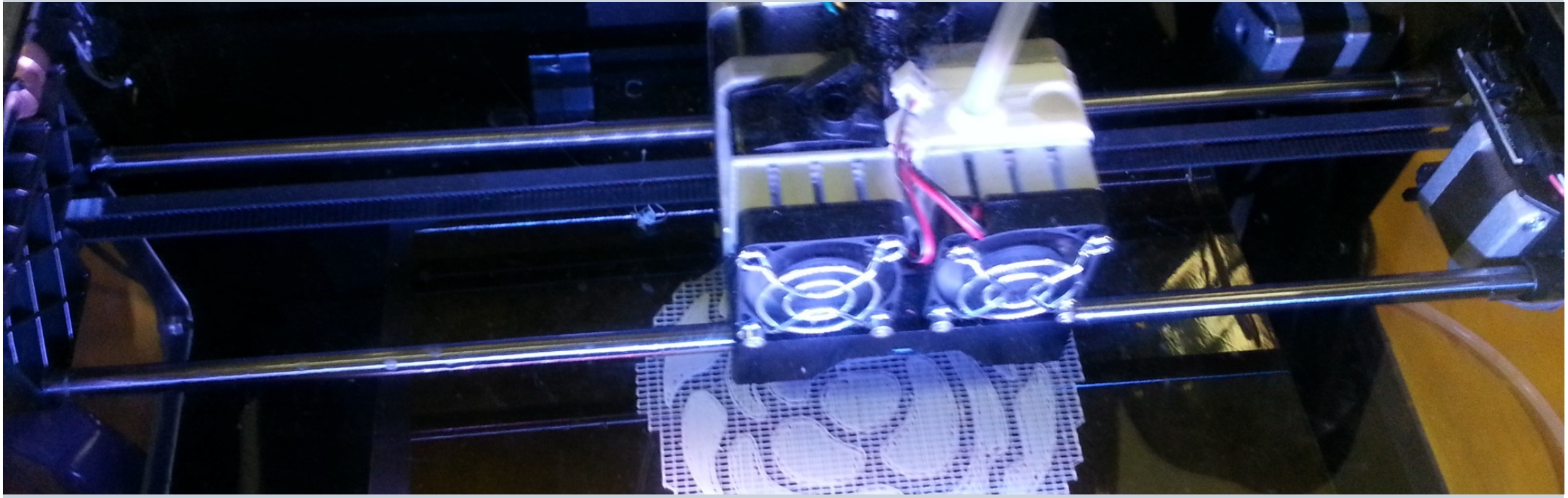
SAMPL
SECURE 3D PRINTING



Institut für Verteilte Systeme
Institute of Distributed Systems

ulm university universität ulm

Geheimhaltung in der Blockchain

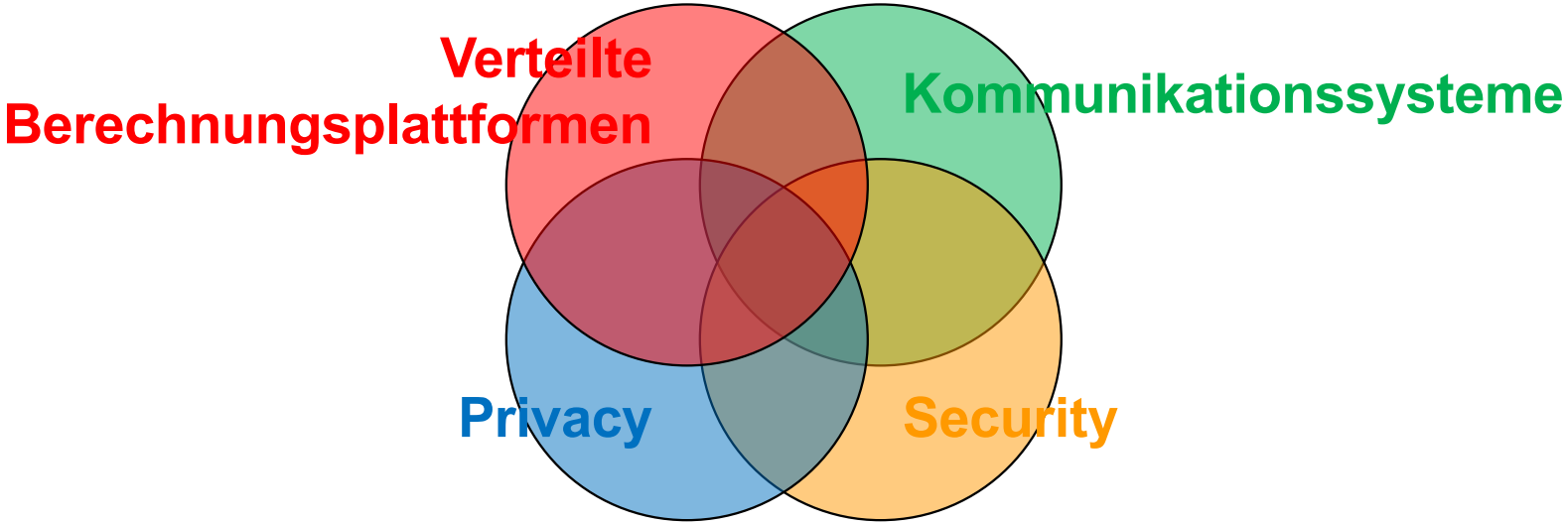
Wie kann die Blockchain anonymisiert werden?

