Compliance in business processes by design:
examples from insurance, aviation, carsharing

Prof. Dr. Philipp Sandner
Blockchain Center
Frankfurt School of Finance & Management

E-Mail: p.sandner@fs.de
Phone: +49 151 25339641

Unsere **Aktivitäten**

- **Education:** Studenten und Manager in Trainings und Workshops
- **Research:** gemeinsame Forschungsprojekte und Studien
- **Prototyping:** Implementierung von Prototypen, Proof-of-Concept
- **Community:** regelmäßige Veranstaltung, Expertenrunden
- **Startups:** Unterstützung von Startups, Netzwerk

Fokus auf Branchen

- **Banken und Versicherungen**
- **Industrie 4.0**
- **Energie**
- **Mobilität**
- **Öffentlicher Sektor**

Das **Team**

- Prof. Dr. **Philipp Sandner**
  E-Mail: p.sandner@fs.de
- Prof. Dr. **Peter Rossbach**
- Prof. Dr. **Daniel Beimborn**
- **Vahe Andonians**
- +4 others

Past and current **projects**

- **6th Central Banking Workshop:** gemeinsam mit der Deutschen Bundesbank organisiert
- **Implementierungsprojekt:** Blockchain-basierte Policierung von situativen Versicherungen
- **Workshop für Top Manager:** Auswirkungen von dezentralen Blockchain-basierten Energiemärkten auf das Geschäftsmodell von Energieversorgern
- **Studie:** Potenzial von Blockchain-basierten Anwendungen in Entwicklungsländern

Executive summary

So far: transparency of transactions provides possibilities for regulators and compliance challenges

Transparency of blockchain transactions provided by limited fungibility → Regulation by monitoring of transparent transactions → Compliance

Executive summary

So far: transparency of transactions provides possibilities for regulators and compliance challenges

Transparency
of blockchain transactions provided by limited fungibility

Regulation by monitoring of transparent transactions

Compliance

New: differentiating between asset fungibility and usage fungibility allows for a „built-in regulation“ or, in other words, for a „compliance by design“

Asset fungibility
through technical features allowing full fungibilty of assets

Executive summary

So far: transparency of transactions provides possibilities for regulators and compliance challenges

Transparency
of blockchain transactions provided by limited fungibility

Regulation by monitoring of transparent transactions

Compliance

New: differentiating between asset fungibility and usage fungibility allows for a „built-in regulation" or, in other words, for a „compliance by design"

Usage fungibility
through smart contracts and „permission oracles"; can be temporary

+

Asset fungibility
through technical features allowing full fungibilty of assets

„Built-in regulation"

Compliance

- Use case requirements
- Corporate rules
- Legal requirements
- Regulatory requirements

Compliance

Compliance and blockchain features

Definition

- Compliance means **committing to and matching the legal rules, policies and laws**.
- Companies therefore have set up **procedures and compliance controls** which should ensure that regulatory requirements are met.
- With regard to this presentation, we also include committing to and matching **business rules** in the term compliance.

Important features

- Blockchain unites several **features which can support companies** in their reporting processes and legal authorities in their monitoring capabilities.
  - Through its record-keeping mechanism, the blockchain can create **transparency** and improve monitoring practices.
  - The blockchain is **immutable** by its design. Once a record is saved, it can not be changed which makes it a reliable source for regulatory institutions.
  - As a distributed network, the blockchain allows the implementation of shared data-bases for companies and **regulators**.
- Operational and compliance efficiency can be increased through the **bundling** of resources.
  - E.g. shared databases about customers' data might improve identification processes

Source: http://www.corporatecomplianceinsights.com/blockchain-regulatory-compliance/

How companies and regulators benefit

Quality

- **Read-only access** could be granted to regulators
- **Life-monitoring** helps regulators to intervene earlier and to have a better overview about recent events
- **Accuracy and confidence** is improved

Cost and speed

- Regulators and companies can **save costs** due to less human controls and intermediary systems
- **Automated processes** can be established (smart contracts) in order to reduce regulatory reports

