HOME/testnet_tapd"

ASSET_LIST="$(pwd)/full_asset_list.txt"
$TAPCMD a l > "$(pwd)"/full_asset_list.txt
PROOF_EXPORT="$TAPCMD p e"

ASSET_JSON_ARRAY="$(cat "$ASSET_LIST" | jq '.assets')"
NUM_ASSETS="$(cat "$ASSET_LIST" | jq '.assets | length')"

echo "Current asset count: $NUM_ASSETS"

fetch_asset_info() {
        IND=$2
        QUERY=".[$IND]"
        echo "$1" | jq "$QUERY"
}

fetch_script_key() {
        echo "$1" | jq '.script_key' | tr -d '"'
}

fetch_asset_id() {
        echo "$1" | jq '.asset_genesis | .asset_id' | tr -d '"'
}

export_proof() {
        $PROOF_EXPORT --asset_id $1 --script_key $2 --proof_file $3
}

BASE_FILE_NAME="cryptopunk"
PROOF_SUFFIX=".tap"

# Offset to ignore test assets
STARTVAL=0

ASSET_COUNT=$(($NUM_ASSETS-$STARTVAL))
echo "Verifying $ASSET_COUNT assets."

for ((i=STARTVAL; i<NUM_ASSETS; i++)); do
        PROOF_FILE="$BASE_FILE_NAME$i$PROOF_SUFFIX"
        ASSET_INFO=$(fetch_asset_info "$ASSET_JSON_ARRAY" "$i")
        SCRIPT_KEY=$(fetch_script_key "$ASSET_INFO")
        ASSET_ID=$(fetch_asset_id "$ASSET_INFO")

        export_proof "$ASSET_ID" "$SCRIPT_KEY" "$PROOF_FILE"
done
```



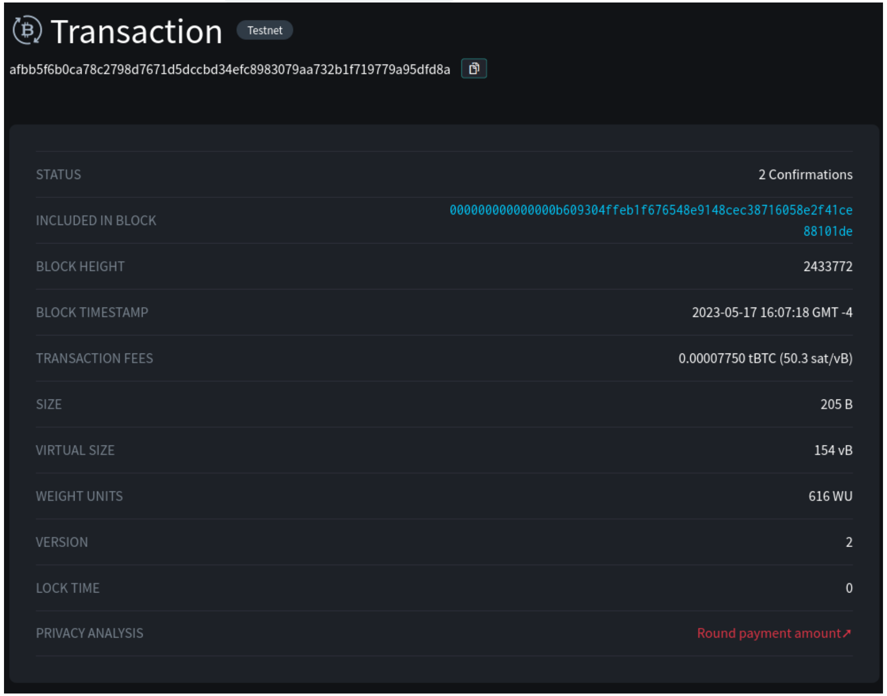
```
TAPCMD_2="$HOME/tap/tap/tapcli-debug -n testnet \
        --tapddir $HOME/testnet_tapd_2 --rpcserver=localhost:8090 \
        --tlscertpath=$HOME/testnet_tapd_2/tls.cert"