Prof. Dr. Frank Kargl | Institut für Vert. Systeme | Uni Ulm

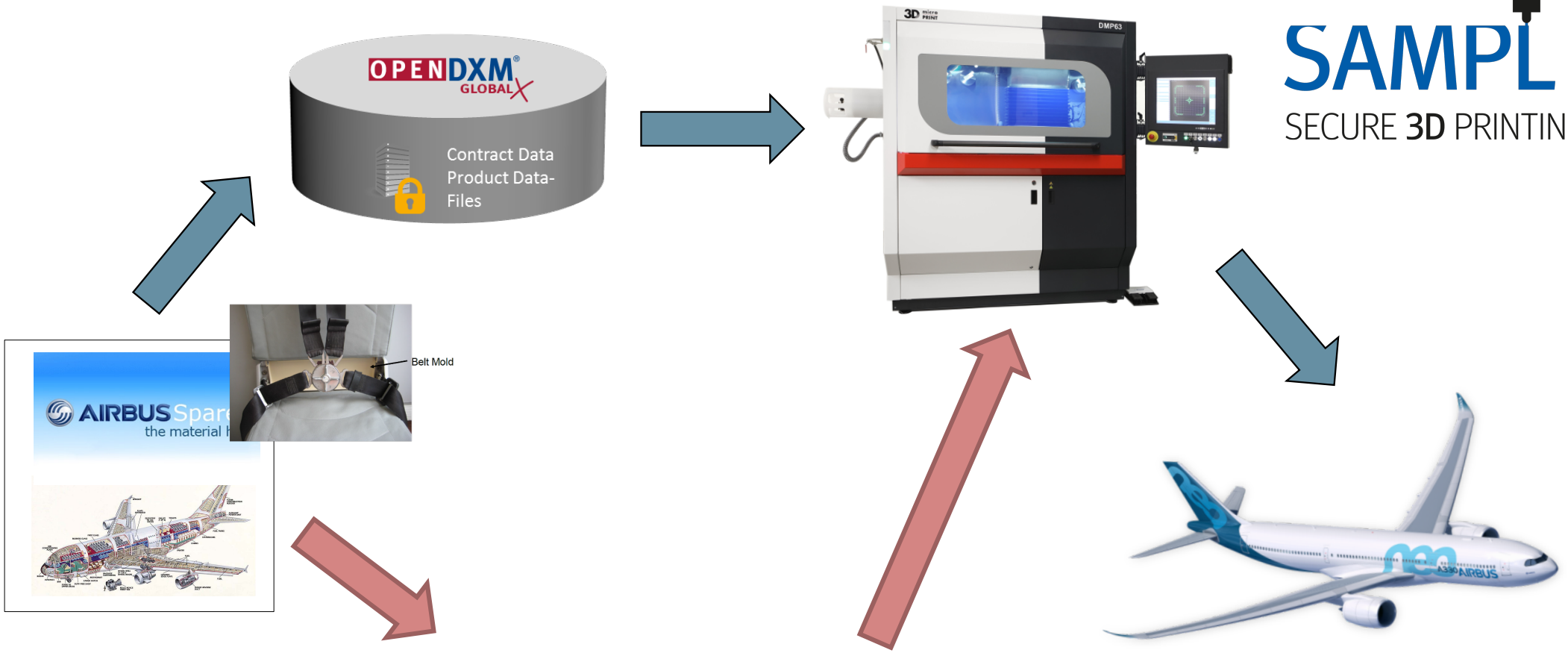
Prof. Frank Kargl

Prof. Franz Hauck

Institut für Verteilte Systeme
Institute of Distributed Systems



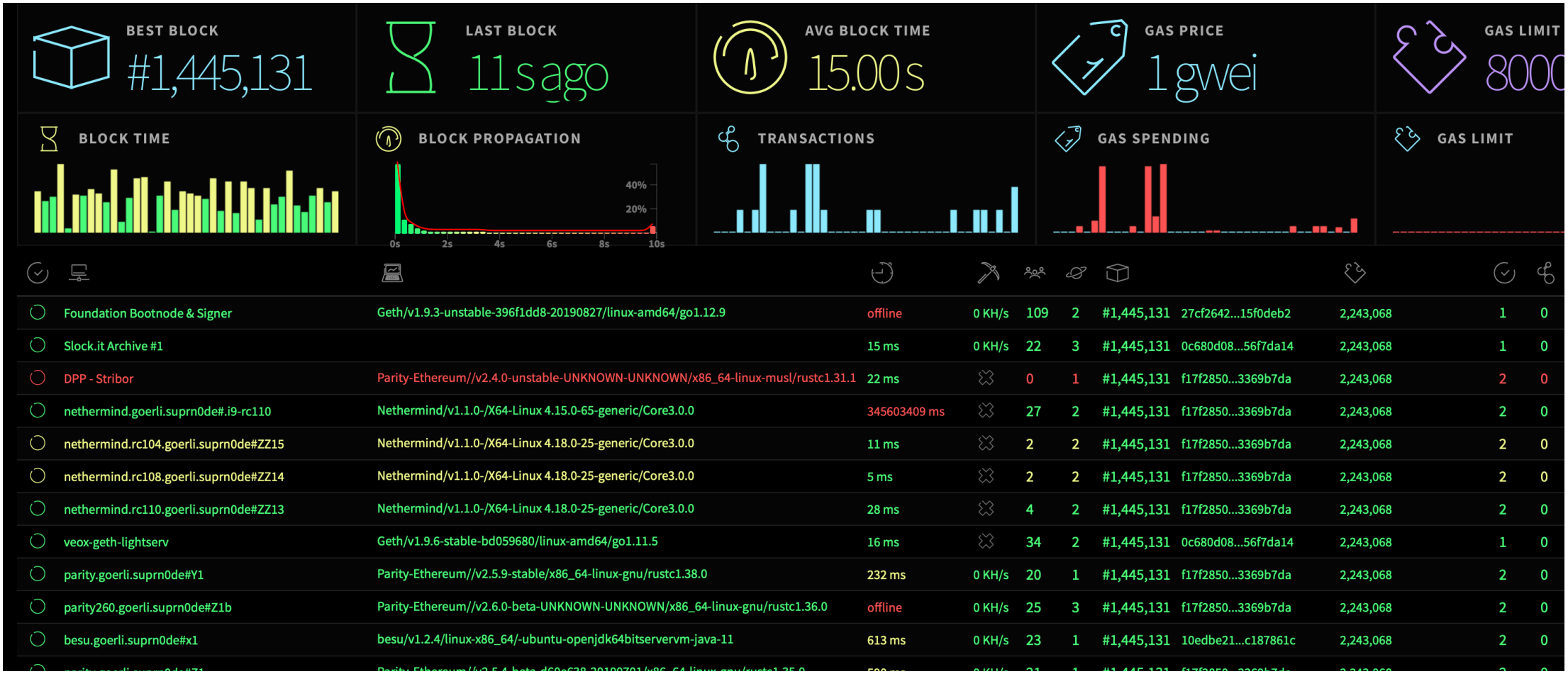
SAMPL
SECURE 3D PRINTING



Blockchain Lizenzdaten

Sampl3D Blockchain

SAMPL
SECURE 3D PRINTING



Foundation Bootnode & Signer	Geth/v1.9.3-unstable-396f1dd8-20190827/linux-amd64/go1.12.9	offline	0 KH/s	109	2	#1,445,131	27cf2642...15f0deb2	2,243,068	1	0
Slock.it Archive #1		15 ms	0 KH/s	22	3	#1,445,131	0c680d08...56f7da14	2,243,068	1	0
DPP - Stribor	Parity-Ethereum//v2.4.0-unstable-UNKNOWN-UNKNOWN/x86_64-linux-musl/rustc1.31.1	22 ms		0	1	#1,445,131	f17f2850...3369b7da	2,243,068	2	0
nethermind.goerli.suprn0de#.i9-rc110	Nethermind/v1.1.0-/X64-Linux 4.15.0-65-generic/Core3.0.0	345603409 ms		27	2	#1,445,131	f17f2850...3369b7da	2,243,068	2	0
nethermind.rc104.goerli.suprn0de#ZZ15	Nethermind/v1.1.0-/X64-Linux 4.18.0-25-generic/Core3.0.0	11 ms		2	2	#1,445,131	f17f2850...3369b7da	2,243,068	2	0
