Previous Name: D3

Fourth Estate

A secure, decentralized news data storing and sharing solution for journalists

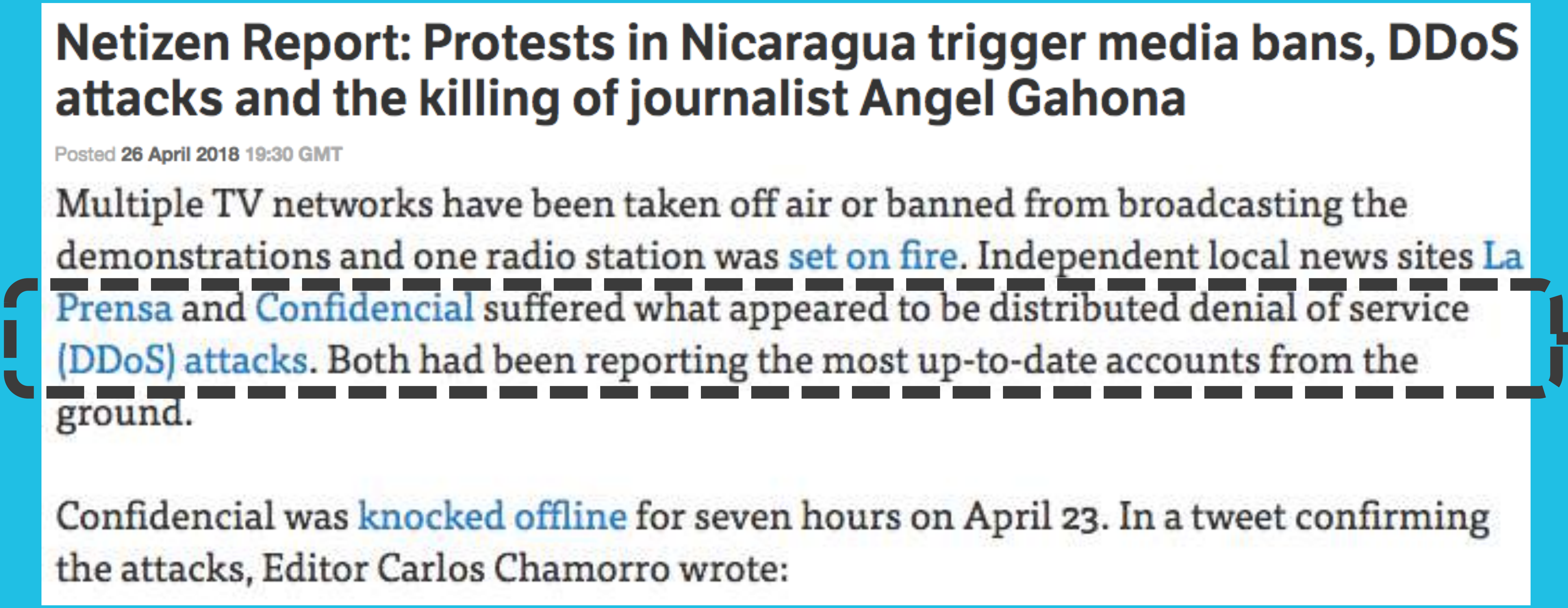
Aaron Chong | Remini Yip

International Student Blockchain Competition's Presentation

Problem

Content availability is not guaranteed

News sites with traditional database/cloud: Vulnerable to single point of failure risk



Netizen Report: Protests in Nicaragua trigger media bans, DDoS attacks and the killing of journalist Angel Gahona

Posted 26 April 2018 19:30 GMT

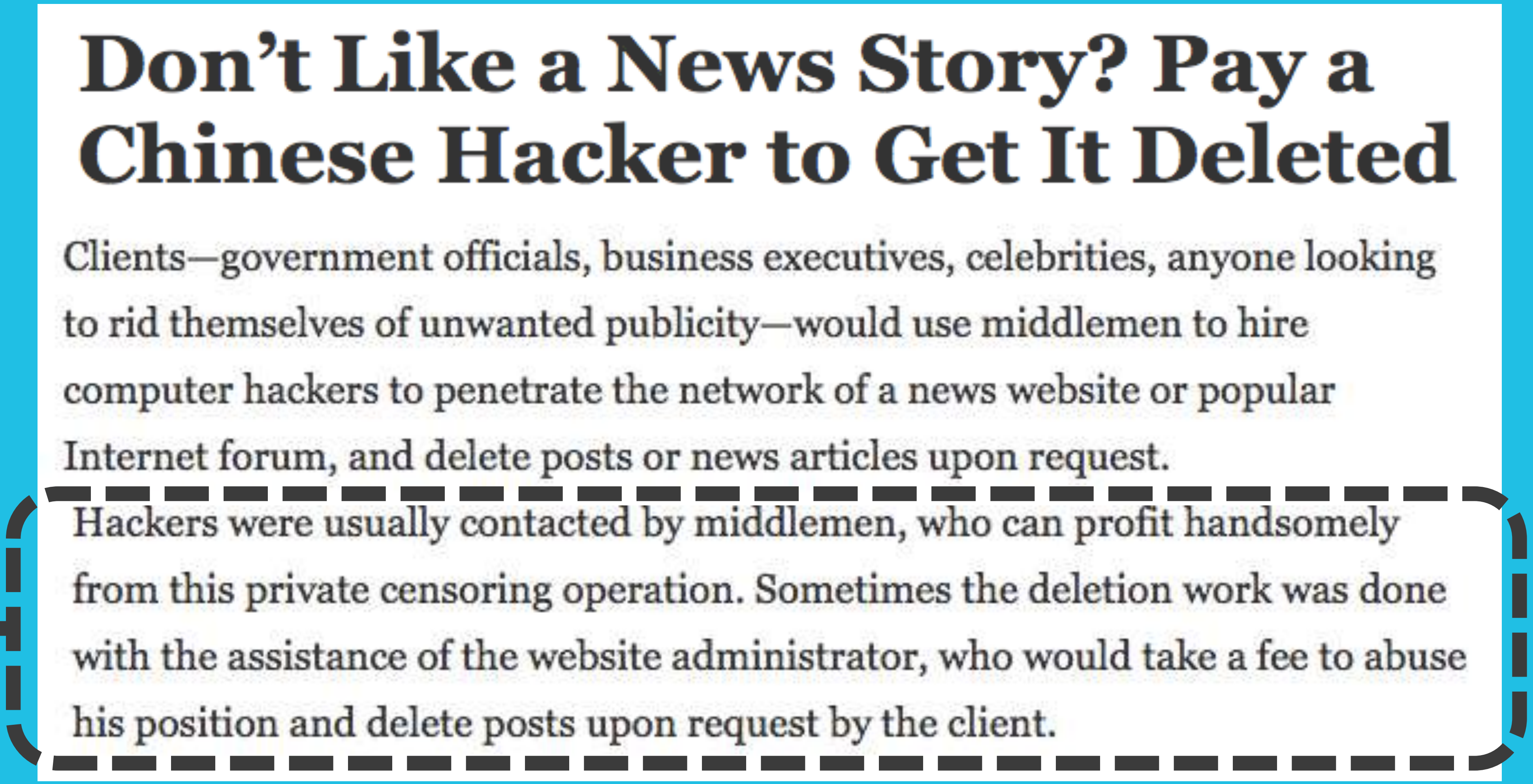
Multiple TV networks have been taken off air or banned from broadcasting the demonstrations and one radio station was set on fire. Independent local news sites La Prensa and Confidencial suffered what appeared to be distributed denial of service (DDoS) attacks. Both had been reporting the most up-to-date accounts from the ground.

Confidencial was knocked offline for seven hours on April 23. In a tweet confirming the attacks, Editor Carlos Chamorro wrote:

Central server or DB down, contents become unavailable

Problem (Cont.)
Content availability is not guaranteed

News sites with traditional database/cloud: Vulnerable to single point of failure risk



Don’t Like a News Story? Pay a Chinese Hacker to Get It Deleted

Clients—government officials, business executives, celebrities, anyone looking to rid themselves of unwanted publicity—would use middlemen to hire computer hackers to penetrate the network of a news website or popular Internet forum, and delete posts or news articles upon request.

Hackers were usually contacted by middlemen, who can profit handsomely from this private censoring operation. Sometimes the deletion work was done with the assistance of the website administrator, who would take a fee to abuse his position and delete posts upon request by the client.

Content modifications or deletions by malicious users or site owners

Our Offers

1

Decentralized Storage

- Possible to get contents even when the original uploader is down.
- Immutable contents. Censorship-free

2

Secure Sharing

- Support 3 use cases
- Full access control. Only the intended recipient can read the content, e.g. your subscriber

3

Charge Per File

- Size does NOT matter
- Same costs for uploading a 5KB document and a 5MB video

Use Cases

Public Sharing + Unencrypted Content

- Anyone can read the content
- Example: News articles/Related data (pictures, videos, tapes, etc.) accessible by the public

Private Sharing + Unencrypted Content

- Only the specified recipients can read the content
- Example: Analyses/Related data accessible by the subscribers

Private Sharing + Encrypted Content

- For a single recipient or a small group of recipients
- Example: Drafts/Information exchange between journalists

Key Terms

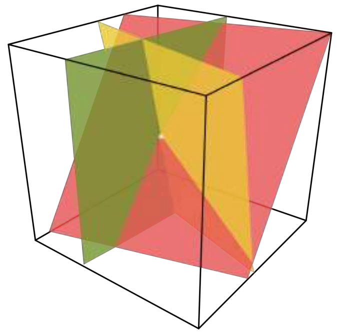
Ethereum

- Distributed computing platform
- Store data references & control data access
- Smart Contract: a program on Ethereum.
- Ethereum Node: a computer connected to the Ethereum network.

InterPlanetary File System

- Distributed file system
- Store data (in file format)
- IPFS Node: a computer connected to the IPFS network.

Key Terms (Cont.)



Shamir Secret Sharing

- Split a message into n pieces
- Require at least t pieces to reconstruct the message, where t ≤ n

Public Key Cryptography

- The sender encrypts a message with the receiver's public key
- The receiver decrypts the message with his private key

Digital Signature

- The sender calculates the *hash of a message, then encrypts the hash with his private key
- The sender sends the encrypted hash and the message to the receiver
- The receiver decrypts the hash with the sender's public key. He also calculates the hash of the message
- The hash from the decryption should = the hash from the calculation

*hash = a numeric value that uniquely identifies the message

Roles & Responsibilities

Owner

Example:
Journalist

Responsibilities

- Store contents (-$)
- Control content access (-$)

Recipient

Example:
Public/Subscriber/Journalist

Responsibilities

- Retrieve contents

Supervisor

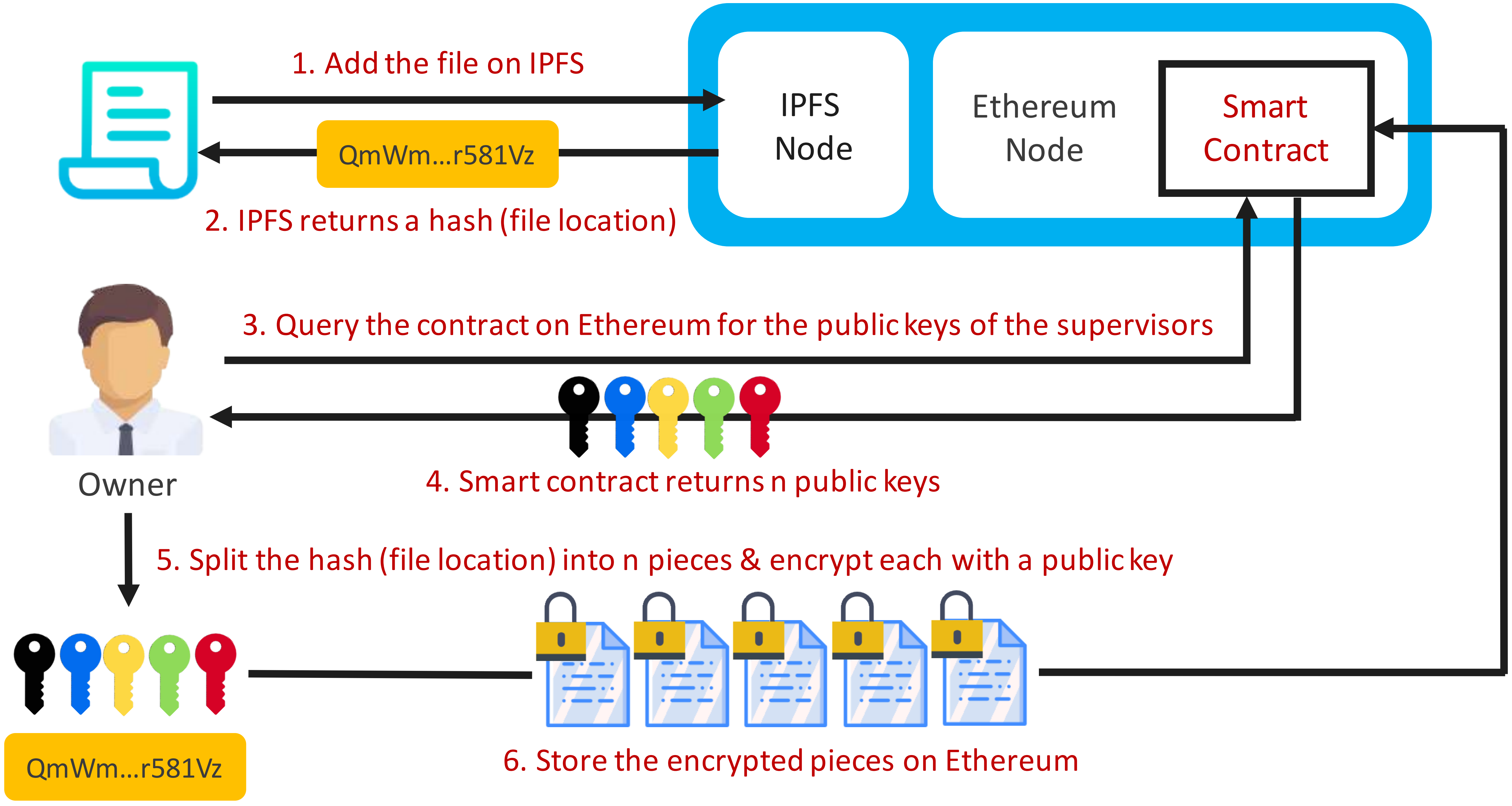
Example:
Altruistic netizen/Media company/Press Assoc.