PROOF_IMPORT="$TAPCMD_2 p i"

import_proof() {
        $PROOF_IMPORT --proof_file $1
}

BASE_FILE_NAME="cryptopunk"
PROOF_SUFFIX=".tap"

NUM_PROOFS=$(ls "$(pwd)" | wc -l)
echo "Importing $NUM_PROOFS asset proofs."

for ((i=0; i<NUM_PROOFS; i++)); do
        PROOF_FILE="$BASE_FILE_NAME$i$PROOF_SUFFIX"

        import_proof "$PROOF_FILE"
done
```



```
2023-05-17 16:14:41.352 [INF] CONF: Starting HTTPS REST proxy listener at 127.0.0.1:10030
2023-05-17 16:14:41.353 [INF] RPCS: gRPC proxy started at 127.0.0.1:10030
2023-05-17 16:14:41.353 [INF] SRVR: Taproot Asset Daemon fully active!
2023-05-17 16:14:41.353 [INF] GRDN: Resuming 0 pending inbound asset events
2023-05-17 16:14:41.353 [INF] GRDN: Loading wallet transactions starting at block height 0
2023-05-17 16:14:41.354 [INF] GRDN: Checking 0 wallet transactions for inbound assets, this might take a while
2023-05-17 16:14:41.354 [INF] GRDN: Starting main custodian event loop
2023-05-17 16:18:02.303 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.341 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.381 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.423 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.463 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.502 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.543 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.586 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.626 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.666 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.705 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.744 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.785 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.825 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.865 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.906 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.949 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:02.992 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.034 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.077 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.120 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.162 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.205 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.247 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.288 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.330 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.370 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.412 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.453 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.493 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.538 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.580 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.621 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.661 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.704 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.744 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.785 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.830 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.871 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.913 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.956 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:03.999 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.040 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.083 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.125 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.167 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.207 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.247 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.288 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.329 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.369 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.410 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.451 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.491 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.532 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.574 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.618 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.660 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.702 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.744 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.783 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.823 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.865 [INF] GRDN: Received new proof file, version=0, num_proofs=1
2023-05-17 16:18:04.905 [INF] GRDN: Received new proof file, version=0, num_proofs=1
```



```bash
TAPCMD_2_BASE="$HOME/tap/tap/tapcli-debug -n testnet \
        --tapddir $HOME/testnet_tapd_2 --rpcserver=localhost:8090 \
        --tlscertpath=$HOME/testnet_tapd_2/tls.cert"

FETCH_META="$TAPCMD_2_BASE a meta --asset_id"

if [[ $1 == "" ]]; then
        echo "Must provide asset ID."
        exit
fi

fetch_meta() {
        $FETCH_META "$1"
}

parse_meta() {
        META_HEX=$(echo "$1" | jq '.data' | tr -d '"')
        echo "$META_HEX" | xxd -r -p > "$2"
}

META=$(fetch_meta "$1")

echo "Raw metadata from tapd:"
echo ""
echo "$META"

echo ""
echo "Converting metadata to image."

FILE_NAME="$(pwd)/$1.png"
parse_meta "$META" "$FILE_NAME"

echo ""
echo "Wrote parsed metadata to $FILE_NAME."

echo ""
echo "Displaying parsed metadata."

