KI group

BLOCKCHAIN DIE DATA PLATTFORM PERSPEKTIVE

Christoph Seck | KI Group

INTRODUCING KI group

KI group

EVERYTHING IS ABOUT DATA

KI performance KI analytics

BUSINESS MODELLS ARE CHANGING

KI capital KI mobility KI finance KI retail

YOU CAN'T INNOVATE ALONE

KI capital

SOFTWARE EATS THE WORLD

KI performance KI labs KI decentralized

MobiLab

CONTENT IS CRUCIAL

dreaminc dreaminc Food Experts Group

LEARNING NEVER STOPS

KI academy

HUMAN RESOURCES ARE THE LARGEST CAPITAL

KI professionals KI academy KI connect

KI group Facts & Figures

>125 Employees

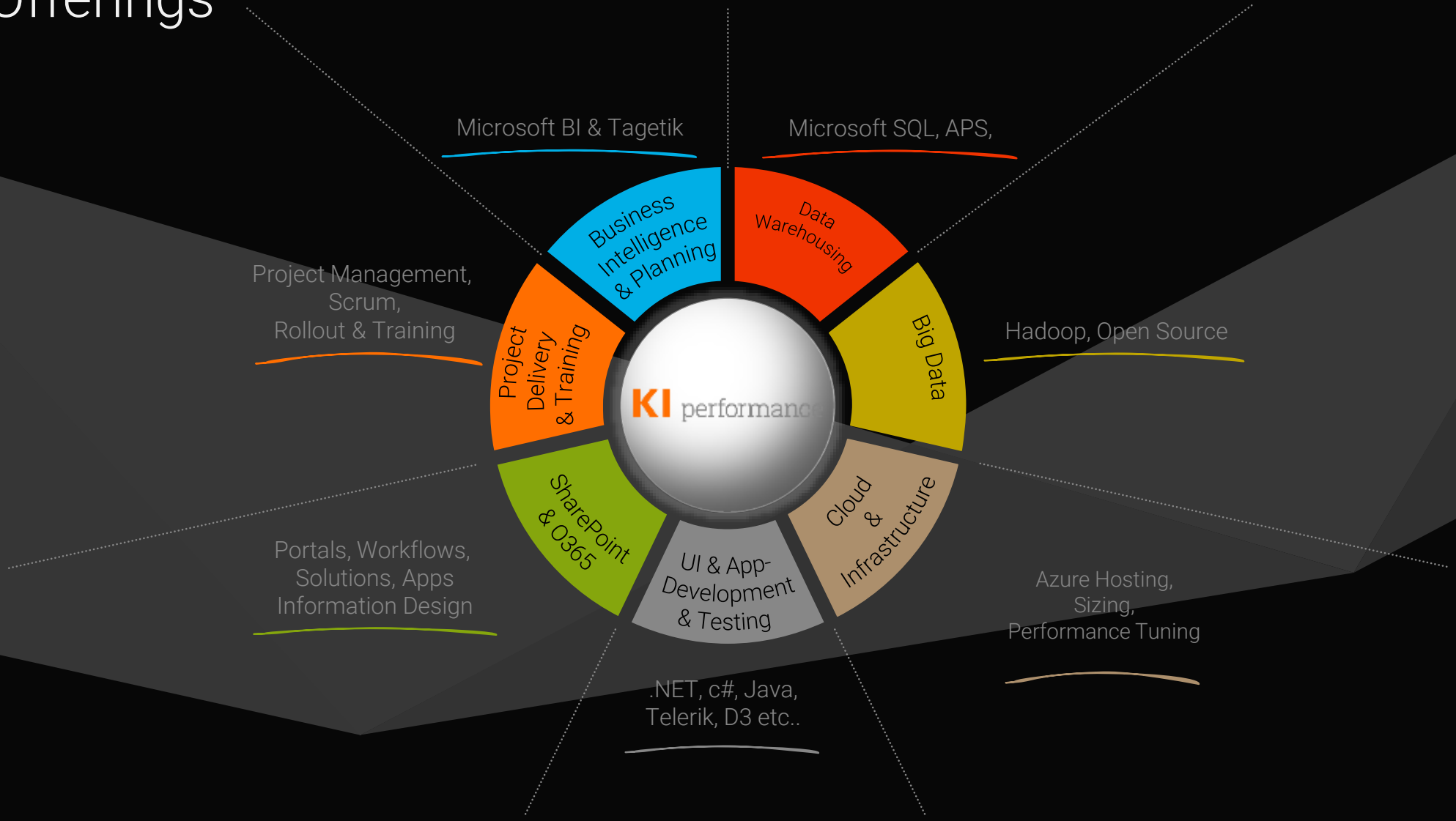
approx. 200 Projects

KI group

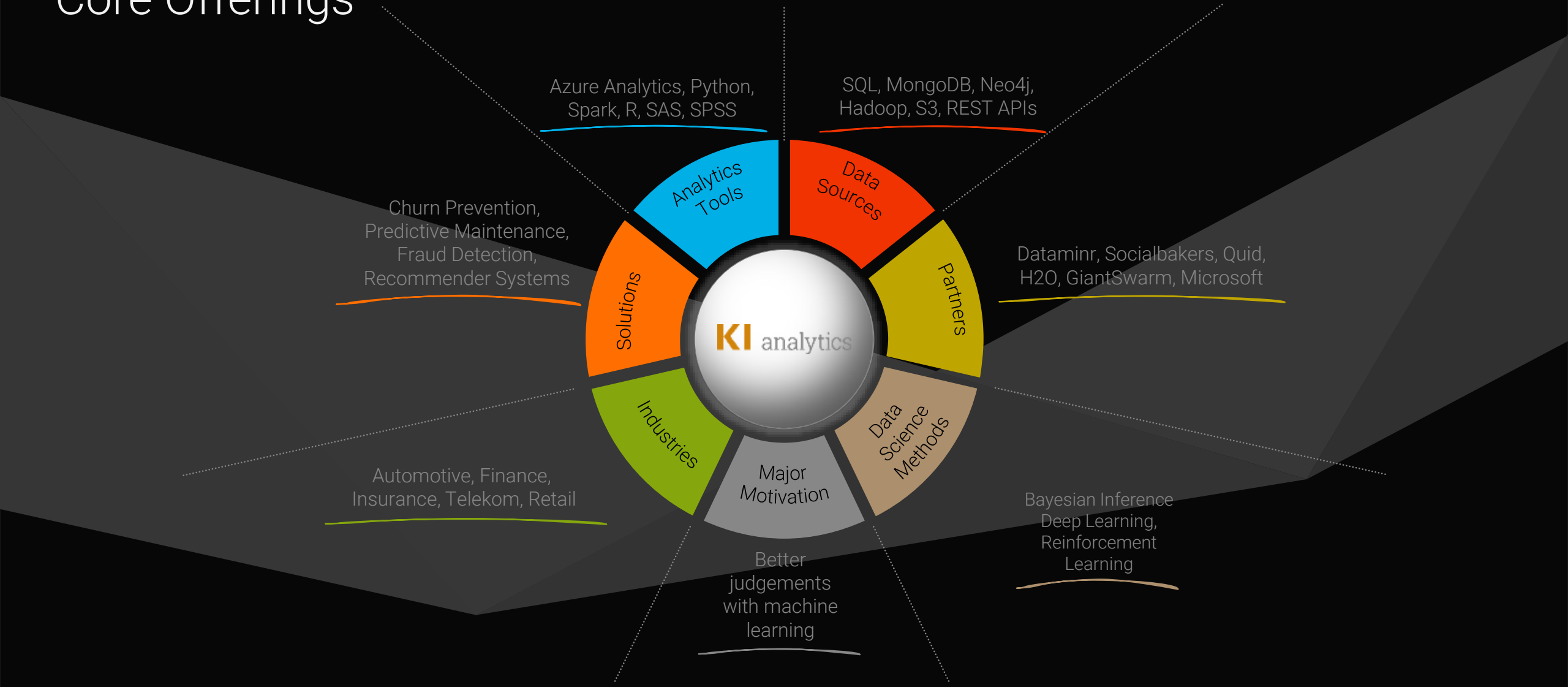
7 Segments

4 Locations

KI performance
Core Offerings



KI analytics
Core Offerings



KI group Partners (Extract)

Microsoft Partner – Gold Data Analytics, Silver Collaboration and Content, Silver Application Development	Analytics, Data Collaboration, Cloud
THEOBALD SOFTWARE	SAP Linkage
NINTEX Workflow for Everyone, harmon.ie	Workflows in SharePoint, Outlook SharePoint
H2O.ai	Algorithms Skalierung
tableau	Frontend
Crossbeat	Crossbeat – Digital Agency NYC
BISSANTZ DeltaMaster	Data Mining, Dashboards
Tagetik	Planning, Consolidation
RI	On Shelf Availability
Dataminr	real-time information Discovery
Quid	Qualitative Data Analytics & Visualization
ADTELLIGENCE	
socialbakers	Social Media Analytics
Prism	Camera Analytics, Heat maps products
Giant Swarm	Containerization, Microservices as solutions for the scale-out
AI NexusLab	Intensive four-month program for young AI companies in New York
GitHub	Collaborative Coding, Largest open source platform worldwide
AXIOM	

KI group References (Extract)

KI group Investments

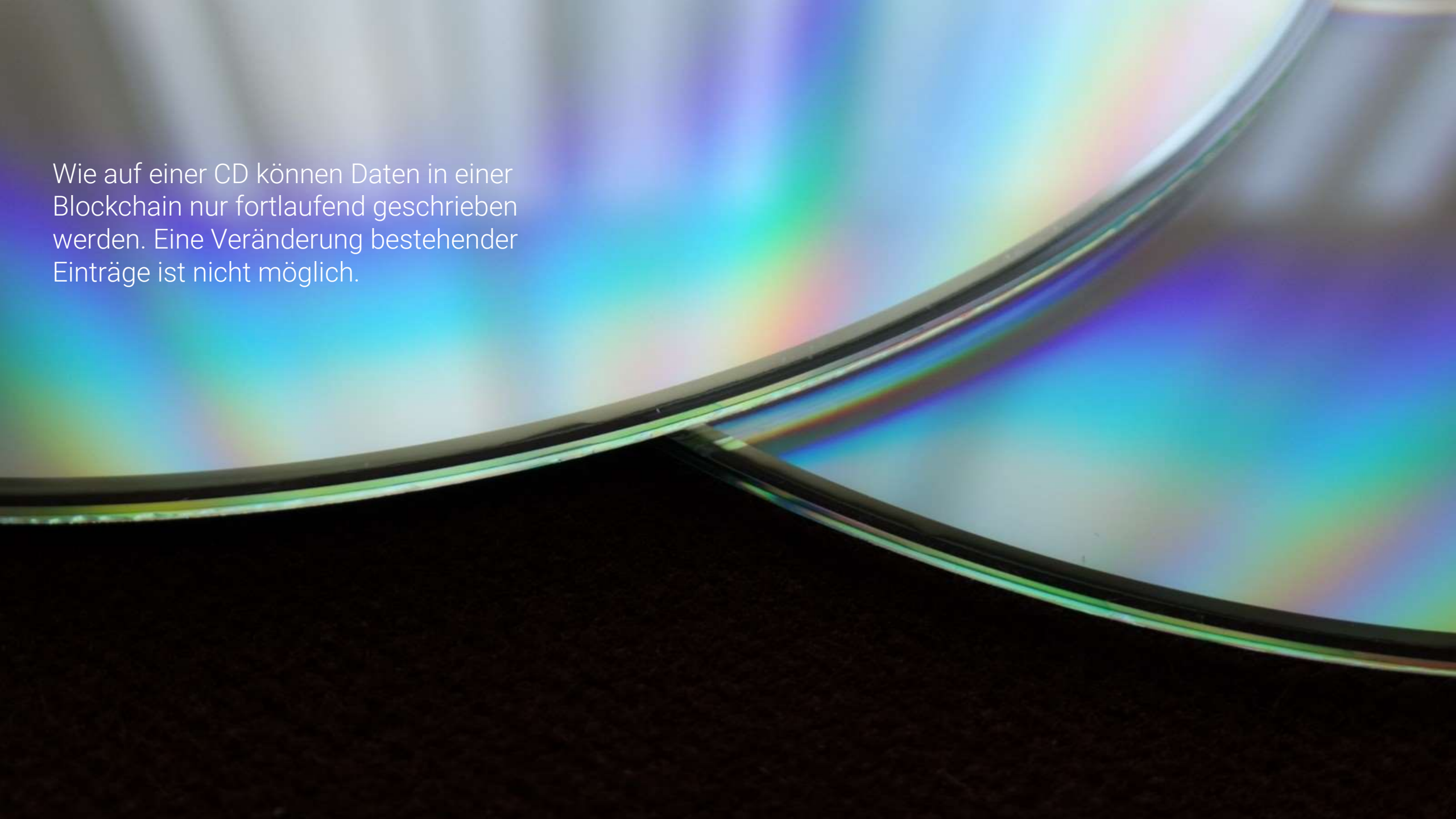
Agenda

- **Introduction**
- **Block Chain Basics**
- **Anonym versus Pseudonym**
- **Getting Data: The one and the many**
- **Getting Data: Doing the Power BI**

Agenda

- **Introduction**
- Block Chain Basics
- Anonym versus Pseudonym
- Getting Data: The one and the many
- Getting Data: Doing the Power BI


Eine dezentrale **Datenbank** für
Transaktionen



Wie auf einer CD können Daten in einer Blockchain nur fortlaufend geschrieben werden. Eine Veränderung bestehender Einträge ist nicht möglich.

Bitcoin - der Ursprung
10 Millionen Bitcoin-Wallets
200.000 Transaktionen

Banking the Unbanked
Ein Handy -> ein Konto

Banken-Infrastruktur
Ausschalten von Zwischen Instanzen

Blockchain 2.0 – „Smart Contracts“
State Machines - Der digitale Vertrag in der Blockchain

Versicherungen


Internet of Things

Unzählige weitere Use Cases vorstellbar

I. Finanzinstrumente, Datensätze und Modelle

- Währung
- Private Equity
- Public Equity
- Anleihen
- Derivate (Futures, Forwards, Swaps, Optionen und komplexere Varianten)
- Stimmrechte
- Rohstoffen
- Verwendung der Haushaltsmitte
- Handelsaufzeichnungen
- Hypotheken- / Darlehensaufzeichnungen
- Wartungsaufzeichnungen
- Crowdfunding
- Micro-Finance
- Micro-Charity

II. Öffentliche Aufzeichnungen

- Landrechte
- Fahrzeugregister
- Geschäftslizenz
- Geschäftsaufnahme/ -auflösung
- Geschäftseigentümerverzeichnisse
- Regulatorische Aufzeichnungen
- Strafregister
- Reisepässe
- Geburtsurkunden
- Sterbeurkunden
- Wähler-ID
- Wahlen
- Gesundheit / Sicherheitsinspektionen
- Baugenehmigung
- Waffenscheine
- forensische Beweise
- Gerichtsakten
- Abstimmungsergebnisse
- Non-Profit-Aufzeichnungen
- Regierungs- / Non-Profit-Buchhaltung

III. Private Einträge

- Verträge
- Unterschriften
- Testamente
- Stiftungen
- Treuhand
- GPS Spuren (persönlich)

IV. Andere Halböffentliche Einträge

- Abschluss
- Zertifizierungen
- Lernerfolge
- Noten
- HR Aufzeichnungen (Gehalt, Leistungsbeurteilungen)
- Krankenakten
- Rechnungsunterlagen
- Geschäftsabschlussaufzeichnungen
- Erbgutdaten
- GPS Spuren (institutionelle)
- Zustellungsbestätigung
- Schlichtung

V. Physische Anlagenschlüssel

- Heim- / Wohnungsschlüssel
- Ferienhaus- / Teilzeitnutzungsschlüssel
- Hotelzimmer Schlüssel
- Autoschlüssel
- Mietauto Schlüssel
- Leasingauto Schlüssel
- Spind Schlüssel
- Safe Schlüssel
- Paketzustellung (Schlüssel für Lieferfirma und Empfänger)
- Wett-Aufzeichnungen
- Fantasy Sports Aufzeichnungen

VI. Immaterielle Werte

- Gutscheine
- Coupons
- Reservierungen (Restaurants, Hotels, Warteschlangen, etc.)
- Kinokarten
- Patente
- Urheberrechte
- Marken
- Software-Lizenzen
- Videospiel-Lizenzen
- Musik / Film / Buch-Lizenzen
- Domain Namen
- Online-Identitäten
- Urheber- / Stand der Technik Nachweis

VI. Andere

- Aufzeichnungen (Fotos, Audio, Video)
- Datensätze (Sportergebnisse, Temperatur, etc.)
- Sim-Karten
- GPS-Netzwerkidentität
- Pistolen Entsperrungscodes
- Waffen Entsperrungscodes
- Nuklear Start-Codes
- Spam-Kontrolle (Mikrozahlungen für die Buchung)

Data Plattform?