Responsibilities

- Provide verification services on request
- Provide decryption services on request

Mechanism – Storage

[Private Sharing]



1. Add the file on IPFS

2. IPFS returns a hash (file location)

3. Query the contract on Ethereum for the public keys of the supervisors

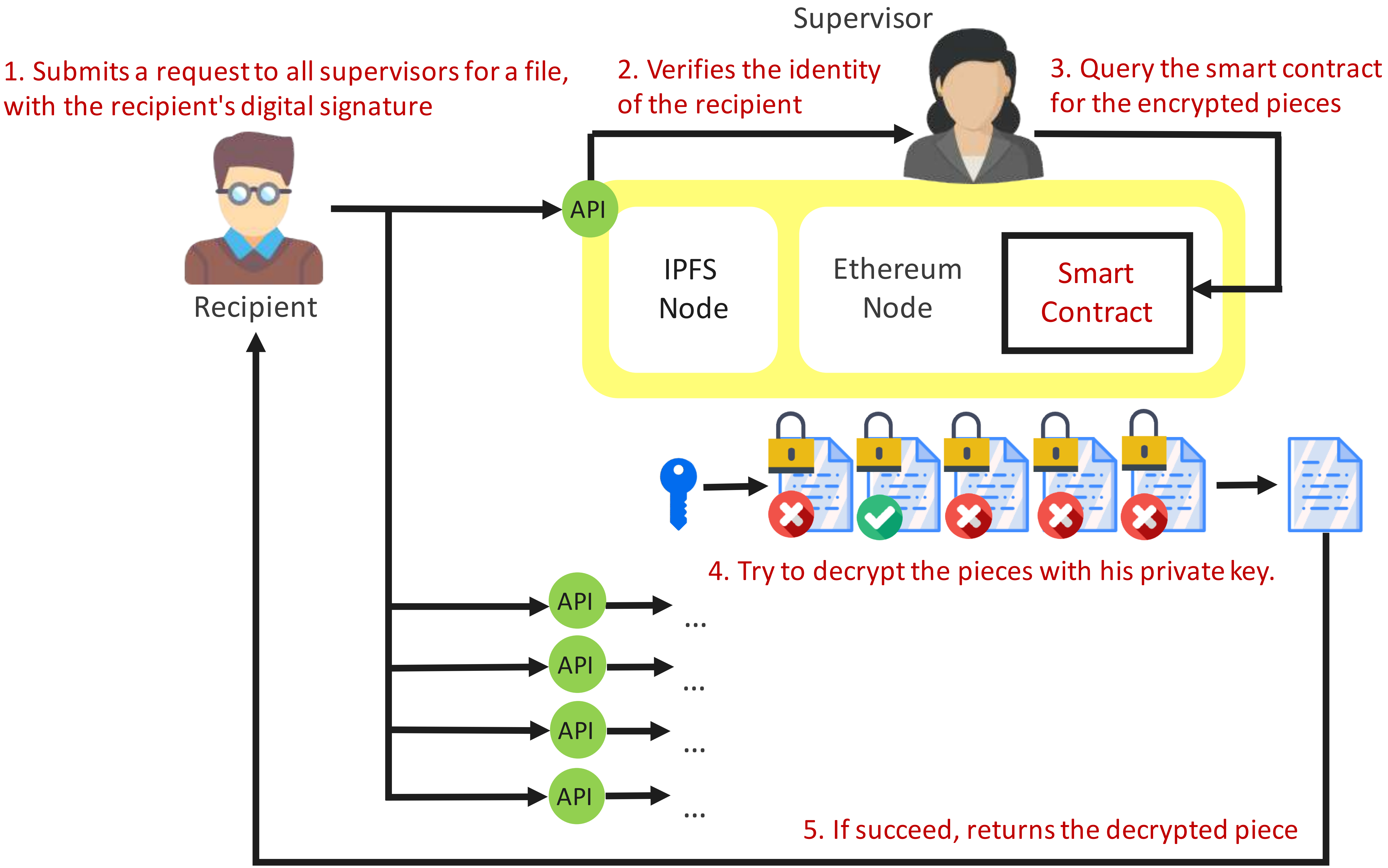
4. Smart contract returns n public keys

5. Split the hash (file location) into n pieces & encrypt each with a public key

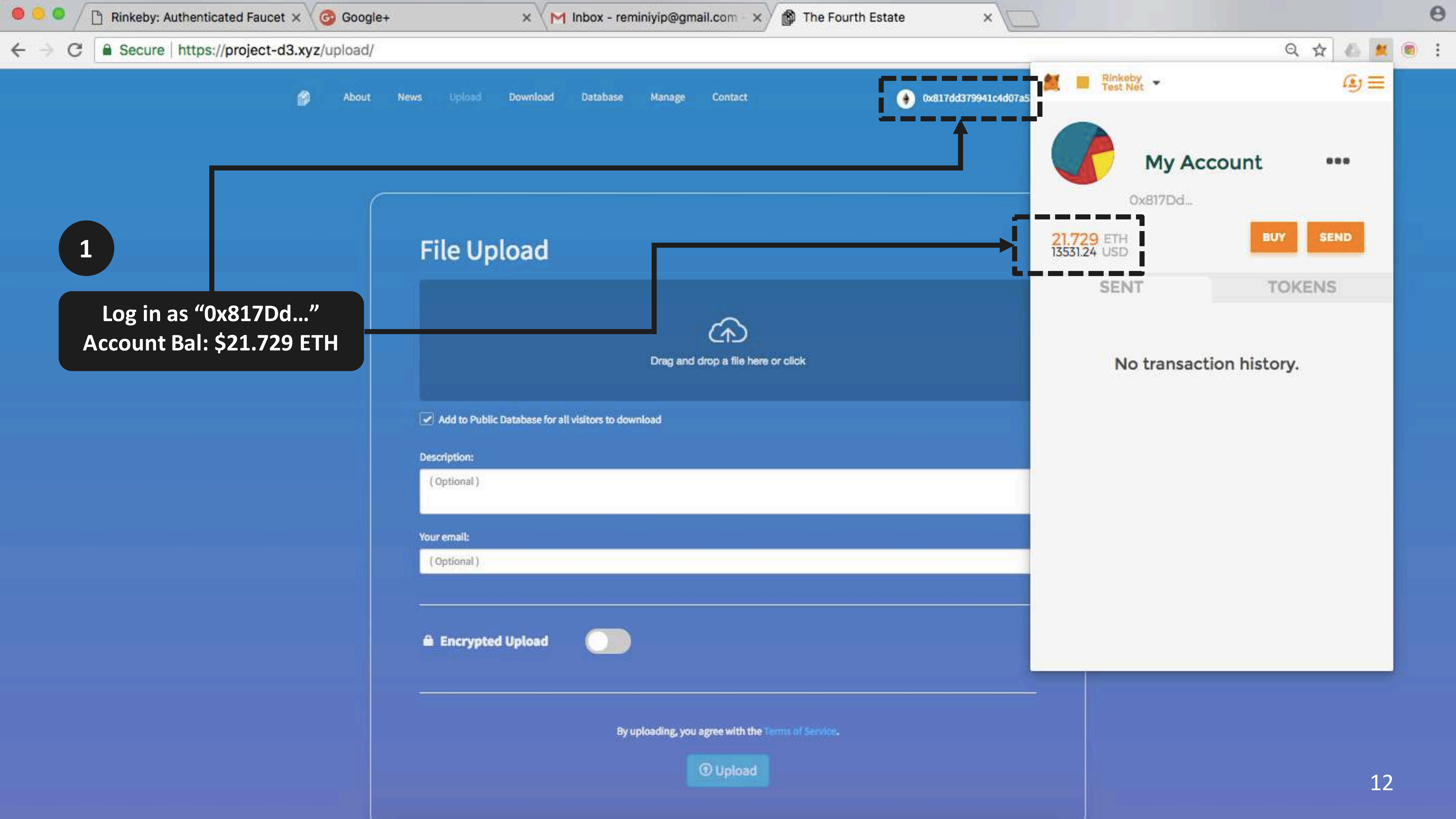
6. Store the encrypted pieces on Ethereum

Mechanism – Retrieval

[Private Sharing]


Supervisor
1. Submits a request to all supervisors for a file, with the recipient's digital signature
2. Verifies the identity of the recipient
3. Query the smart contract for the encrypted pieces
Recipient
API
IPFS Node
Ethereum Node
Smart Contract
4. Try to decrypt the pieces with his private key.
API
...
API
...
API
...
API
...
5. If succeed, returns the decrypted piece

Demonstration Screenshots



1

Log in as “0x817Dd…”
Account Bal: $21.729 ETH

File Upload

Drag and drop a file here or click

☑ Add to Public Database for all visitors to download

Description:
(Optional)

Your email:
(Optional)

Encrypted Upload

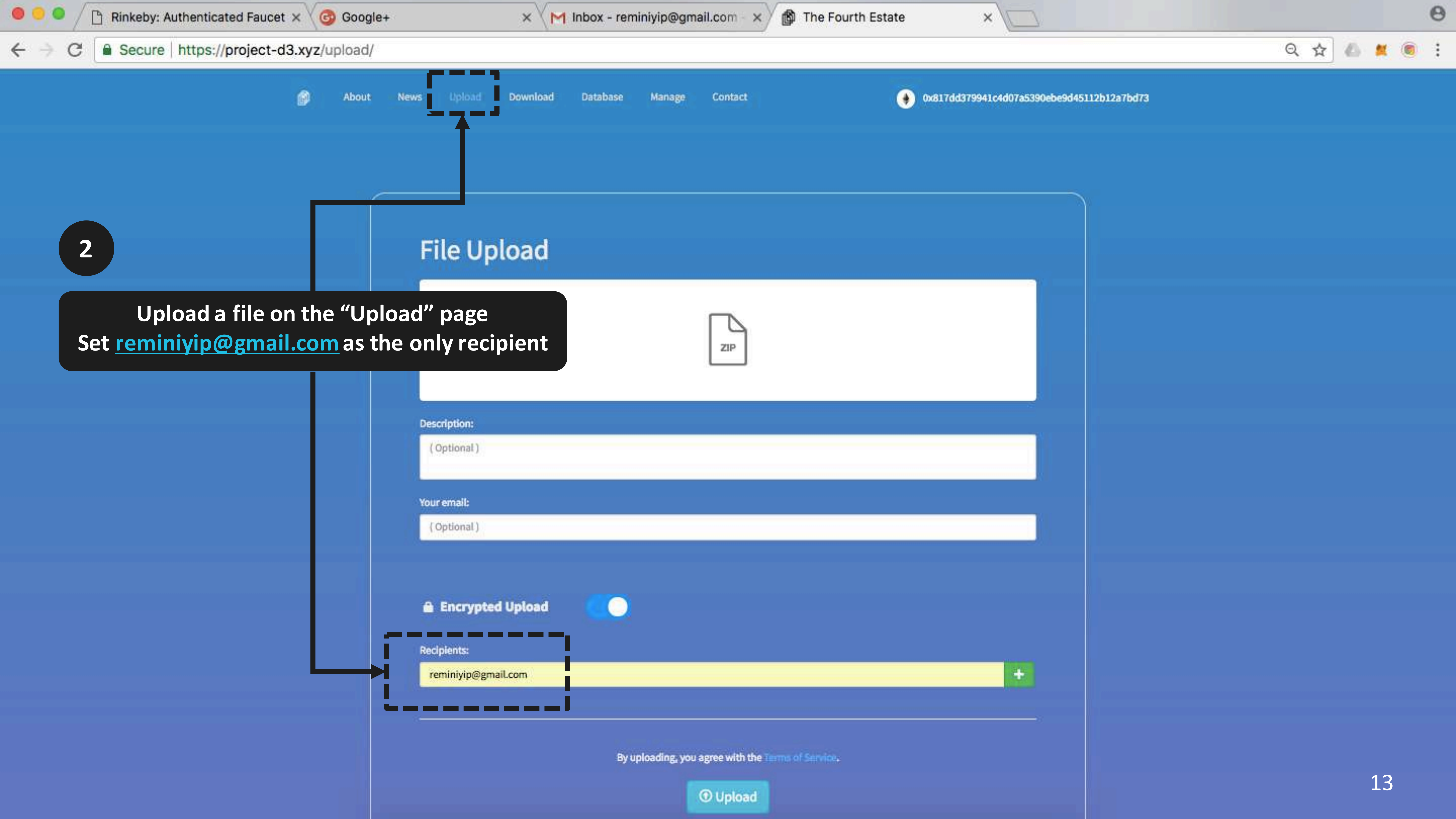
By uploading, you agree with the Terms of Service.

My Account

0x817Dd...

21.729 ETH
13531.24 USD

No transaction history.



https://project-d3.xyz/upload/

0x817dd379941c4d07a5390ebe9d45112b12a7bd73

2

Upload a file on the “Upload” page
Set reminiyip@gmail.com as the only recipient

File Upload

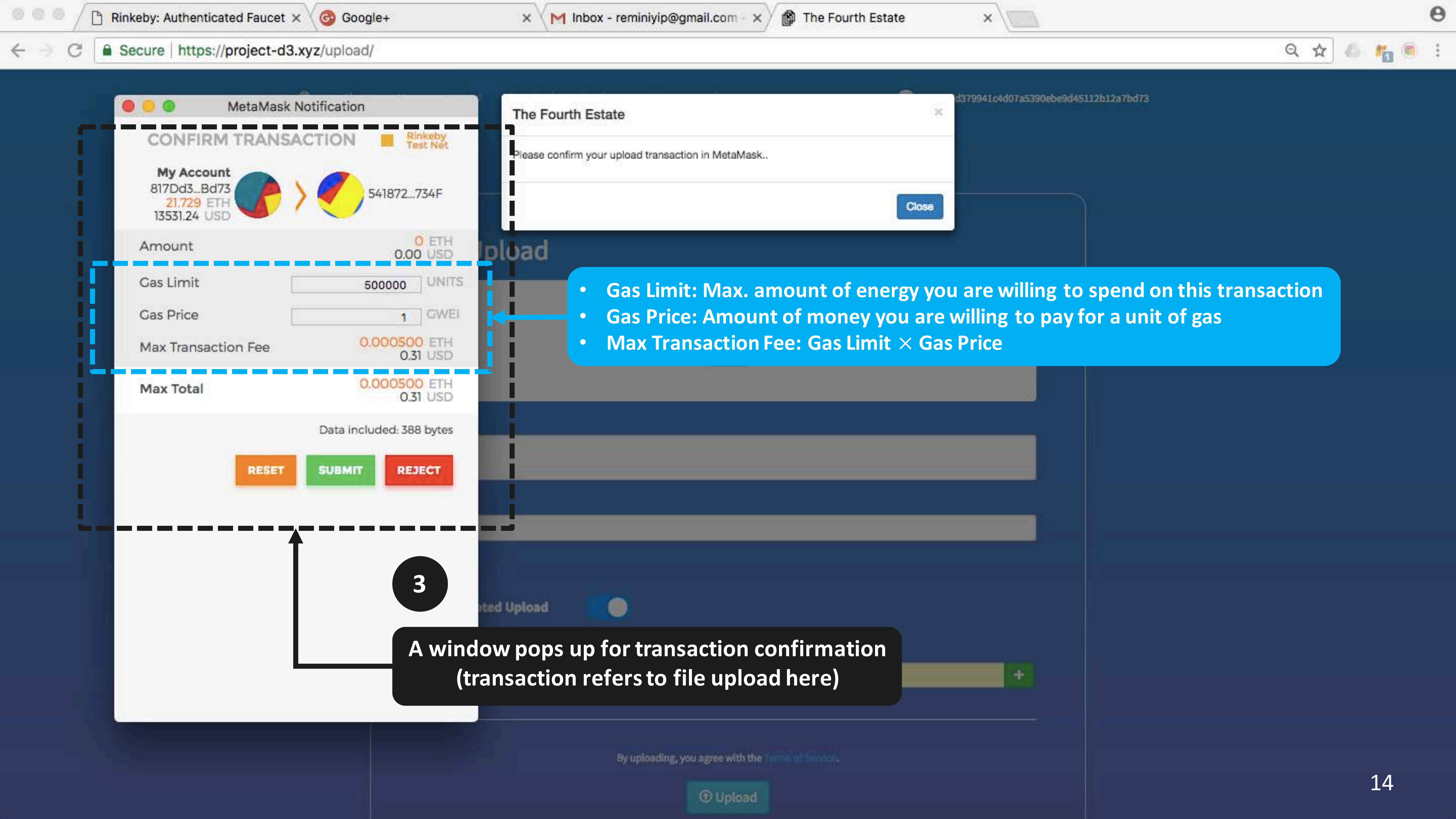
Description: (Optional)

Your email: (Optional)

Encrypted Upload

Recipients: reminiyip@gmail.com

By uploading, you agree with the Terms of Service.