nethermind.rc108.goerli.suprn0de#ZZ14	Nethermind/v1.1.0-/X64-Linux 4.18.0-25-generic/Core3.0.0	5 ms		2	2	#1,445,131	f17f2850...3369b7da	2,243,068	2	0
nethermind.rc110.goerli.suprn0de#ZZ13	Nethermind/v1.1.0-/X64-Linux 4.18.0-25-generic/Core3.0.0	28 ms		4	2	#1,445,131	f17f2850...3369b7da	2,243,068	2	0
veox-geth-lightserv	Geth/v1.9.6-stable-bd059680/linux-amd64/go1.11.5	16 ms		34	2	#1,445,131	0c680d08...56f7da14	2,243,068	1	0
parity.goerli.suprn0de#Y1	Parity-Ethereum//v2.5.9-stable/x86_64-linux-gnu/rustc1.38.0	232 ms	0 KH/s	20	1	#1,445,131	f17f2850...3369b7da	2,243,068	2	0
parity260.goerli.suprn0de#Z1b	Parity-Ethereum//v2.6.0-beta-UNKNOWN-UNKNOWN/x86_64-linux-gnu/rustc1.36.0	offline	0 KH/s	25	3	#1,445,131	f17f2850...3369b7da	2,243,068	2	0
besu.goerli.suprn0de#x1	besu/v1.2.4/linux-x86_64/-ubuntu-openjdk64bitservervm-java-11	613 ms	0 KH/s	23	1	#1,445,131	10edbe21...c187861c	2,243,068	2	0

SAMPL 3D Blockchain

SAMPL
SECURE 3D PRINTING

Transaction Details

0x96aaa80729121a7d9ae2fa24562702dfbb556af00222866275ccead16254f261