Potential

Know your customer (KYC)

- Know your customer checks could be made **faster and more efficient**
- **Updates about clients** could be distributed between companies
- Transactions between clients could **only be allowed** if adequate KYC evidence and credentials exist

Anti-Money Laundering (AML)

- Especially Anti-Money Laundering programs are **difficult to implement** and contribute a major stake in compliance
- With the blockchain, past transactions **can be checked and investigated** which helps to identify illegal activities

Source: https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-banking.pdf
https://www.finextra.com/blogposting/13186/can-blockchain-prevent-money-laundering

Fungibility

The idea of fungibility

Definition

- Two goods are characterized as **fungible when they belong to the same asset class** and are perfectly interchangeable meaning that they bear the same value.
- A common example are **currencies**.
- One **20€ bill** is worth exactly as much as another 20€ bill or two 10€ bills and therefore is perfectly interchangeable.

Perspective

- Fungibility from the **owner of assets**

Economic meaning

- Fungibility is relevant to economic activities due to several reasons:
  - **Trust** in acceptance of assets
  - **Common value** perceptions
  - **Simplify** the trade process
  - **Reduce** transaction costs

Source: http://bitscan.com/articles/why-you-should-care-about-fungibility

Currency is fungible

Which assets are fungible?

Gold ounces

Stocks

Bonds

Blockchain items?

Fiat money

Oil

Unopened consumer goods

Fungibility in the blockchain design

Blockchain design

- For validation purposes **transactions are linked to previous transactions** which are linked to previous transaction.
- Hence, a history of all transactions and hence **the history of all items** is publicly known.

Problems

- Due to the transaction history, one can **trace the items and classify them as "clean"** or "dirty".
- Clean items are not associated with any illegal activities whereas dirty items are.
  - **Dirty items are regarded as less valuable**
  - Some **participants have technical infrastructure** to check if items are associated with illegal activities while other participants do not have the capabilities
  - Participants with this **ability have superior information** about the items and can abuse their knowledge which challenges trust in the network
  - Participants can **use third parties in order to check if items** are dirty or clean
  - If third parties have to be used, **transactions again rely on third parties** to establish trust which eliminates one of the biggest blockchain advantages

Source: http://bitscan.com/articles/why-you-should-care-about-fungibility ; http://www.coindesk.com/ensuring-bitcoin-fungibility-in-2017-and-beyond/

How blockchain looses its fungibility

Cooperation of different services

- **Through the cooperation** of blockchain related services (e.g. payment processors, exchanges, wallets services etc.) and the sharing/aggregation of their data (including transaction data), **transactions and their purpose can be identified**
- **Mining companies collaborate** and perform a taint analysis
- A **taint analysis** shows you if a item or coin was used for illegal activities or if it was stolen

Establish fungibility

- In order to re-establish fungibility on the blockchain several solutions are possible:
  - **Restore anonymity and privacy**
  - **Regulatory environment**
- Theoretical solutions are **ring signatures** which reduce the traceability (trade-off between fungibility and scalability) or the **Schnorr algorithm** (creates a single signature to represent many)

Source: https://prezi.com/cjcjkeuwoyrg/fungibility-on-the-blockchain/
https://decentralize.today/bitcoin-fungibility-the-most-important-feature-of-bitcoin-4b87a381f21a#.yk741w6vc

Current solution attempts for crypto currencies

Solution	Key components
Lightning Network	▪ It allows two parties which do not know each other to make off-chain transaction through their network
TumbleBit	▪ It is a decentralized application which mixes transactions and allows two parties to interact anonymously
Zcash	▪ A new cryptocurrency which claims to achieve full fungibility ▪ Only modern devices can run this protocol
Monero	▪ All transactions are mixed which solves the problem that dishonest users tend to utilized mixers before and therefore mixing was associated with illegal activities
Bottom line	▪ A third party is often used as a middleman ▪ Transactions are mixed and performed off-chain ▪ Schnorr algorithm is used

Source: http://www.coindesk.com/ensuring-bitcoin-fungibility-in-2017-and-beyond/
https://news.bitcoin.com/tumblebit-unlinkable-payment-hub/

Compliance
vs.
fungibility

Compliance vs. fungibility

Blockchain use cases

Frankfurt School of Finance & Management
German Excellence. Global Relevance.