Rinkeby: Authenticated Faucet
Google+
Inbox - reminiyip@gmail.com
The Fourth Estate
Secure
https://project-d3.xyz/upload/
d379941c4d07a5390ebe9d45112b12a7bd73
Upload
Close
RESET
SUBMIT
REJECT
3
Upload

MetaMask Notification

CONFIRM TRANSACTION

Rinkeby Test Net

My Account
817Dd3...Bd73
21.729 ETH
13531.24 USD

541872...734F

Amount	0 ETH 0.00 USD
Gas Limit	500000 UNITS
Gas Price	1 GWEI
Max Transaction Fee	0.000500 ETH 0.31 USD
Max Total	0.000500 ETH 0.31 USD

Data included: 388 bytes

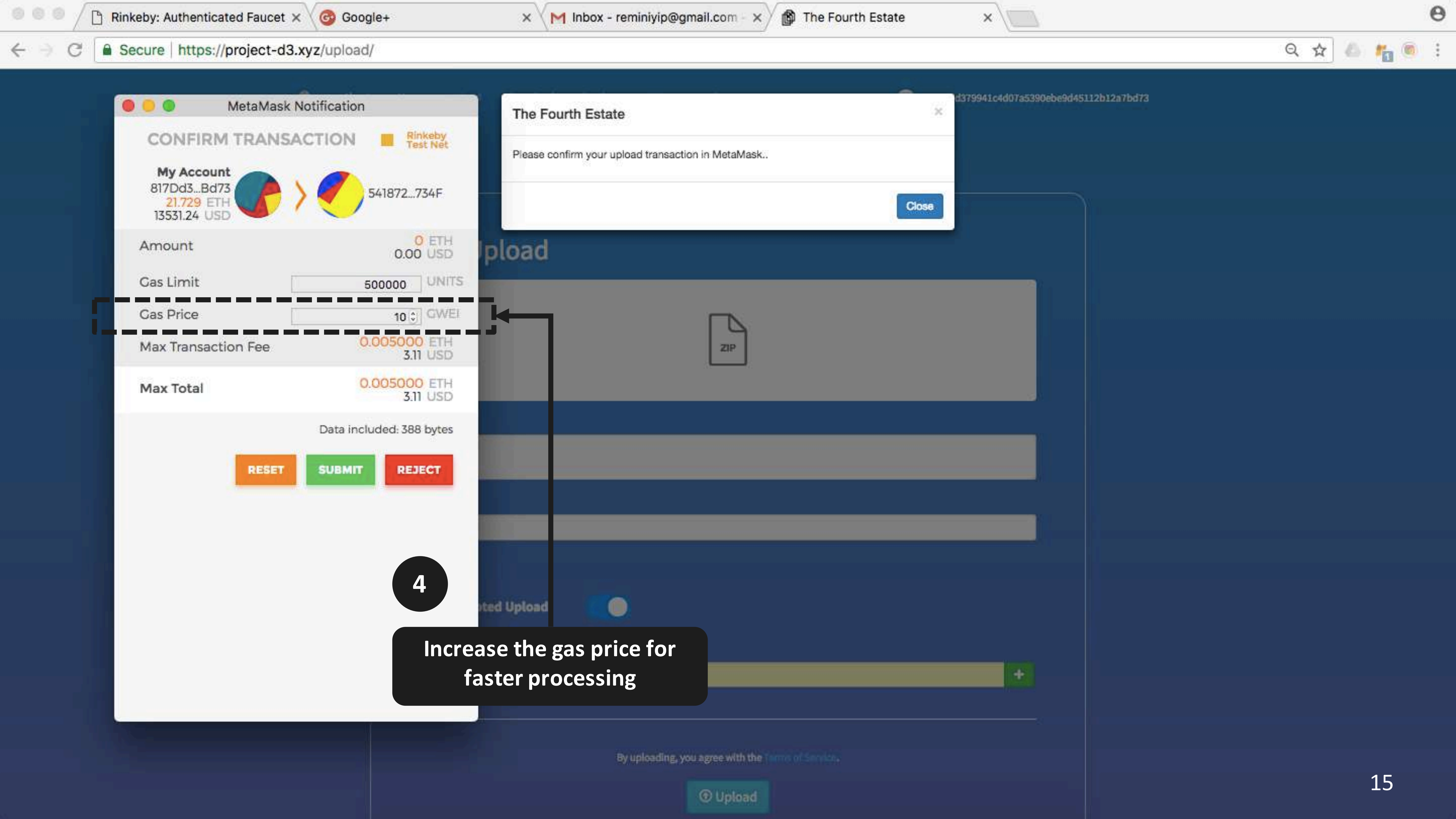
The Fourth Estate

Please confirm your upload transaction in MetaMask..

- Gas Limit: Max. amount of energy you are willing to spend on this transaction
- Gas Price: Amount of money you are willing to pay for a unit of gas
- Max Transaction Fee: Gas Limit × Gas Price

A window pops up for transaction confirmation (transaction refers to file upload here)

By uploading, you agree with the Terms of Service.


Rinkeby: Authenticated Faucet
Google+
Inbox - reminiyip@gmail.com
The Fourth Estate
Secure
https://project-d3.xyz/upload/
d379941c4d07a5390ebe9d45112b12a7bd73
Upload
ZIP
ted Upload
+
Upload

MetaMask Notification

CONFIRM TRANSACTION

Rinkeby Test Net

My Account
817Dd3...Bd73
21.729 ETH
13531.24 USD

541872...734F

Amount 0 ETH 0.00 USD

Gas Limit 500000 UNITS

Gas Price 10 GWEI

Max Transaction Fee 0.005000 ETH 3.11 USD

Max Total 0.005000 ETH 3.11 USD

Data included: 388 bytes

RESET SUBMIT REJECT

The Fourth Estate

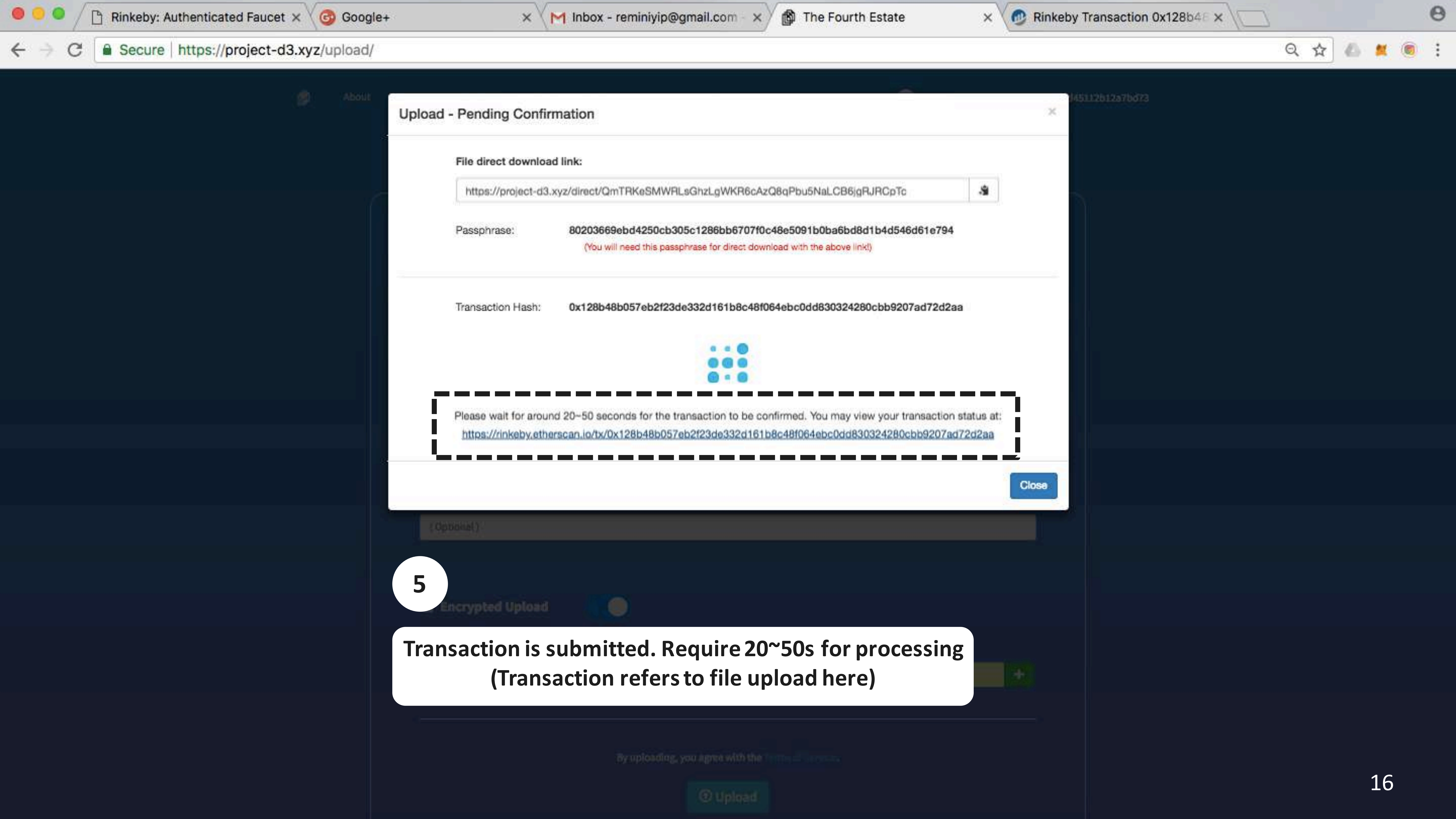
Please confirm your upload transaction in MetaMask..

Close

By uploading, you agree with the Terms of Service.

4

Increase the gas price for faster processing


Rinkeby: Authenticated Faucet
Google+
Inbox - reminiyip@gmail.com
The Fourth Estate
Rinkeby Transaction 0x128b4
Secure
https://project-d3.xyz/upload/
About
Encrypted Upload
(Optional)
By uploading, you agree with the Terms of Service.
Upload
Close

Upload - Pending Confirmation

File direct download link:

https://project-d3.xyz/direct/QmTRKeSMWRLsGhzLgWKR6cAzQ8qPbu5NaLCB6jgRJRCpTc

Passphrase: **80203669ebd4250cb305c1286bb6707f0c48e5091b0ba6bd8d1b4d546d61e794**

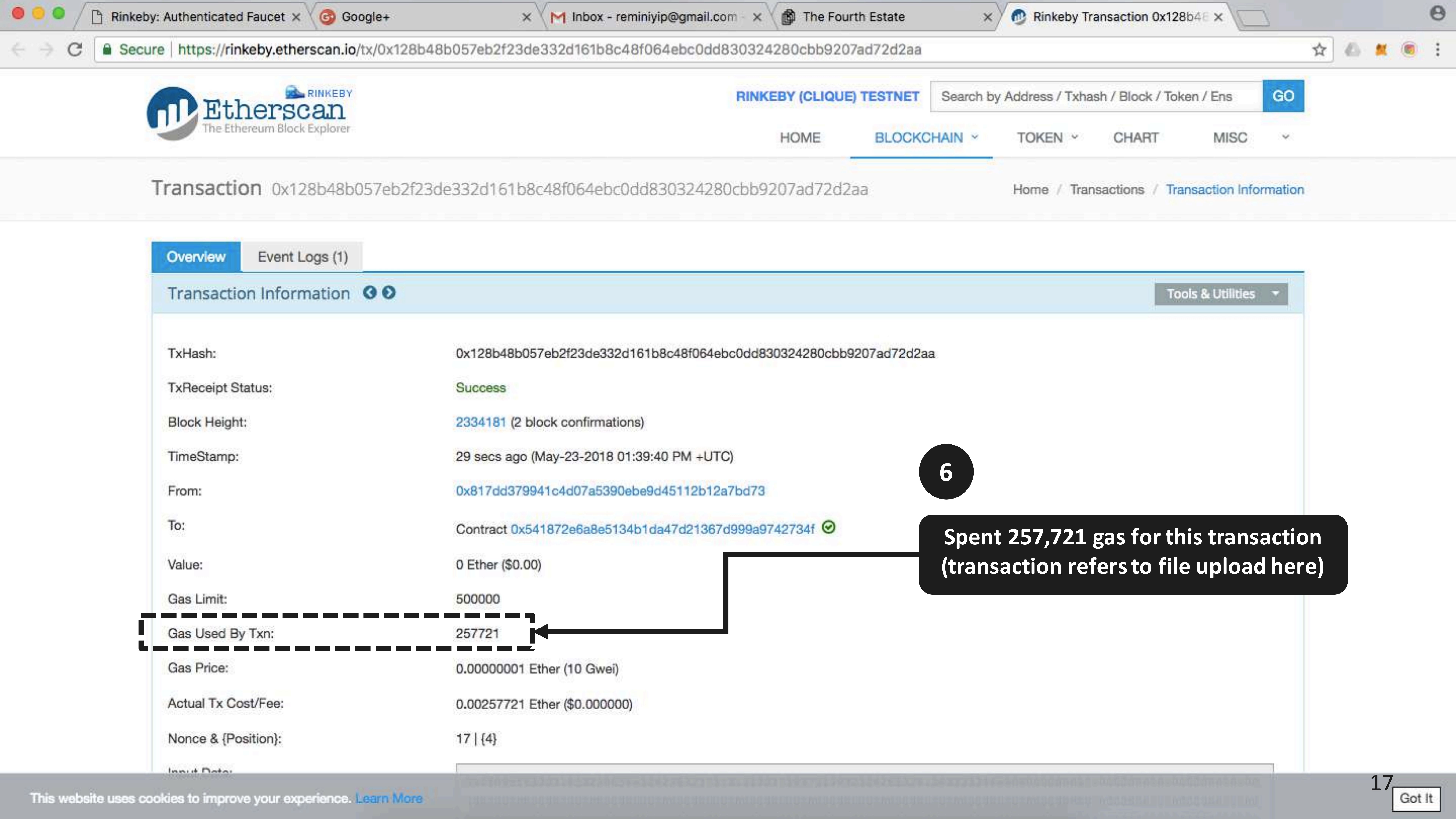
(You will need this passphrase for direct download with the above link!)