Distributed Database

- 6000 Replica
- 500 Googles needed
- Financal Value: 39 Mrd $
- 40.000.000 Petaflops

Core Transactional System

- International Finance
- Via Smart Contracts:
  The Master Data of our managed Interactions

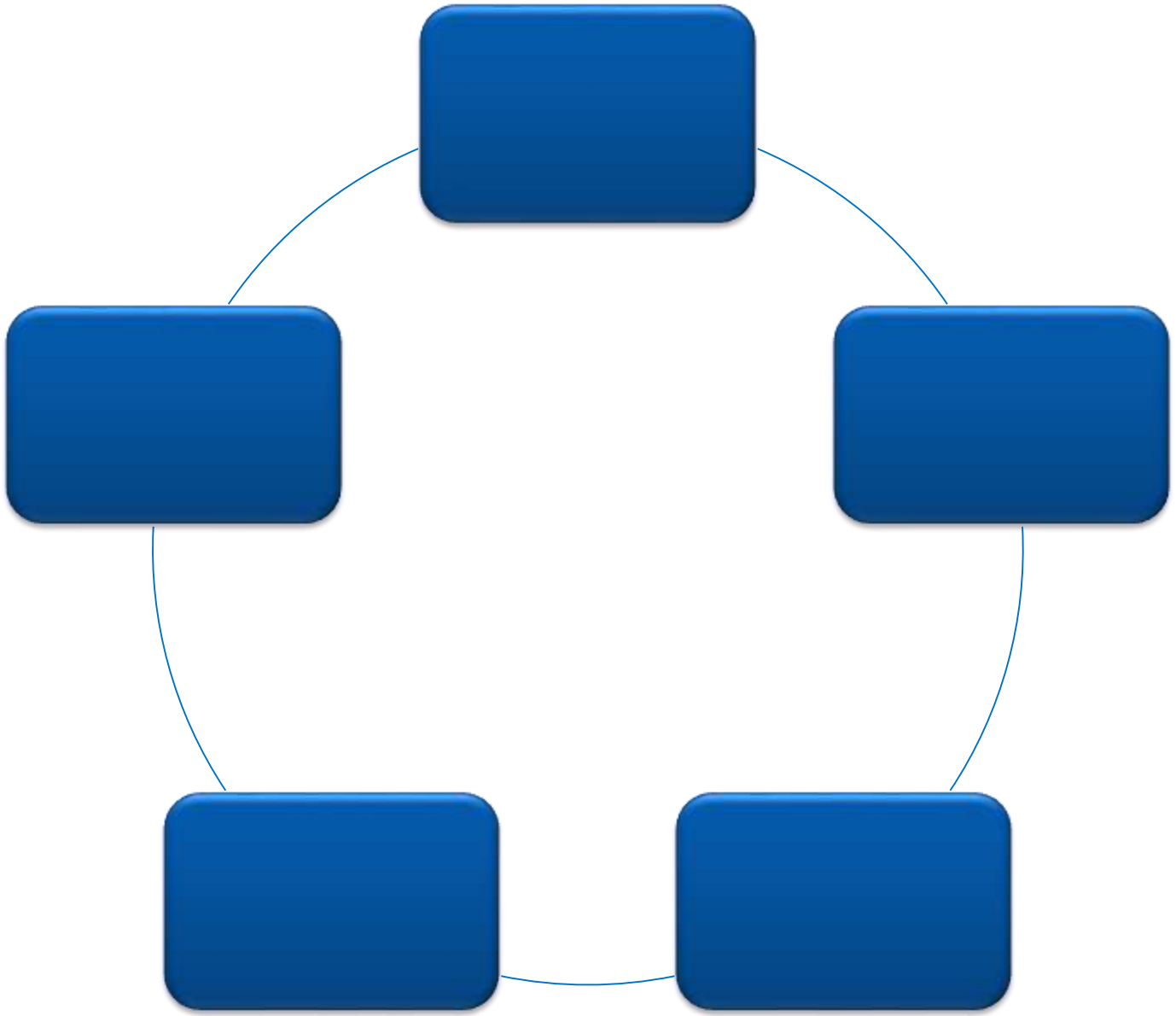
Distributed Database

- 6000 Replica
- 500 Googles needed
- Financal Value: 36 Mrd $
- 40.000.000 Petaflops

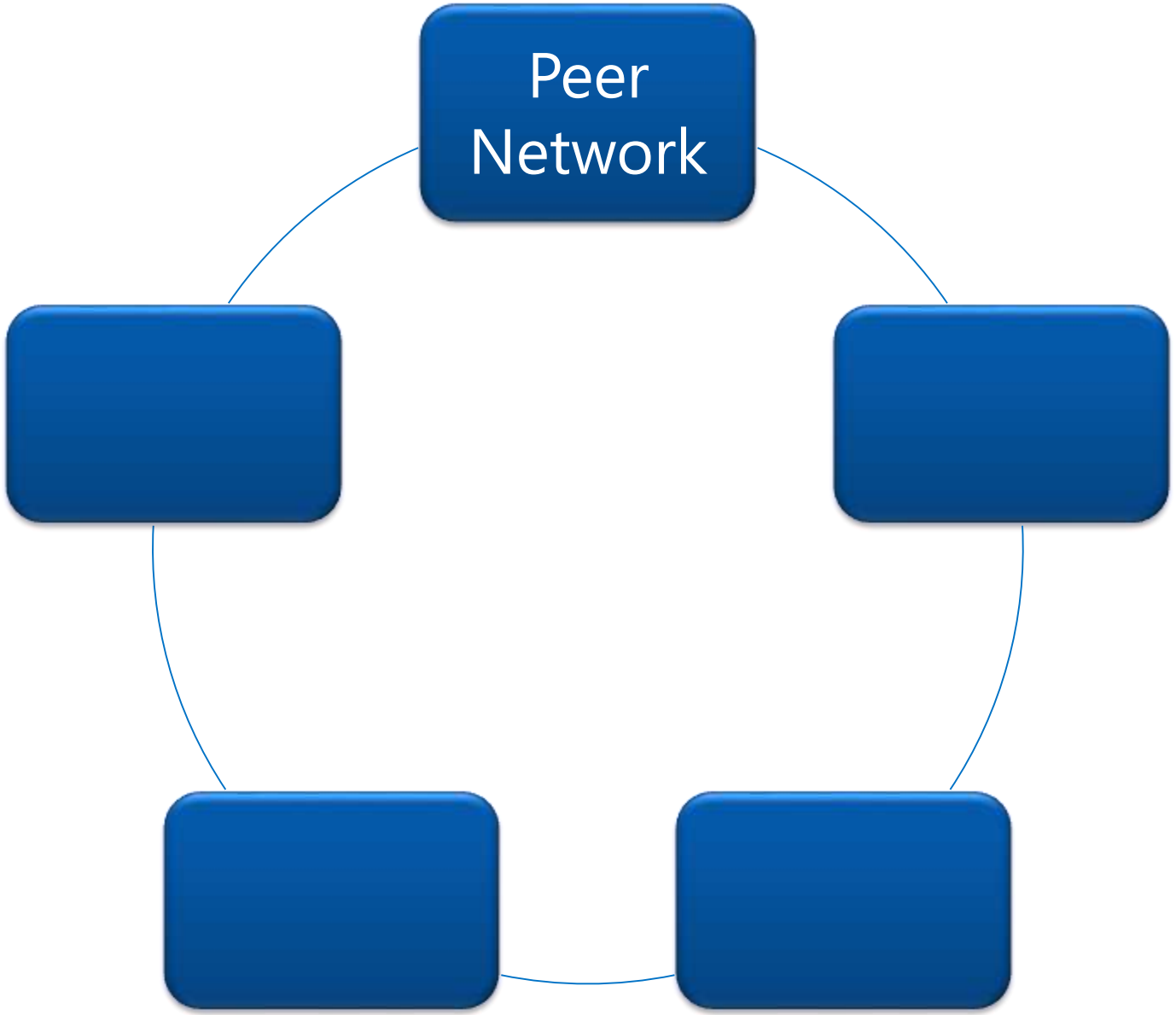
Agenda

- Introduction
- **Block Chain Basics**
- Anonym versus Pseudonym
- Getting Data: The one and the many
- Getting Data: Doing the Power BI

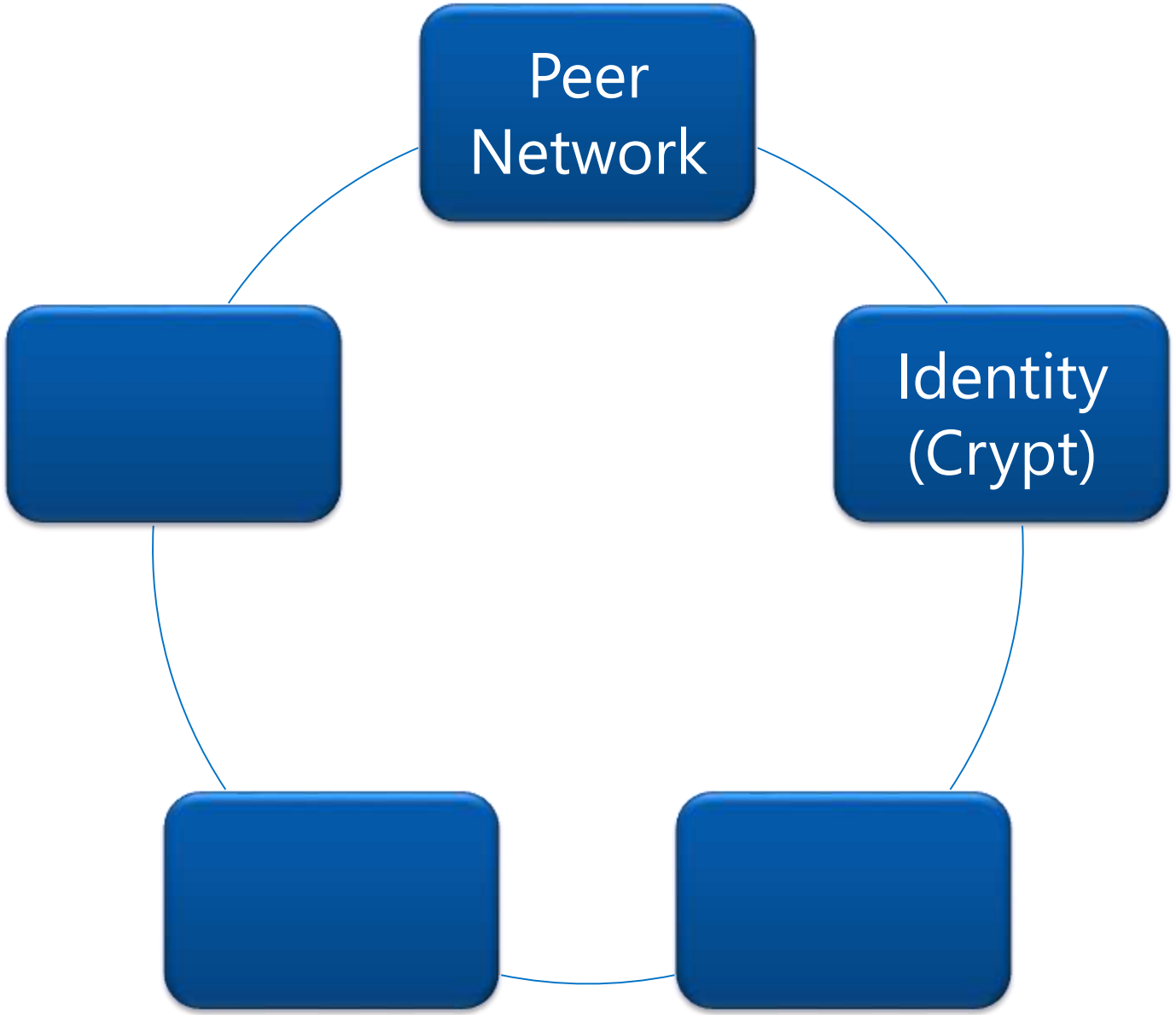
Components



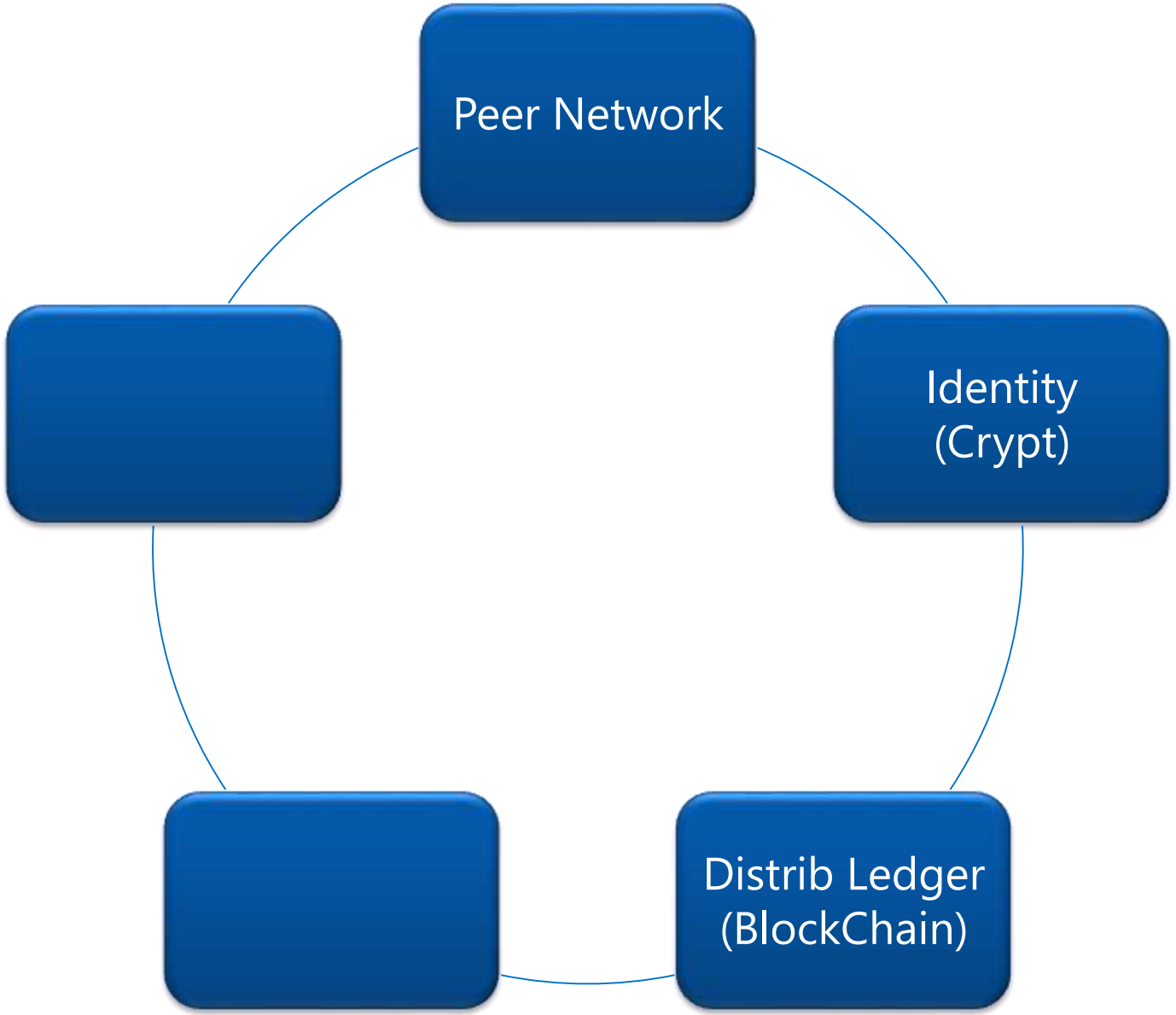
Components



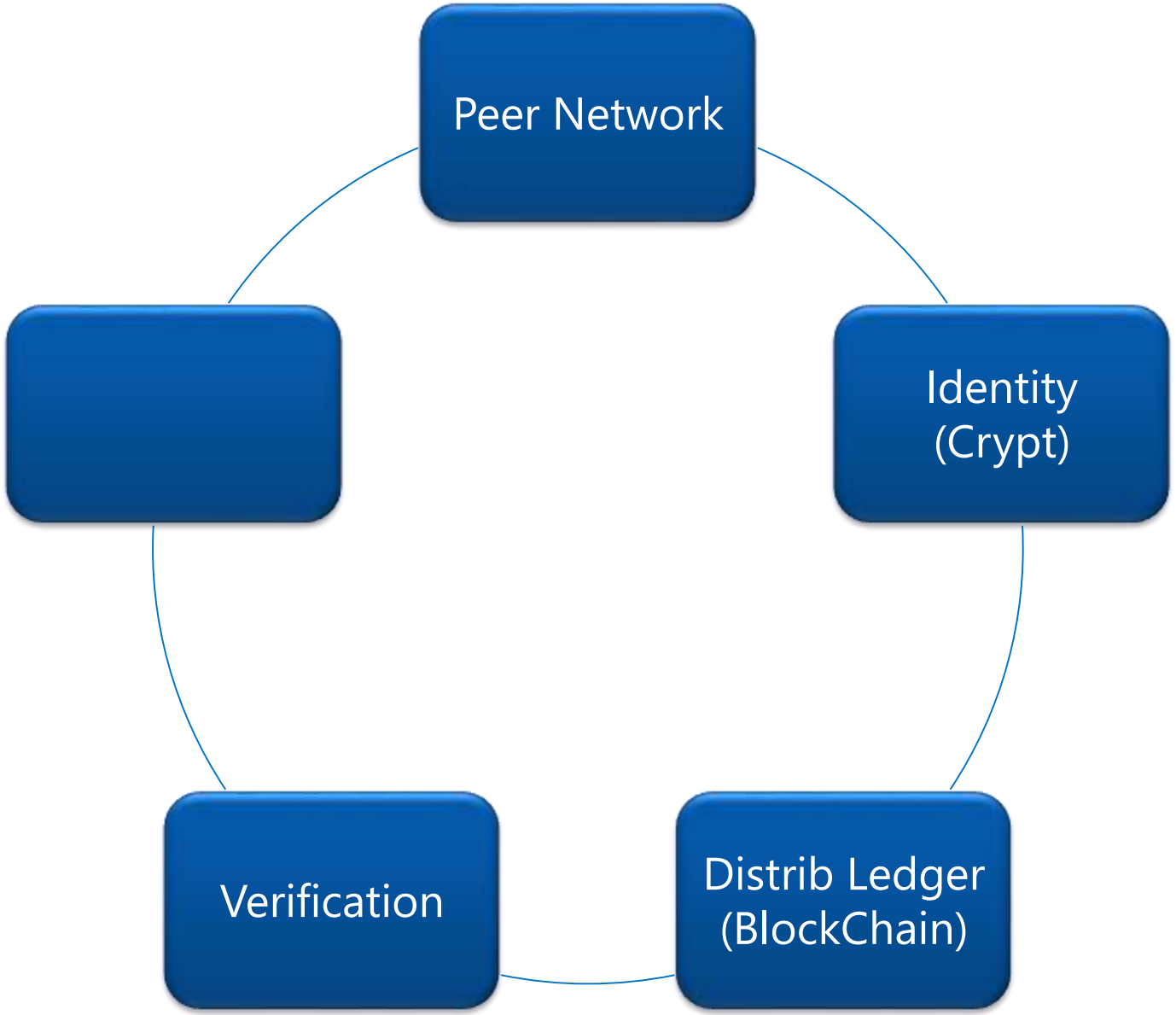
Components



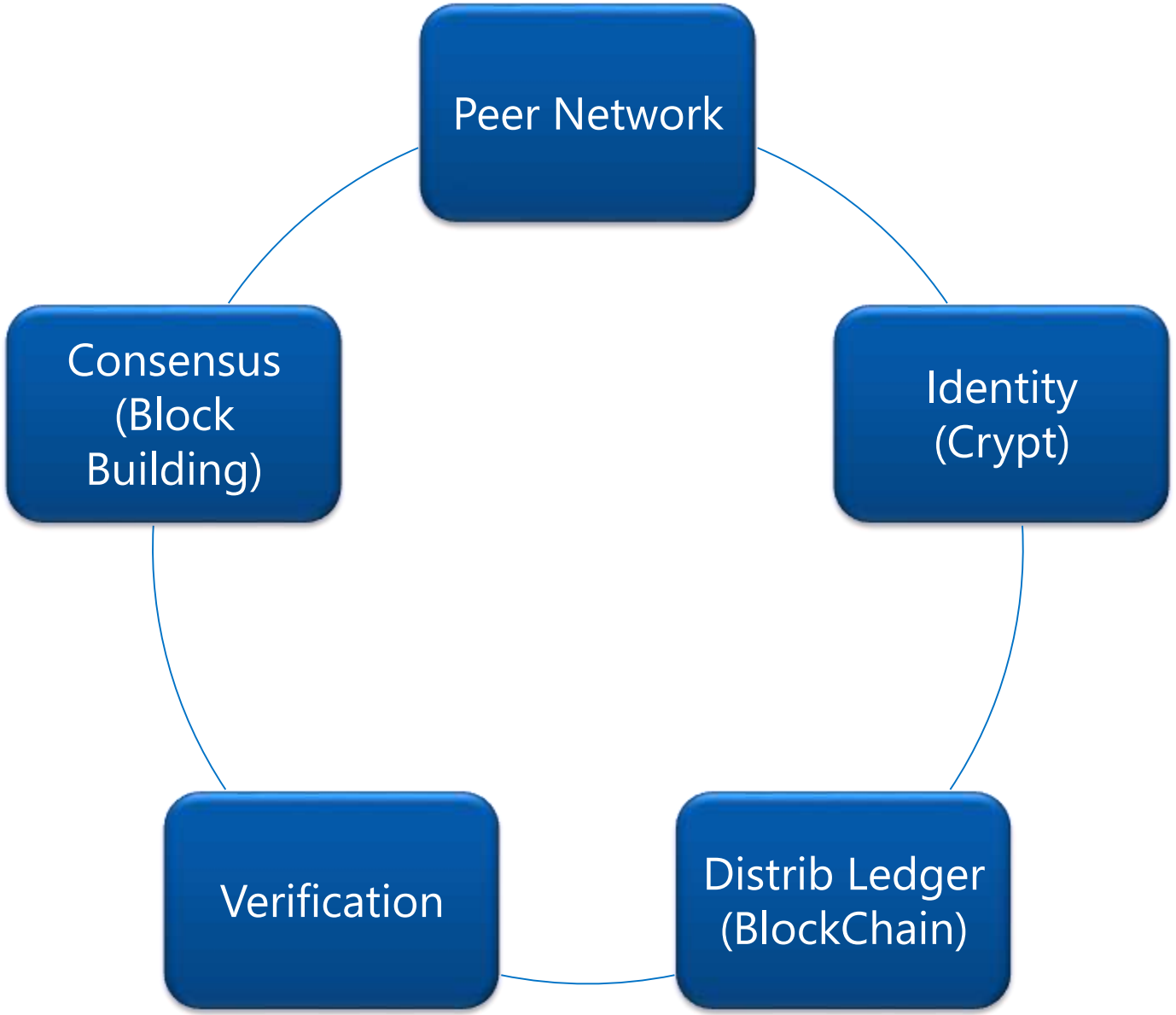
Components



Components


Peer Network
Identity
(Crypt)
Distrib Ledger
(BlockChain)
Verification

Components


Peer Network
Identity (Crypt)
Distrib Ledger (BlockChain)
Verification
Consensus (Block Building)

Money: The two Problems

Counterfeit?