There are use cases where assets need to be fully fungible

Micro payments

Other use cases need assets that are only partly fungible

Supply chain networks

Currency is fungible

Can stolen money be identified?

ATMs mark stolen money with ink

Reconciling fungibility and compliance

Smart Contracts

- Idea of smart contract back to 1994 (Nick Szabo)

- Self-executing agreement that
  - Securely hold value
  - Verifies whether the conditions are met
  - Automatically release value

```
If (…)
Then (…)
Else (…)
```

- „Oracle“
  - Online service providers broadcasting data
  - Can be used as input for verification
  - Connection between real world and blockchain

- Distributed Autonomous Organizations
  - Complex and/or combined smart contracts

Source: Quantoz (2016)

Adding a compliance layer through smart contracts

1. **Standard transaction**
   - Example: Bitcoin

```
send 70€ from A to B
```

Adding a compliance layer through smart contracts

Frankfurt School of Finance & Management
German Excellence. Global Relevance.

1 **Standard transaction**

- Example: Bitcoin

```
send 70€ from A to B
```

2 **Compliance layer through smart contracts and „permission oracles“**

- Execute payment only if condition holds
- Condition concerns whether a planned transaction is compliant

```
if (compliance rule = true)
then (send 70€ from A to B)
```

- „Permission oracles“
  - Decides about compliance of a planned transaction
  - Can be „on-chain“

Permission oracles could be reflected in a simple matrix which itself could be stored on a blockchain

Frankfurt School of Finance & Management
German Excellence. Global Relevance.

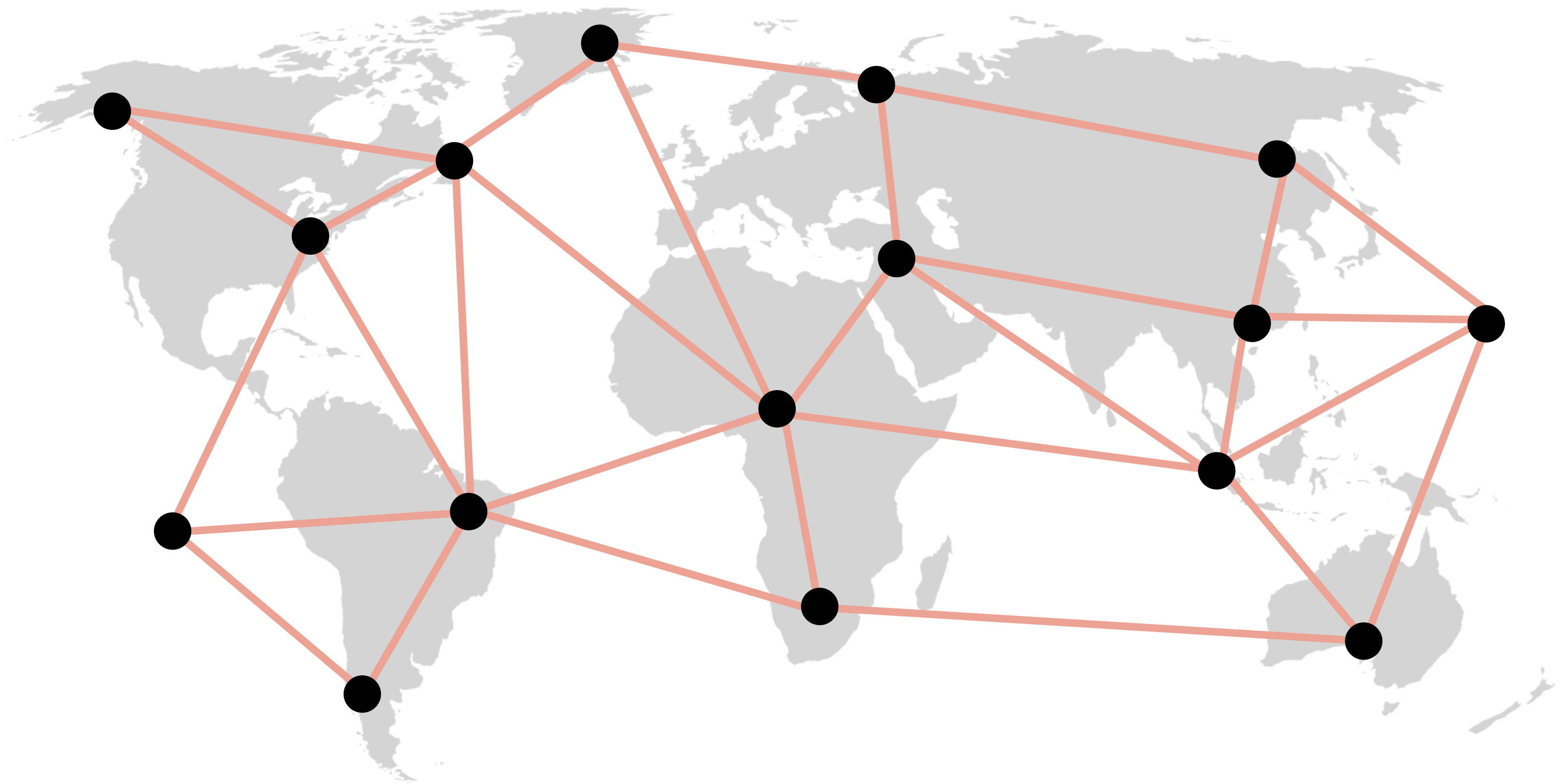
```
if (compliance rule = true) then (send [amount] from [sender] to [recipient])
```