Transaction Hash: **0x128b48b057eb2f23de332d161b8c48f064ebc0dd830324280cbb9207ad72d2aa**

Please wait for around 20~50 seconds for the transaction to be confirmed. You may view your transaction status at:
https://rinkeby.etherscan.io/tx/0x128b48b057eb2f23de332d161b8c48f064ebc0dd830324280cbb9207ad72d2aa

5

Transaction is submitted. Require 20~50s for processing
(Transaction refers to file upload here)


Rinkeby: Authenticated Faucet
Google+
Inbox - reminiyip@gmail.com
The Fourth Estate
Rinkeby Transaction 0x128b4
Secure
https://rinkeby.etherscan.io/tx/0x128b48b057eb2f23de332d161b8c48f064ebc0dd830324280cbb9207ad72d2aa
RINKEBY
Etherscan
The Ethereum Block Explorer
RINKEBY (CLIQUE) TESTNET
Search by Address / Txhash / Block / Token / Ens
GO
HOME
BLOCKCHAIN
TOKEN
CHART
MISC
Home / Transactions / Transaction Information
Overview
Event Logs (1)
Tools & Utilities

Transaction 0x128b48b057eb2f23de332d161b8c48f064ebc0dd830324280cbb9207ad72d2aa

Transaction Information

TxHash: 0x128b48b057eb2f23de332d161b8c48f064ebc0dd830324280cbb9207ad72d2aa

TxReceipt Status: Success

Block Height: 2334181 (2 block confirmations)

TimeStamp: 29 secs ago (May-23-2018 01:39:40 PM +UTC)

From: 0x817dd379941c4d07a5390ebe9d45112b12a7bd73

To: Contract 0x541872e6a8e5134b1da47d21367d999a9742734f ✓

Value: 0 Ether ($0.00)

Gas Limit: 500000

Gas Used By Txn: 257721

Gas Price: 0.00000001 Ether (10 Gwei)

Actual Tx Cost/Fee: 0.00257721 Ether ($0.000000)

Nonce & {Position}: 17 | {4}

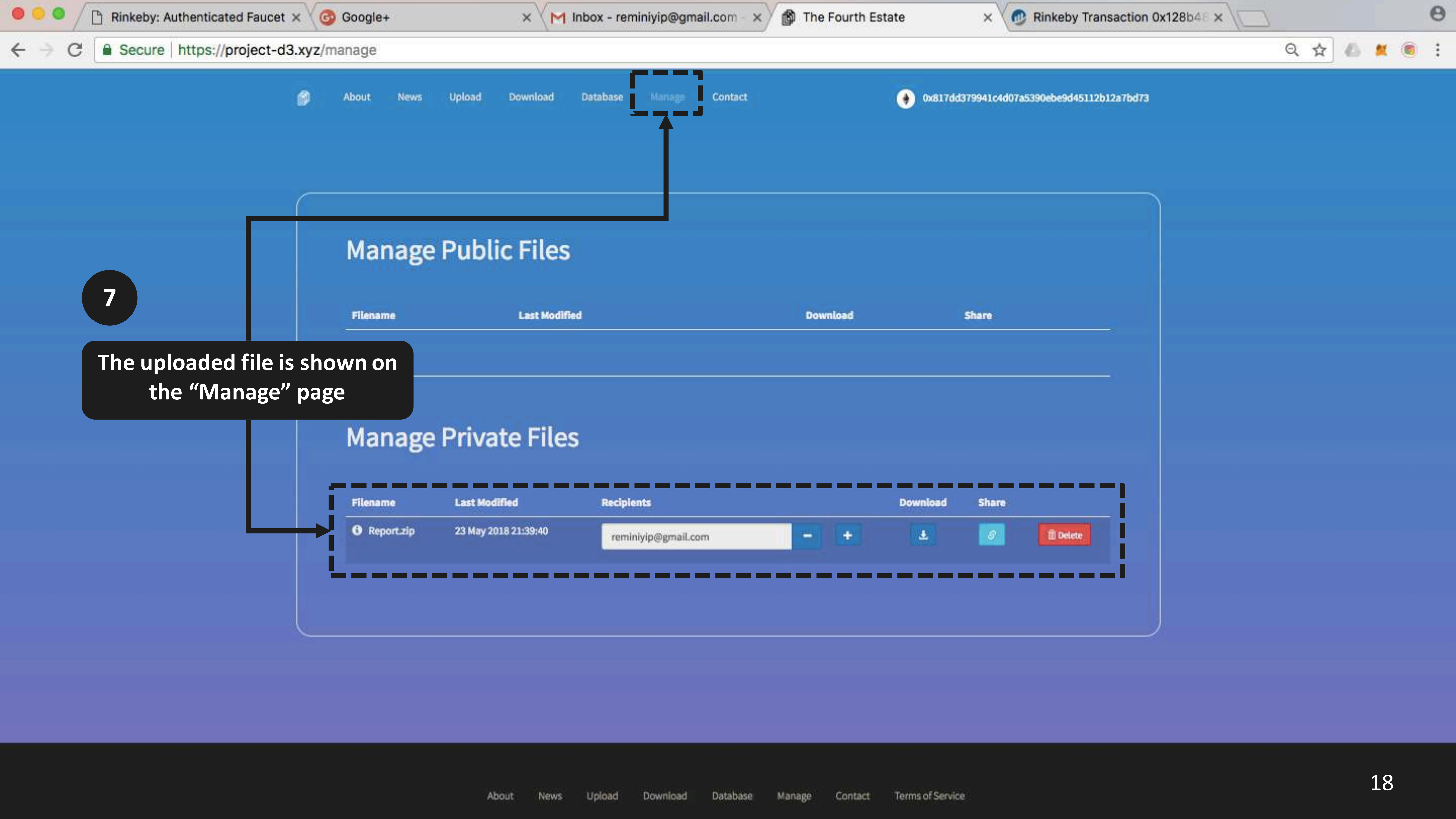
Input Data:

This website uses cookies to improve your experience. Learn More

Got It

6

Spent 257,721 gas for this transaction (transaction refers to file upload here)


Rinkeby: Authenticated Faucet
Google+
Inbox - reminiyip@gmail.com
The Fourth Estate
Rinkeby Transaction 0x128b4
Secure
https://project-d3.xyz/manage
About
News
Upload
Download
Database
Manage
Contact
0x817dd379941c4d07a5390ebe9d45112b12a7bd73

7

The uploaded file is shown on the “Manage” page

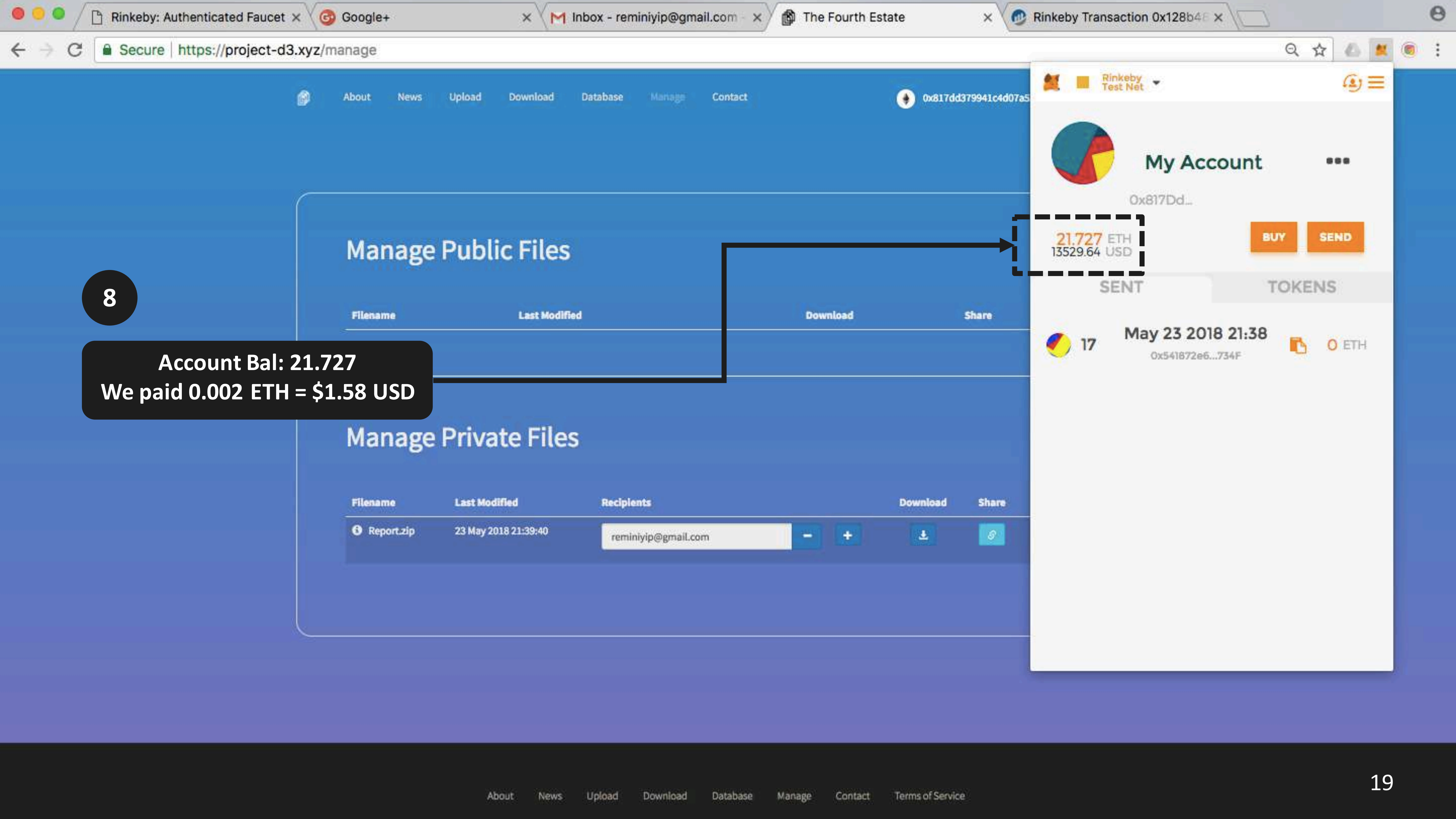
Manage Public Files

Filename	Last Modified	Download	Share

Manage Private Files

Filename	Last Modified	Recipients			Download	Share	
Report.zip	23 May 2018 21:39:40	reminiyip@gmail.com	−	+			Delete

About
News
Upload
Download
Database
Manage
Contact
Terms of Service



21.727 ETH
13529.64 USD

17 May 23 2018 21:38 0x541872e6...734F 0 ETH

Manage Public Files

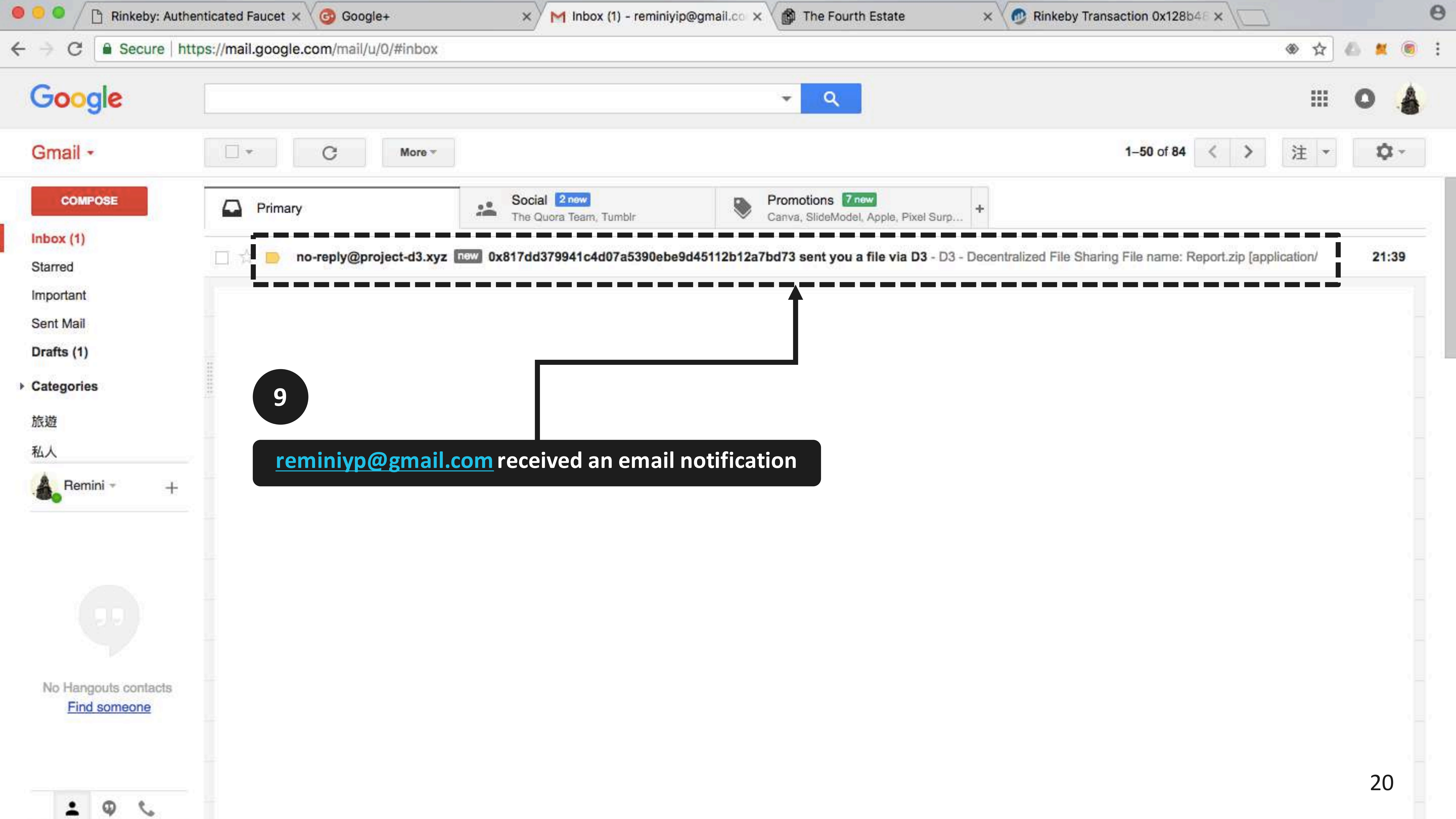
Filename	Last Modified	Download	Share

Manage Private Files

Filename	Last Modified	Recipients	Download	Share
Report.zip	23 May 2018 21:39:40	reminiyip@gmail.com		

