IEEE International Conference on Blockchain and Cryptocurrency
27–31 May 2024 // Dublin, Ireland

Portal: Time-Bound and Replay-Resistant Zero-Knowledge Proofs for Single Sign-On

Jan Lauinger, Serhat Bezmez, Jens Ernstberger, Sebastian Steinhorst

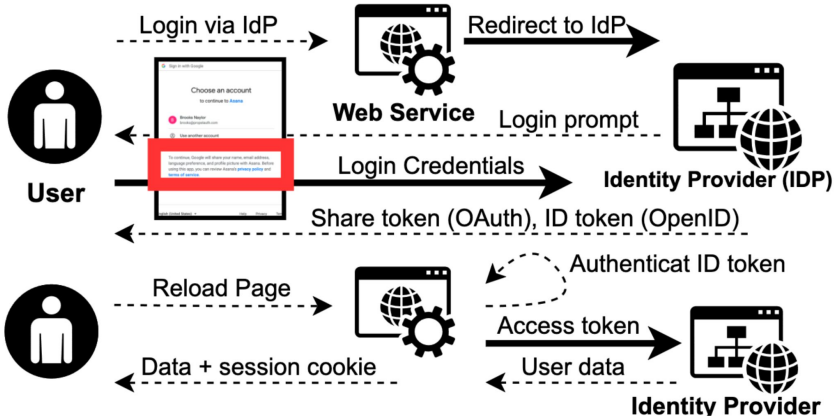
Technical University of Munich

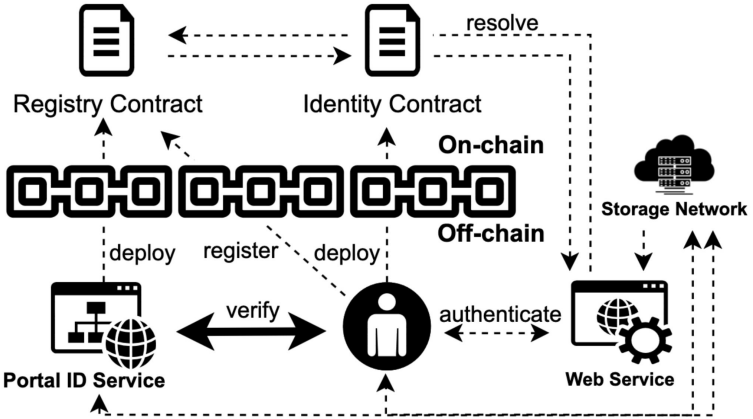
TUM Department of Electrical and Computer Engineering

Associate Professorship of Embedded Systems and Internet of Things

Munich, May 2024

Motivation


Login via IdP
Redirect to IdP
Web Service
Login prompt
User
Login Credentials
Identity Provider (IDP)
Share token (OAuth), ID token (OpenID)
Reload Page
Authenticat ID token
Access token
Data + session cookie
User data
Identity Provider


resolve
Registry Contract
Identity Contract
On-chain
Off-chain
Storage Network
deploy
register
deploy
verify
authenticate
Portal ID Service
Web Service