0x8a3D90C1764B111C5AF2161aAb33072c55d71747 → PrintingLicenseStore (0x18ebde..)

Contract Call Success 8 hours ago (October-01-2019 11:23:57 AM +2 UTC)

Verify with other Explorers: Etherscan.io https://goerli.ethers...

Block Number	1393551
Block Confirmations	2,011
Nonce	166
TX Fee	0.002475942 GöETH ($0.441243 USD)
Transaction Speed	11.3 seconds
Raw Input	Hex (Default)

```
63ad51e64ef9caa4c3aa4493c00d849210d28f6073312fa6fa0000000000000000000000
0000000000000000000000000000000000000000000001
```

Input

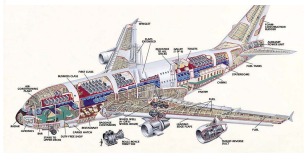
Method Id	0x7df86031
Call	Methodenname grantLicense(uint256 id, address from, address to, uint256 fileHash, uint

	Name	Type	Data
	id	uint256	Lizenz-ID 290018653595771131295839398385756797
	from	address	Lizenzgeber 0x8a3d90c1764b111c5af2161aab33072c55d71
	to	address	Lizenznehmer 0x01f488f7cea28e02f1b357d78c5518cba6924
	fileHash	uint256	Dateiprüfsumme 47504740061117572249172992084851764215821629569
	count	uint64	Anzahl der Lizenzen 1