8

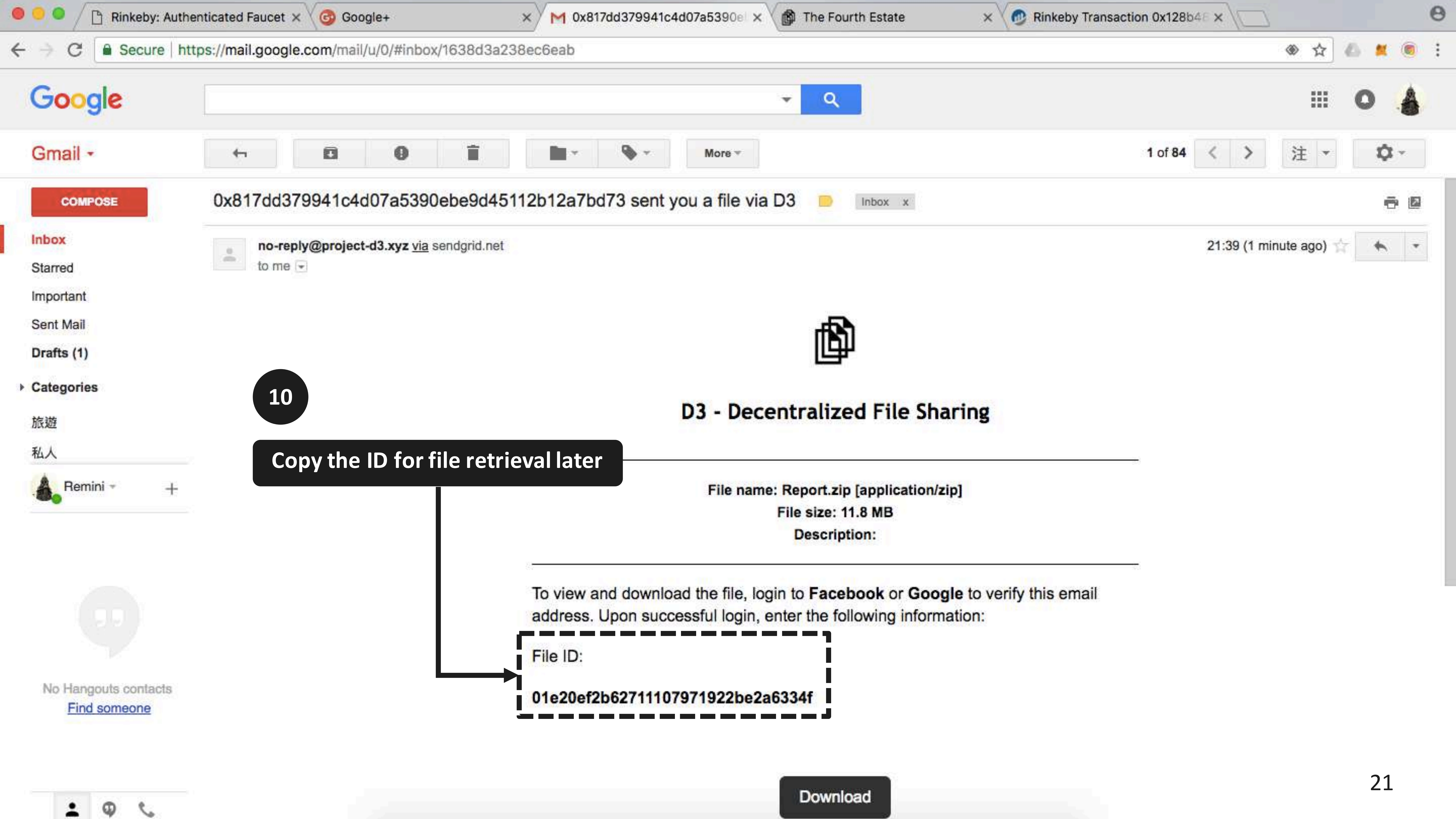
Account Bal: 21.727
We paid 0.002 ETH = $1.58 USD



no-reply@project-d3.xyz new 0x817dd379941c4d07a5390ebe9d45112b12a7bd73 sent you a file via D3 - D3 - Decentralized File Sharing File name: Report.zip [application/ 21:39

9

reminiyp@gmail.com received an email notification



0x817dd379941c4d07a5390ebe9d45112b12a7bd73 sent you a file via D3

no-reply@project-d3.xyz via sendgrid.net
to me

21:39 (1 minute ago)

D3 - Decentralized File Sharing

File name: Report.zip [application/zip]
File size: 11.8 MB
Description:

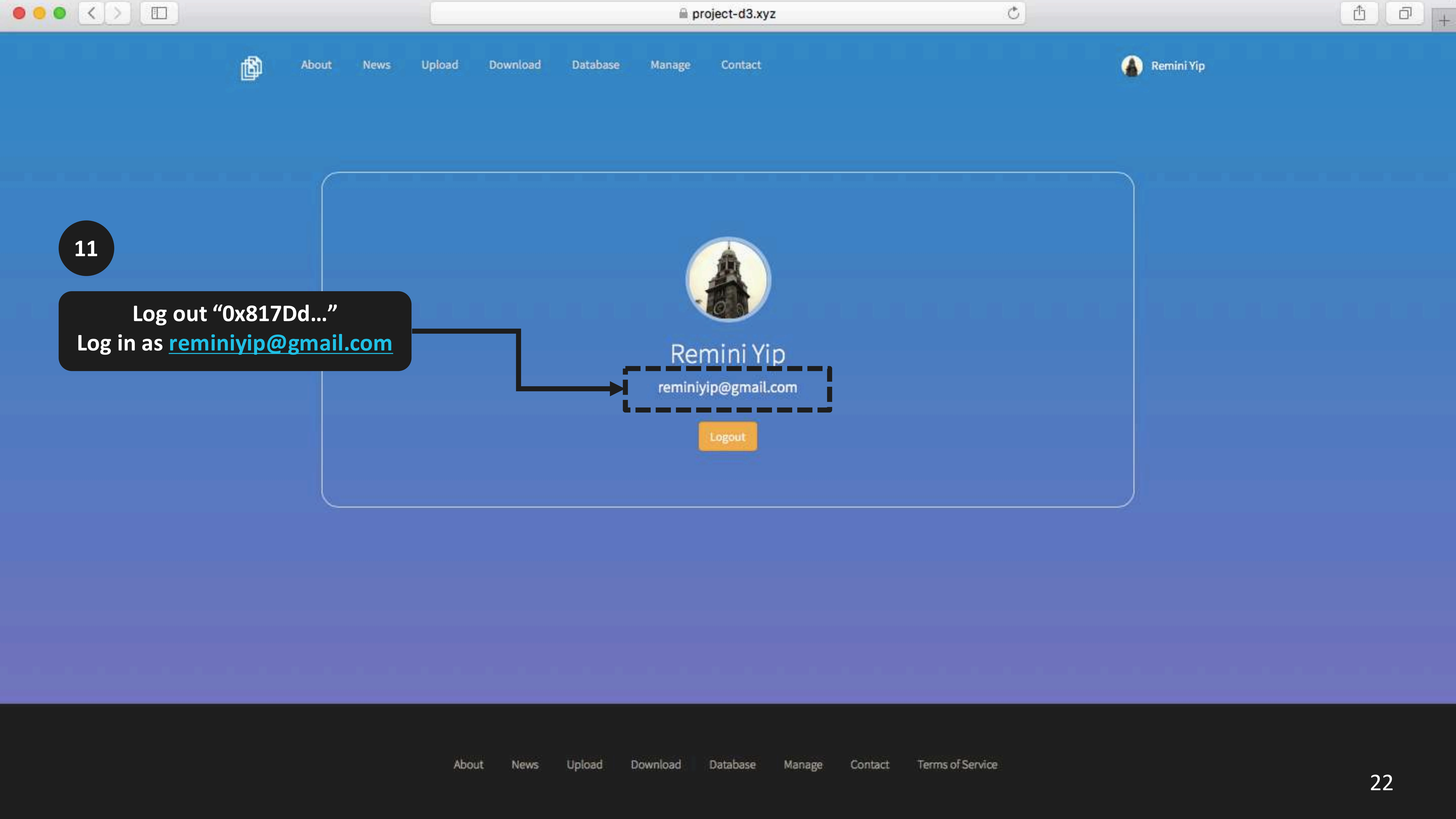
To view and download the file, login to **Facebook** or **Google** to verify this email address. Upon successful login, enter the following information:

File ID:

01e20ef2b62711107971922be2a6334f

10

Copy the ID for file retrieval later

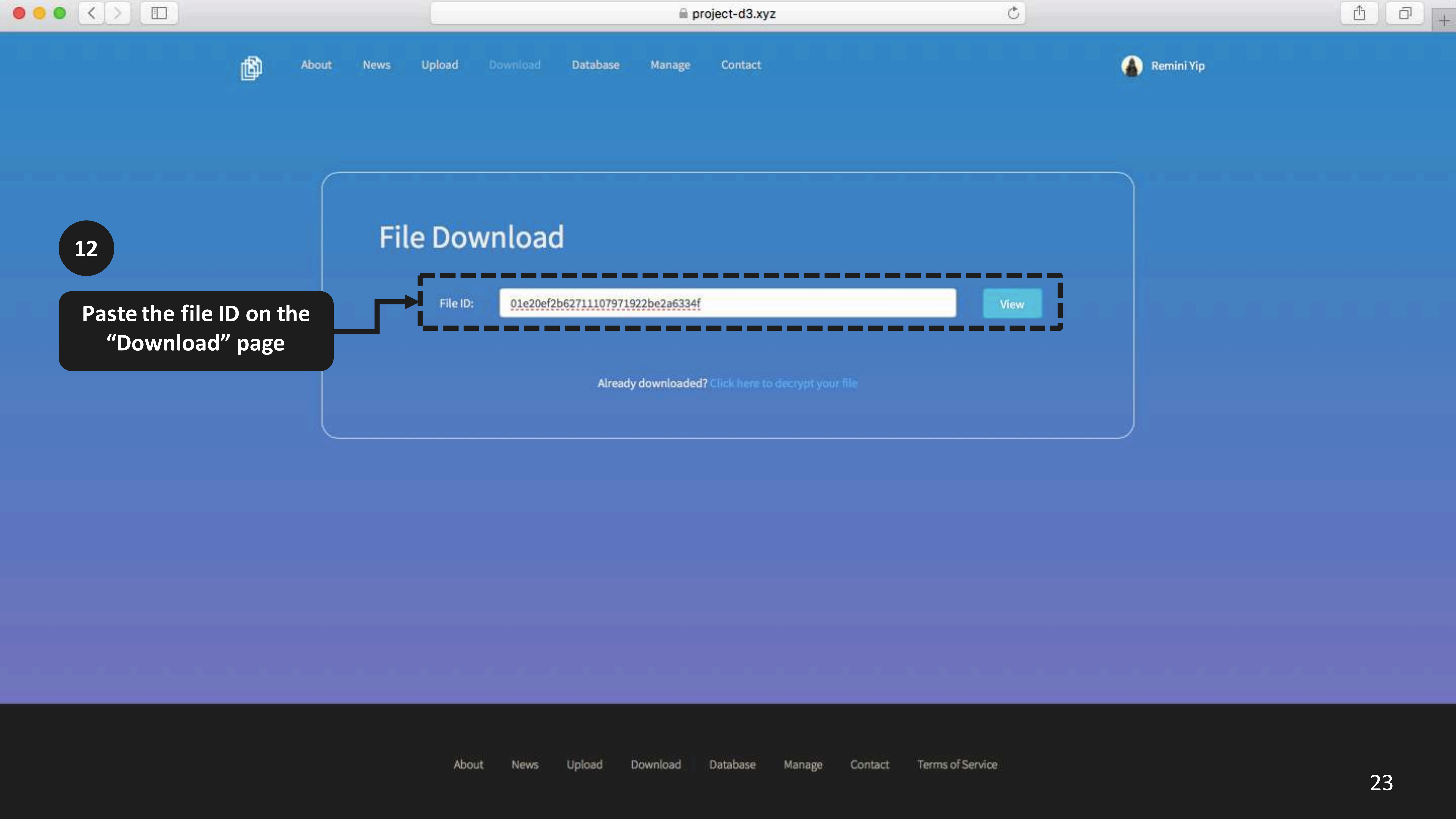


Remini Yip

reminiyip@gmail.com

11

Log out “0x817Dd…”
Log in as reminiyip@gmail.com



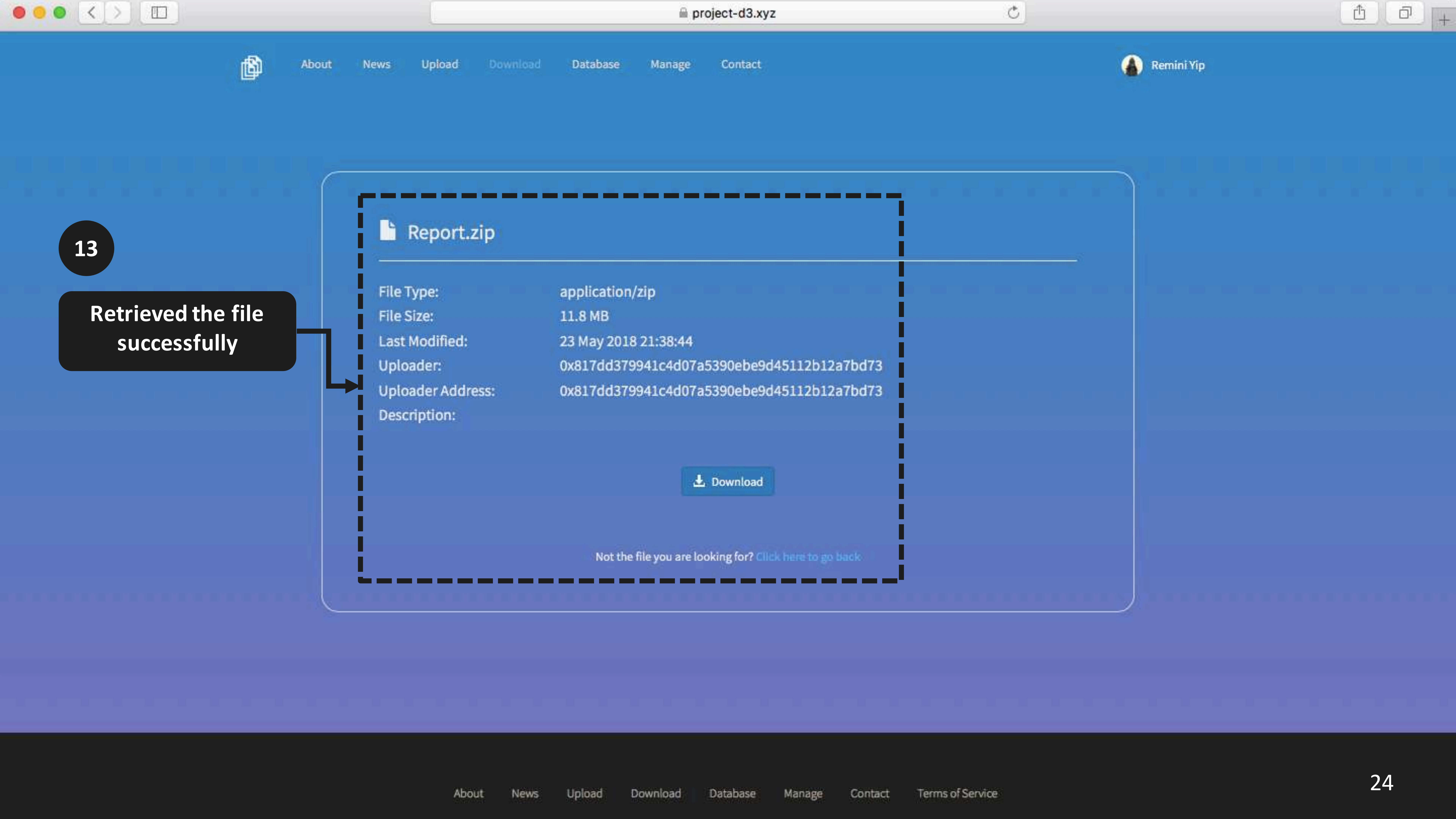
File Download

File ID: 01e20ef2b62711107971922be2a6334f

Already downloaded? Click here to decrypt your file

12

Paste the file ID on the "Download" page



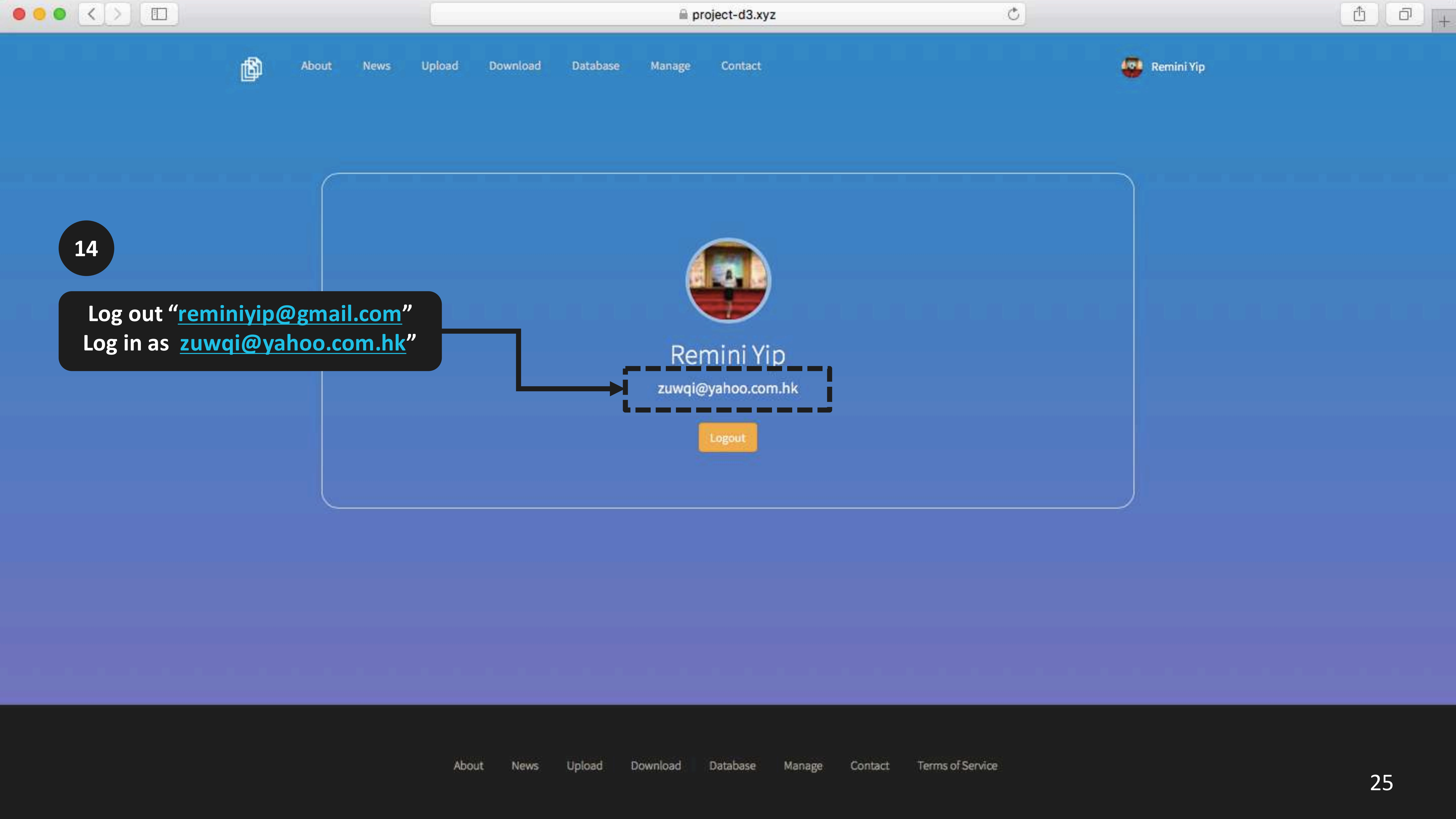
Report.zip

File Type:	application/zip
File Size:	11.8 MB
Last Modified:	23 May 2018 21:38:44
Uploader:	0x817dd379941c4d07a5390ebe9d45112b12a7bd73
Uploader Address:	0x817dd379941c4d07a5390ebe9d45112b12a7bd73
Description:	

Not the file you are looking for? Click here to go back

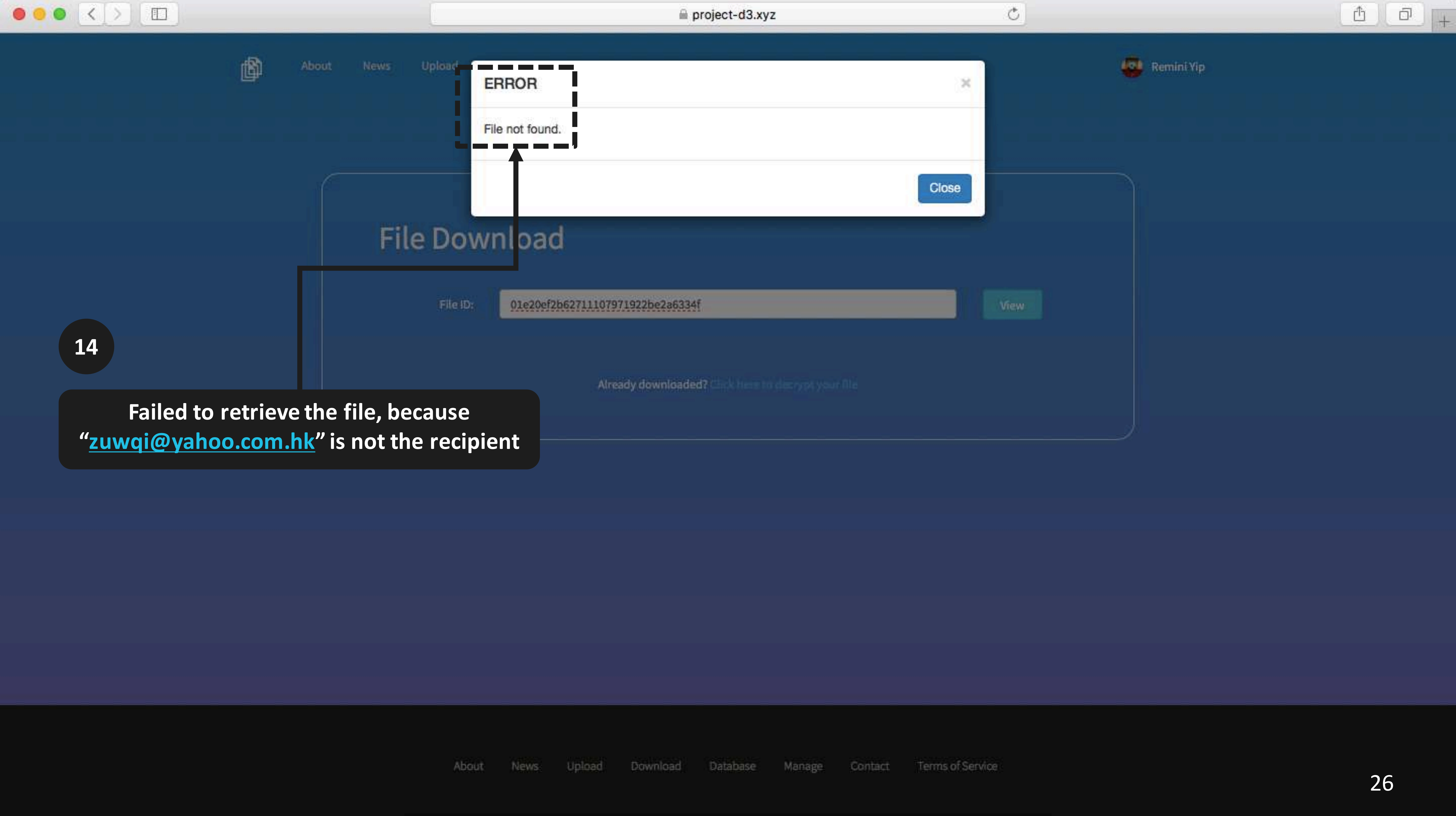
13

Retrieved the file successfully



14

Log out “reminiyip@gmail.com”
Log in as zuwqi@yahoo.com.hk”



ERROR

File not found.

File Download

File ID: 01e20ef2b62711107971922be2a6334f

Already downloaded? Click here to decrypt your file

14

Failed to retrieve the file, because “zuwqi@yahoo.com.hk” is not the recipient

Cost Evaluation

Action	Gas Consumption (May 21, 2018)	Transaction Cost in USD (May 21, 2018)
Add a file with 0 recipient	257,785	$1.82515
Remove a file with 0 recipient	44,900	$0.31789
Add a recipient	76,749	$0.54399
Remove a recipient	69,692	$0.49341
Set visibility, e.g. public → private	34,995	$0.2478

Based on ETH Gas Station with the following settings,

- Shamir Secret Sharing splits the hash (file location) into 5 pieces, that is n = 5
- Gas price is 10 gwei

Conclusion

	Fourth Estate	Publishing Sites/Blogs, e.g. Sina, Medium, etc.	Personal Sites
Zero downtime, e.g. defend DDoS Attack	✓	✗	✗
Preserve content integrity, e.g. NOT modified by hackers	✓	✗	✗
Censorship Free, e.g. NOT removed by site owners	✓	✗	✓
Support Access Control, e.g. private sharing	✓	✓	Depends on how you built it

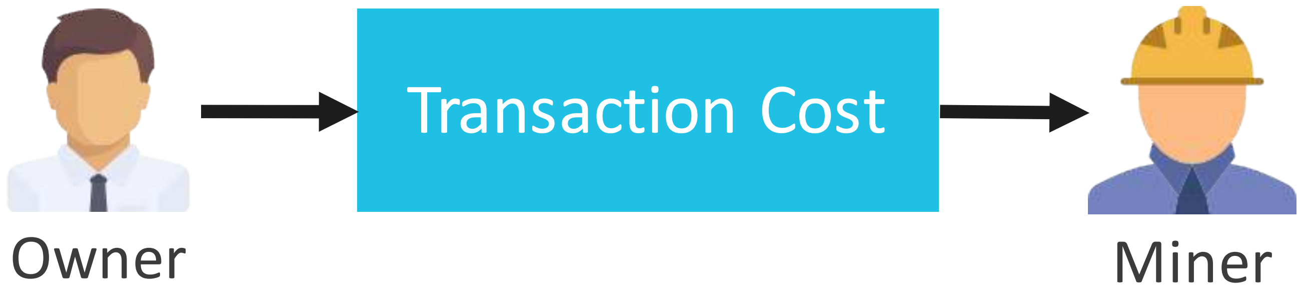
There are also technical advantages offered by the underlying IPFS architecture, e.g. de-duplication, caching etc.

Thank you!