shotwell "$FILE_NAME"
```

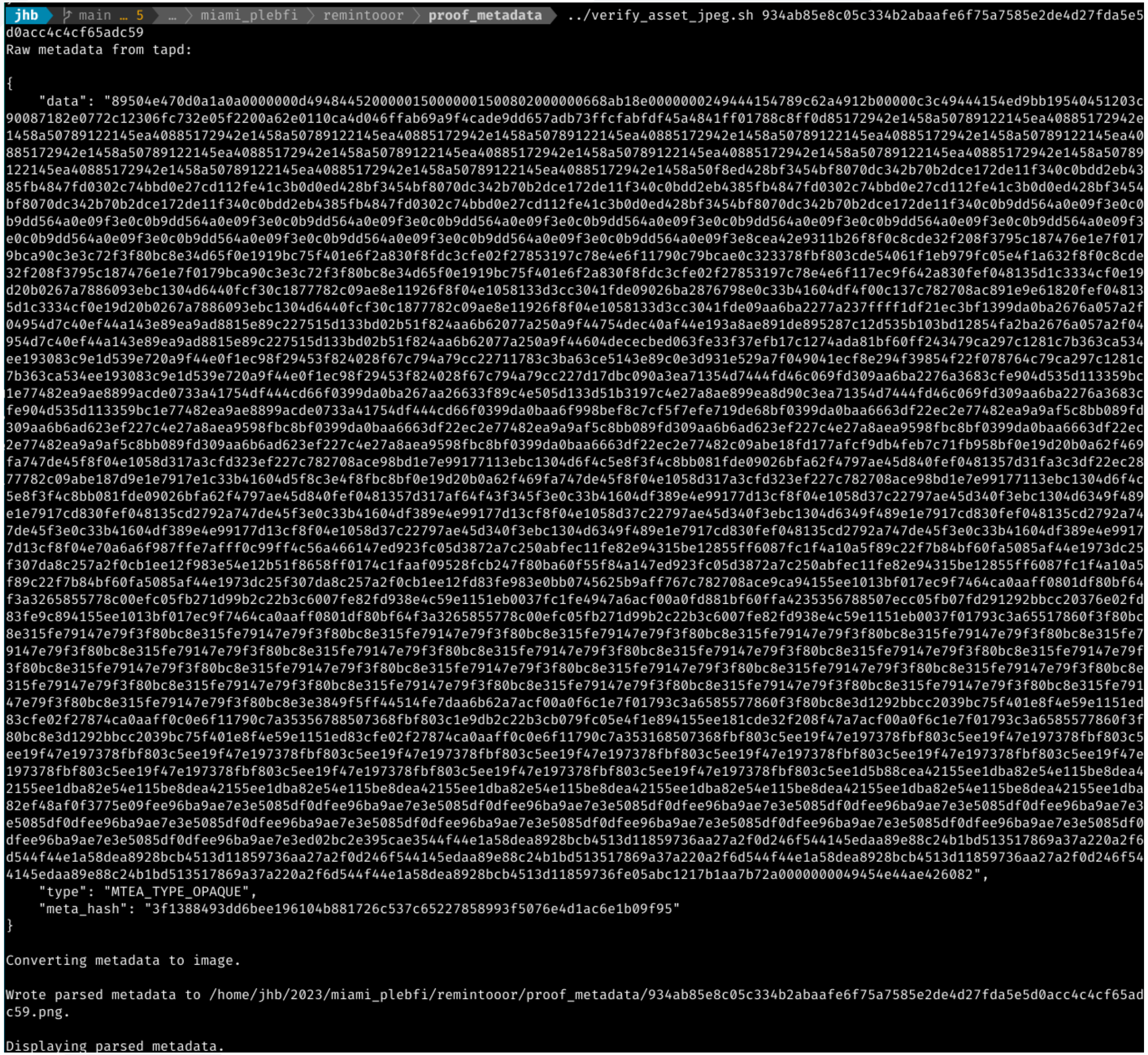


Transaction

Testnet

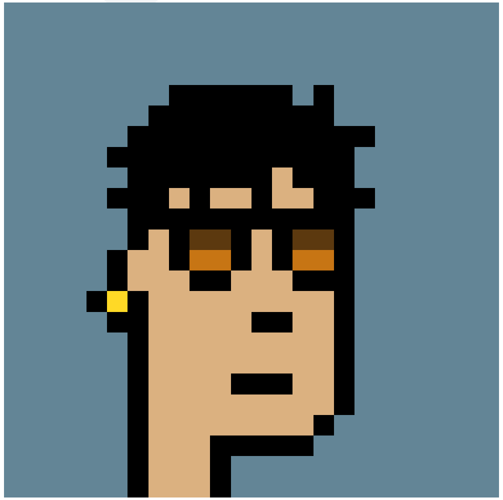
afbb5f6b0ca78c2798d7671d5dccbd34efc8983079aa732b1f719779a95dfd8a

STATUS	2 Confirmations
INCLUDED IN BLOCK	000000000000000b609304ffeb1f676548e9148cec38716058e2f41ce88101de
BLOCK HEIGHT	2433772
BLOCK TIMESTAMP	2023-05-17 16:07:18 GMT -4
