DresdenTech

Digitorney

JUG SAXONY DAY 2018

Digitorney Messenger: Blockchain basierte Datenkommunikation für juristische Fallbearbeitung

M.Sc. Arno Pfefferling
DresdenTech

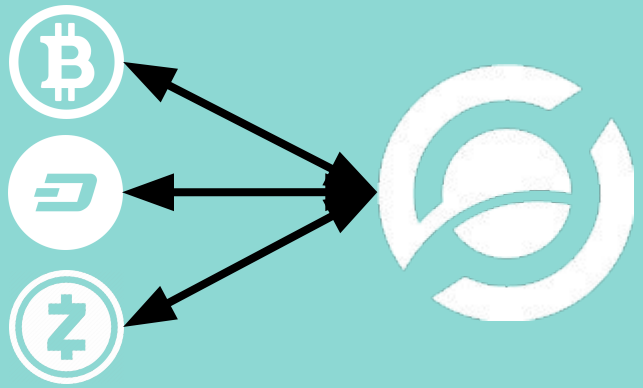
Blockchain - Wie und Warum? 1 / 3

→ public Blockchain

→ Node Infrastruktur

→ zk-SNARK

Transaktionen



HORIZEN:

Bringing privacy to life™

❑ autonome Vertrauensbildung

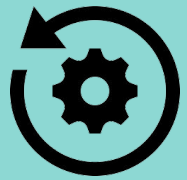
❑ Datenhierarchie/-struktur

❑ dezentral und hoch verschlüsselt

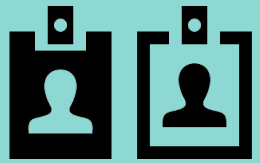
❑ End-zu-Endnutzer Schnittstellen

Blockchain - Wie und Warum? 2 / 3

→ public Blockchain



→ Node Infrastruktur



~JSON RPC implementation

```
private static final Bitcoin bitcoin = new
BitcoinJSONRPCClient();
    public static void sendCoins() throws
BitcoinException {
bitcoin.sendToAddress("1EzGDMdqKW5ubTDNHS
qCKciPkybGSvW", 10);    }
```

~tlsmanager.cpp

```
bool TLSManager::isNonTLSAddr(const string& strAddr, const vector<NODE_ADDR>& vPool,
CCriticalSection& cs)
{
    LOCK(cs);
    return (find(vPool.begin(), vPool.end(), NODE_ADDR(strAddr)) != vPool.end());
}
/**
* @brief Removes non-TLS node addresses based on timeout.
```

Blockchain - Wie und Warum? 3 / 3

→ zk-SNARK Transaktionen

mathematische Grundlagen:
(1) jede Coin1 = (pubk1, snr1)
(2) zwei Listen auf allen Nodes
A=Hash(CoinN); B=Hash(spent(snrN))

(3) Beweis ob Coin1 Alice ausgeben kann
check (pubk1, privk1, snr1, Hash(snr1))
*nur Hash(snr1) wird preisgegeben
**nicht interaktiv - Bob hat keine Feedback Funktion

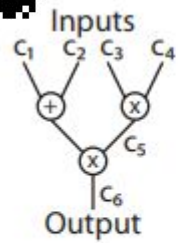
(4) Alice muss noch privk1 nachweisen
t= g^r mod p; c= Hash(t) mod p; s= r+cx
*x, p sind Protokoll gegeben → CRS
**r ist von Alice (Beweiser) zufaellig gewaehlt
***Hash(t), c und s werden public gemacht

(5) Bob und alle anderen pruefen Alice (4)
c= Hash(g^s h^-c)