OPENDXM GLOBAL

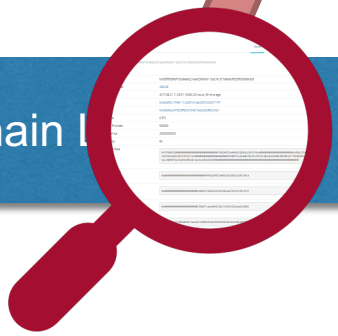
Contract Data
Product Data-
Files

AIRBUS Spares
the material hub



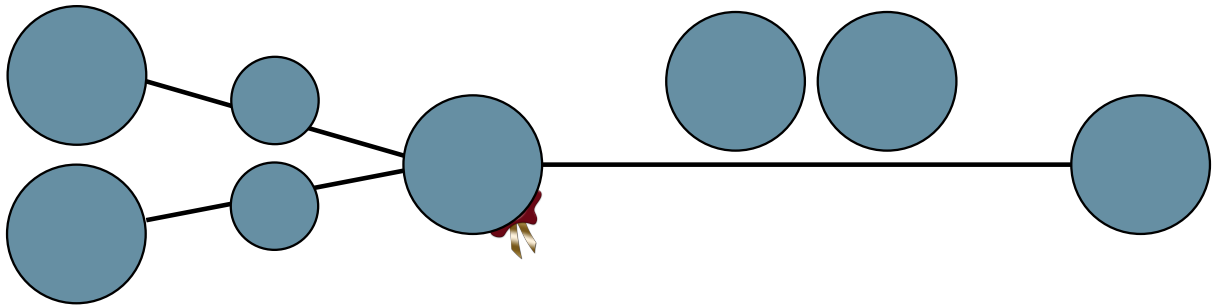
SAMPL
SECURE 3D PRINTING

Blockchain l



BOEING

Transaktionen und Privacy-Ziele



Aber: wie können Miner dann TXs auf Gültigkeit prüfen?

Kriterien für Gültigkeit einer Transaktion

Jede Transaktion muss durch jeden
Blockchain Teilnehmer auf Gültigkeit geprüft werden!

Werterhaltung

$$\sum A_{in} = \sum A_{out}$$

Beweis des Besitzes von Transaktionsinputs

$$\text{sign}_{sk}(p_k)$$

Multi-Type Ring Confidential Transactions

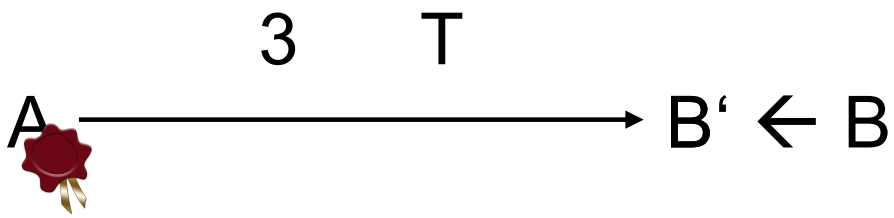
Baustein 1: One-Time Addresses für Empfänger-Anonymität

Baustein 2: Linkable Ring Signatures für Sender-Anonymität

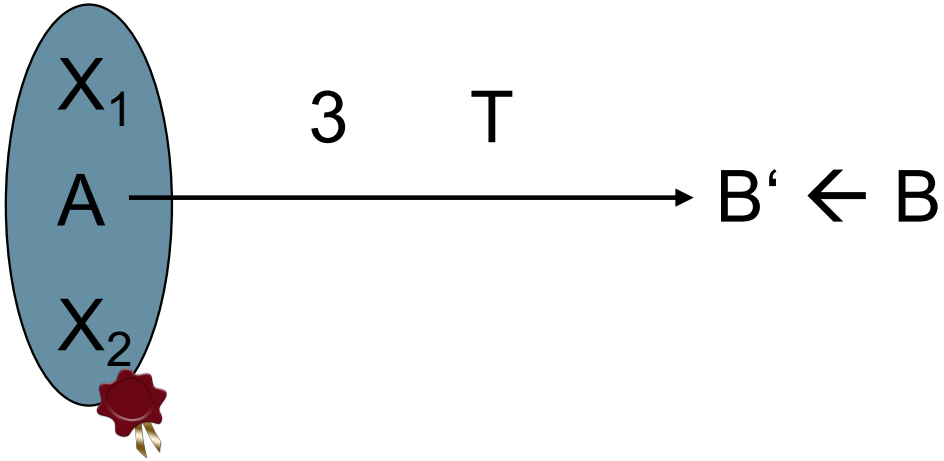
Baustein 3: Pedersen Commitments für geheime Beträge