Problem: Replay attack of transaction payloads

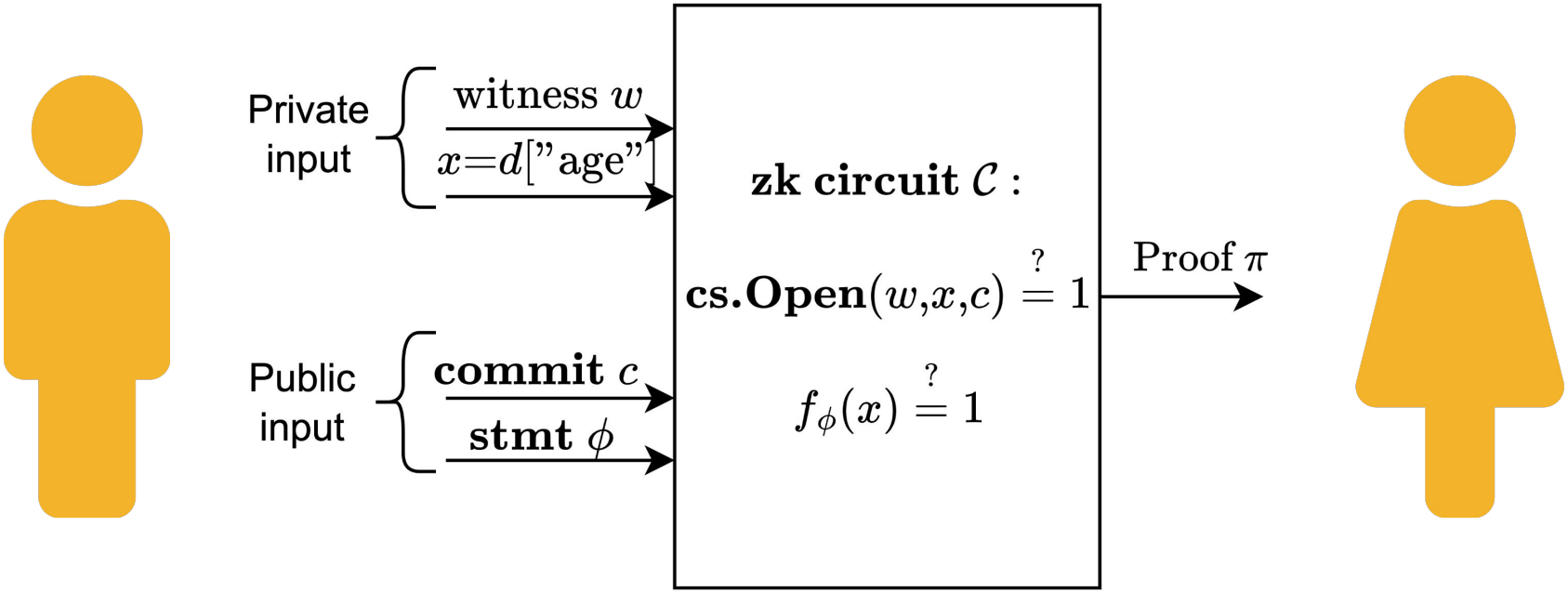
- Public claims
  - Users remain accountable if any misbehaviour is detected
- Private claims
  - **Open issue**, which we solve

Contributions

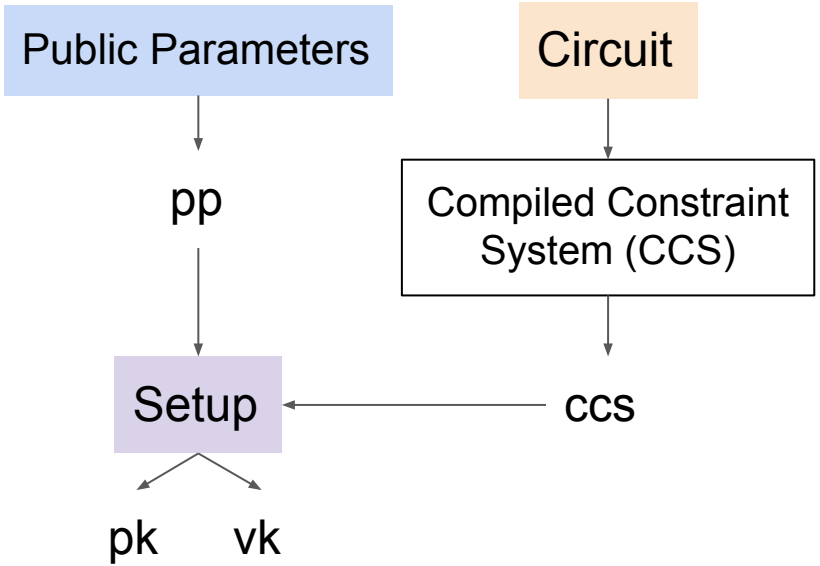
- New transaction sequence which secures on-chain ZKP verifications against replay attacks
- Portal, an alternative SSO solution with enhanced privacy and control
- Open-source[1] the Portal proof of concept and evaluate operation cost