Appendix 1 – Business Model

Non Profit Business Model (Current)

- We don't earn any revenues
- File upload/change of access incurs transaction cost
- Transaction cost's payer: Owner
- Transaction cost's payee: Ethereum miner



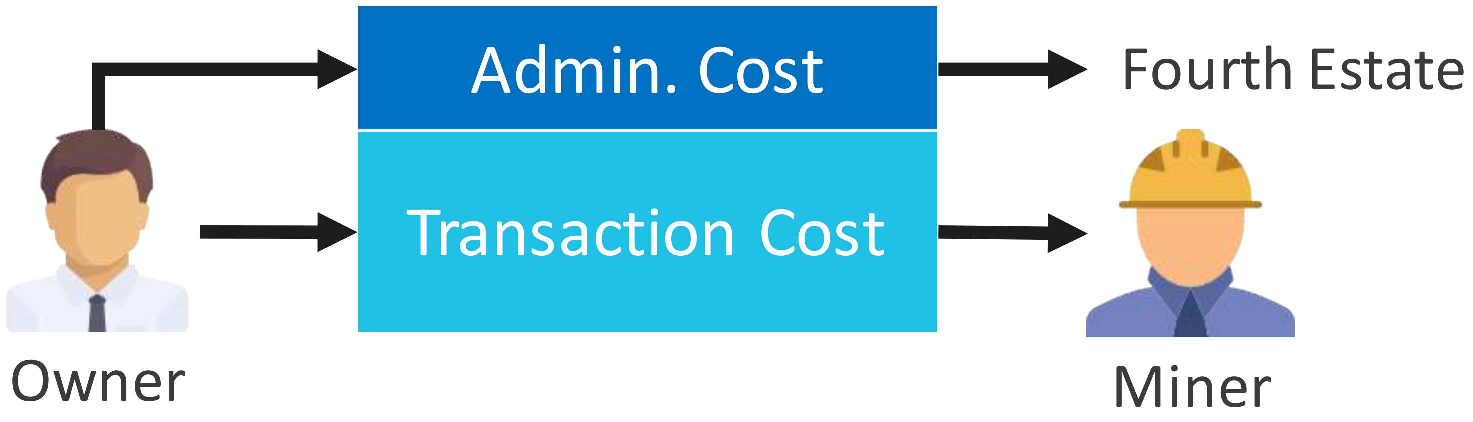
Owner

Transaction Cost

Miner

Profit Business Model

- We charge administration cost per transaction
- Admin. cost's payer: Owner
- Admin. cost's payee: Fourth Estate



Admin. Cost

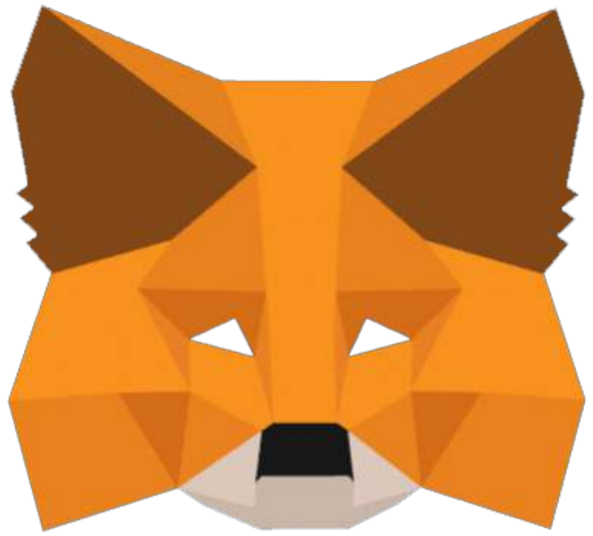
Fourth Estate

Owner

Transaction Cost

Miner

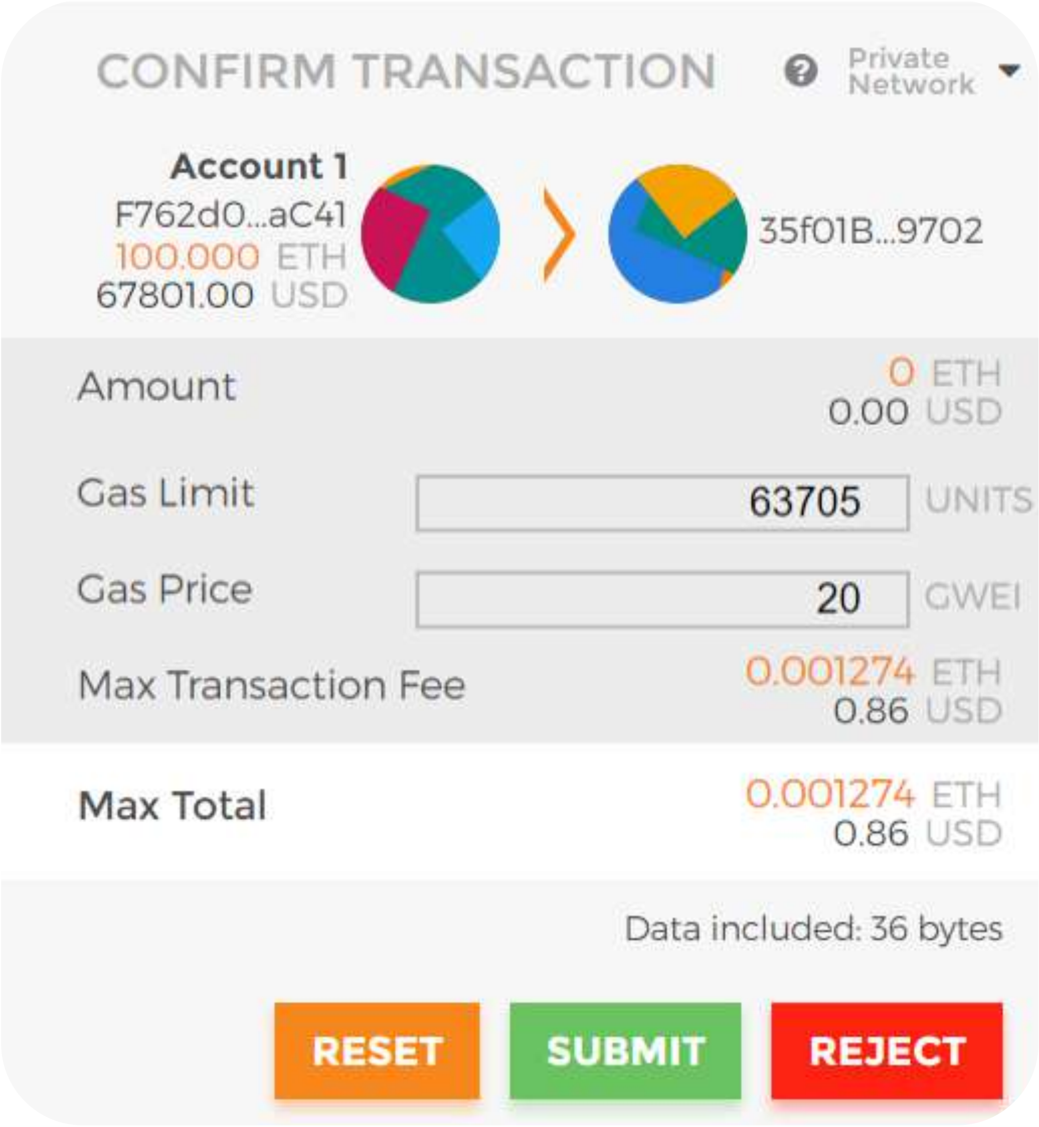
Appendix 2 – More Key Terms



MetaMask

- Chrome's plugin
- Provide wallet management, e.g. check your upload cost
- Connect you to the Ethereum network

  (so you don't need to run an Ethereum node on your PC)



CONFIRM TRANSACTION

Private Network

Account 1
F762d0...aC41
100.000 ETH
67801.00 USD

35f01B...9702

Amount: 0 ETH, 0.00 USD

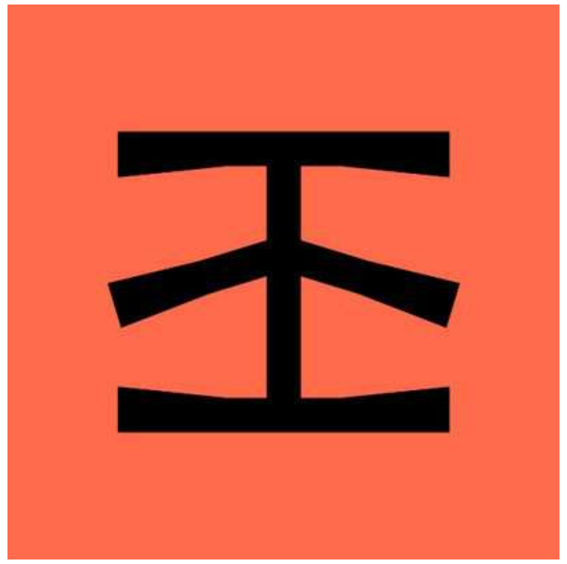
Gas Limit: 63705 UNITS

Gas Price: 20 GWEI

Max Transaction Fee: 0.001274 ETH, 0.86 USD

Max Total: 0.001274 ETH, 0.86 USD

Data included: 36 bytes



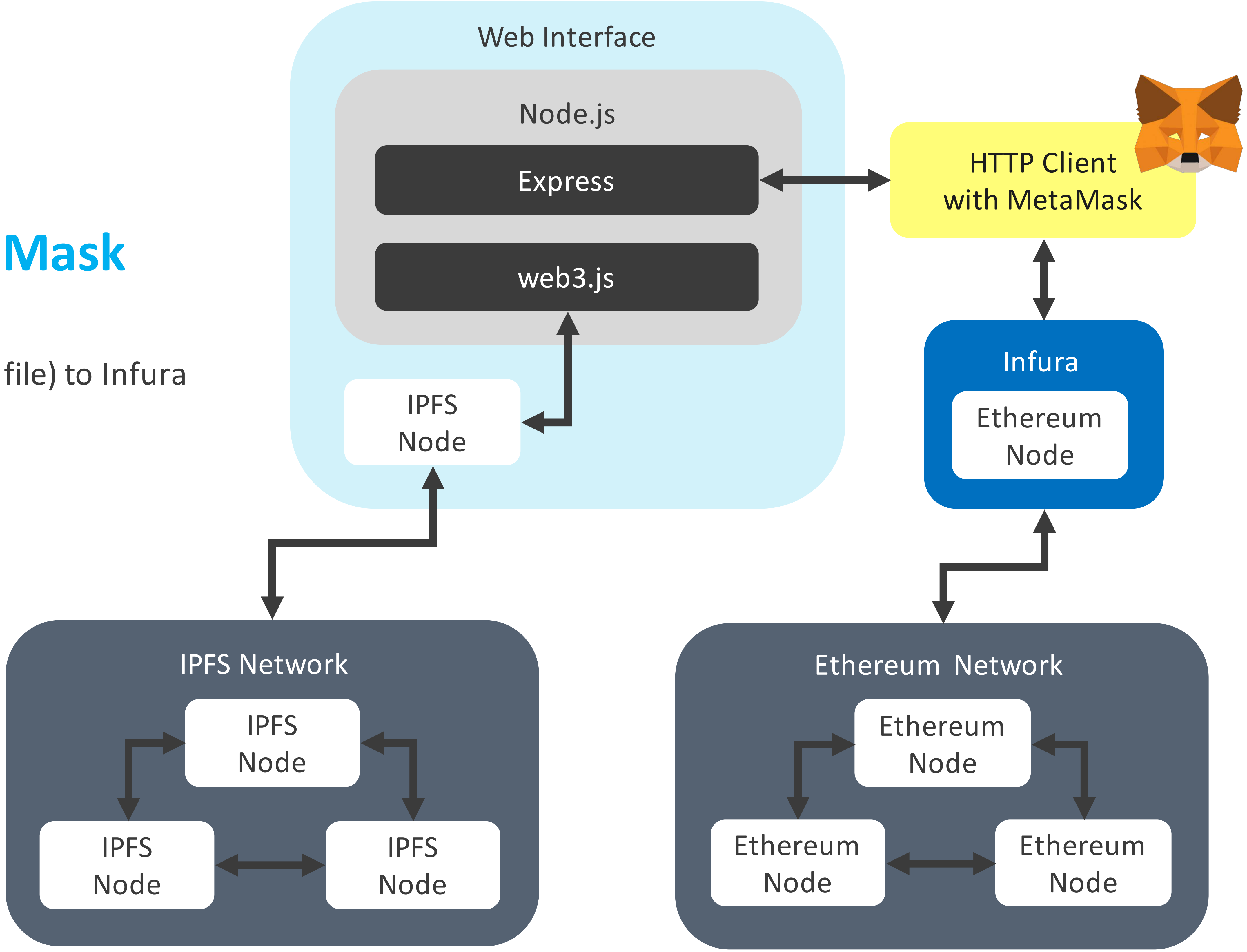
Infura

- Gateway to the Ethereum network
- Run Ethereum nodes for public use
- MetaMask routes your transaction to these public Ethereum nodes

Appendix 3 – Infrastructure

Case 1: HTTP Client with MetaMask

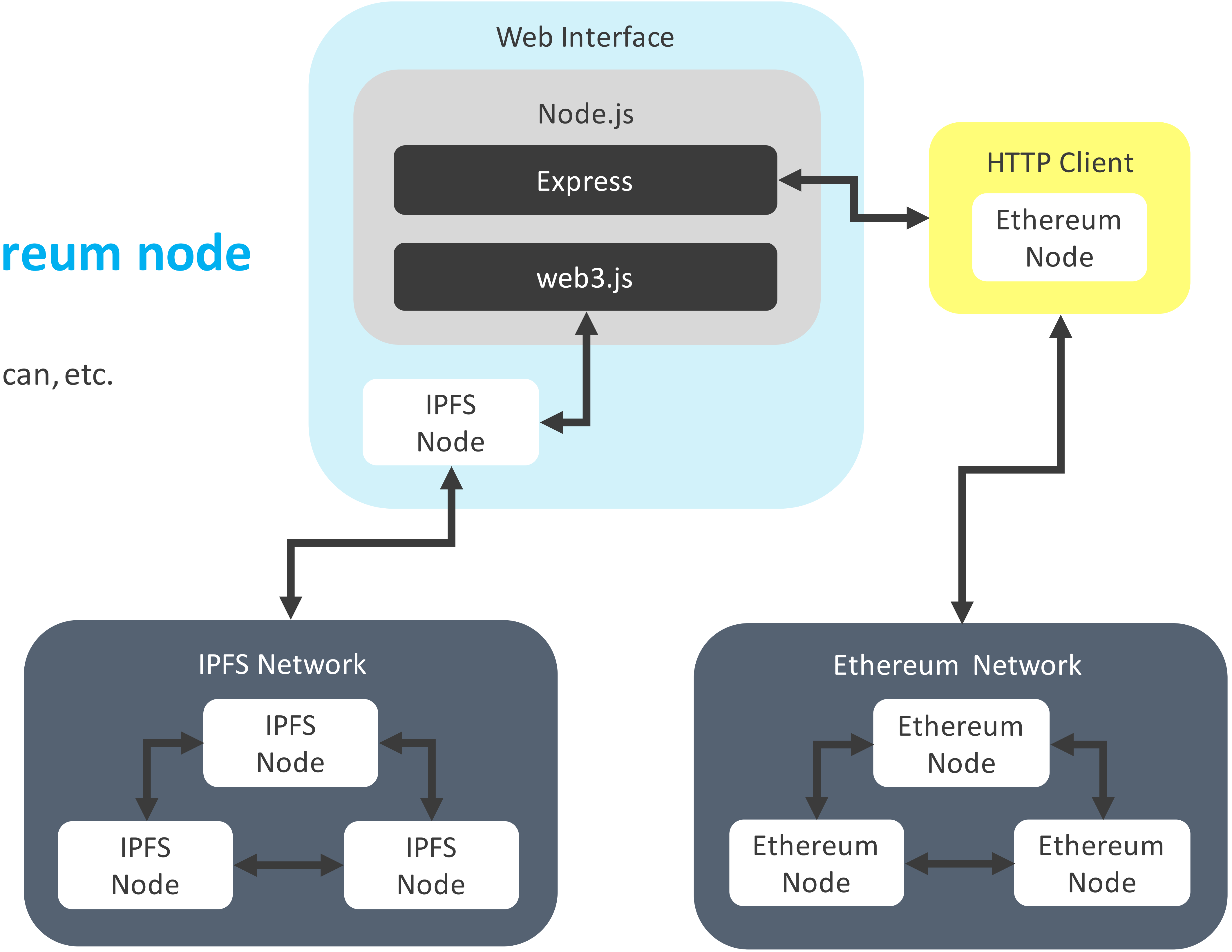
- Client doesn’t run an Ethereum node on his PC
- MetaMask routes his transaction (e.g. adding a file) to Infura
- Client can confirm the cost via MetaMask



Appendix 3 – Infrastructure (Cont.)

