Transpiling Policies to Secure Computation Circuits

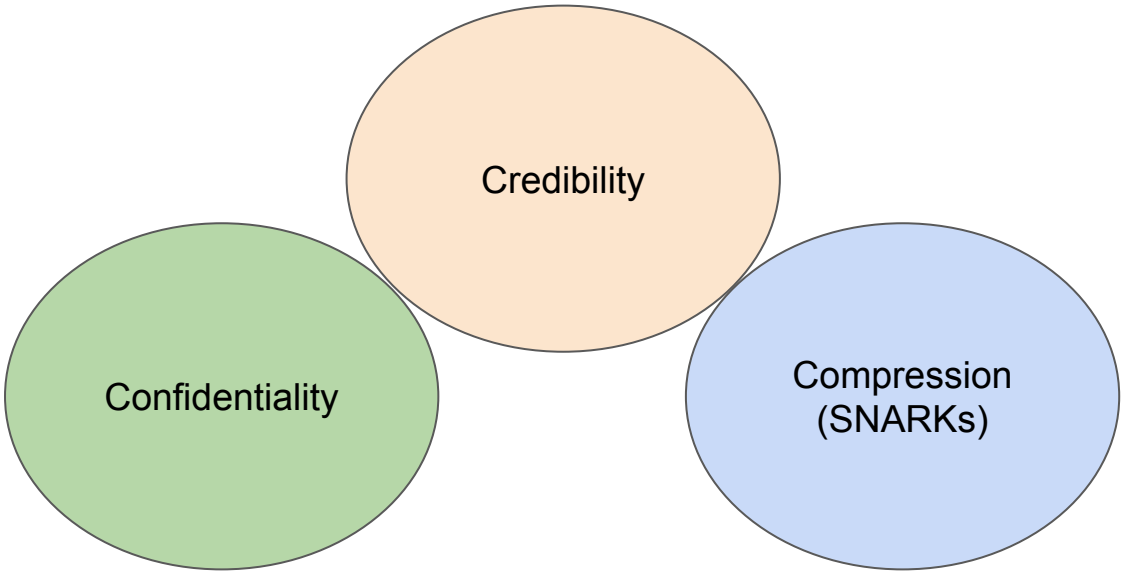
Jan Lauinger

Munich, May 2024

Secure Computation Circuits

Zero-knowledge Circuit, MPC Circuits, FHE Circuits