Money: The two Problems

Counterfeit?

Money: The two Problems

Double Spend?

Counterfeit?

Money: The two Problems

Double Spend?

Counterfeit?

Money: The two Problems

Double Spend?

Counterfeit?

Four Eyes Prinicple

Many Eyes Prinicple

Distributed Database

Distributed Database

All Transactions (Spendings)

Distributed Database

All Transactions (Spendings)

BlockChain

Integrity?

Distributed Database
All Transactions (Spendings)
BlockChain

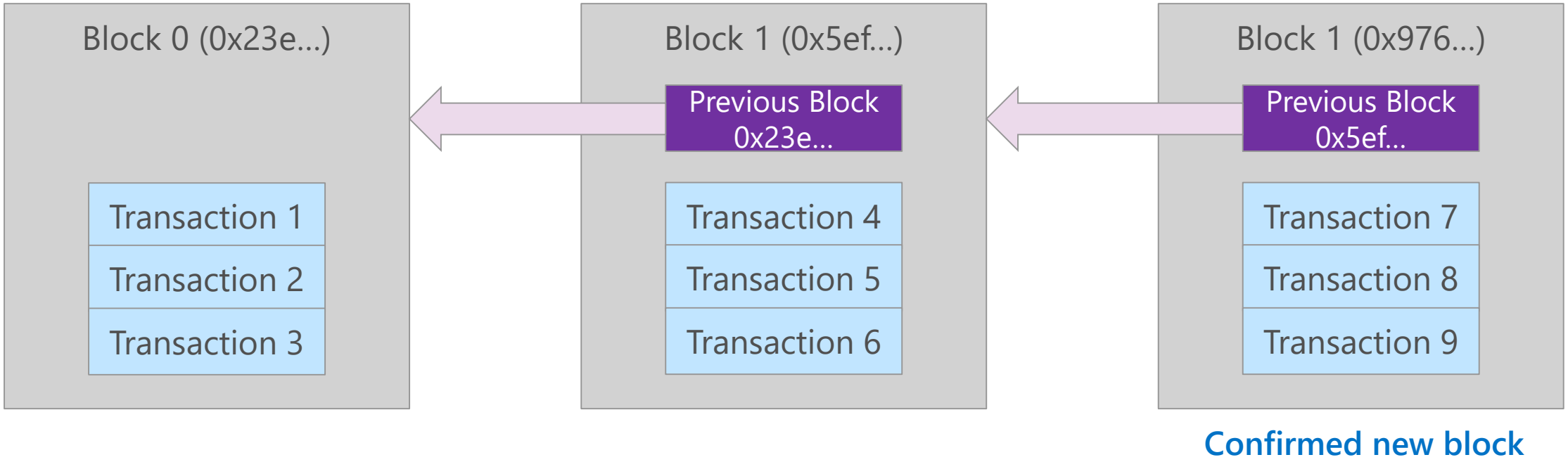
Consensus?

<u>Distributed Database</u>
All Transactions (Spendings)
BlockChain

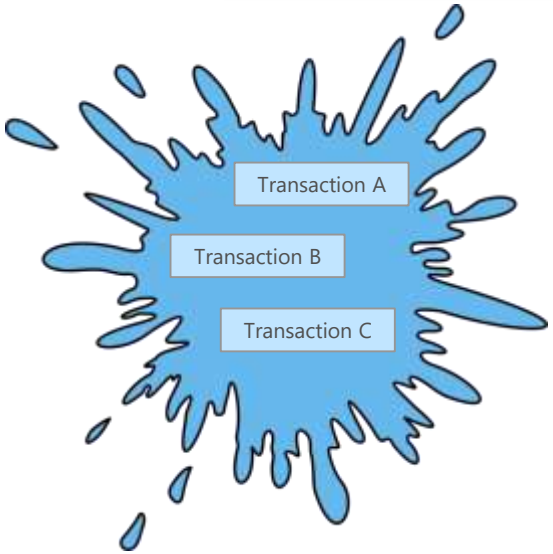
Consensus

Distributed Database
All Transactions (Spendings)
BlockChain

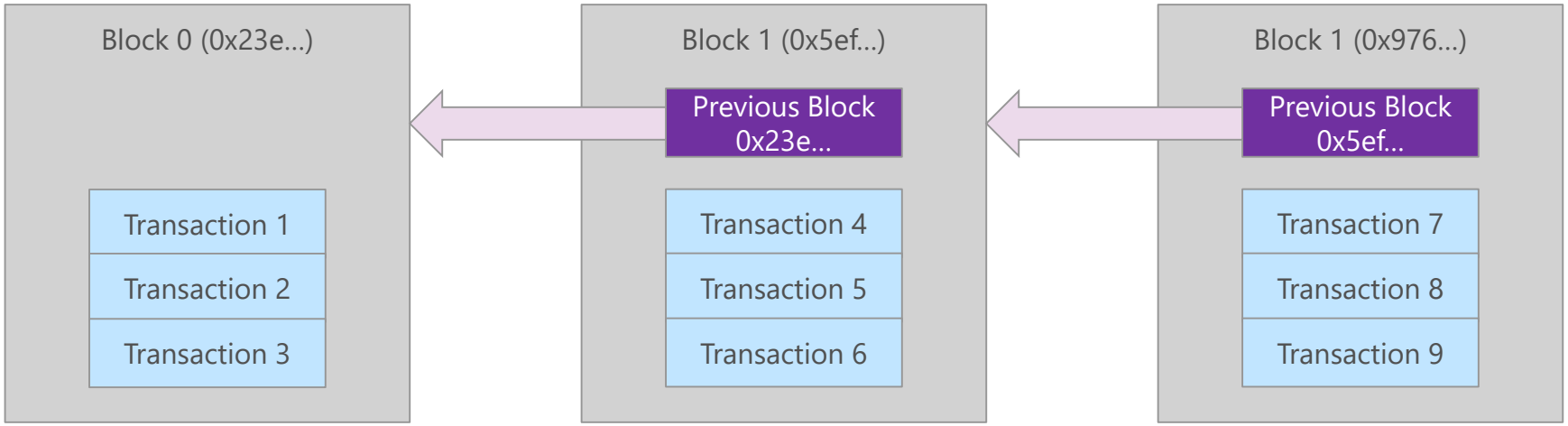
Transactions and Blocks



Transactions and Blocks



Pool



Confirmed new block

Block Building

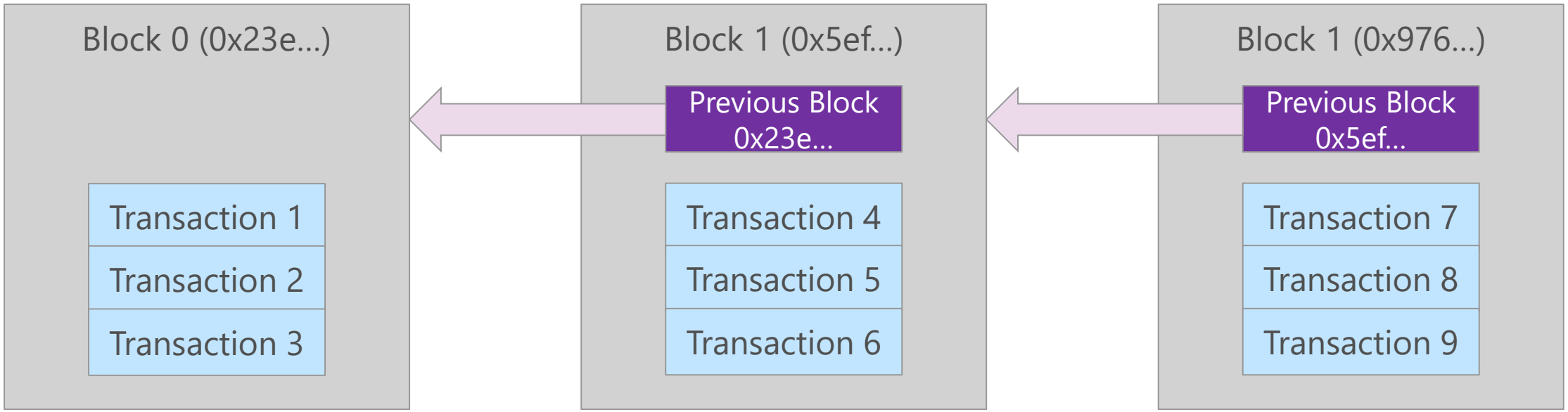
Mining and Consense

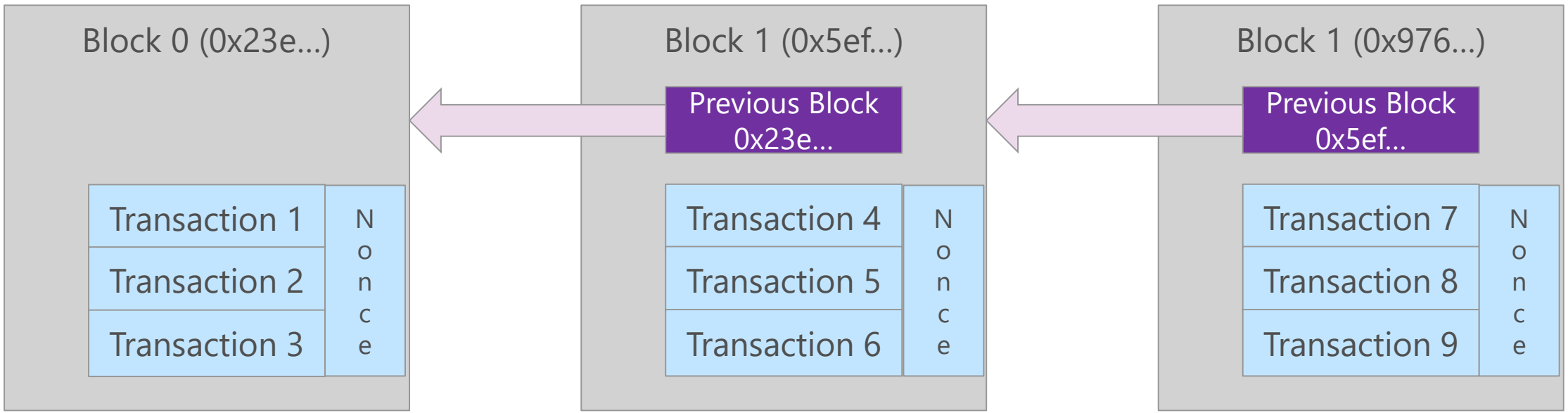
Longest Chain → Get Trans from Pool → Build Block → Find Hash (Mine) → Transmit Block

Block Building

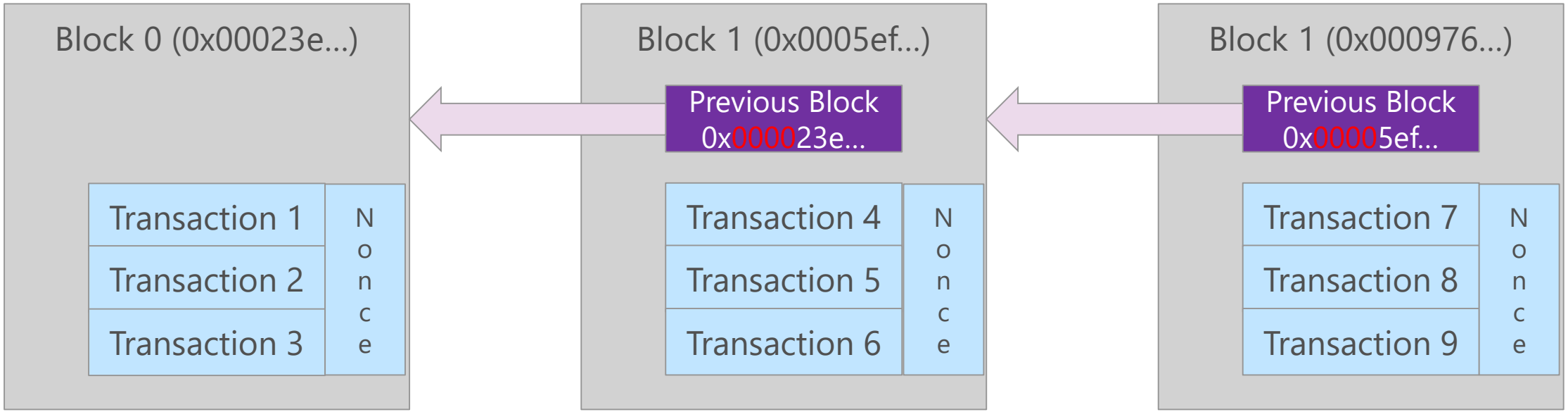
Mining and Consense

Longest Chain → Get Trans from Pool → Build Block → Find Hash (Mine) → Transmit Block

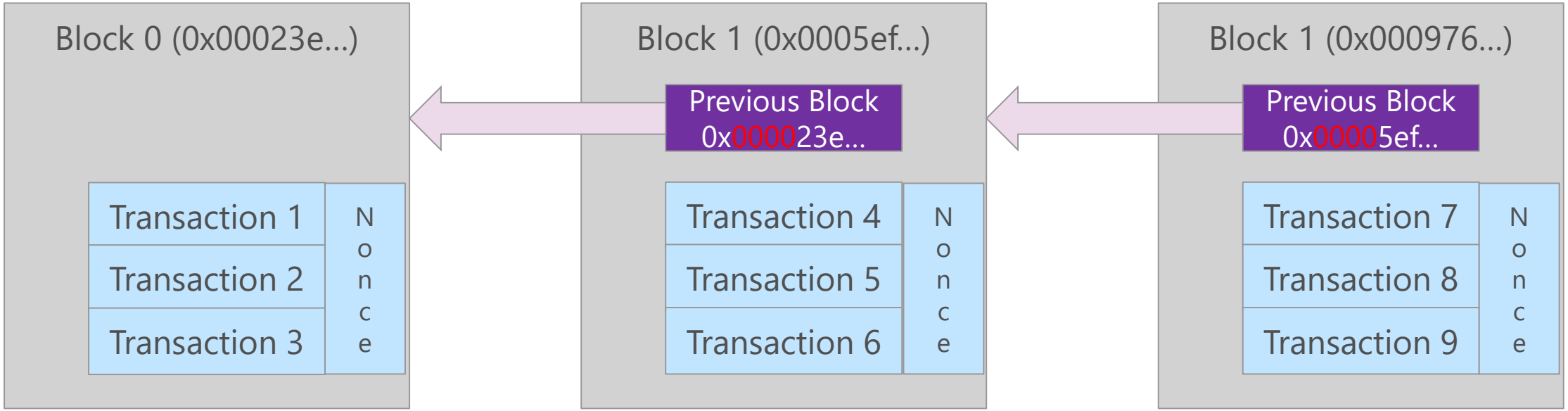

Block 0 (0x23e...)
Transaction 1
Transaction 2
Transaction 3
Block 1 (0x5ef...)
Previous Block 0x23e...
Transaction 4
Transaction 5
Transaction 6
Block 1 (0x976...)
Previous Block 0x5ef...
Transaction 7
Transaction 8
Transaction 9



Confirmed new block


Block 0 (0x00023e...)
Transaction 1
Transaction 2
Transaction 3
Nonce
Block 1 (0x0005ef...)
Previous Block
0x00023e...
Transaction 4
Transaction 5
Transaction 6
Nonce
Block 1 (0x000976...)
Previous Block
0x0005ef...
Transaction 7
Transaction 8
Transaction 9
Nonce