TRANSACTION FEES	0.00007750 tBTC (50.3 sat/vB)
SIZE	205 B
VIRTUAL SIZE	154 vB
WEIGHT UNITS	616 WU
VERSION	2
LOCK TIME	0
PRIVACY ANALYSIS	Round payment amount↗



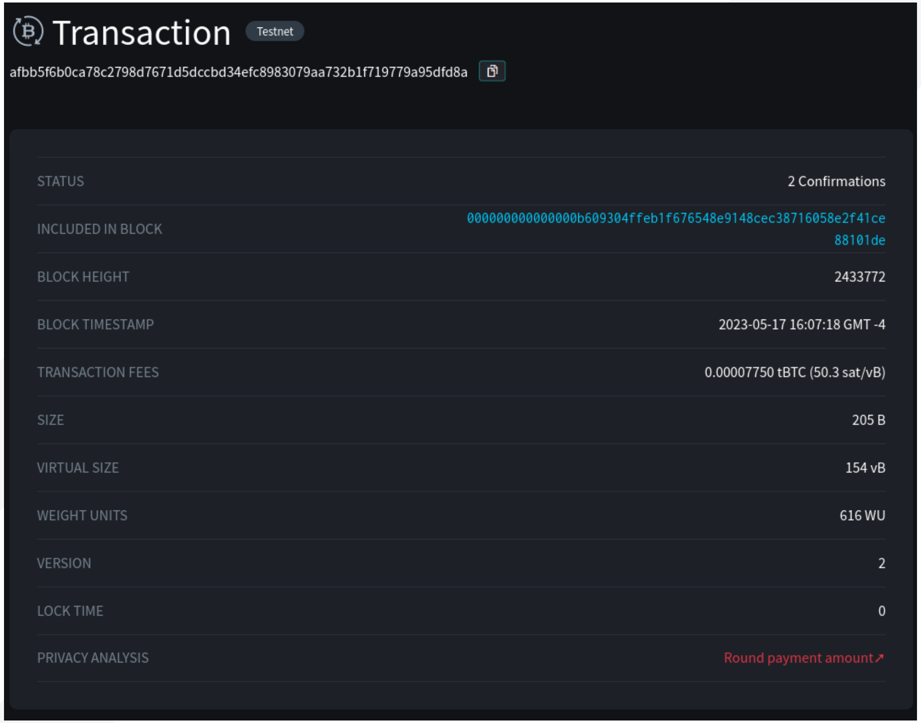
```
 jhb  main … 5  …  miami_plebfi  remintoooor  proof_metadata  ../verify_asset_jpeg.sh 934ab85e8c05c334b2abaafe6f75a7585e2de4d27fda5e5
d0acc4c4cf65adc59
Raw metadata from tapd:

{
    "data": "89504e470d0a1a0a0000000d4948445200000015000000150802000000668ab18e0000000249444154789c62a4912b00000c3c49444154ed9bb19540451203c
90087182e0772c12306fc732e05f2200a62e0110ca4d046ffab69a9f4cade9dd657adb73ffcfabfdf45a4841ff01788c8ff0d85172942e1458a50789122145ea40885172942e
1458a50789122145ea40885172942e1458a50789122145ea40885172942e1458a50789122145ea40885172942e1458a50789122145ea40885172942e1458a50789122145ea40
885172942e1458a50789122145ea40885172942e1458a50789122145ea40885172942e1458a50789122145ea40885172942e1458a50789122145ea40885172942e1458a50789
122145ea40885172942e1458a50789122145ea40885172942e1458a50789122145ea40885172942e1458a50f8ed428bf3454bf8070dc342b70b2dce172de11f340c0bdd2eb43
85fb4847fd0302c74bbd0e27cd112fe41c3b0d0ed428bf3454bf8070dc342b70b2dce172de11f340c0bdd2eb4385fb4847fd0302c74bbd0e27cd112fe41c3b0d0ed428bf3454
bf8070dc342b70b2dce172de11f340c0bdd2eb4385fb4847fd0302c74bbd0e27cd112fe41c3b0d0ed428bf3454bf8070dc342b70b2dce172de11f340c0b9dd564a0e09f3e0c0
b9dd564a0e09f3e0c0b9dd564a0e09f3e0c0b9dd564a0e09f3e0c0b9dd564a0e09f3e0c0b9dd564a0e09f3e0c0b9dd564a0e09f3e0c0b9dd564a0e09f3e0c0b9dd564a0e09f3
e0c0b9dd564a0e09f3e0c0b9dd564a0e09f3e0c0b9dd564a0e09f3e0c0b9dd564a0e09f3e0c0b9dd564a0e09f3e8cea42e9311b26f8f0c8cde32f208f3795c187476e1e7f017
9bca90c3e3c72f3f80bc8e34d65f0e1919bc75f401e6f2a830f8fdc3cfe02f27853197c78e4e6f11790c79bcae0c323378fbf803cde54061f1eb979fc05e4f1a632f8f0c8cde
32f208f3795c187476e1e7f0179bca90c3e3c72f3f80bc8e34d65f0e1919bc75f401e6f2a830f8fdc3cfe02f27853197c78e4e6f117ec9f642a830fef048135d1c3334cf0e19
d20b0267a7886093ebc1304d6440fcf30c1877782c09ae8e11926f8f04e1058133d3cc3041fde09026ba2876798e0c33b41604df4f00c137c782708ac891e9e61820fef04813
5d1c3334cf0e19d20b0267a7886093ebc1304d6440fcf30c1877782c09ae8e11926f8f04e1058133d3cc3041fde09aa6ba2277a237ffff1df21ec3bf1399da0ba2676a057a2f
04954d7c40ef44a143e89ea9ad8815e89c227515d133bd02b51f824aa6b62077a250a9f44754dec40af44e193a8ae891de895287c12d535b103bd12854fa2ba2676a057a2f04
954d7c40ef44a143e89ea9ad8815e89c227515d133bd02b51f824aa6b62077a250a9f44604dececbed063fe33f37efb17c1274ada81bf60ff243479ca297c1281c7b363ca534