Recipient

Sender

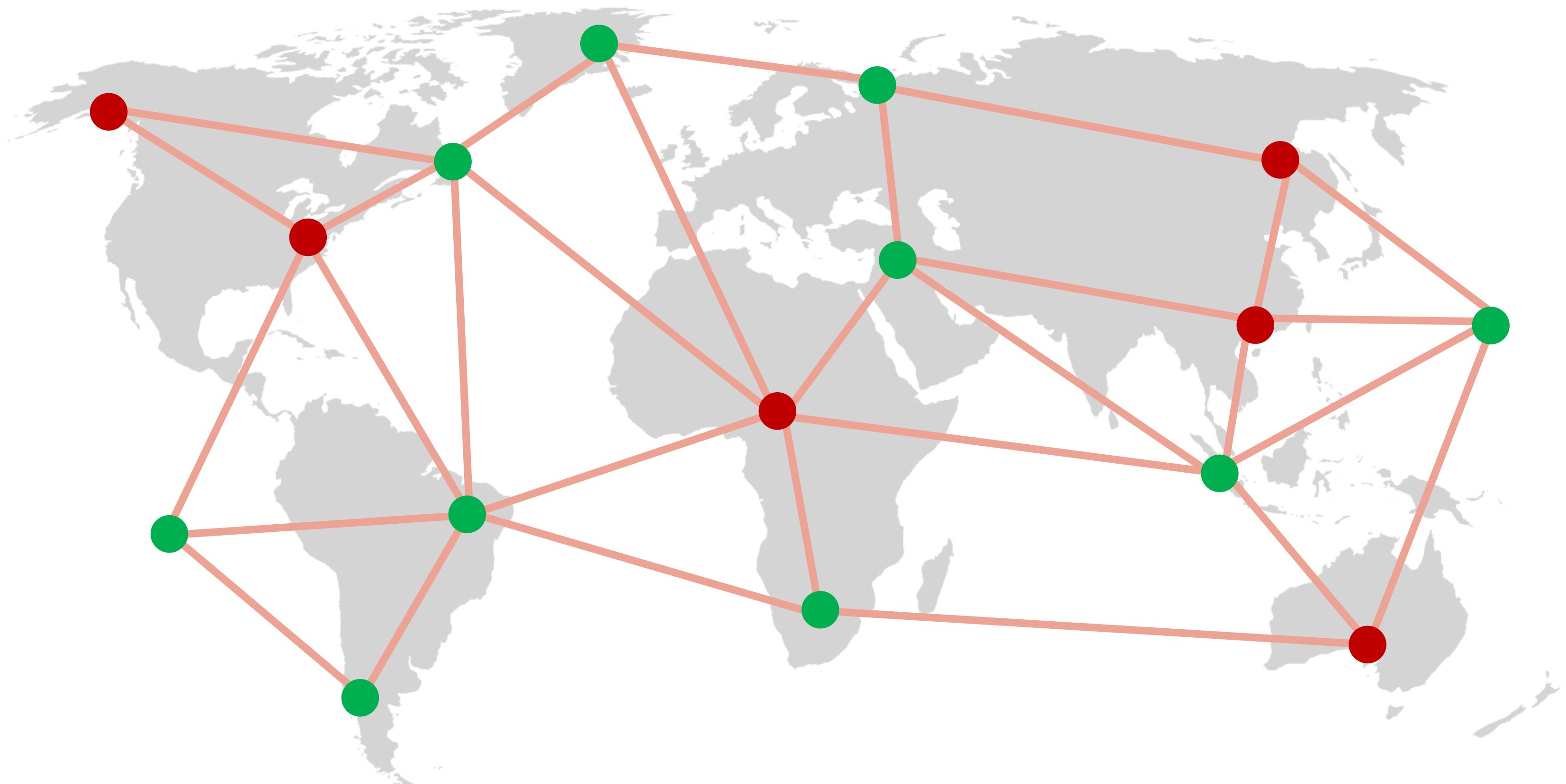
	A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	I_2
A_1	-		1						
B_1		-	1						
C_1			-						
D_1			1	-					
E_1			1		-				
F_1	1	1	1	1	1	-	1	1	1
G_1			1				-		
H_1			1					-	
I_1			1						-

Blockchain architecture: all wallet owners can be equal



Blockchain architecture: wallet owners can have different permission settings based on sending and receiving assets

Frankfurt School of Finance & Management
German Excellence. Global Relevance.



- Wallet owner can receive assets (green)
- Wallet owner can send assets (red)

Blockchain architecture: wallet owners can have different permission settings based on sending and receiving assets