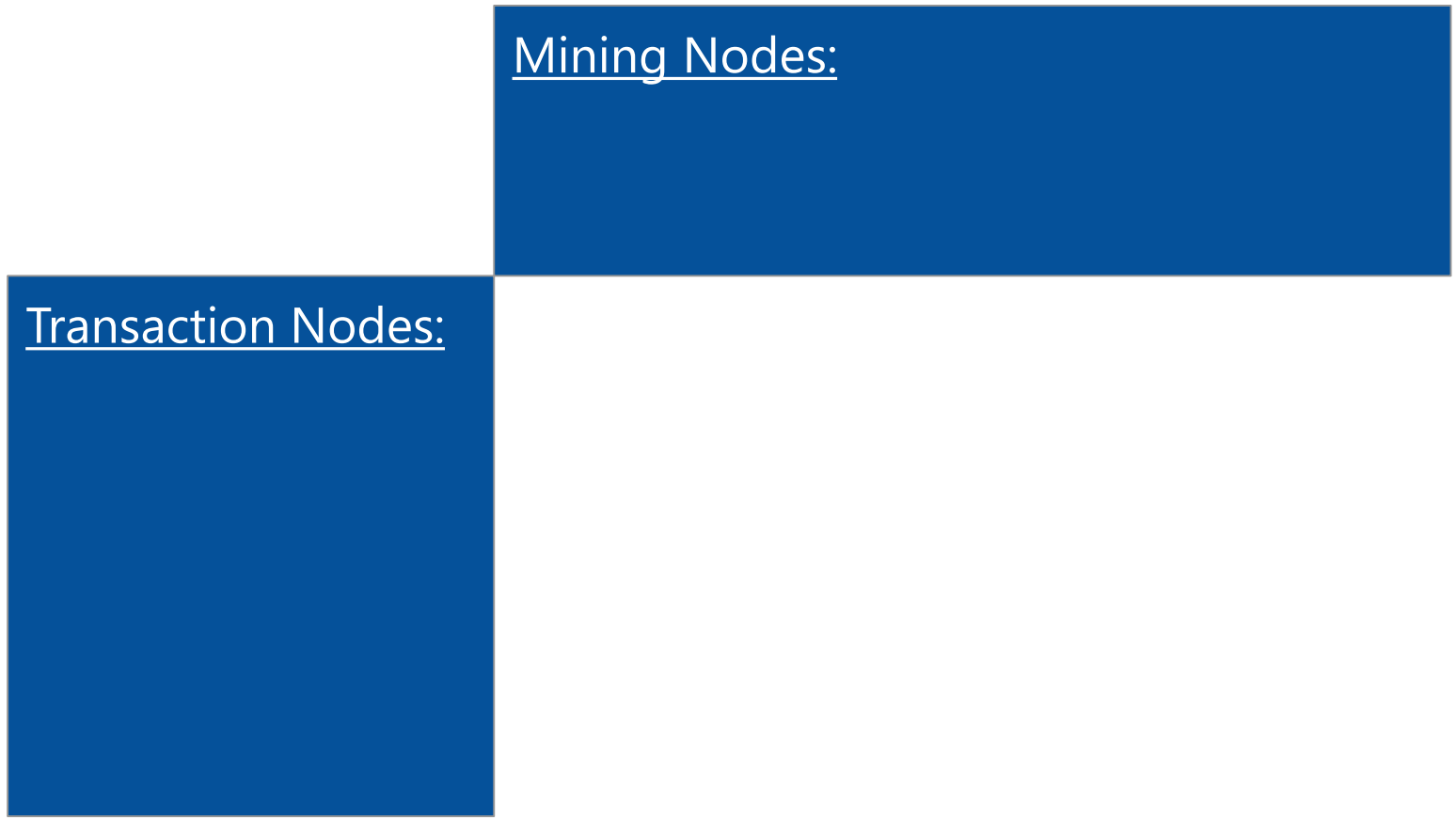
Proof of Work



Consensus and Proof of Work

- Longest Chain wins (Most Work)
- Incentives
- Changing History is very expensive

Node Types



Node Types

Mining Nodes:

Transaction Nodes:

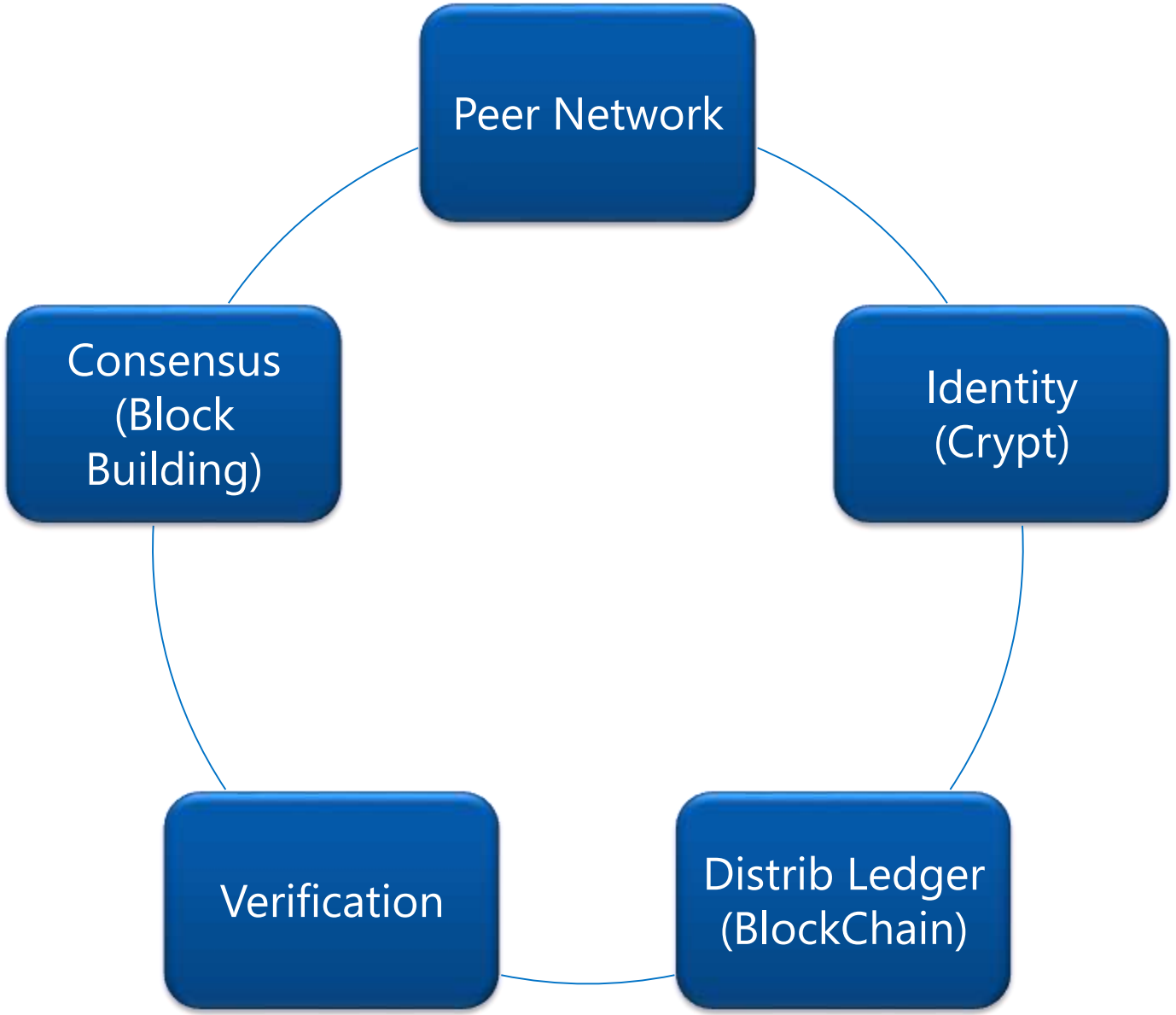
- Look 4 longest Chain
- Watch
- Verify
- Send Transaction

Node Types

Mining Nodes:
- Look 4 longest Chain, …
- Create Blocks
- Earn BitCoin

Transaction Nodes:
- Look 4 longest Chain
- Watch
- Verify
- Send Transaction

Components


Peer Network
Identity (Crypt)
Distrib Ledger (BlockChain)
Verification
Consensus (Block Building)

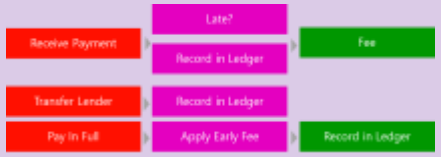

Transition to 2.0

Blockchain 2.0 & Smart Contracts

Contract

Smart Contract Package

Logic

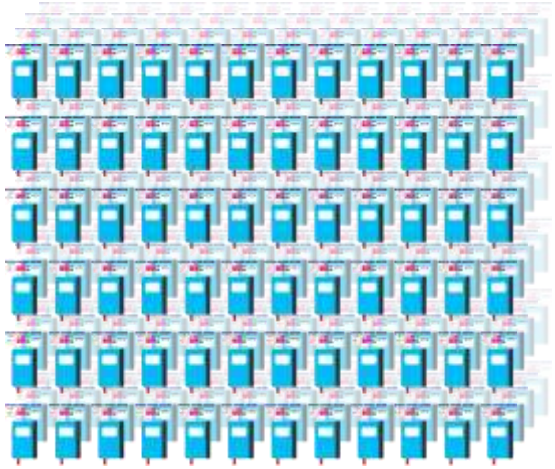


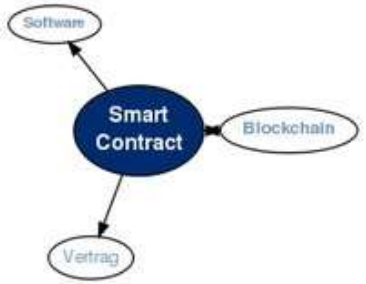
Properties

Ledger

Date	Payment	Late Fee
12/1/2016	$500.00	$0
1/1/2017	$500.00	$0

Deployed to Nodes





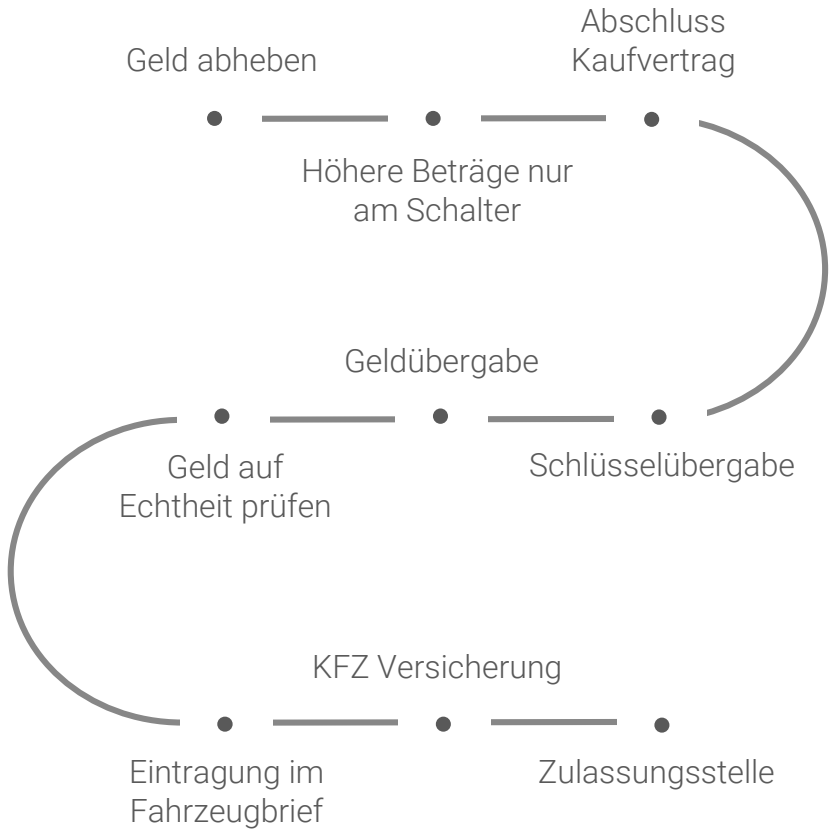
Code

Schema
- State

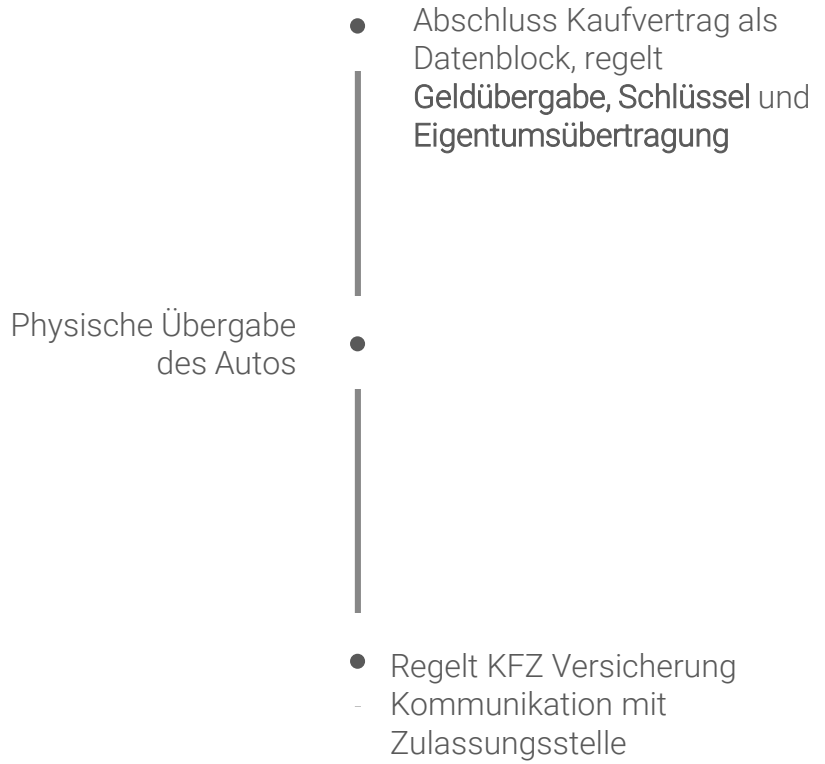
Fixed Entity
- Address

Beispiel: Privater Gebrauchtwagenkauf

STATUS QUO



BLOCKCHAIN



A Summary of Blockchain 1.0 to 2.0 Changes

Blockchain 1.0		Blockchain 2.0	BENEFITS
Bitcoin Blockchain		Ethereum, Corda, Hyperledger, many others yet to come	Not locked into one vendor
Simple Transactions		Generic Contracts	Can handle more complex needs
One Blockchain		Multiple, Linked Blockchains	Can partition information & pick different chains for different needs (location, regulation, speed, privacy, etc.)
Public Only		Public, Private, Consortium, or Domain Specific	Solves many regulatory and privacy needs
Proof of Work Only		Different ways to reach Consensus optimized for need – Proof of Work, Stake, Identity, Vote, etc.	Overcomes some of the existing Blockchain issues such as speed and computational cost
Always Open & Distributed		User Choice	Craft blockchain solutions around the business needs

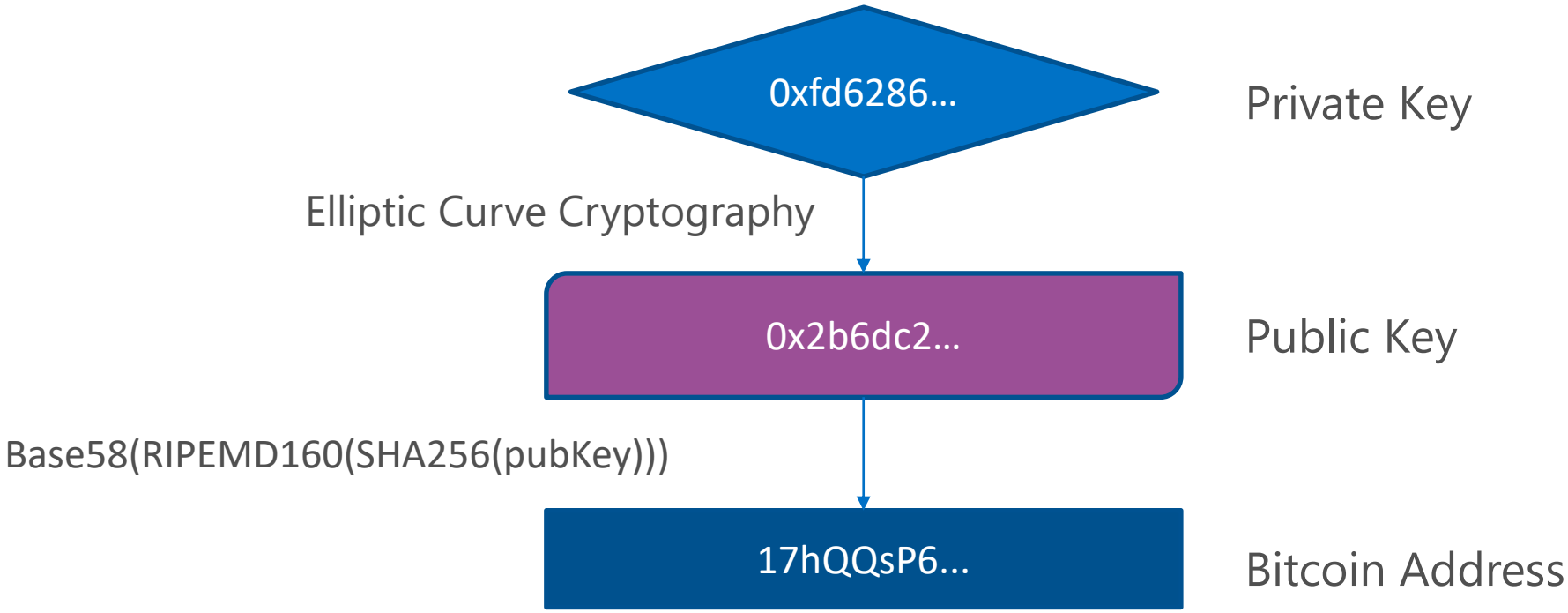
Challenges


Legislation/
Governance
Technical:
• Energy
• Transactions
Business Cases

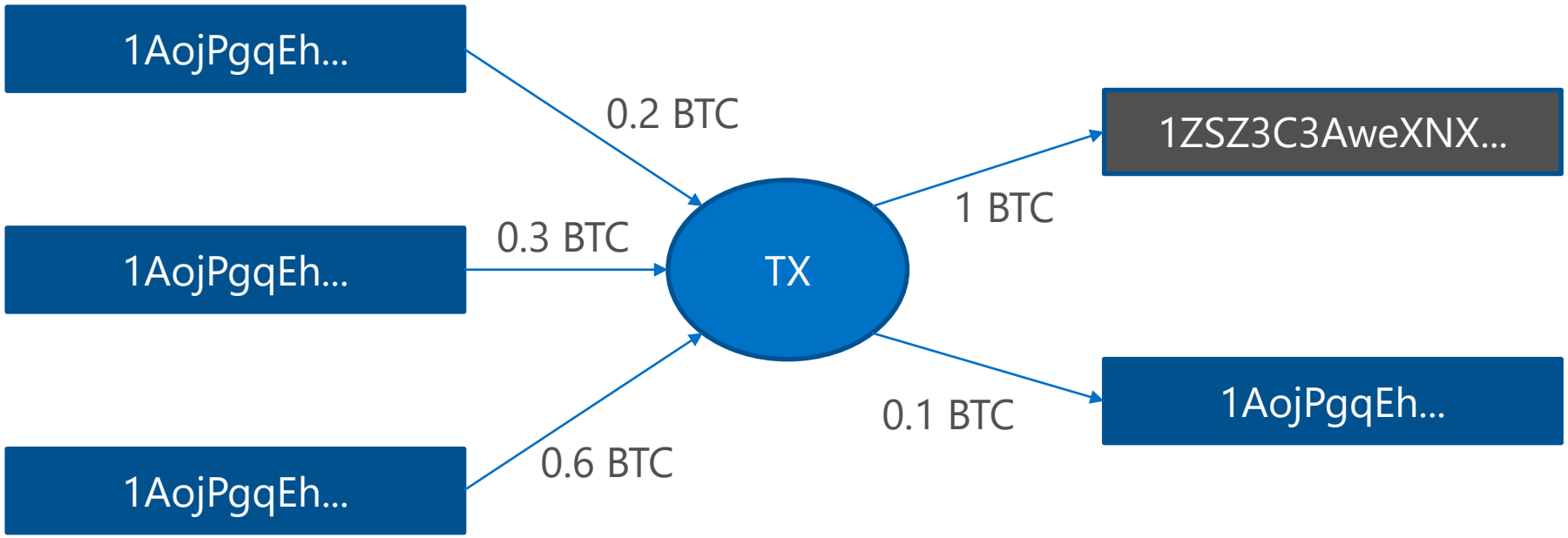
Agenda

- Introduction
- Block Chain Basics
- **Anonym versus Pseudonym**
- Getting Data: The one and the many
- Getting Data: Doing the Power BI

Wie eine Bitcoin Adresse zustande kommt



Eine Bitcoin Transaktion



1AojPgqEh...