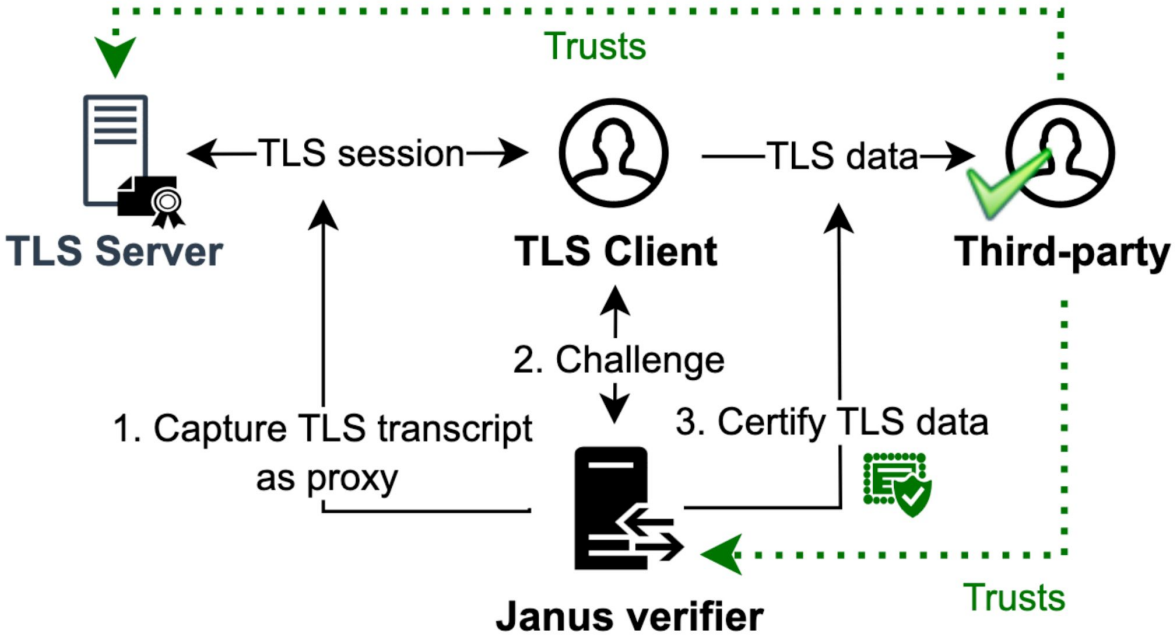
Zero-knowledge Application Fields



ZK Credibility for Data Provenance

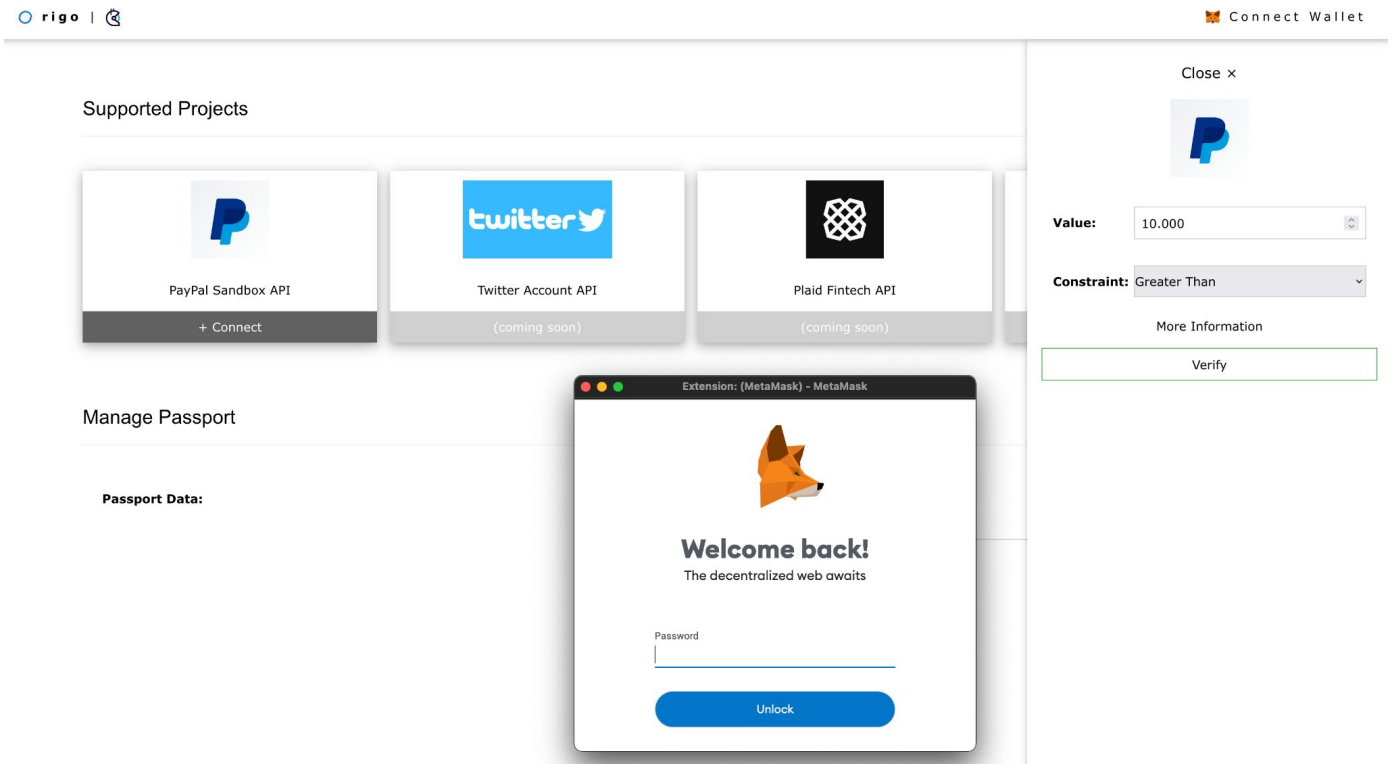
How can you verify where data originates from and has not been tampered?