Baustein 4: Hierarchische Commitments für geheime Typen

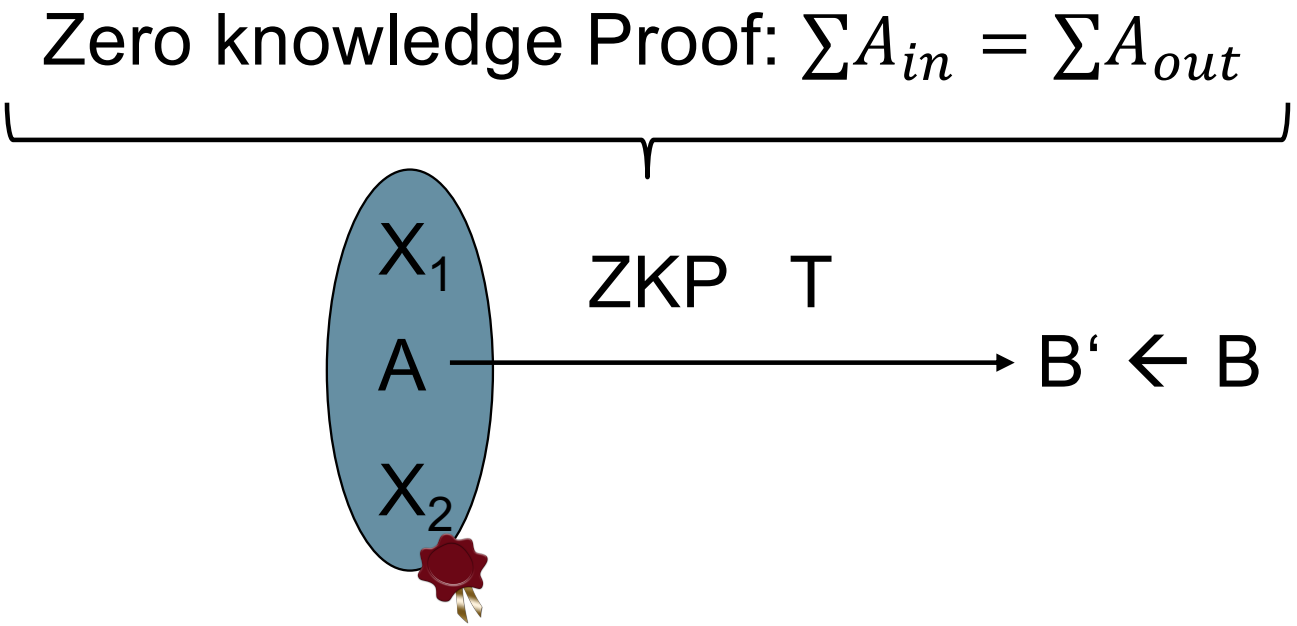
Baustein 1: One-Time Addresses



Baustein 2: Linkable Ring Signatures

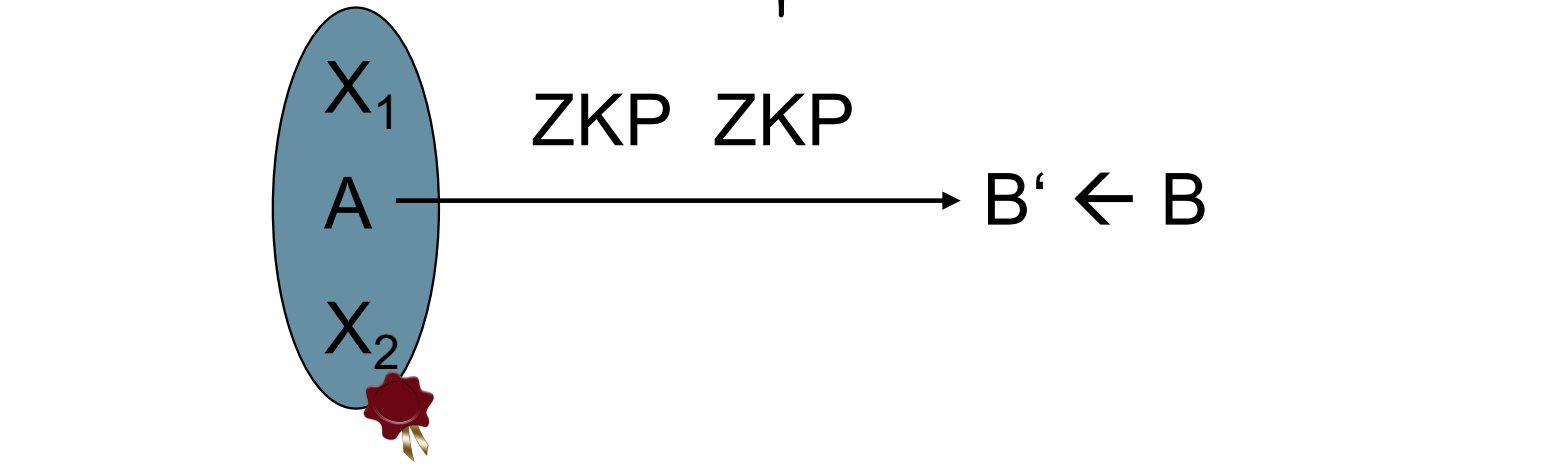


Baustein 3: Pedersen Commitments



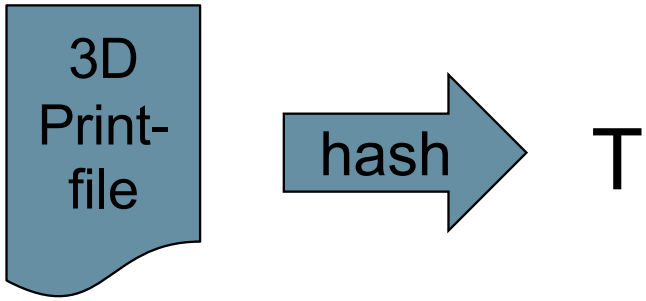
Baustein 4: Hierarchische Pedersen Commitments

