I See You Blockchain User, or Not! Privacy in the Age of Blockchains

Ghada Almashaqbeh
UConn
@g_almashaqbeh

Enigma 2022
Big Dreams … Bitcoin 2009

Blockchain

Miners
Big Dreams ...

Blockchain

Miners

Tx
addr1 pays addr2 0.005 BTC
Limited Functionality

Decentralized currency transfer

Limited scripting language

Is it all about currency transfer guarded by simple scripts??!!!
No Privacy

Pseudo-anonymity

Transaction Linkability

All can tell that I ordered a video from that vendor??!!!

Solutions Went Different Directions

Bitcoin

Privacy

Public

Limited

Functionality
Solutions Went Different Directions

- Privacy
- Public

Limited Functionality
Ethereum was Born in 2015

Other systems: Algorand, Cardano, …
Smart Contracts

Public Inputs

```
0100110
10011
1000001001
```

Public Outputs

```
10000111
1010101
```
Smart Contracts

Computing on demand!
Solutions Went Different Directions

Privacy

Public

Bitcoin

Limited

Ethereum

Arbitrary

Functionality
Several Initiatives Out There

- Zcash
- Monero
- Zerocoin
- Quisquis

...
General Paradigm

Starring:
Commitment/encryption +
Zero knowledge proofs (ZKP)
Private Payments

I own an address that has some BTC
Total output = total input
Private Payments

I own an address that has some BTC
Total output = total input

Bitcoin is still public!!!
Bigger Dreams ...

Privacy

Public

Limited

Bitcoin

Functionality
Bigger Dreams ...

Privacy

Public

Bitcoin

Limited

Functionality

Ethereum

Arbitrary
Bigger Dreams ...

Privacy

Public

Private

Limited

Arbitrary

Functionality

Zcash

✔

Bitcoin

Ethereum

✔
Bigger Dreams ...

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Public</th>
<th>Limited</th>
<th>Arbitrary</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>?</td>
</tr>
<tr>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Zcash

Bitcoin

Ethereum
Privacy-preserving Smart Contracts?

Private Inputs

Private Outputs
More Initiatives

Zether

Hawk

Kachina

Zexe

smartFHE

Arbitrum

Ekiden

Zkay
Solutions Spectrum

Off-chain
Others compute

On-chain
Miners compute
Off-chain Private Computing

Compute + Hide & Prove

Starring: ZKP

Steffen et al. "zkay: Specifying and enforcing data privacy in smart contracts." ACM CCS. 2019
Compute over inputs

Encrypt input/output, provide ZKPs

Verify ZKPs, apply state changes
On-chain Private Computing

Starring:
Fully homomorphic encryption (FHE) +
Zero knowledge proofs (ZKP)
FHE

\[ \text{Enc}(x) + \text{Enc}(y) = \text{Enc}(x + y) \]

\[ \text{Enc}(x) \cdot \text{Enc}(y) = \text{Enc}(x \cdot y) \]

ZKP

System/application specific conditions
Encrypt inputs, provide ZKPs

Compute, produce encrypted outputs

Decrypt outputs
Encrypt inputs, provide ZKPs

Compute, produce encrypted outputs

Decrypt outputs

Private computing on demand!
Several Challenges…
Concurrency

A state change will invalidate all pending ZKPs

Solutions rely on locking and delaying deposits
Multi-User Inputs

Interactivity and high computation cost!
Efficiency

Computation cost
- Generating a ZKP can take a minute

Ciphertext size
- Homomorphic multiplication ciphertext > 100 KB
The Path Forward?! 

On-chain  
+  
Off-chain
Take-home Message

Privacy is critical for the future of blockchain systems

Many open questions

A long path ahead...
This is just the beginning!