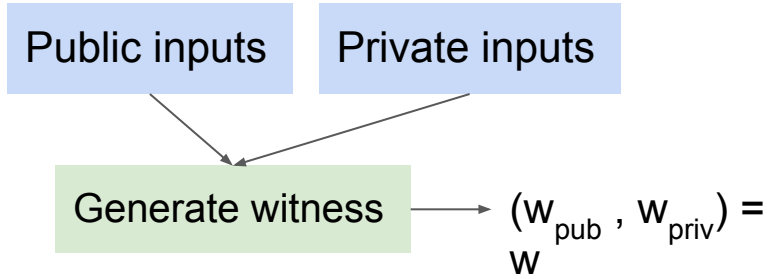
1: https://github.com/jplaui/portal

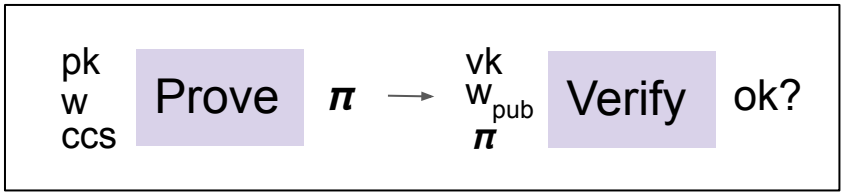
Zero-knowledge Systems



Zero-knowledge Systems







Blockchain Transactions

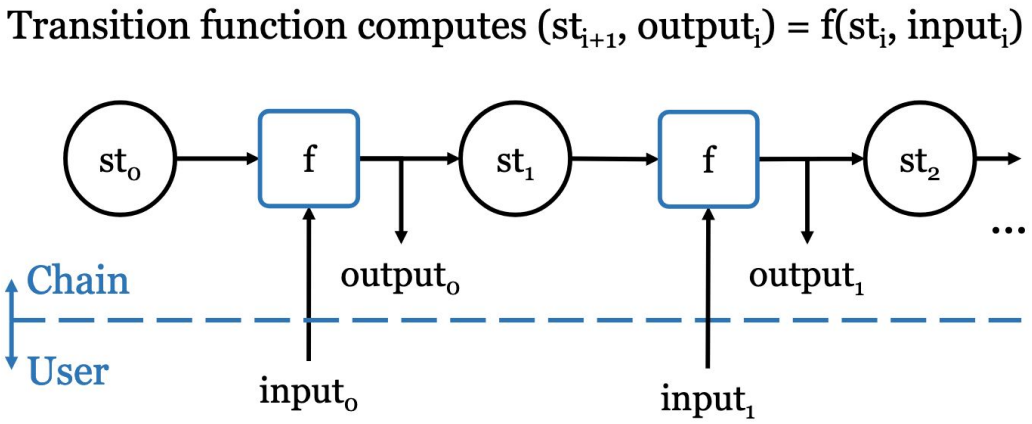
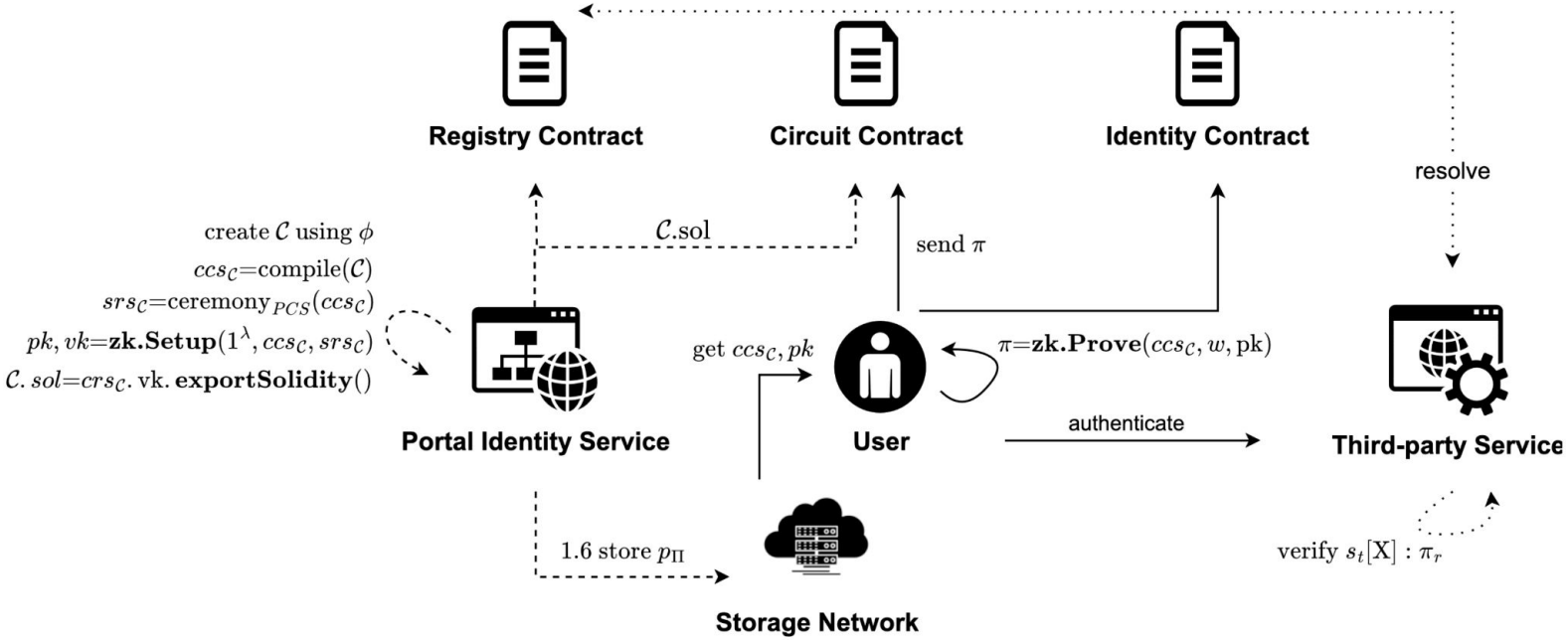