1AojPgqEh...

0.2 BTC

1AojPgqEh...

0.3 BTC

TX

1 BTC

1ZSZ3C3AweXNX...

0.1 BTC

1AojPgqEh...

1AojPgqEh...

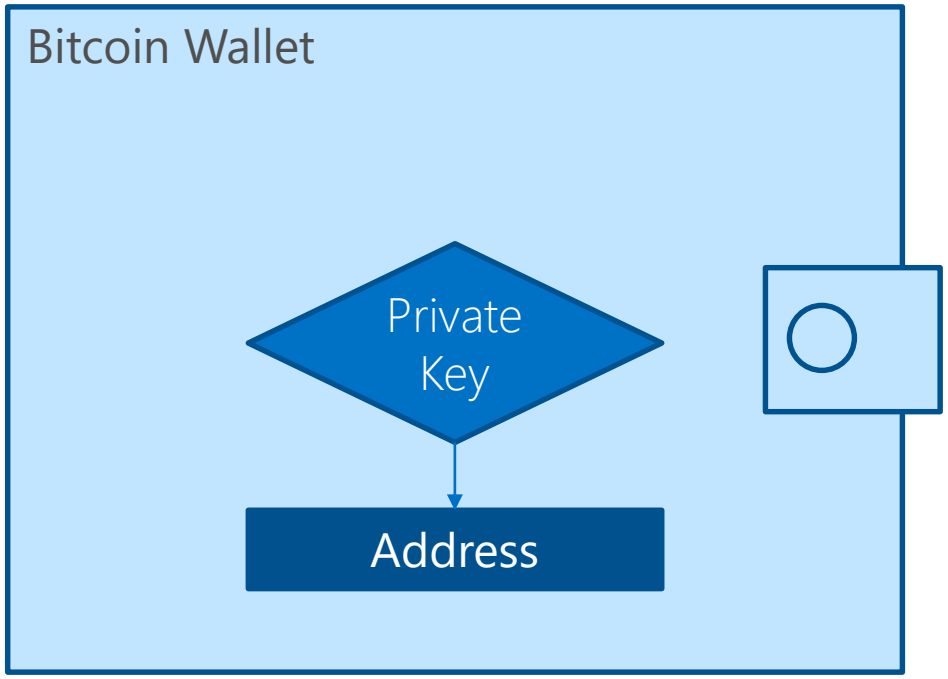
0.6 BTC

Wiederverwendung von Bitcoin Adressen verrät viel über meine Transaktionen.

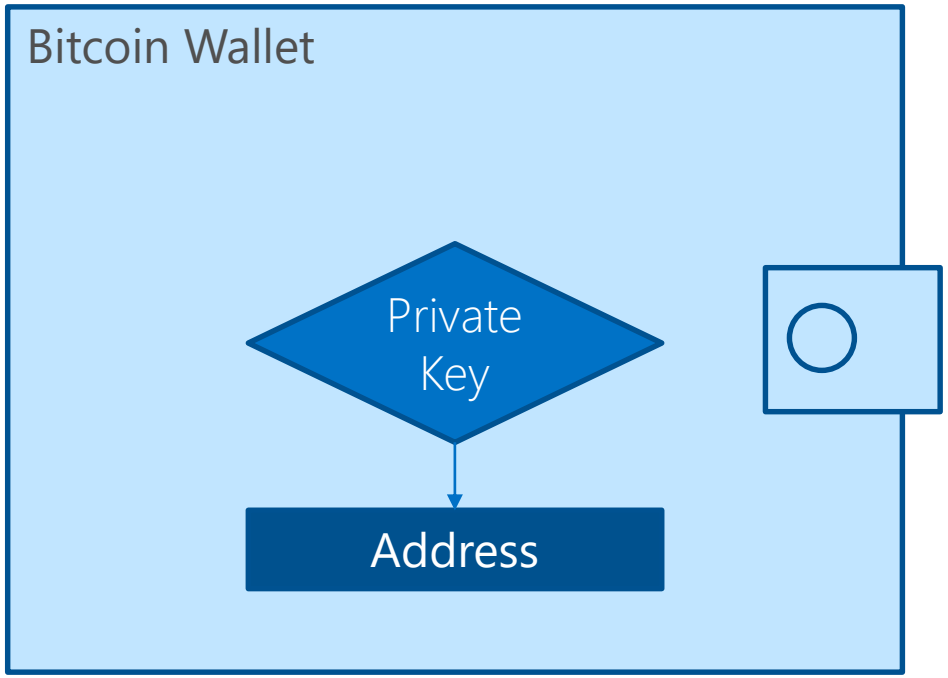
Agenda

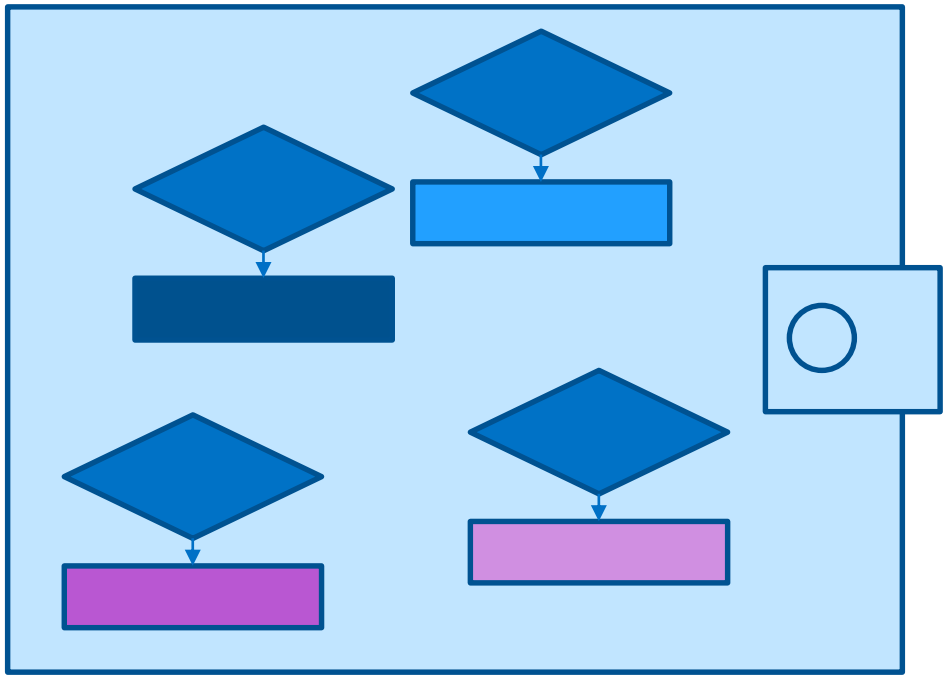
- Introduction
- Block Chain Basics
- Anonym versus Pseudonym
- **Getting Data: The one and the many**
- Getting Data: Doing the Power BI