ee193083c9e1d539e720a9f44e0f1ec98f29453f824028f67c794a79cc22711783c3ba63ce5143e89c0e3d931e529a7f049041ecf8e294f39854f22f078764c79ca297c1281c
7b363ca534ee193083c9e1d539e720a9f44e0f1ec98f29453f824028f67c794a79cc227d17dbc090a3ea71354d7444fd46c069fd309aa6ba2276a3683cfe904d535d113359bc
1e77482ea9ae8899acde0733a41754df444cd66f0399da0ba267aa26633f89c4e505d133d51b3197c4e27a8ae899ea8d90c3ea71354d7444fd46c069fd309aa6ba2276a3683c
fe904d535d113359bc1e77482ea9ae8899acde0733a41754df444cd66f0399da0baa6f998bef8c7cf5f7efe719de68bf0399da0baa6663df22ec2e77482ea9a9af5c8bb089fd
309aa6b6ad623ef227c4e27a8aea9598fbc8bf0399da0baa6663df22ec2e77482ea9a9af5c8bb089fd309aa6b6ad623ef227c4e27a8aea9598fbc8bf0399da0baa6663df22ec
2e77482ea9a9af5c8bb089fd309aa6b6ad623ef227c4e27a8aea9598fbc8bf0399da0baa6663df22ec2e77482c09abe18fd177afcf9db4feb7c71fb958bf0e19d20b0a62f469
fa747de45f8f04e1058d317a3cfd323ef227c782708ace98bd1e7e99177113ebc1304d6f4c5e8f3f4c8bb081fde09026bfa62f4797ae45d840fef0481357d31fa3c3df22ec28
77782c09abe187d9e1e7917e1c33b41604d5f8c3e4f8fbc8bf0e19d20b0a62f469fa747de45f8f04e1058d317a3cfd323ef227c782708ace98bd1e7e99177113ebc1304d6f4c
5e8f3f4c8bb081fde09026bfa62f4797ae45d840fef0481357d317af64f43f345f3e0c33b41604df389e4e99177d13cf8f04e1058d37c22797ae45d340f3ebc1304d6349f489
e1e7917cd830fef048135cd2792a747de45f3e0c33b41604df389e4e99177d13cf8f04e1058d37c22797ae45d340f3ebc1304d6349f489e1e7917cd830fef048135cd2792a74
7de45f3e0c33b41604df389e4e99177d13cf8f04e1058d37c22797ae45d340f3ebc1304d6349f489e1e7917cd830fef048135cd2792a747de45f3e0c33b41604df389e4e9917
7d13cf8f04e70a6a6f987ffe7afff0c99ff4c56a466147ed923fc05d3872a7c250abfec11fe82e94315be12855ff6087fc1f4a10a5f89c22f7b84bf60fa5085af44e1973dc25
f307da8c257a2f0cb1ee12f983e54e12b51f8658ff0174c1faaf09528fcb247f80ba60f55f84a147ed923fc05d3872a7c250abfec11fe82e94315be12855ff6087fc1f4a10a5
f89c22f7b84bf60fa5085af44e1973dc25f307da8c257a2f0cb1ee12fd83fe983e0bb0745625b9aff767c782708ace9ca94155ee1013bf017ec9f7464ca0aaff0801df80bf64
f3a3265855778c00efc05fb271d99b2c22b3c6007fe82fd938e4c59e1151eb0037fc1fe4947a6acf00a0fd881bf60ffa4235356788507ecc05fb07fd291292bbcc20376e02fd