Image from: [Navigating Privacy on Public Blockchains]

SSO Smart Contract Architecture



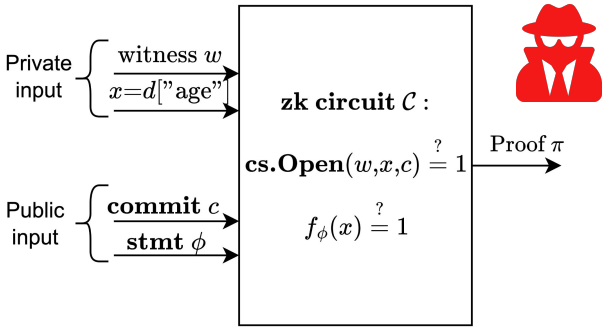
Replay Attack

```
https://api.etherscan.io/api
   ?module=logs
   &action=getLogs
   &fromBlock=15073139
   &toBlock=15074139
   &address=0x59728544b08ab483533076417fbbb2fd0b17ce3a
   &topic0=0x27c4f0403323142b599832f26acd21c74a9e5b809f2215726e244a4ac588cd7d
   &topic0_1_opr=and
   &topic1=0x000000000000000000000000023581767a106ae21c074b2276d25e5c3e136a68b
   &page=1
   &offset=1000
   &apikey=YourApiKeyToken
```


```
{
   "status":"1",
   "message":"OK",
   "result":[
      {
         "address":"0x59728544b08ab483533076417fbbb2fd0b17ce3a",
         "topics":[
            "0x27c4f0403323142b599832f26acd21c74a9e5b809f2215726e244a4ac588cd7d",
            "0x000000000000000000000000023581767a106ae21c074b2276d25e5c3e136a68b",
            "0x0000000000000000000000000000000000000000000000000000000000000236d",
            "0x000000000000000000000000c8a5592031f93debea5d9e67a396944ee01bb2ca"
         ],
         "data":"0x0000000000000000000000000c02aaa39b223fe8d0a0e5c4f27ead9083c756cc200
         "blockNumber":"0xe60262",
         "timeStamp":"0x62c26caf",
         "gasPrice":"0x5e2d742c9",
         "gasUsed":"0xfb7f8",
         "logIndex":"0x4b",
         "transactionHash":"0x26fe1a0a403fd44ef11ee72f3b4ceff590b6ea533684cb279cb4242
         "transactionIndex":"0x39"
      },
```


From:

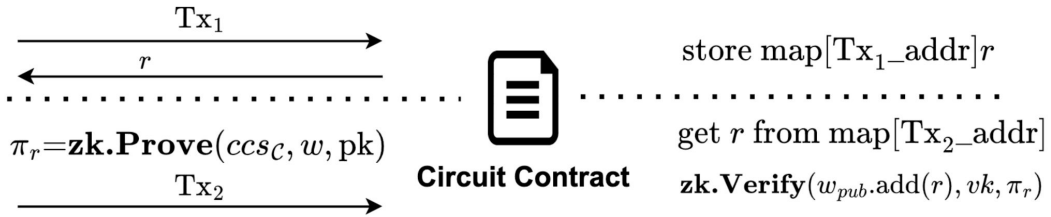
https://docs.etherscan.io/api-endpoints/logs