Bitcoin Wallet

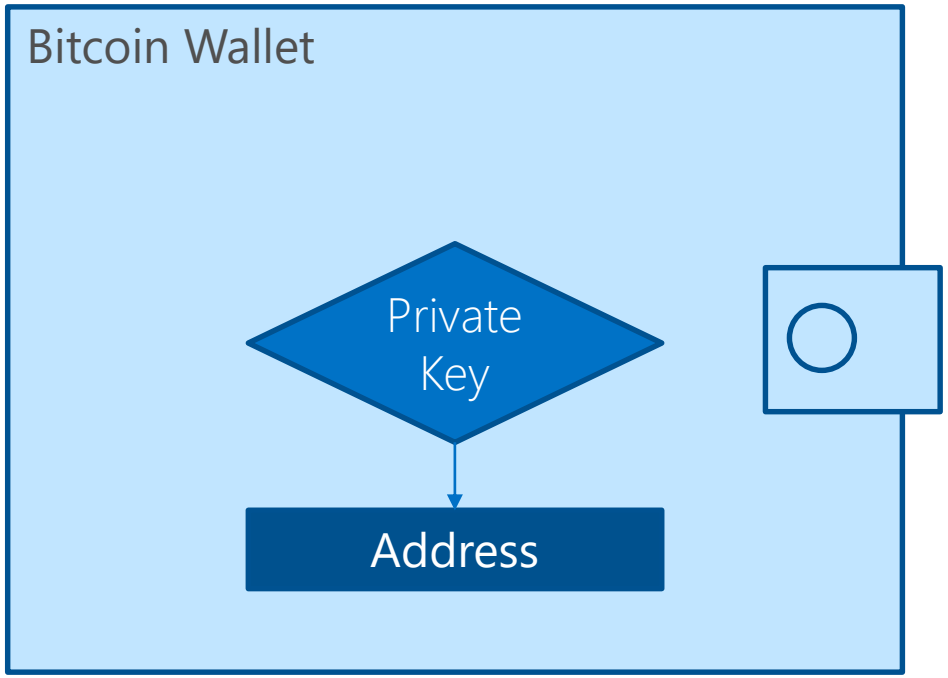


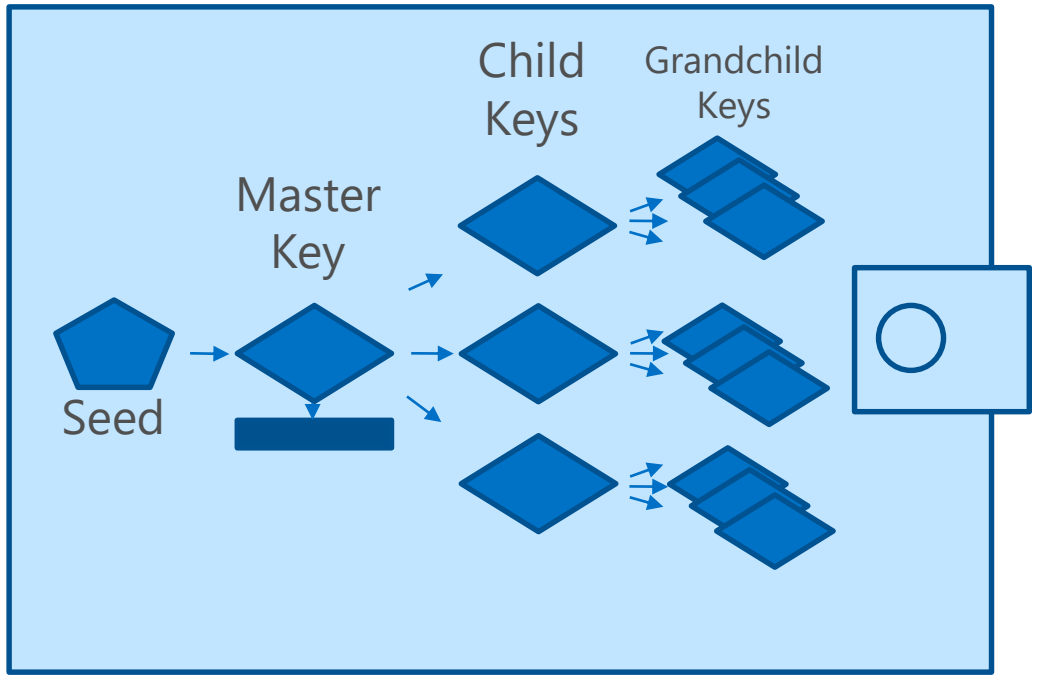
Wallets mit mehreren Adressen



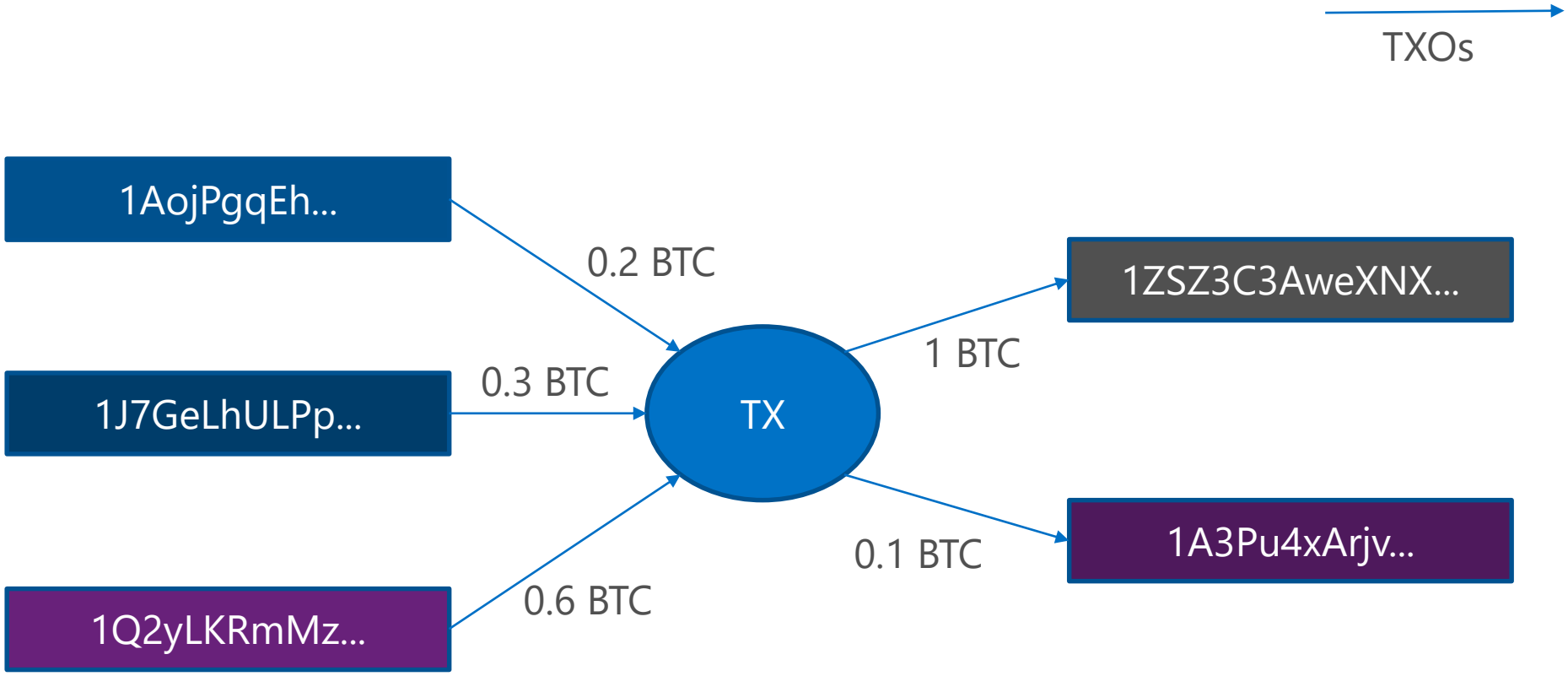


Deterministic Wallets



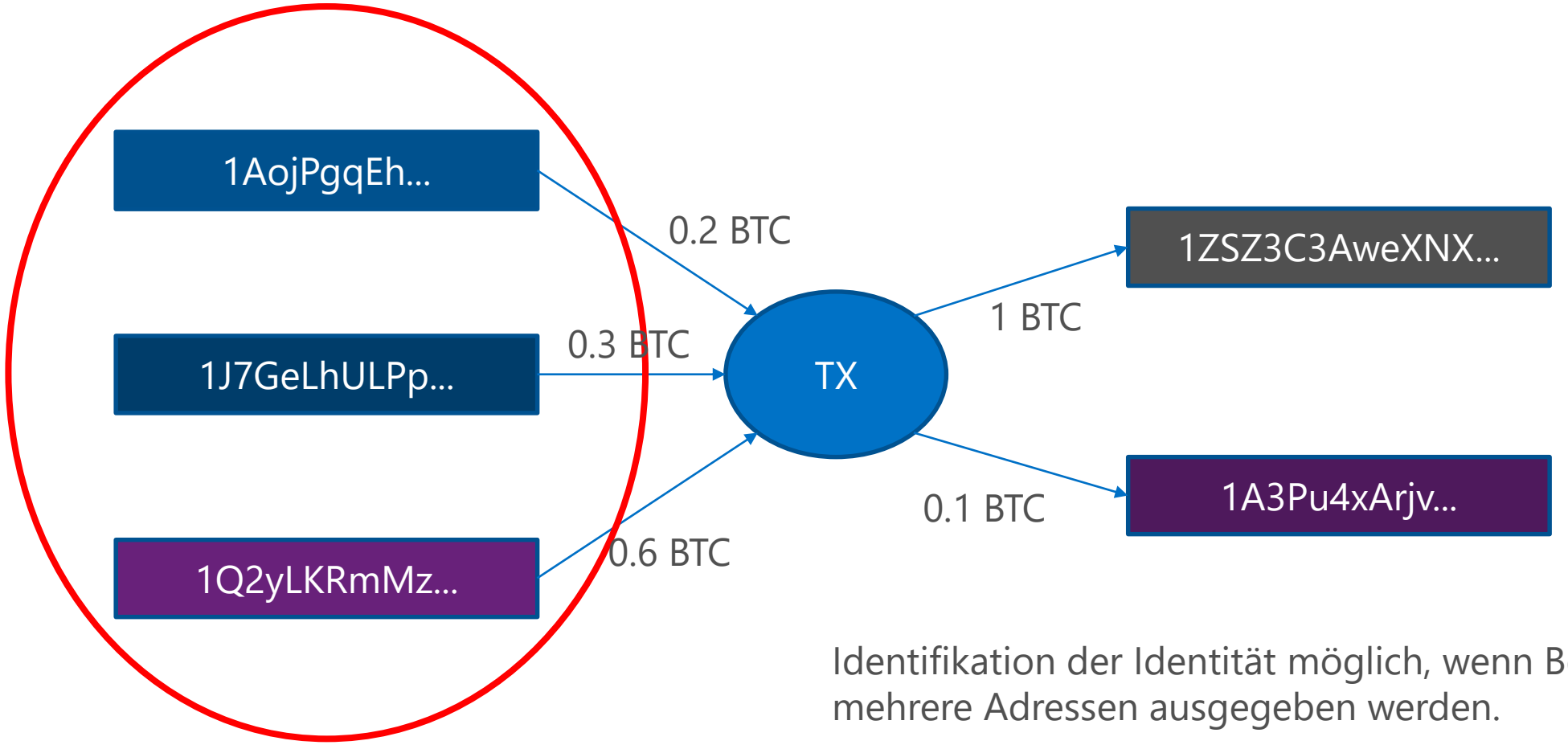


BTC TX / Verwendung mehrerer Adressen



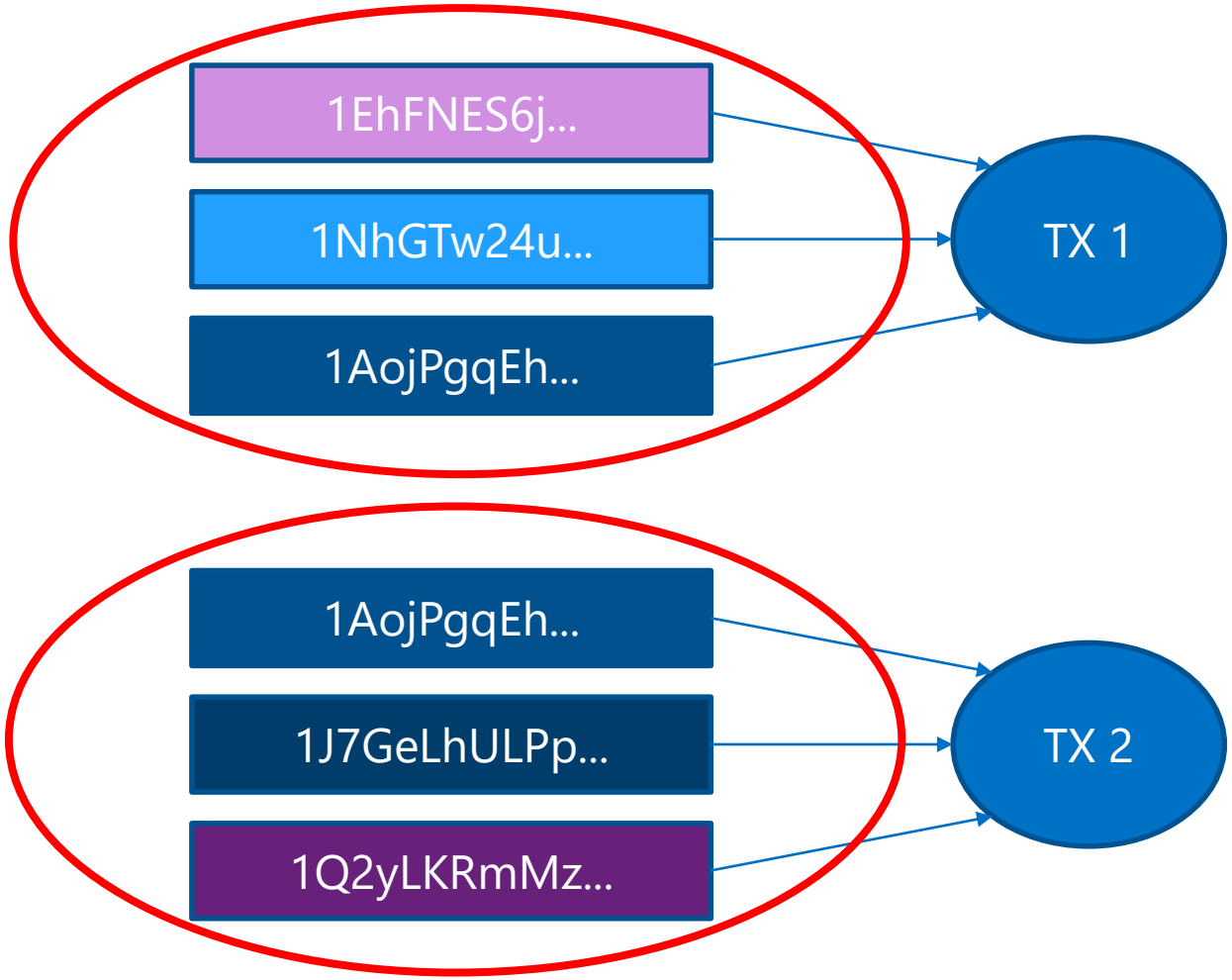
Bitcoin Adressen sollten nur ein mal verwendet werden.

Gemeinsame Signierung der Inputs

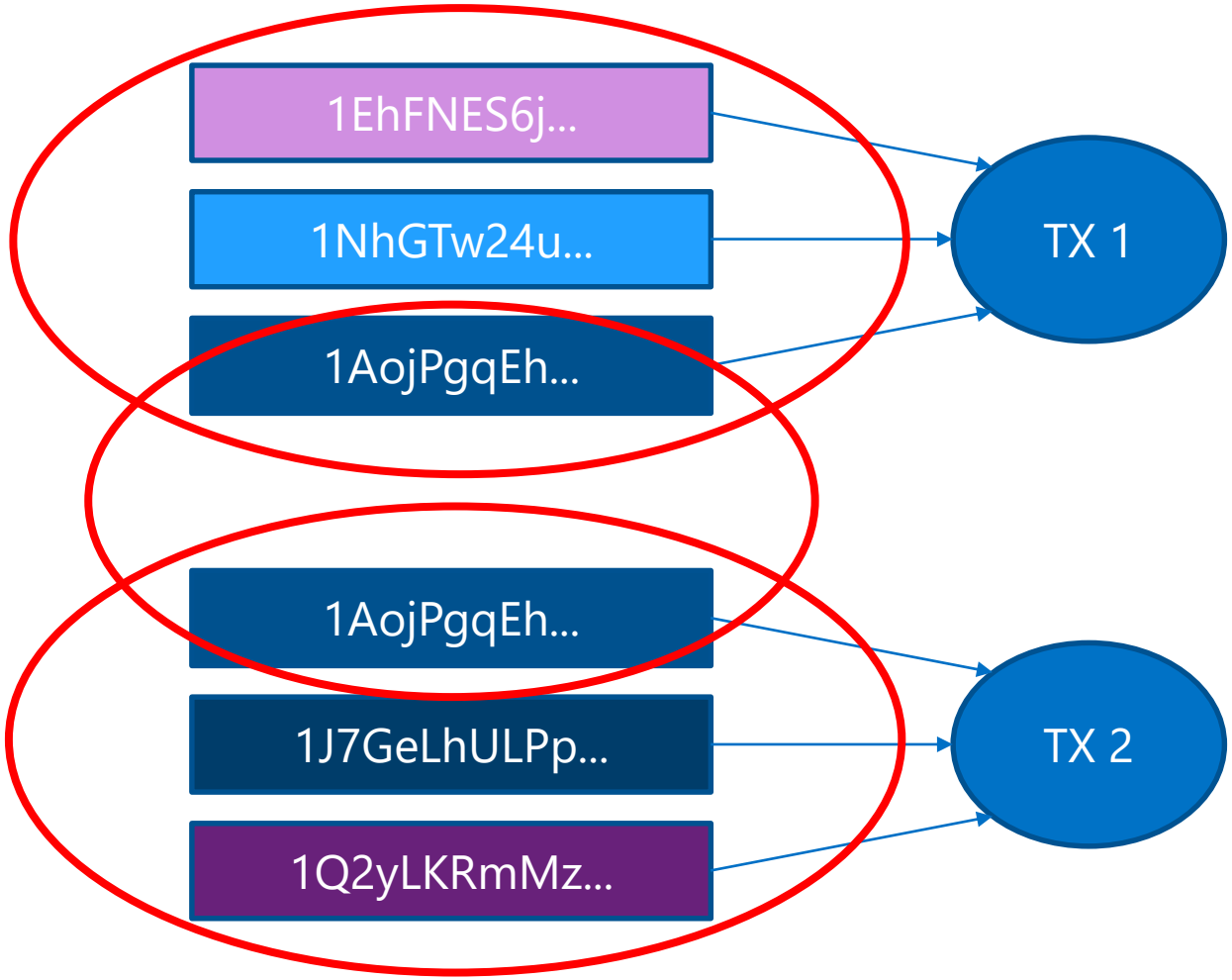


Identifikation der Identität möglich, wenn Beträge von mehrere Adressen ausgegeben werden.