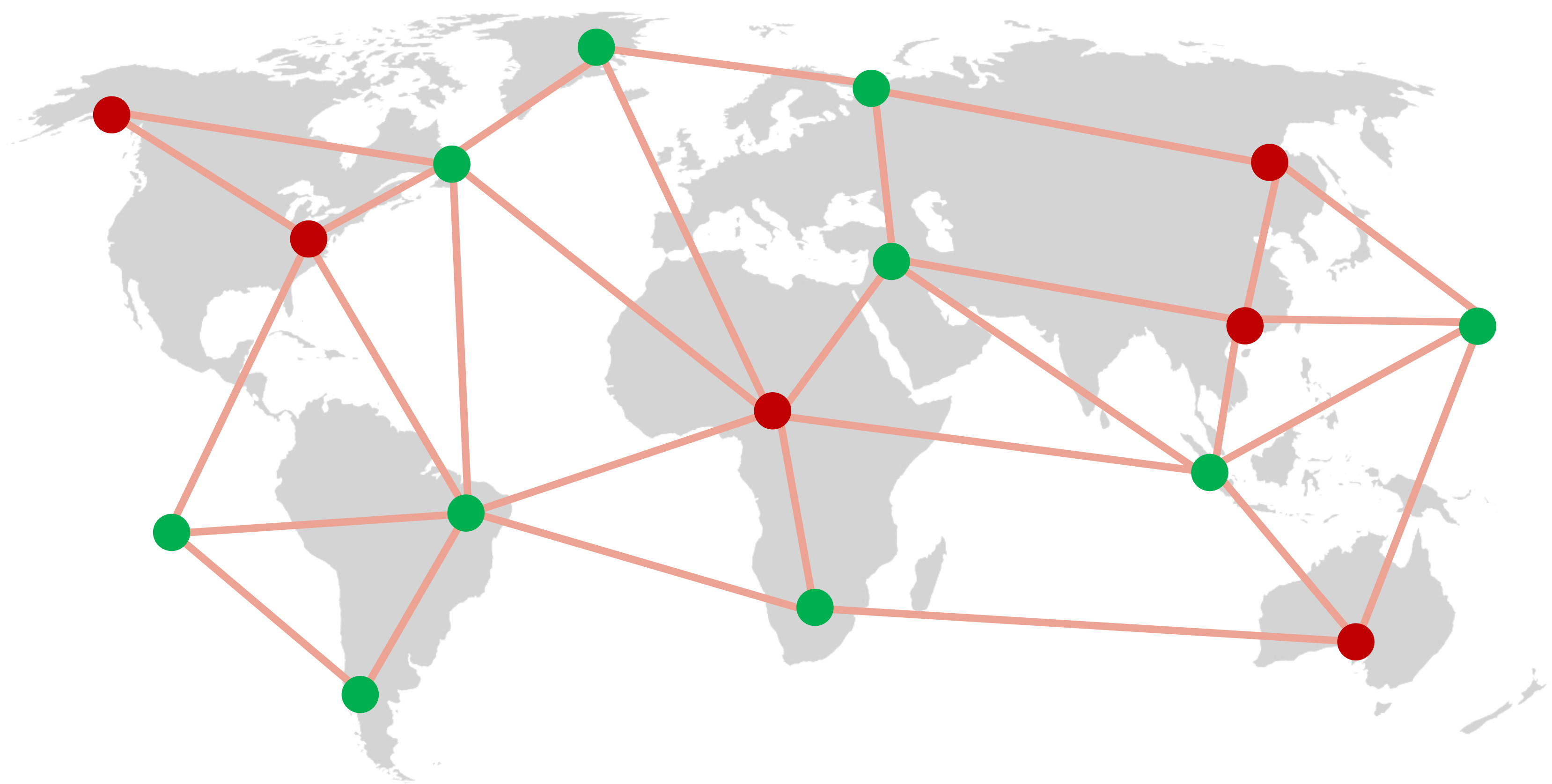
```
if (compliance rule = true) then (send [amount] from [sender] to [recipient])
```

Recipient

Sender

	A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	I_2
A_1	-		1						1
B_1		-	1						1
C_1			-						1
D_1	1	1	1	-	1	1	1	1	1
E_1			1		-				1
F_1	1	1	1	1	1	-	1	1	1
G_1			1				-		1
H_1			1					-	1
I_1			1						-

Blockchain architecture: wallet owners can have different permission settings based on subordinate networks



Wallet owners of subordinate network A

Wallet owners of subordinate network B

Blockchain architecture: wallet owners can have different permission settings based on subordinate networks


```
if (compliance rule = true) then (send [amount] from [sender] to [recipient])
```

Recipient

Sender

	A_2	B_2	C_2	D_2	E_2	F_2	G_2	H_2	I_2
A_1	-	1	1	1					
B_1	1	-	1	1					
C_1	1	1	-	1					
D_1	1	1	1	-					
E_1					-	1	1	1	1
F_1					1	-	1	1	1
G_1					1	1	-	1	1
H_1					1	1	1	-	1
I_1					1	1	1	1	-

Transferring value is possible, since a blockchain database has "built-in trust"