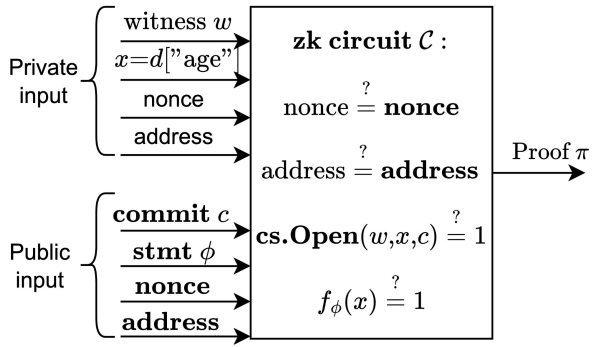


Time-bound Replay-resistant ZKPs

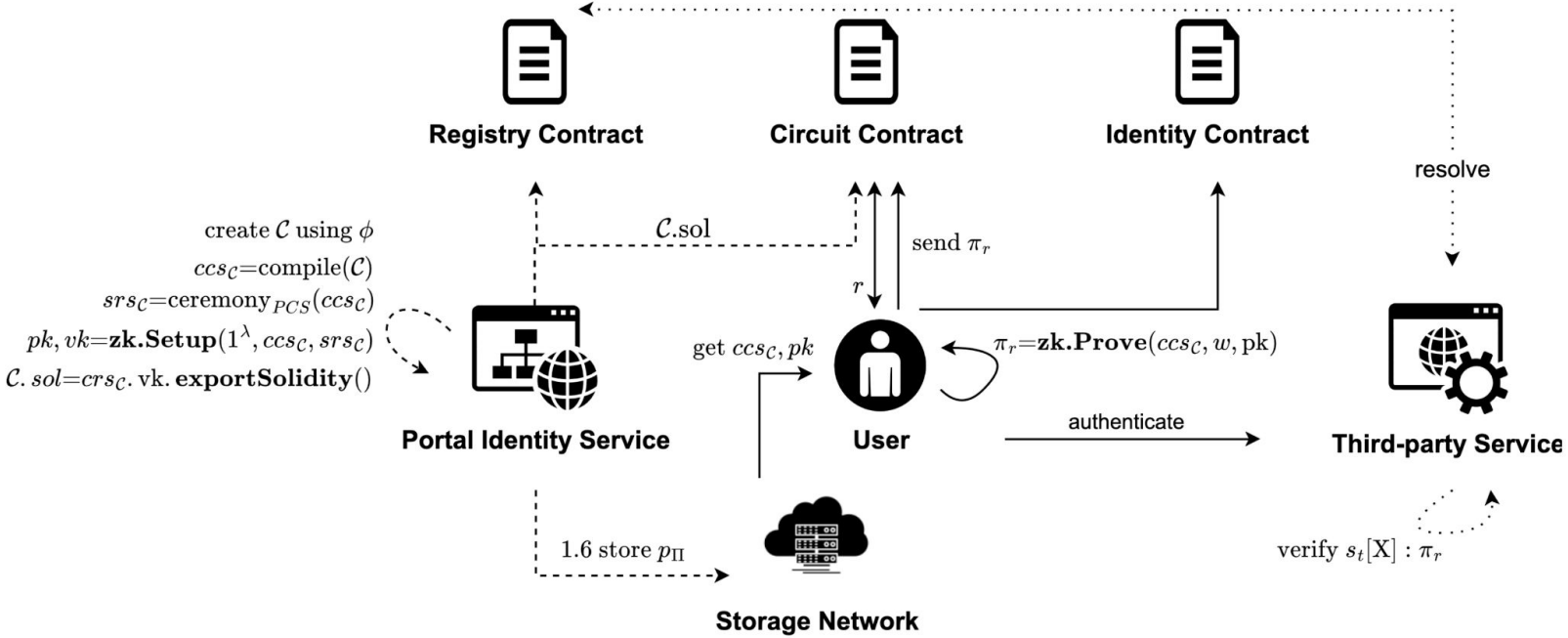
New transaction sequence

- Tx_1 samples randomness at contract and maps it to Tx_1 sender address
- Proof computation bound by Tx_1 transaction time
- Tx_2 sends proof $\boldsymbol{\pi}$ with additional circuit logic (asserts nonce & address)