Zero knowledge Proof: $\forall t \in T: \sum A_{in,t} = \sum A_{out,t}$



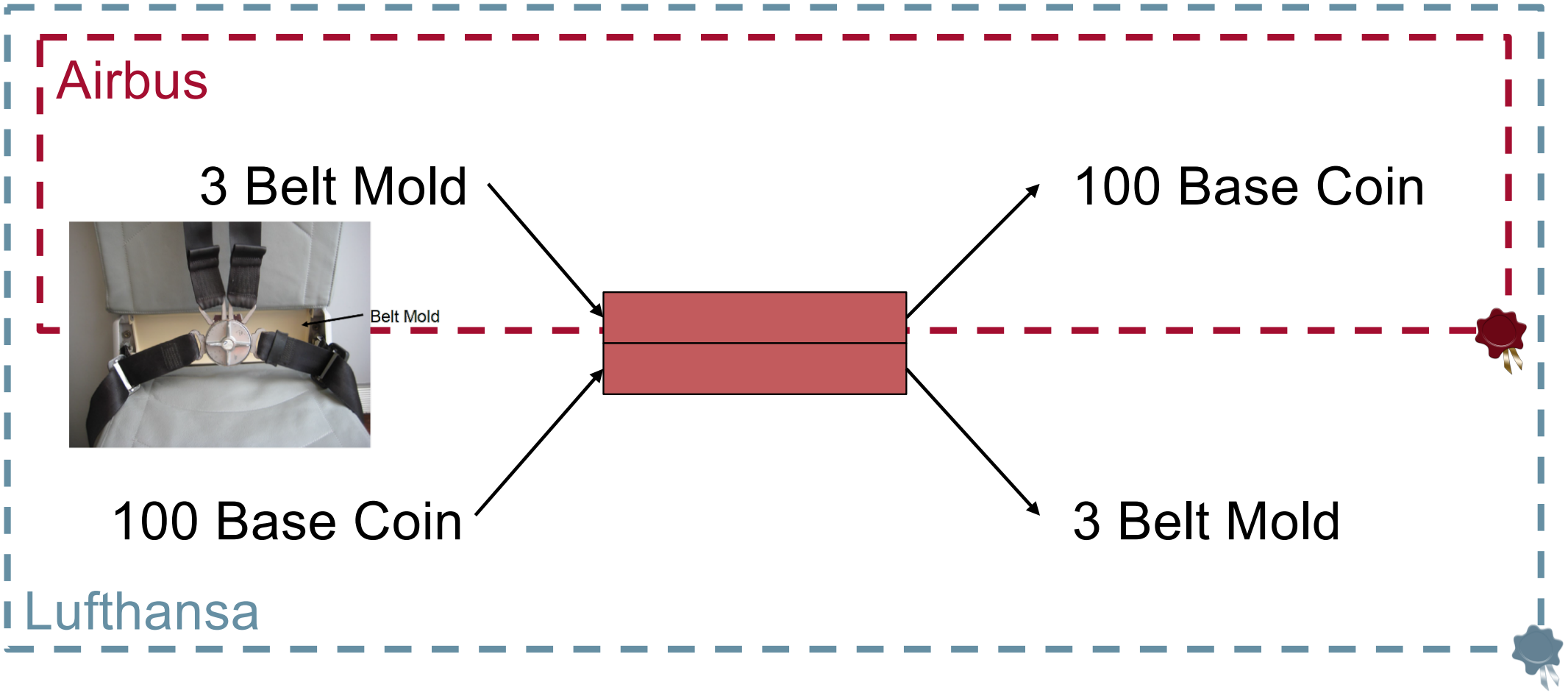
Konzept zum Lizenzmanagement in SAMPL

- Printfiles werden auf Tokentypen T abgebildet, entspricht Lizenzen für Objekte

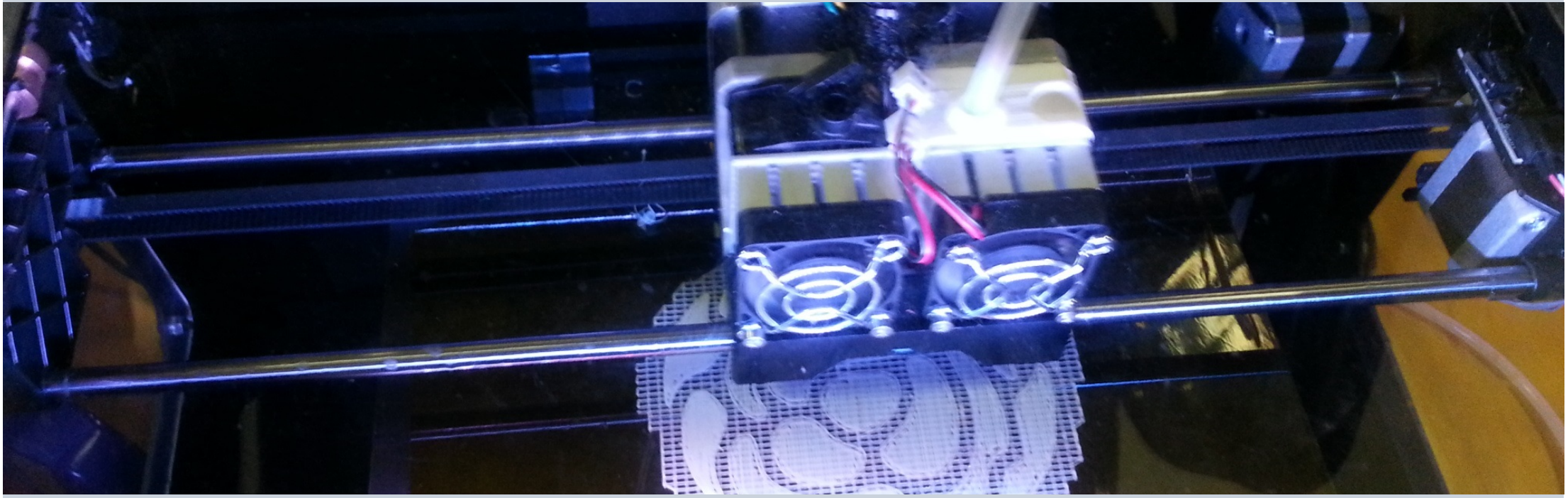


- Abbildung weiterer Objekteigenschaften auf gedruckte Teile durch weitere Transaktionen (z.B. Ergebnis einer Materialprüfung)
- **Atomic Swap-Transaktionen zur Umwandlung von Geldtokens in Drucklizenzen für Objekt T**

Atomic Swaps: Handeln von Lizenzen



SAMPL
SECURE 3D PRINTING



Institut für Verteilte Systeme
Institute of Distributed Systems

ulm university universität ulm

Danke für die Aufmerksamkeit