83fe9c894155ee1013bf017ec9f7464ca0aaff0801df80bf64f3a3265855778c00efc05fb271d99b2c22b3c6007fe82fd938e4c59e1151eb0037f01793c3a65517860f3f80bc
8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe7
9147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f
3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e
315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe79147e79f3f80bc8e315fe791
47e79f3f80bc8e315fe79147e79f3f80bc8e3e3849f5ff44514fe7daa6b62a7acf00a0f6c1e7f01793c3a6585577860f3f80bc8e3d1292bbcc2039bc75f401e8f4e59e1151ed
83cfe02f27874ca0aaff0c0e6f11790c7a35356788507368fbf803c1e9db2c22b3cb079fc05e4f1e894155ee181cde32f208f47a7acf00a0f6c1e7f01793c3a6585577860f3f
80bc8e3d1292bbcc2039bc75f401e8f4e59e1151ed83cfe02f27874ca0aaff0c0e6f11790c7a353168507368fbf803c5ee19f47e197378fbf803c5ee19f47e197378fbf803c5
ee19f47e197378fbf803c5ee19f47e197378fbf803c5ee19f47e197378fbf803c5ee19f47e197378fbf803c5ee19f47e197378fbf803c5ee19f47e197378fbf803c5ee19f47e
197378fbf803c5ee19f47e197378fbf803c5ee19f47e197378fbf803c5ee19f47e197378fbf803c5ee19f47e197378fbf803c5ee1d5b88cea42155ee1dba82e54e115be8dea4
2155ee1dba82e54e115be8dea42155ee1dba82e54e115be8dea42155ee1dba82e54e115be8dea42155ee1dba82e54e115be8dea42155ee1dba82e54e115be8dea42155ee1dba
82ef48af0f3775e09fee96ba9ae7e3e5085df0dfee96ba9ae7e3e5085df0dfee96ba9ae7e3e5085df0dfee96ba9ae7e3e5085df0dfee96ba9ae7e3e5085df0dfee96ba9ae7e3
e5085df0dfee96ba9ae7e3e5085df0dfee96ba9ae7e3e5085df0dfee96ba9ae7e3e5085df0dfee96ba9ae7e3e5085df0dfee96ba9ae7e3e5085df0dfee96ba9ae7e3e5085df0
dfee96ba9ae7e3e5085df0dfee96ba9ae7e3ed02bc2e395cae3544f44e1a58dea8928bcb4513d11859736aa27a2f0d246f544145edaa89e88c24b1bd513517869a37a220a2f6
d544f44e1a58dea8928bcb4513d11859736aa27a2f0d246f544145edaa89e88c24b1bd513517869a37a220a2f6d544f44e1a58dea8928bcb4513d11859736aa27a2f0d246f54
4145edaa89e88c24b1bd513517869a37a220a2f6d544f44e1a58dea8928bcb4513d11859736fe05abc1217b1aa7b72a0000000049454e44ae426082",
    "type": "MTEA_TYPE_OPAQUE",
    "meta_hash": "3f1388493dd6bee196104b881726c537c65227858993f5076e4d1ac6e1b09f95"
}