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

~MOONMATH.q

Computation
→ Arithmetic Circuit
→ R1CS → QAP → zk-SNARK

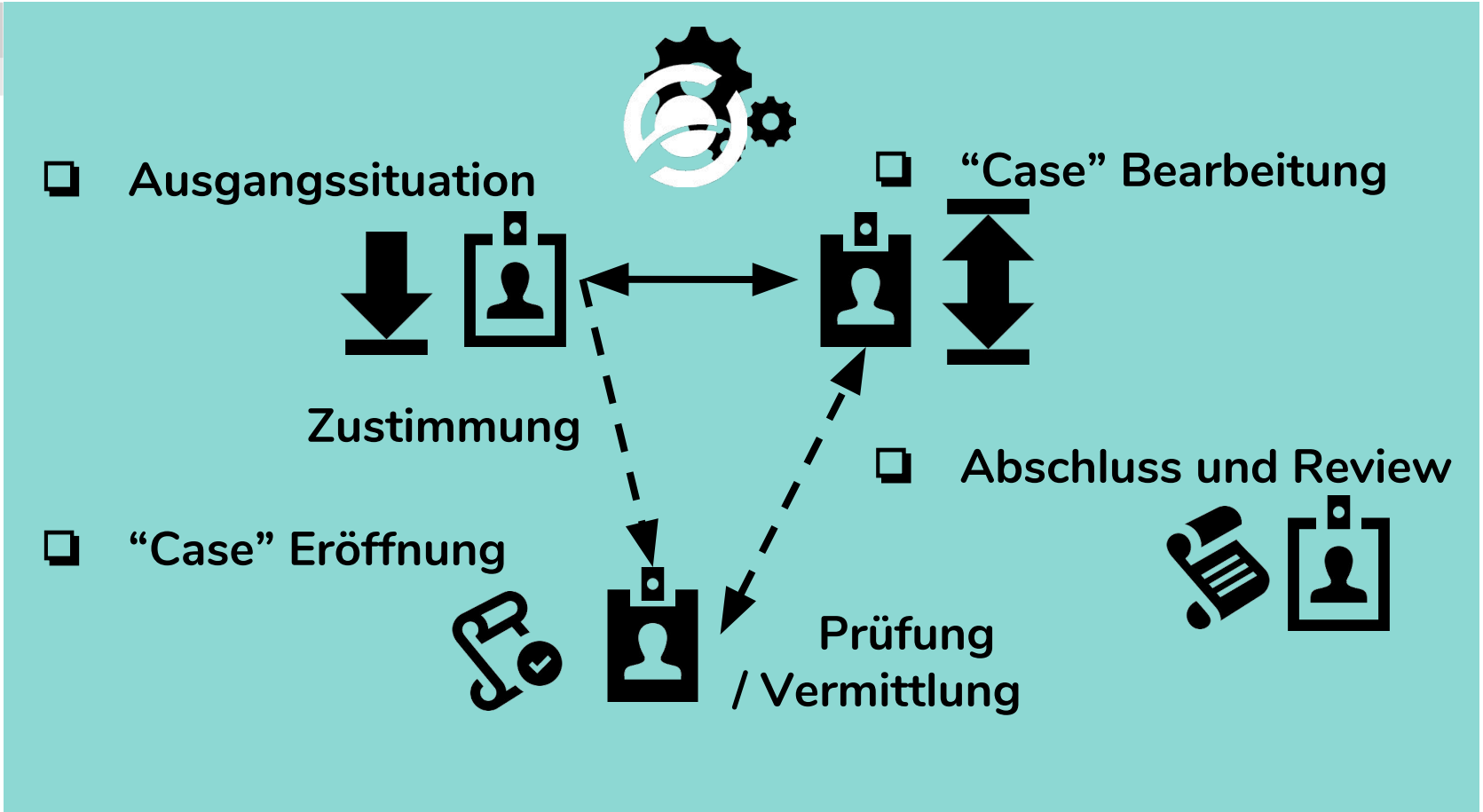


	(r_5, r_6)		(r_5, r_6)		(r_5, r_6)
$v_1(r_i)$	(0,1)	$w_1(r_i)$	(0,0)	$y_1(r_i)$	(0,0)
$v_2(r_i)$	(0,1)	$w_2(r_i)$	(0,0)	$y_2(r_i)$	(0,0)
$v_3(r_i)$	(1,0)	$w_3(r_i)$	(0,0)	$y_3(r_i)$	(0,0)
$v_4(r_i)$	(0,0)	$w_4(r_i)$	(1,0)	$y_4(r_i)$	(0,0)
$v_5(r_i)$	(0,0)	$w_5(r_i)$	(0,1)	$y_5(r_i)$	(1,0)
$v_6(r_i)$	(0,0)	$w_6(r_i)$	(0,0)	$y_6(r_i)$	(0,1)