SSO Smart Contract Architecture



Cost Analysis/Benchmarks

Tx / Call	Type	Cost (eth/$)	Time (ms)	Size (kB)
C^{reg}	deploy	4.1e-3/8.6	18	bc:6.5,tx:6.6
C^{id}	deploy	6.5e-3/13.5	10	bc:10,tx:10
$C^{\mathcal{C}_1}$	deploy	4.9e-3/10.2	**385**	bc:7.4,tx:12
set_$\mathcal{C}_1$	C^{reg}	8.4e-5/0.18	11	tx: 0.46
register	C^{reg}	7.4e-5/0.16	51	tx: 0.3
claim^{pub}	C^{id}	6.4e-05/0.13	3	tx: 0.48
sample	$C^{\mathcal{C}_1}$	6.6e-05/0.14	6	tx: 0.1
verify_π	$C^{\mathcal{C}_1}$	8.4e-4/**1.76**	**252**	tx: 1.20
claim^{priv}	C^{id}	3.9e-4/0.82	21	tx: 0.68
setup$^{\mathcal{C}_1}_{\text{plonk}}$	off-chain	-	1029	p_Π: 7430
prove$^{\mathcal{C}_1}_{\text{plonk}}$	off-chain	-	195	π: 0.552
set/get$^{p_\Pi}_{\text{IPFS}}$	off-chain	-	631 / 66	7430
get$^{W/n/\mathcal{C}_1}$	off-chain	-	10/6.2/4.8	42/78/130

Generated with https://github.com/jplaui/portal

Discussion

- Future Work:
  - Deploying Portal at L2 network, Standardization Compliance (W3C VCs and DIDs, OIDC)
  - Comparing efficiency & cost to related works benchmarks
  - Decentralizing the Portal ID service (multi-signature, register ID service public keys at registry contract)

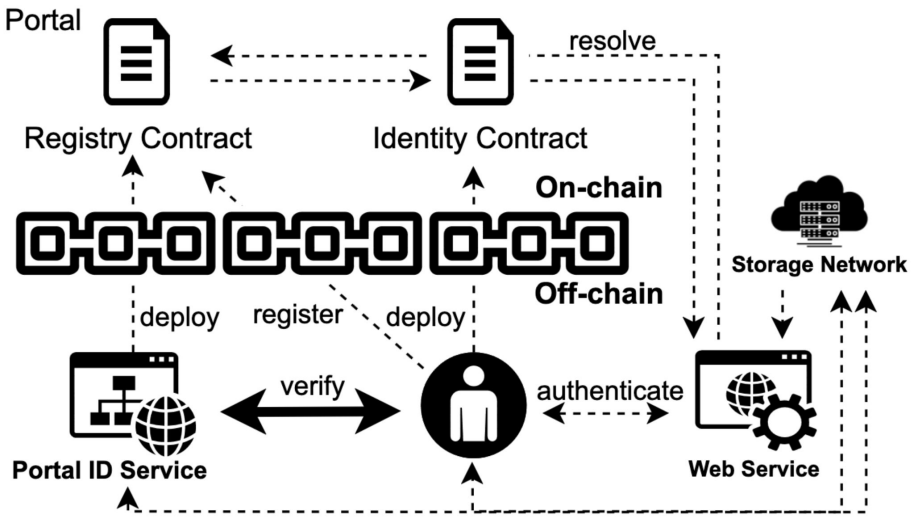
Conclusion

- Conclusion
  - Portal as non-free but cheap SSO alternative
  - Enhanced privacy and control of digital assets