Case 2: HTTP Client with Ethereum node

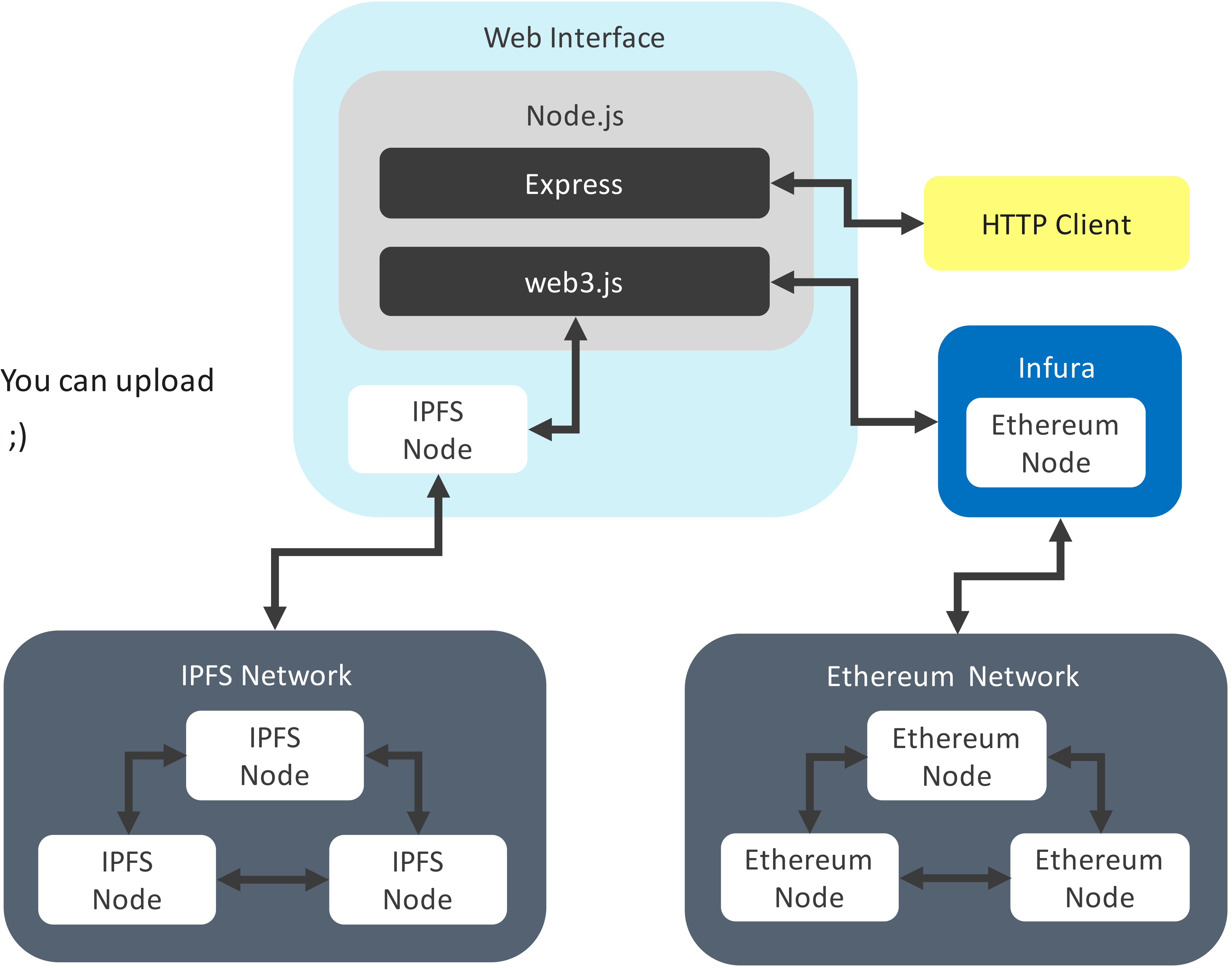
- Client runs an Ethereum node on his PC
- Client can confirm the cost via console, etherscan, etc.



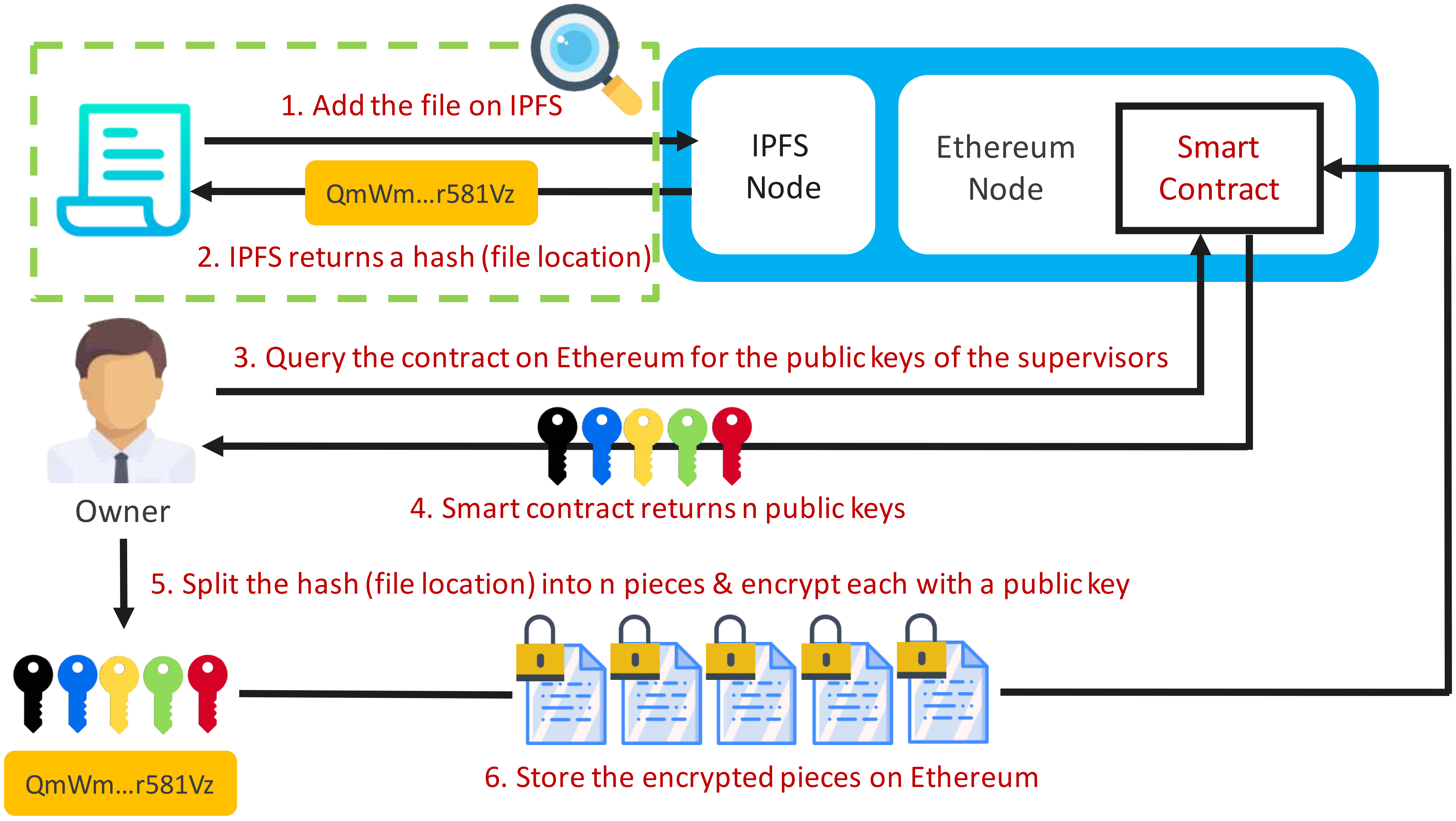
Appendix 3 – Infrastructure (Cont.)

Case 3: HTTP Client

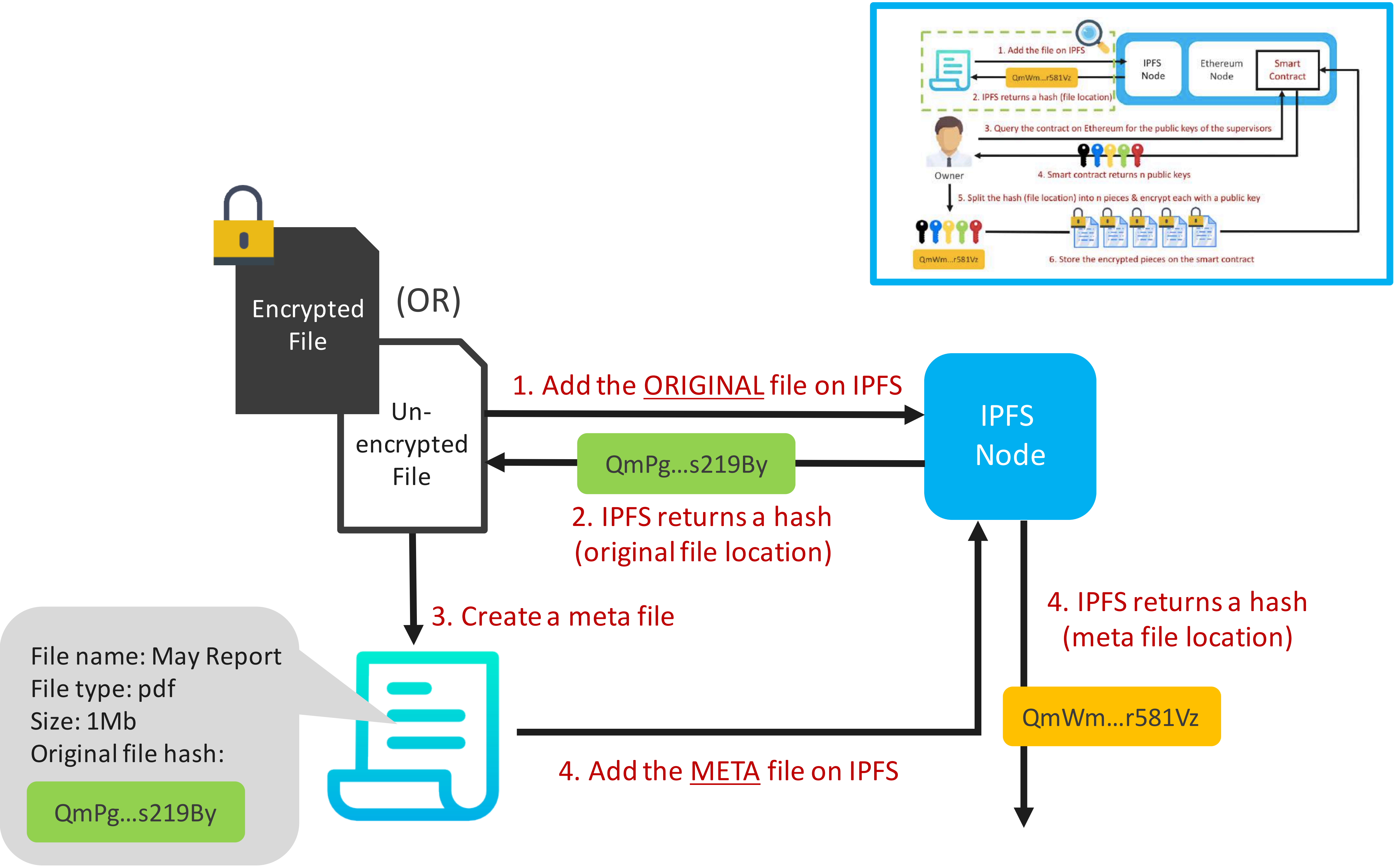
- FOR DEMONSTRATION PURPOSE ONLY
- We hardcoded our wallet key in the prototype. You can upload files and control access for free. We pay for you ;)



Appendix 4 – Storage Details


1. Add the file on IPFS
QmWm...r581Vz
2. IPFS returns a hash (file location)
IPFS Node
Ethereum Node
Smart Contract
Owner
3. Query the contract on Ethereum for the public keys of the supervisors
4. Smart contract returns n public keys
5. Split the hash (file location) into n pieces & encrypt each with a public key
QmWm...r581Vz
6. Store the encrypted pieces on Ethereum

Appendix 4 – Storage Details (Cont.)


1. Add the file on IPFS
QmWm...r581Vz
2. IPFS returns a hash (file location)
IPFS Node
Ethereum Node
Smart Contract
3. Query the contract on Ethereum for the public keys of the supervisors
4. Smart contract returns n public keys
Owner
5. Split the hash (file location) into n pieces & encrypt each with a public key
QmWm...r581Vz
6. Store the encrypted pieces on the smart contract
Encrypted File
(OR)
Un-encrypted File
1. Add the ORIGINAL file on IPFS
IPFS Node
QmPg...s219By
2. IPFS returns a hash (original file location)
3. Create a meta file
File name: May Report
File type: pdf
Size: 1Mb
Original file hash:
QmPg...s219By
4. IPFS returns a hash (meta file location)
QmWm...r581Vz
4. Add the META file on IPFS