$t(x) = (x - r_5)(x - r_6)$

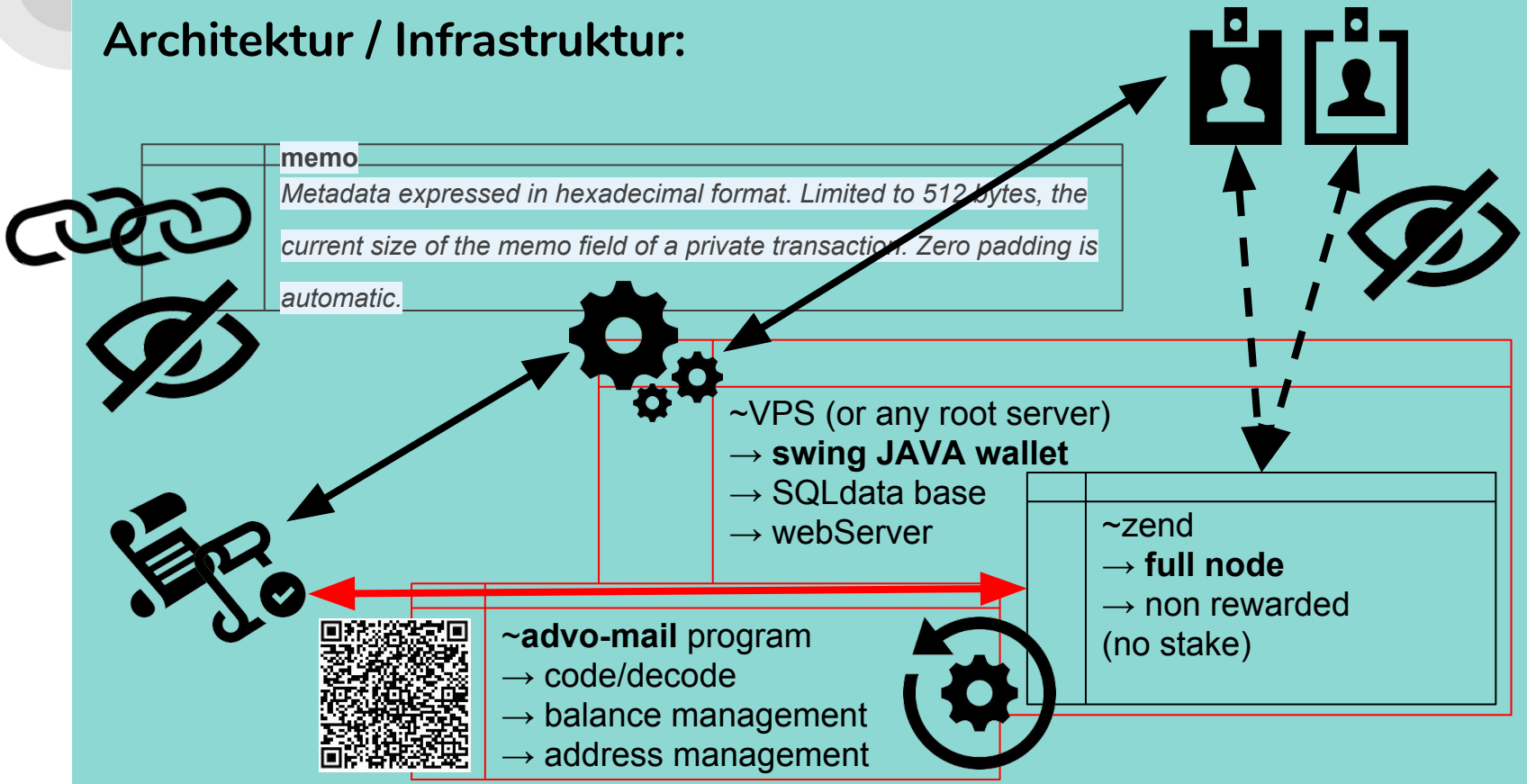
Figure 2: **Arithmetic Circuit and Equivalent QAP.** *Each wire value comes from, and all operations are performed over, a field $\mathbb{F}$. The polynomials in the QAP are defined in terms of their evaluations at the two roots, r_5 and r_6. See text for details.*

Prozessfluss und Funktionsprinzip



DApp mit Java - Wann und Wo?

Architektur / Infrastruktur:



Ausblick

07/18:
closed Beta-Phase
- Workshops...

10/18:
open Beta-Phase
- neue Funktionen?

1/19:
Ausgründung
- neue Märkte!

Digitorney

DRESDENTECH

OVH Innovation is Freedom

HORIZEN FORMERLY ZENCASH

JUG SAXONY DAY 2018

DEMO (POST TALK)

www.DresdenTech.de - Email: info@dresdentech.de