Technical features	„Built-in trust“	Transaction of value

Technical features

- Network
- Ledger
- Blocks
- Nodes
- Wallets
- Transactions
- Miners

„Built-in trust“

- Immutable history of transactions
- Redundant storage of ledger
- Robustness of network

Transaction of value

- Money
- Stocks
- Identities
- Reputation
- Car rentals
- Energy
- Computing power

Source: built on Quantoz (2016)

Transferring value compliant is possible if smart contracts and permission oracles enable a "built-in regulation"

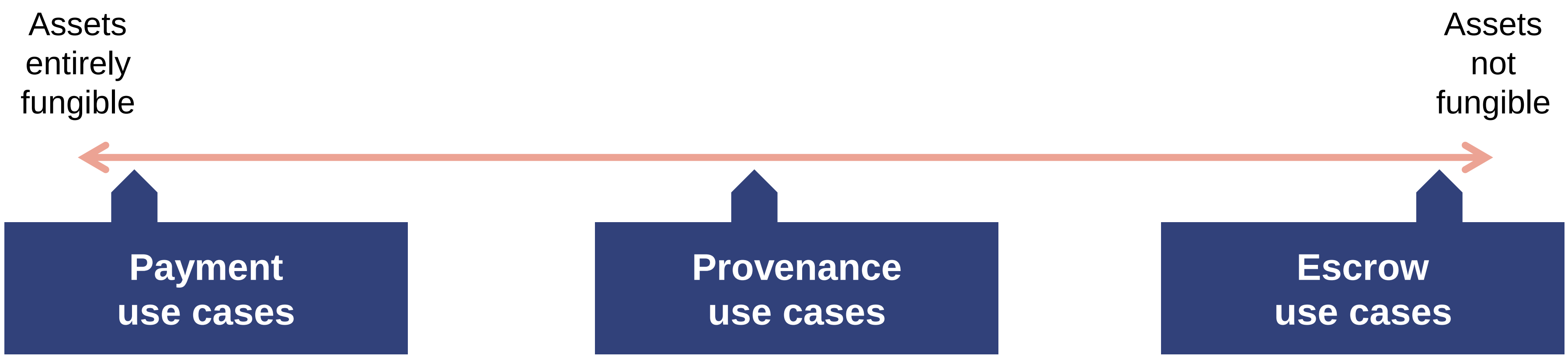
Frankfurt School of Finance & Management
German Excellence. Global Relevance.

Technical features	„Built-in trust“	Compliant transaction of value

• Network
• Ledger
• Blocks
• Nodes
• Wallets
• Transactions
• Miners
• Smart contracts
• Permission oracles
	• Immutable history of transactions
	• Redundant storage of ledger
	• Robustness of network
	• "Built-in regulation"
	  – By companies
	  – By organizations
	  – By regulators
		• Money
		• Stocks
		• Identities
		• Reputation
		• Car rentals
		• Energy
		• Computing power

Source: built on Quantoz (2016)

The degree of fungibility is an important feature for a blockchain architecture



Summary

- Ideal to have full „**asset fungibility**“ for the underlying digital assets
  - Technical features

- Have configurable (sometimes temporary) „**usage fungibility**“ for different use cases
  - Smart contracts
  - „Permission oracles“
    - Permission rights
    - Permission matrices

- Result
  - **„Built-in regulation“** in addition to „built-in trust“
  - **„Compliance by design“**
  - **„Regulation by design“**

Summary

Frankfurt School of Finance & Management
German Excellence. Global Relevance.

So far: transparency of transactions provides possibilities for regulators and compliance challenges

Transparency
of blockchain transactions provided by limited fungibility

→ Regulation by monitoring of transparent transactions → Compliance

New: differentiating between asset fungibility and usage fungibility allows for a „built-in regulation“ or, in other words, for a „compliance by design“

Usage fungibility
through smart contracts and „permission oracles“; can be temporary

\+

Asset fungibility
through technical features allowing full fungibilty of assets

→ „Built-in regulation“ → Compliance

- Use case requirements
- Corporate rules
- Legal requirements
- Regulatory requirements