ZK Credibility for Data Provenance



Janus: Fast Privacy-Preserving Data Provenance For TLS

The Problem



[ORIGO: Proving Provenance of Sensitive Data with Constant Communication]

The Problem

“paypal bank balance > 100$”

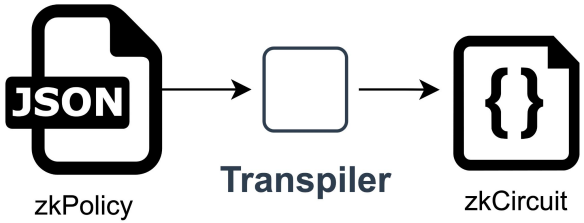
```
commit(r, secret) == c
k = HKDF(secret)
plaintext = decrypt(k, ciphertext)
substring = find(plaintext, pattern)
bank_balance = convert(substring)
bank_balance > 100
```

A simple **statement**

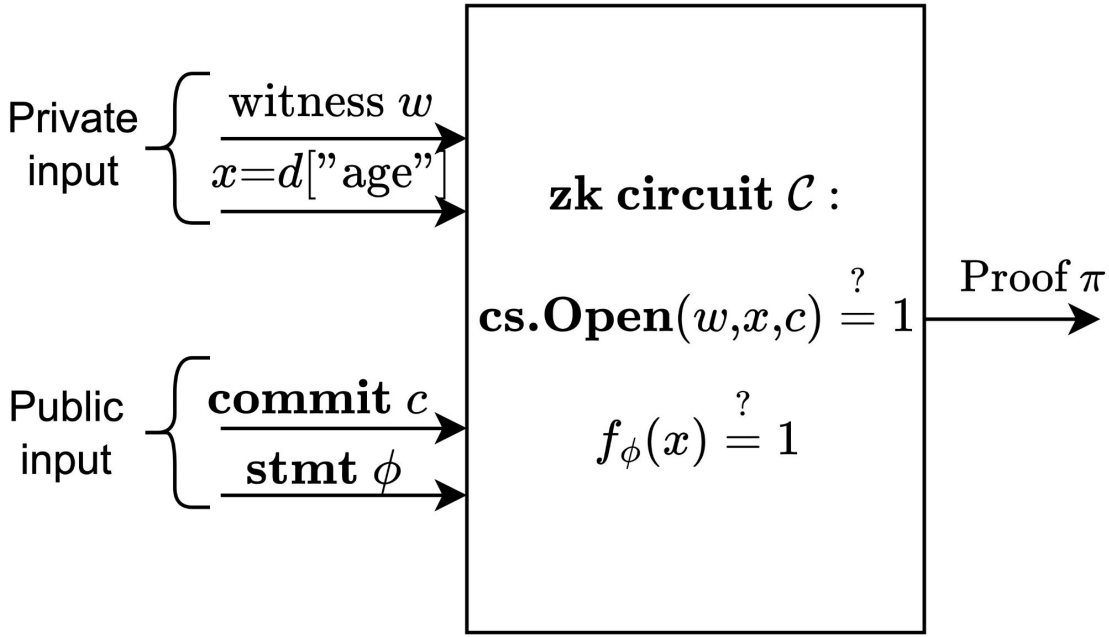
A complex **circuit** (#constraints=1.6million)

The Solution

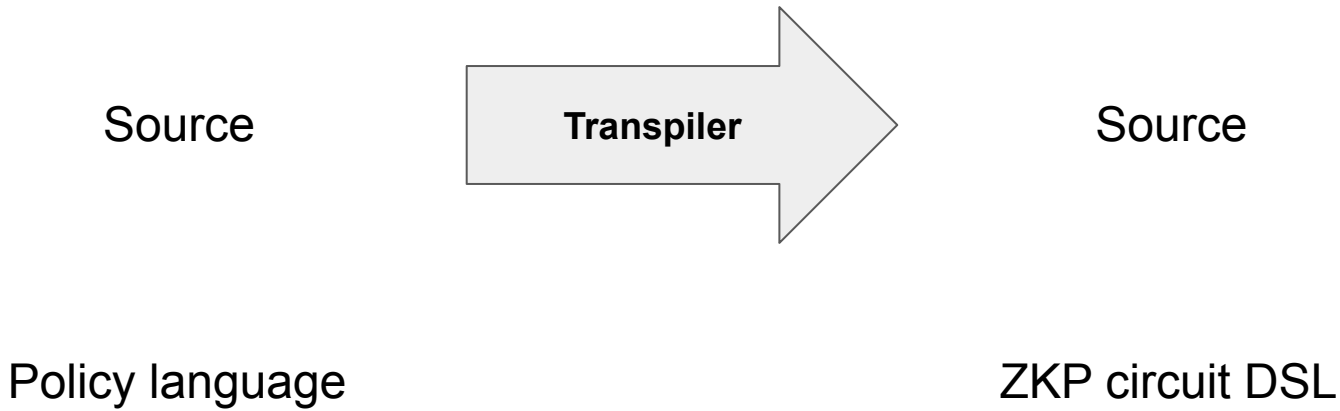
Transpile a user defined policy into a secure computation circuit