Converting metadata to image.

Wrote parsed metadata to /home/jhb/2023/miami_plebfi/remintoooor/proof_metadata/934ab85e8c05c334b2abaafe6f75a7585e2de4d27fda5e5d0acc4c4cf65ad
c59.png.

Displaying parsed metadata.
```

It works!



Demo

What does it look like on-chain?

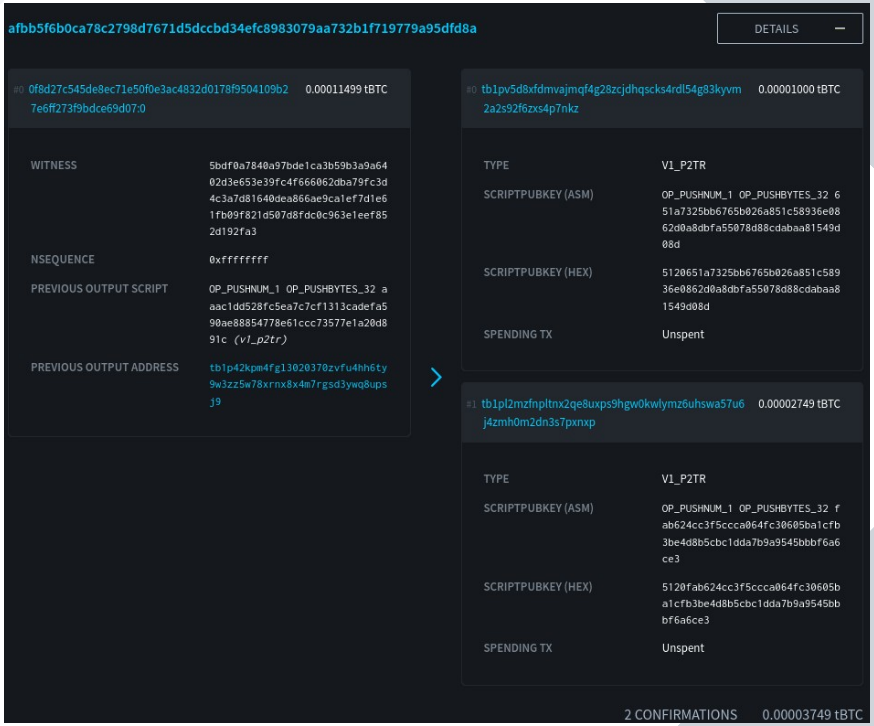


Transaction

Testnet

afbb5f6b0ca78c2798d7671d5dccbd34efc8983079aa732b1f719779a95dfd8a

STATUS	2 Confirmations
INCLUDED IN BLOCK	000000000000000b609304ffeb1f676548e9148cec38716058e2f41ce88101de
BLOCK HEIGHT	2433772
BLOCK TIMESTAMP	2023-05-17 16:07:18 GMT -4
TRANSACTION FEES	0.00007750 tBTC (50.3 sat/vB)
SIZE	205 B
VIRTUAL SIZE	154 vB
WEIGHT UNITS	616 WU
VERSION	2
LOCK TIME	0
PRIVACY ANALYSIS	Round payment amount ↗



afbb5f6b0ca78c2798d7671d5dccbd34efc8983079aa732b1f719779a95dfd8a

#0 0f8d27c545de8ec71e50f0e3ac4832d0178f9504109b27e6ff273f9bdce69d07:0 0.00011499 tBTC

WITNESS	5bdf0a7840a97bde1ca3b59b3a9a6402d3e653e39fc4f666062dba79fc3d4c3a7d81640dea866ae9ca1ef7d1e61fb09f821d507d8fdc0c963e1eef852d192fa3
NSEQUENCE	0xffffffff
PREVIOUS OUTPUT SCRIPT	OP_PUSHNUM_1 OP_PUSHBYTES_32 aaac1dd528fc5ea7c7cf1313cadefa590ae88854778e61ccc73577e1a20d891c *(v1_p2tr)*
PREVIOUS OUTPUT ADDRESS	tb1p42kpm4fgl3020370zvfu4hh6ty9w3zz5w78xrnx8x4m7rgsd3ywq8upsj9

#0 tb1pv5d8xfdmvajmqf4g28zcjdhqscks4rdl54g83kyvm2a2s92f6zxs4p7nkz 0.00001000 tBTC

TYPE	V1_P2TR
SCRIPTPUBKEY (ASM)	OP_PUSHNUM_1 OP_PUSHBYTES_32 651a7325bb6765b026a851c58936e0862d0a8dbfa55078d88cdabaa81549d08d
SCRIPTPUBKEY (HEX)	5120651a7325bb6765b026a851c58936e0862d0a8dbfa55078d88cdabaa81549d08d
SPENDING TX	Unspent

#1 tb1pl2mzfnpltnx2qe8uxps9hgw0kwlymz6uhswa57u6j4zmh0m2dn3s7pxnxp 0.00002749 tBTC

TYPE	V1_P2TR
SCRIPTPUBKEY (ASM)	OP_PUSHNUM_1 OP_PUSHBYTES_32 fab624cc3f5ccca064fc30605ba1cfb3be4d8b5cbc1dda7b9a9545bbbf6a6ce3
SCRIPTPUBKEY (HEX)	5120fab624cc3f5ccca064fc30605ba1cfb3be4d8b5cbc1dda7b9a9545bbbf6a6ce3
SPENDING TX	Unspent

2 CONFIRMATIONS 0.00003749 tBTC

What does it look like off-chain?

- Input file was 4.1k
- Genesis proof is 8.2k
- Proof file grows with each transfer (for now)
- Asset genesis proofs can sync automatically between nodes

Future work

- Tap CLI additions to verify against an input file
- Tap improvements to scale to ∞ leaves
- Draft spec for metadata types