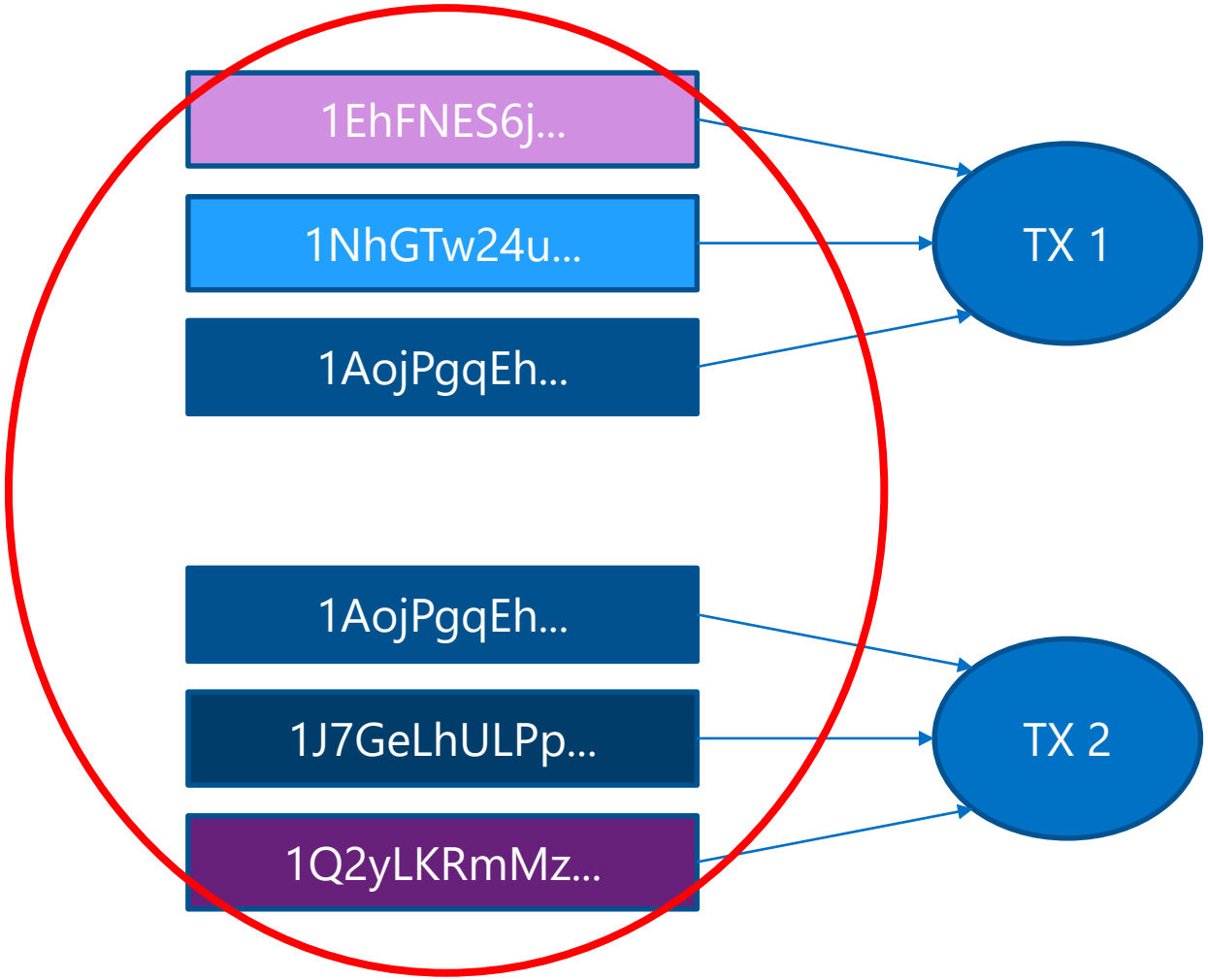
Gemeinsame Signierung der Inputs



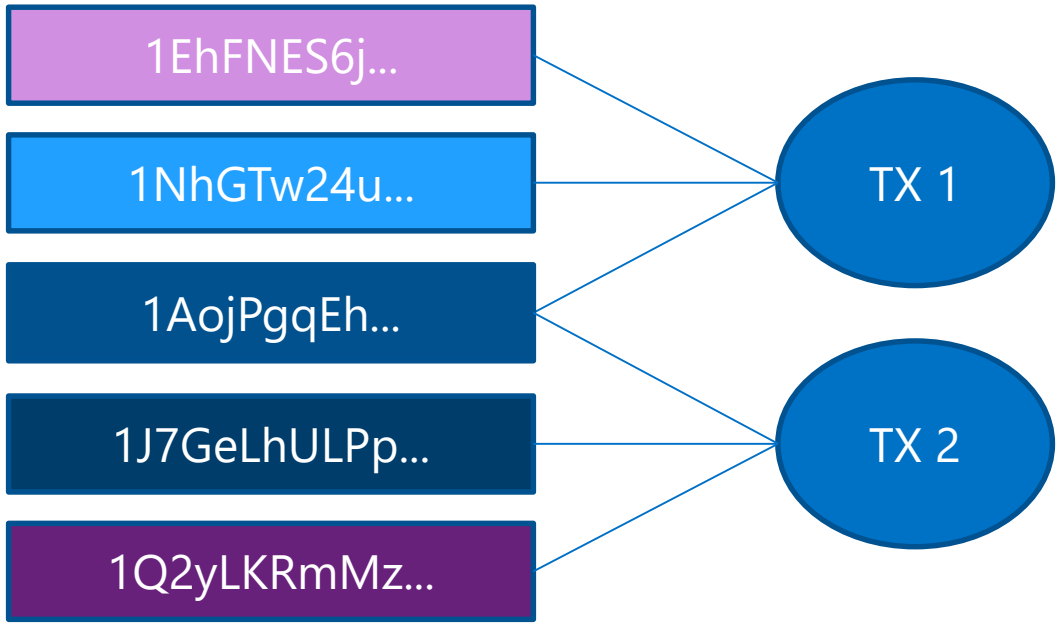
Gemeinsame Signierung der Inputs

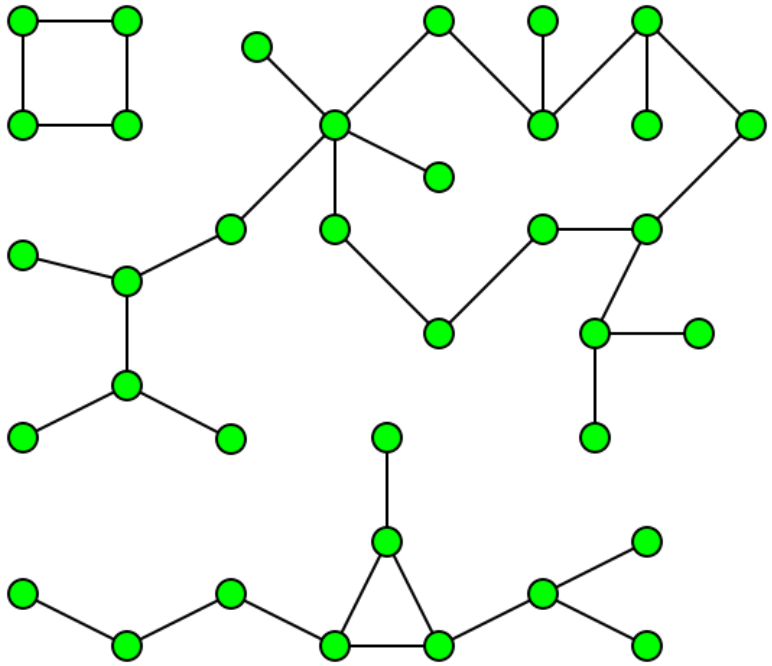


Gemeinsame Signierung der Inputs

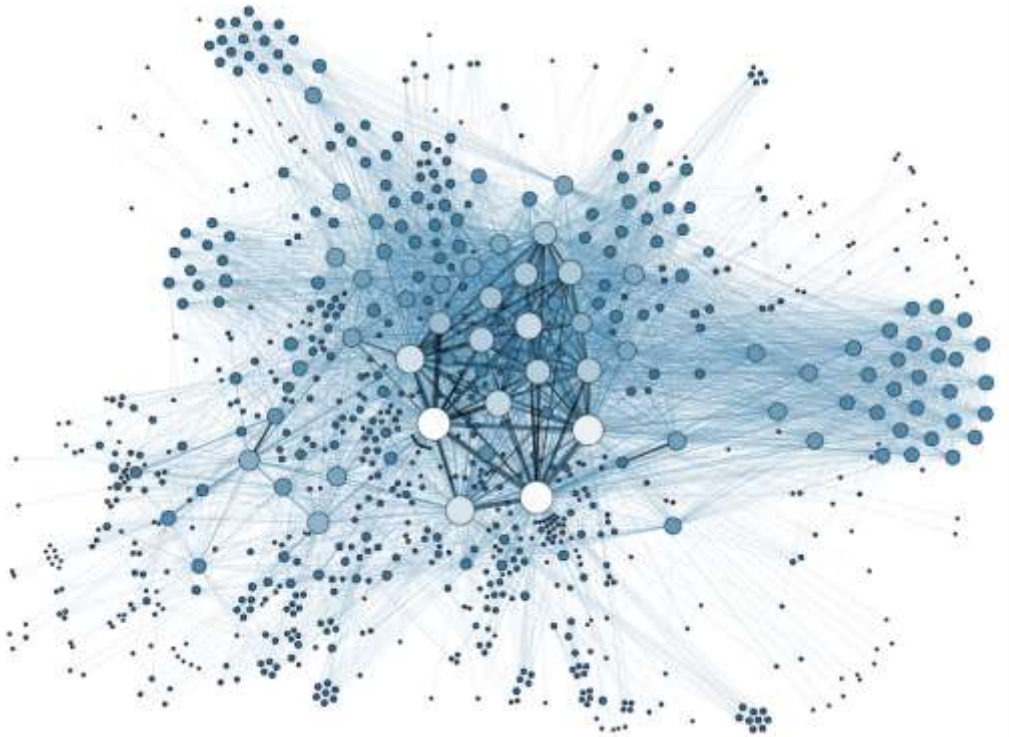


Graphentheorie: Zusammenhängende Komponenten



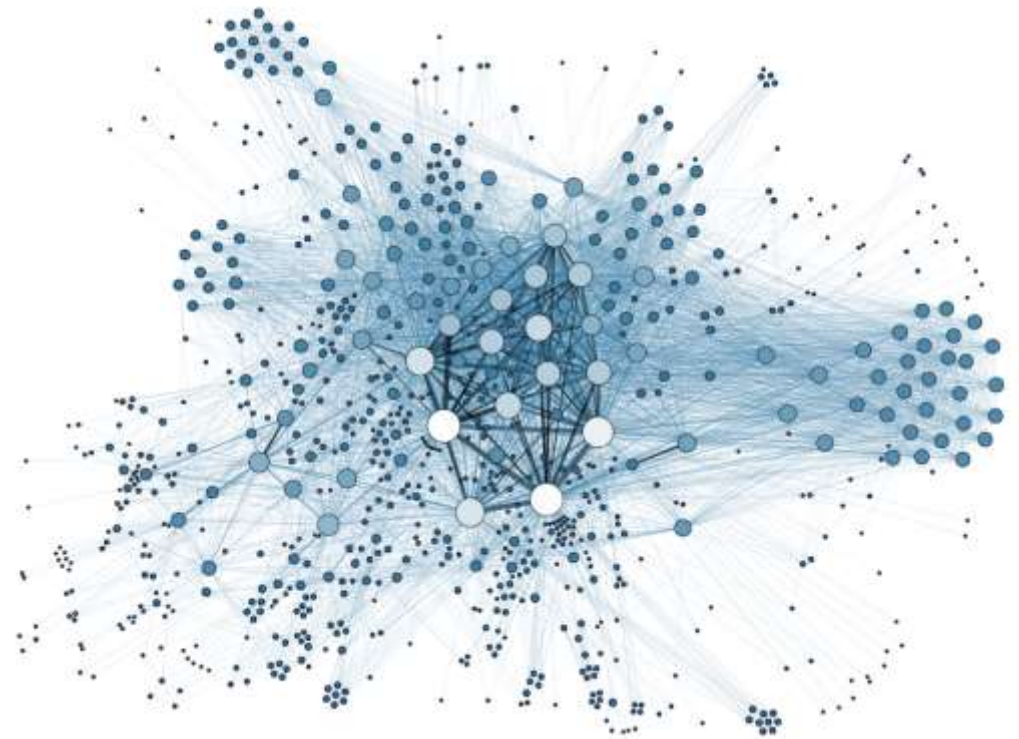


Idee



Neo4J

Exkurs



Edges

Nodes

Relations Part of Data

IsFriend

PersonID1	PersonID2
…	…
N	M
N	L
…	…

PersonID	Name
…	…
N	Peter
…	…

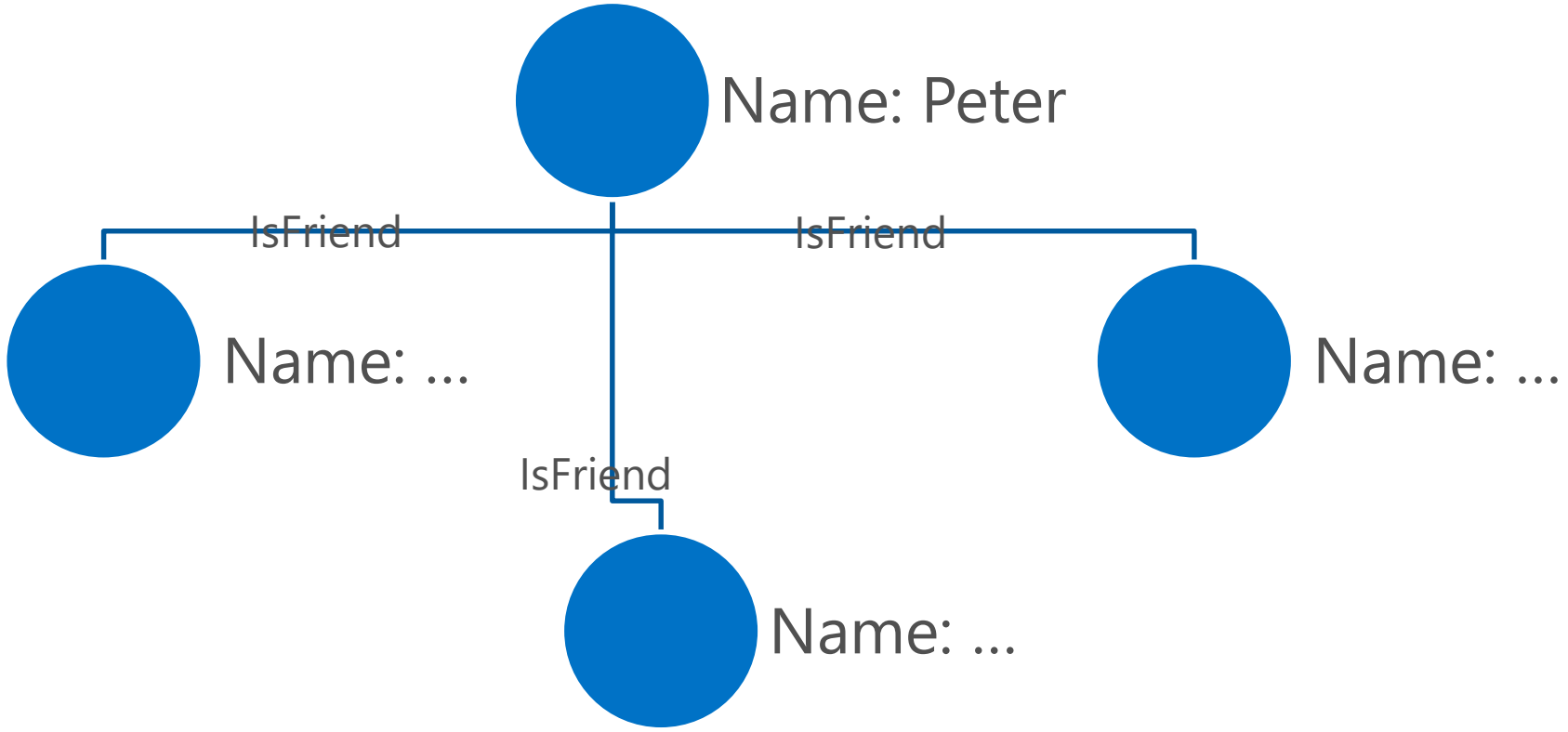
Find Peters friends …

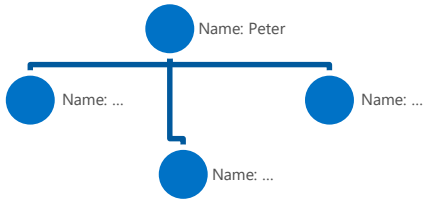
PersonID	Name
…	…
N	Peter
…	…

IsFriend

PersonID1	PersonID2
…	…
N	M
N	L

- Row „Peter“ (Index, O(log n))
- ID Peter (O(1))
- Rows in IsFriend with N (Index, O(log x))
- PersonID2 s(O(k))
- PersonID s (Index O(k log n))
- Names (O(k))

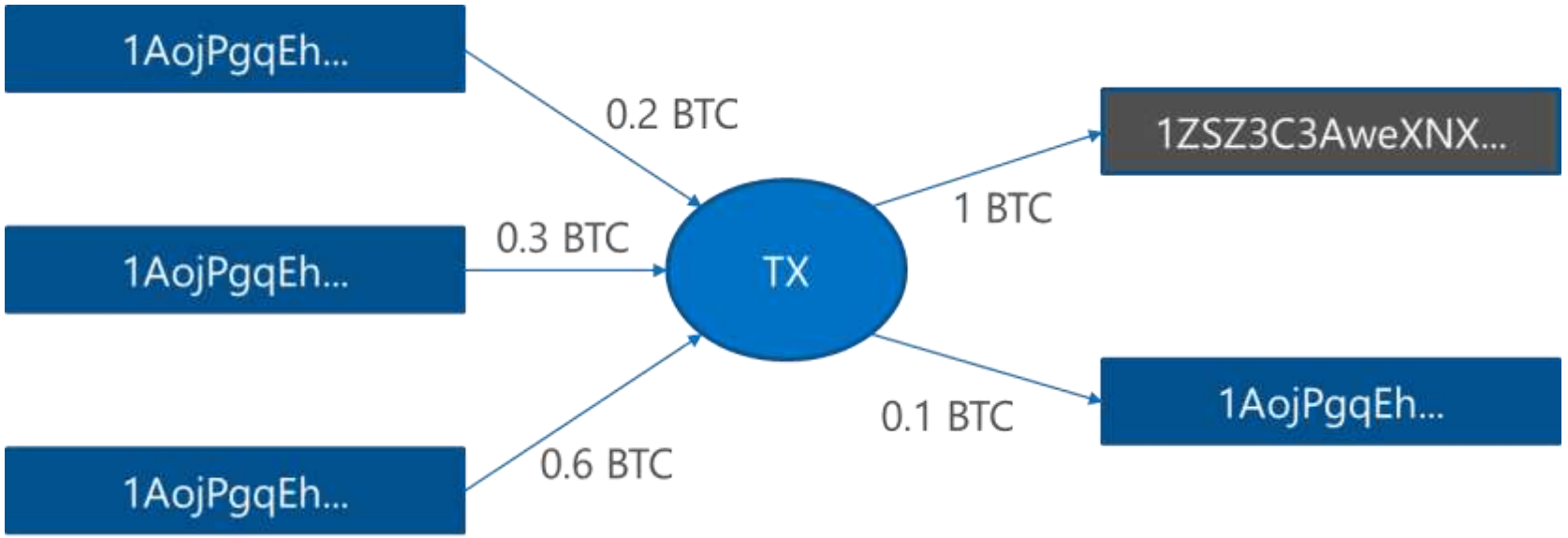

Name: Peter
IsFriend
IsFriend
Name: ...
Name: ...
IsFriend
Name: ...



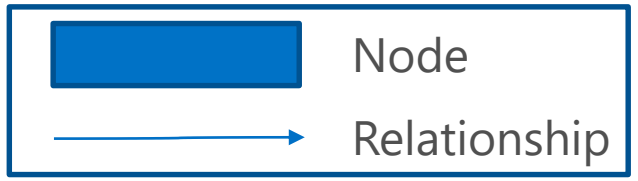
- Node „Peter“ (Index, O(log n))
- IsFriend edges (O(k+x))
- Nodes on ends of edges(O(k))
- Names (O(k * y))