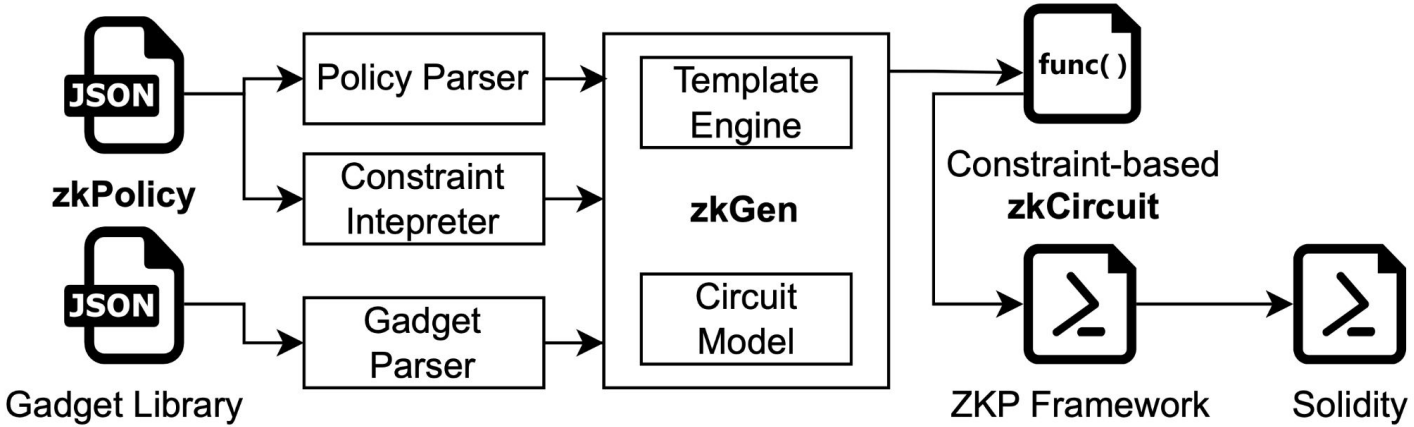
Zero-knowledge Proof



Transpiler



zkGen Transpiler Architecture



zkGen: Policy-to-Circuit Transpiler

zkPolicy Language & Gadget Library

zkpolicy > {} example3_zkFriendlyCommitData.json > ...

```
{
    "name": "AgeCommitCheck",
    "relations":[
        {
            "private_argument": {
                "name": "Age",
                "type": "string",
                "protection": {
                    "algorithm": "commitments:mimc",
                    "parameter": "message"
                }
            },
            "public_argument": {
                "name": "Threshold",
                "type": "integer"
            }
        }
    ],
    "constraints": [
        "0:age-gt-0:threshold"
    ]
}
```

```
{
    "commitments": {
        "mimc": {
            "commit_string": {
                "scope": "public",
                "type": "string",
                "size": 32
            },
            "witness": {
                "scope": "private",
                "type": "string",
                "size": -1
            },
            "message": {
                "scope": "private",
                "type": "string",
                "size": -1
            }
        },
```

From: zkGen repository on Github and gnark_lib repository on Github

Results

zkPolicy	LOC policy	LOC circuit	Transpile time
TLS commit	22	975	2.38 ms
Age commit	20	85	1.70 ms

Last Slide

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

This work will be presented @ICBC24

Speaker: Jan Lauinger

Personal Website: ianzn.com

You can hire me :)

Questions?

Thank You for Listening