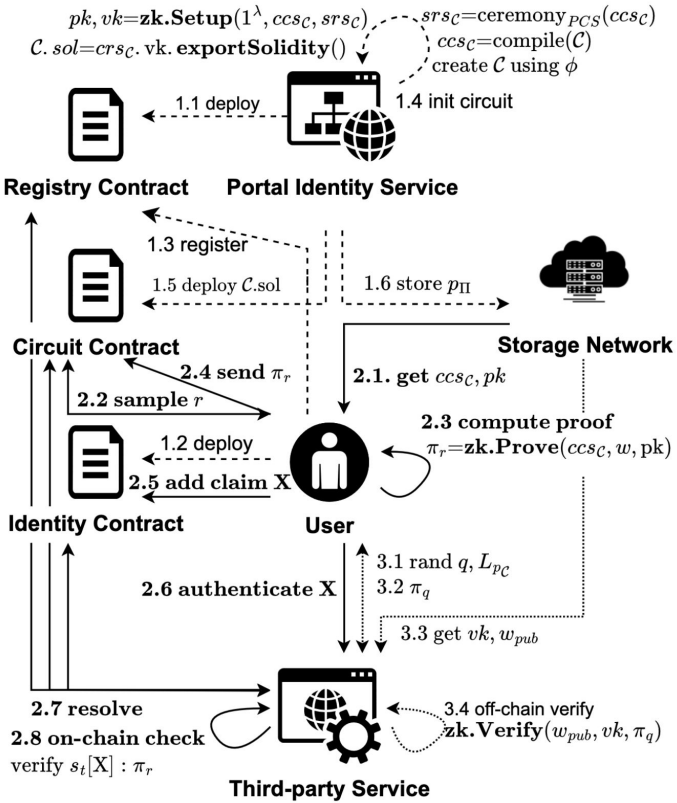
Thank You for Listening

Questions?

SSO Smart Contract Architecture



Portal Identity and Benchmarks



Tx / Call	Type	Cost (eth/$)	Time (ms)	Size (kB)
C^{reg}	deploy	4.1e-3/8.6	18	bc:6.5,tx:6.6
C^{id}	deploy	6.5e-3/13.5	10	bc:10,tx:10
$C^{\mathcal{C}_1}$	deploy	4.9e-3/10.2	**385**	bc:7.4,tx:12
set_$\mathcal{C}_1$	C^{reg}	8.4e-5/0.18	11	tx: 0.46
register	C^{reg}	7.4e-5/0.16	51	tx: 0.3
claim^{pub}	C^{id}	6.4e-05/0.13	3	tx: 0.48
sample	$C^{\mathcal{C}_1}$	6.6e-05/0.14	6	tx: 0.1
verify_π	$C^{\mathcal{C}_1}$	8.4e-4/**1.76**	**252**	tx: 1.20
claim^{priv}	C^{id}	3.9e-4/0.82	21	tx: 0.68
setup$^{\mathcal{C}_1}_{\text{plonk}}$	off-chain	-	1029	p_Π: 7430
prove$^{\mathcal{C}_1}_{\text{plonk}}$	off-chain	-	195	π: 0.552
set/get$^{p_\Pi}_{\text{IPFS}}$	off-chain	-	631 / 66	7430
get$^{W/\text{n}/\mathcal{C}_1}$	off-chain	-	10/6.2/4.8	42/78/130

Verifying ZKP Verification On-chain

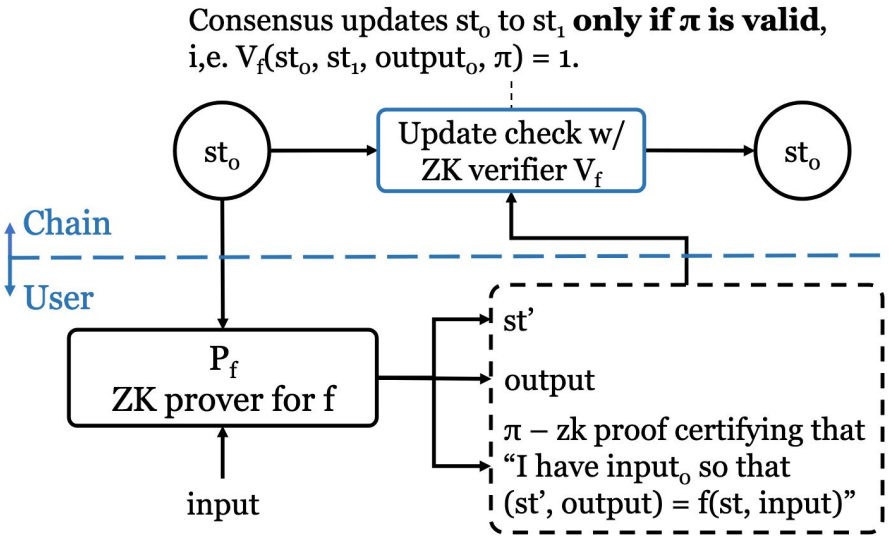


Image from: [Navigating Privacy on Public Blockchains]