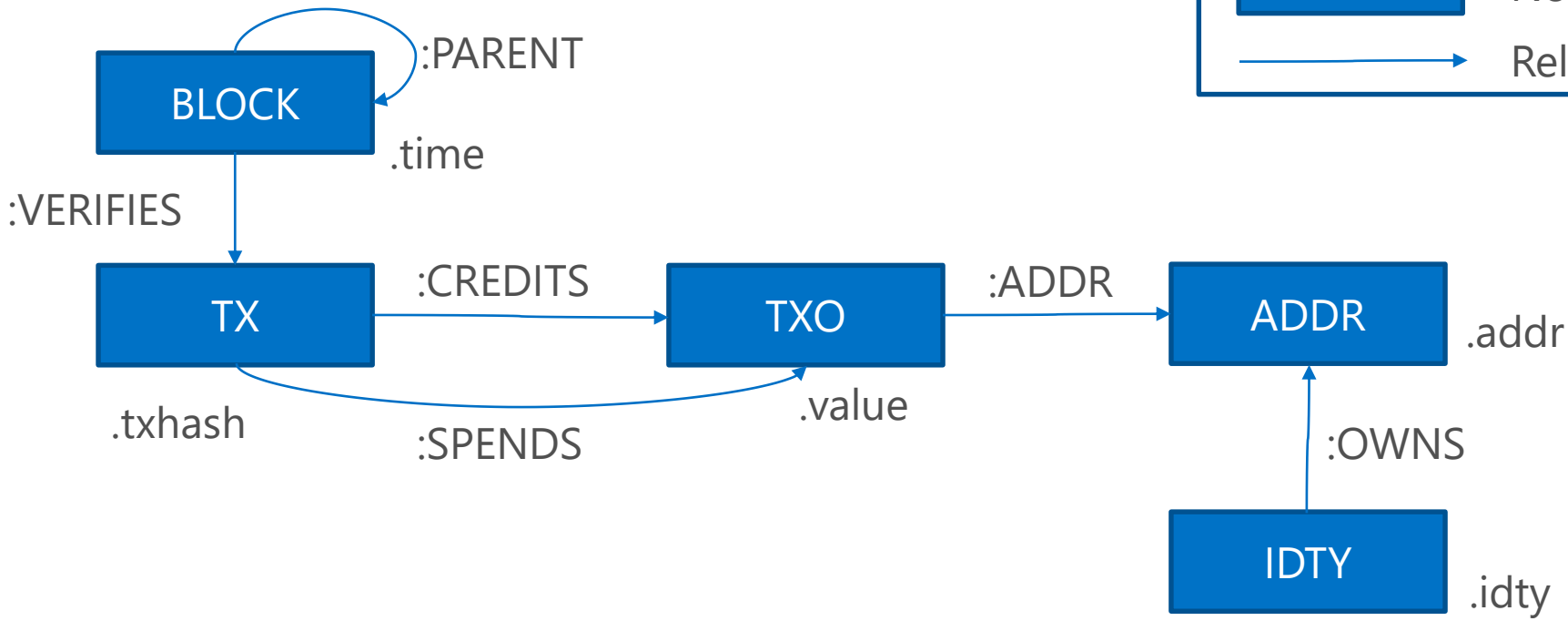
Back to Neo

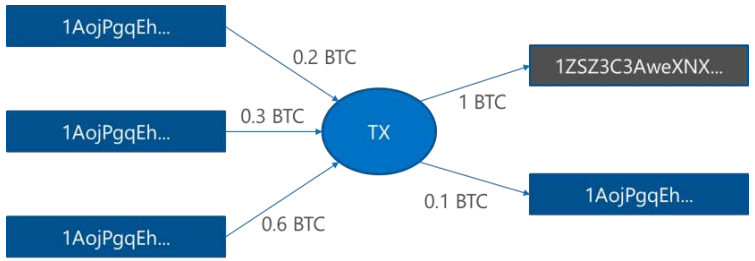
Neo4j Bitcoin Datenmodell



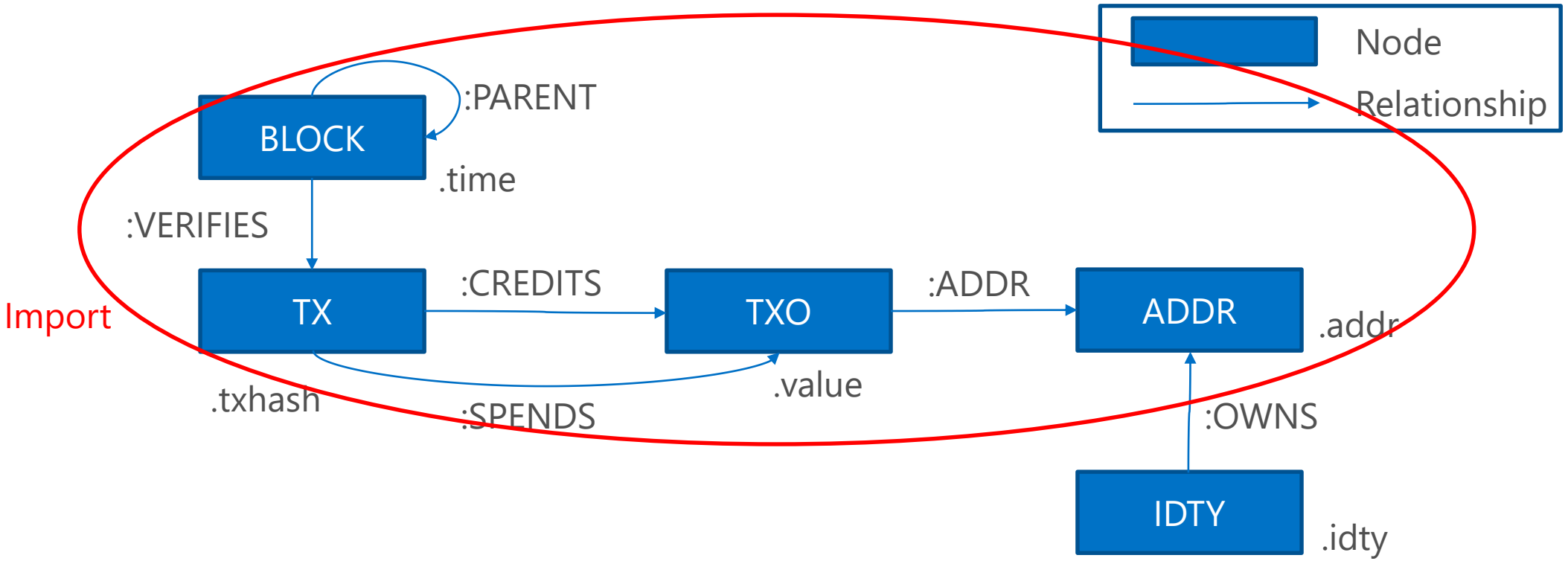
Neo4j Bitcoin Datenmodell



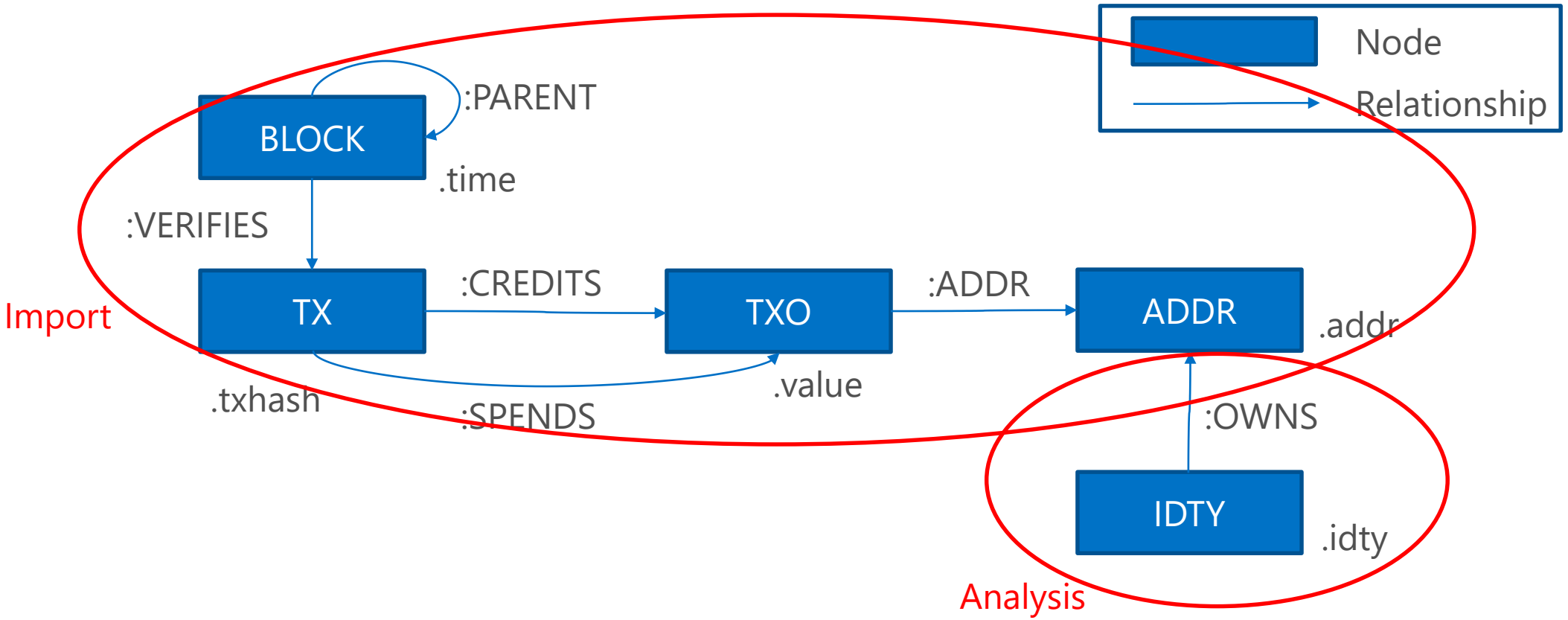




Neo4j Bitcoin Datenmodell

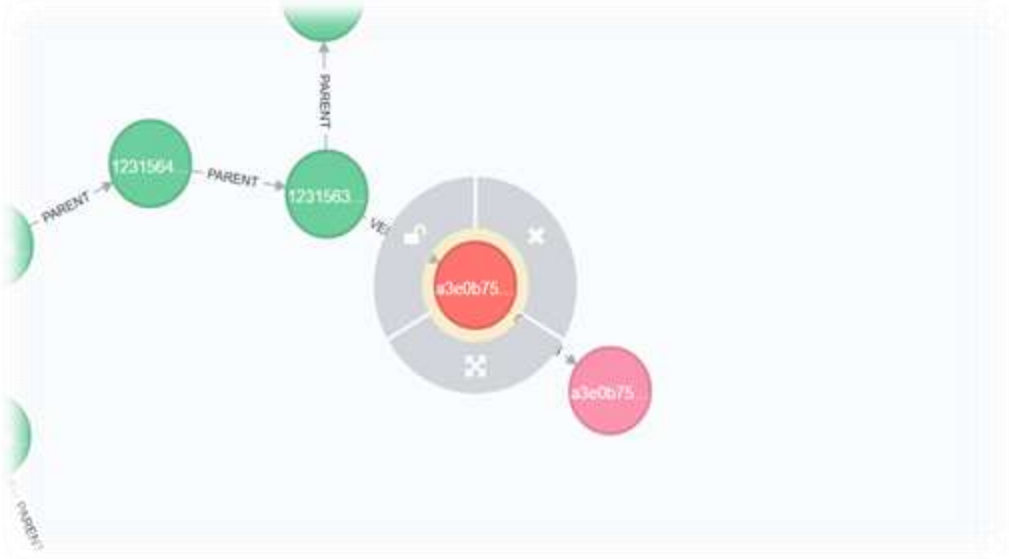


Neo4j Bitcoin Datenmodell

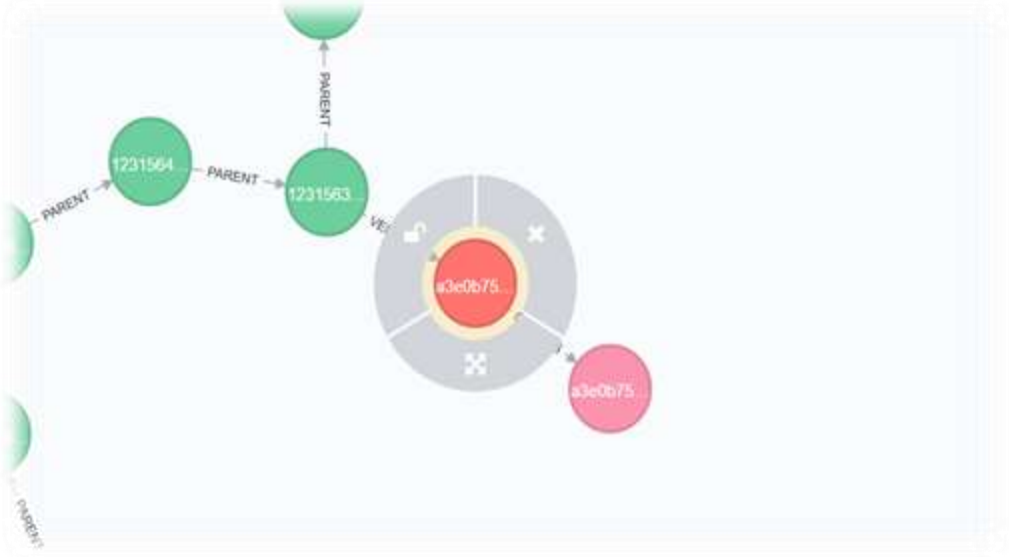


Demo

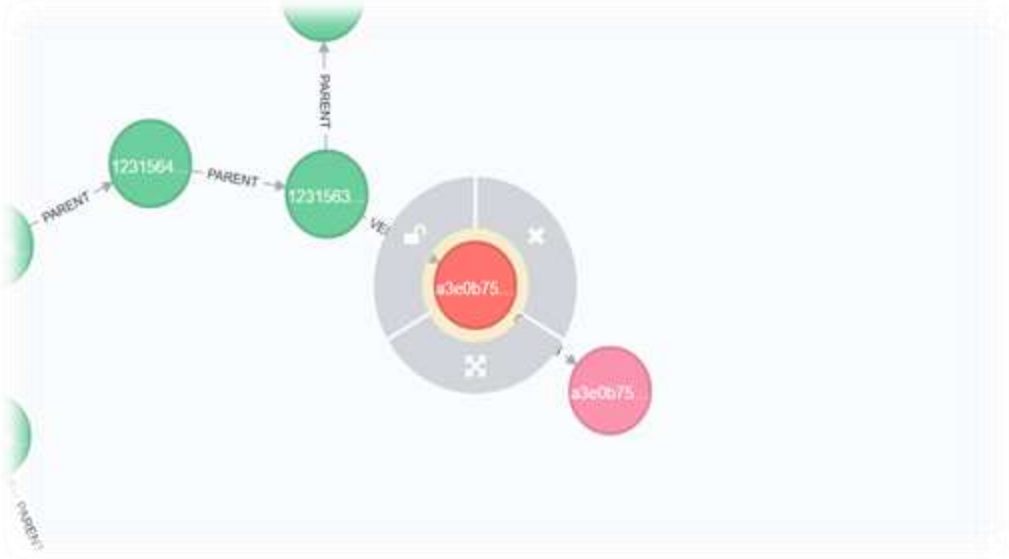
Demo



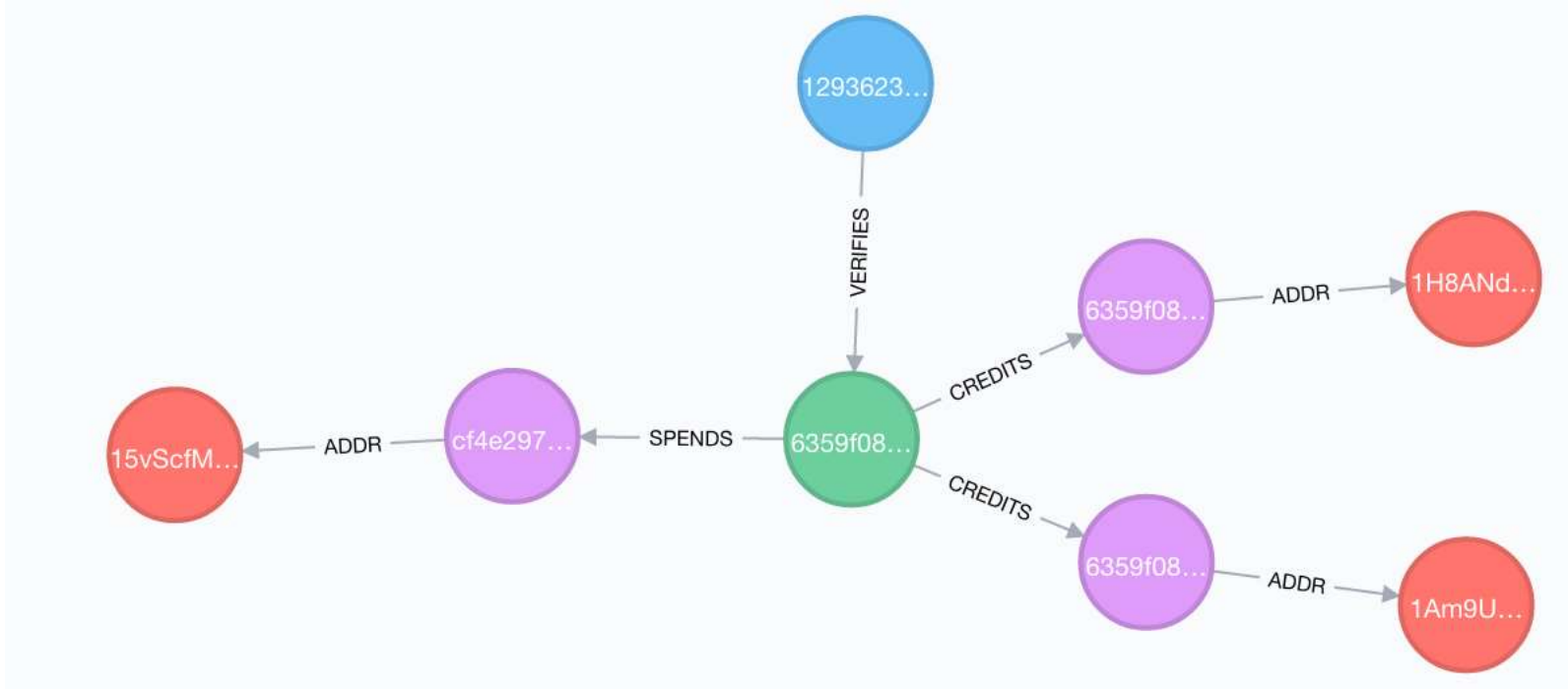
MATCH (n:BLOCK) RETURN n LIMIT 10



MATCH (n:IDTY) RETURN n LIMIT 10




```
MATCH (n:IDTY)-[:OWNS]->(a:ADDR) where a.addr = '...'  RETURN n
```

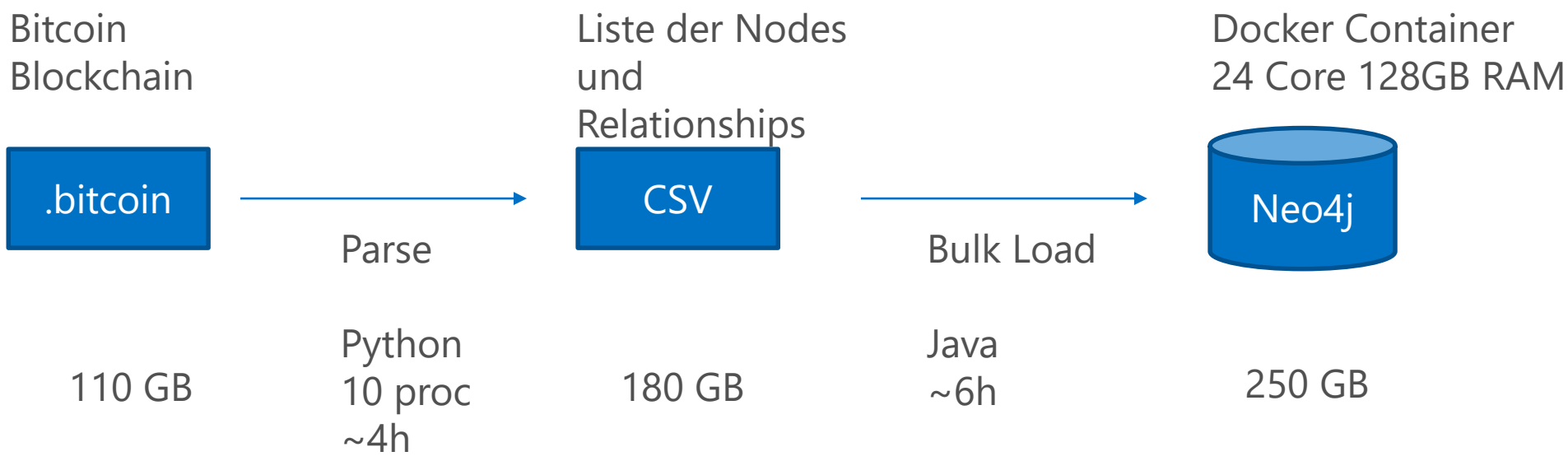



```
MATCH (a:ADDR)<--(txo:TXO)<--(tx:TX)<-[:VERIFIES]-(b:BLOCK)
WHERE tx.txhash = '6359f0868171b1d194cbee1af2f16ea598ae8fad666d9b012c8ed2b79a236ec4'
RETURN a, txo, tx, b
```

ADDRESS	BTC	TIME
15vScfMHNrXN4QvWe54q5hwfVoYwG79CS1	-3	1293623863
1Am9UTGfdnxabvcywYG2hvzr6qK8T3oUZT	2.99	1293623863
1H8ANdafjpqYntniT3Ddxh4xPBMCSz33pj	0.01	1293623863

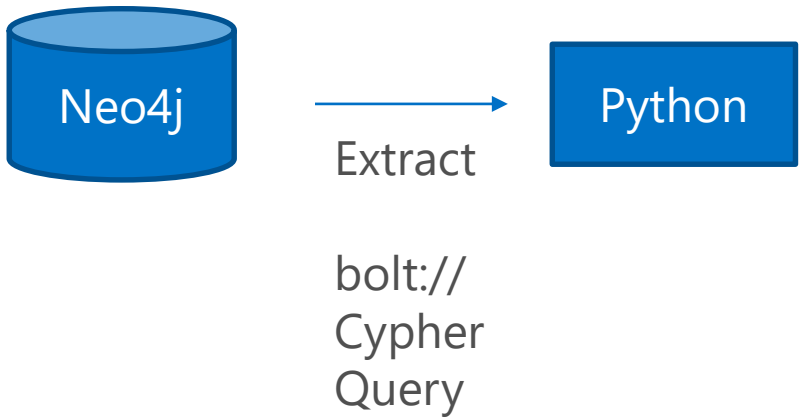
```
MATCH (a:ADDR)<--(txo:TXO)<-[r]-(tx:TX)<-[:VERIFIES]-(b:BLOCK)
WHERE tx.txhash = '6359f0868171b1d194cbee1af2f16ea598ae8fad666d9b012c8ed2b79a236ec4'
RETURN a.addr AS ADDRESS
 , CASE WHEN TYPE(r)='CREDITS' THEN 1 ELSE -1 END * txo.value/10^8 AS BTC
 , b.time AS TIME
```

Vorgehen initiale Befüllung



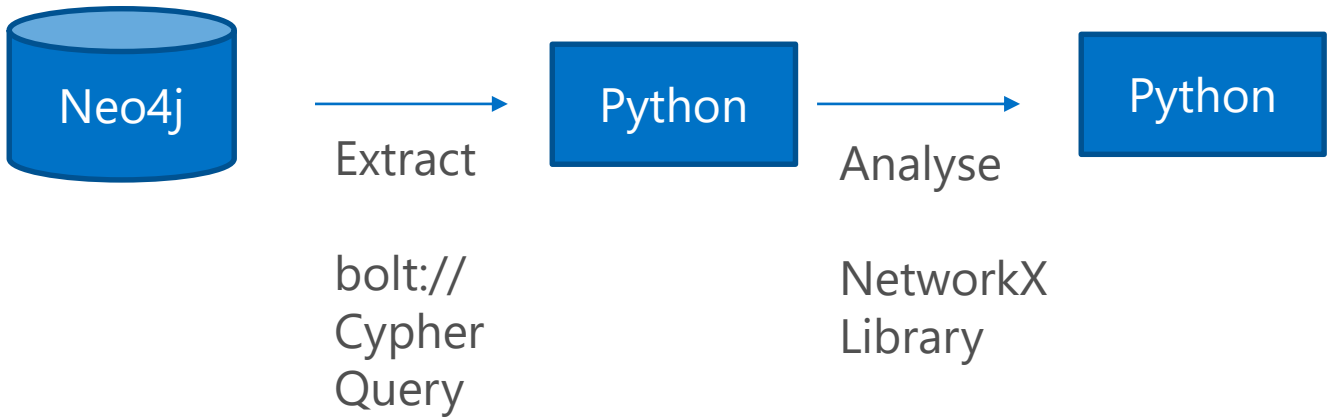
Vorgehen Netzwerkanalyse

```
MATCH (tx:TX)-[:SPENDS]->(:TXO)-[:ADDR]->(a:ADDR)
RETURN tx.txhash AS txhash, a.addr AS addr
```



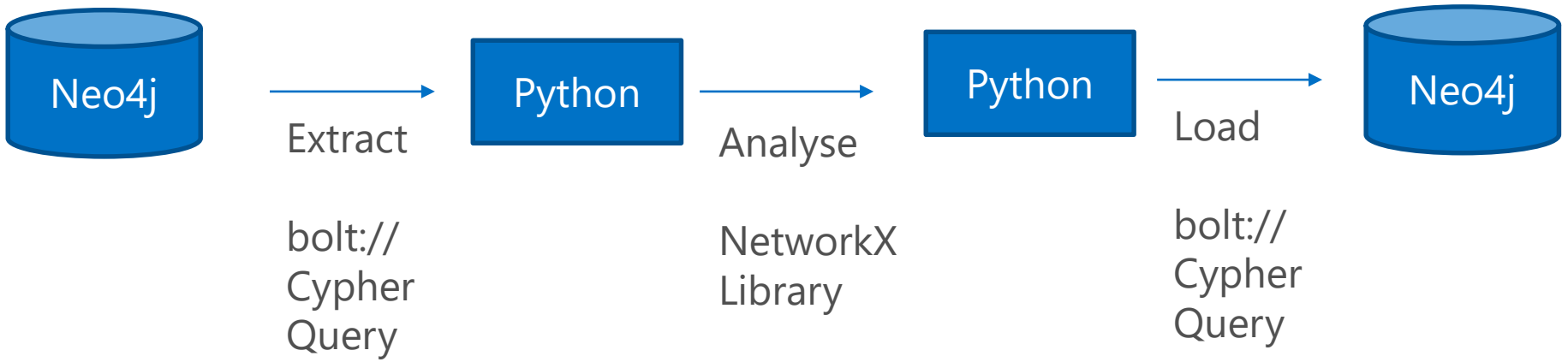
Vorgehen Netzwerkanalyse

```
G = Graph()
for addr, tx in edges:
  G.add_node(addr)
  G.add_node(tx)
  G.add_edge([addr, tx])
for comp in G.connected_components():
  idty = new_idty()
  for node in comp:
    if node in addrs:
      relationships.append([idty, node])
```



Vorgehen Netzwerkanalyse

```
MATCH (addr:ADDR {addr:"1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v"})
MERGE (idty:IDTY {name:"RYZ3T4R9"})
CREATE (idty)-[:OWNS]->(addr)
```



Agenda

- Introduction
- Block Chain Basics
- Anonym versus Pseudonym
- Getting Data: The one and the many
- **Getting Data: Doing the Power BI**

{ REST }

Adapter

KI analytics

Cypher

Demo

{ REST }

```
let
   content = "{""statements"":[{""statement"":""    Cypherquery  ""}]}",
   Quelle = Json.Document(Web.Contents("http://trex.ki-performance.local:5501/db/data/transaction/commit",
                        [Content = Text.ToBinary(content)])),
```

```
MATCH (n:IDTY)-[:OWNS]->(a:ADDR)<-[:ADDR]-(txo:TXO)<-[:CREDITS]-(tx:TX)
, (tx)-[:SPENDS]->(:TXO)-->(u:ADDR)
, (tx)<-[:VERIFIES]-(blk:BLOCK)
WHERE n.name = 'RYZ3T4R9'
WITH n, txo, u, blk
OPTIONAL MATCH (u)--(b:IDTY)
WITH DISTINCT n.name as toi, CASE WHEN b IS NOT NULL THEN b.name ELSE u.addr END as fromi,
CASE WHEN b IS NOT NULL THEN 1 ELSE 0 END as isidty, txo.value/10^8 as BTC, blk.time as time
RETURN toi, fromi, sum(BTC), time, isidty
```

Demo