

BC4IS @ CAiSE 2023

Zaragoza, Spain

12 June 2023

Blockchain for Information Systems

Blockchain Interoperability

Dr. Felix Härer

University of Fribourg, Switzerland



UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG



SWISS NATIONAL SCIENCE FOUNDATION

DIGITS

DIGITALIZATION AND
INFORMATION SYSTEMS

www.unifr.ch/inf/digits

OUTLINE

- 1. Introduction - Open and Permissionless Blockchains**
- 2. Interoperability Challenges**
- 3. Cross-Chain Interoperability**
- 4. Interoperability Beyond Blockchains**
- 5. Conclusion**

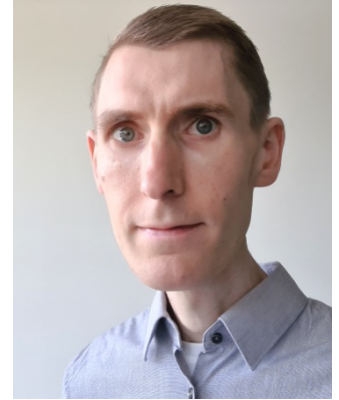
SPEAKER

Dr. Felix Härer

Senior Researcher and Lecturer

Digitalization and Information Systems Group

University of Fribourg, Switzerland



[www.unifr.ch/inf/digits/en/
group/team/haerer.html](http://www.unifr.ch/inf/digits/en/group/team/haerer.html)

Background

- PhD in Information Systems, on Decentralization and Blockchains
- BSc and MSc in Information Systems, Cyber Security MSc specialization
- Industry experience in Software Engineering (Siemens Healthcare, research projects)

Current Events

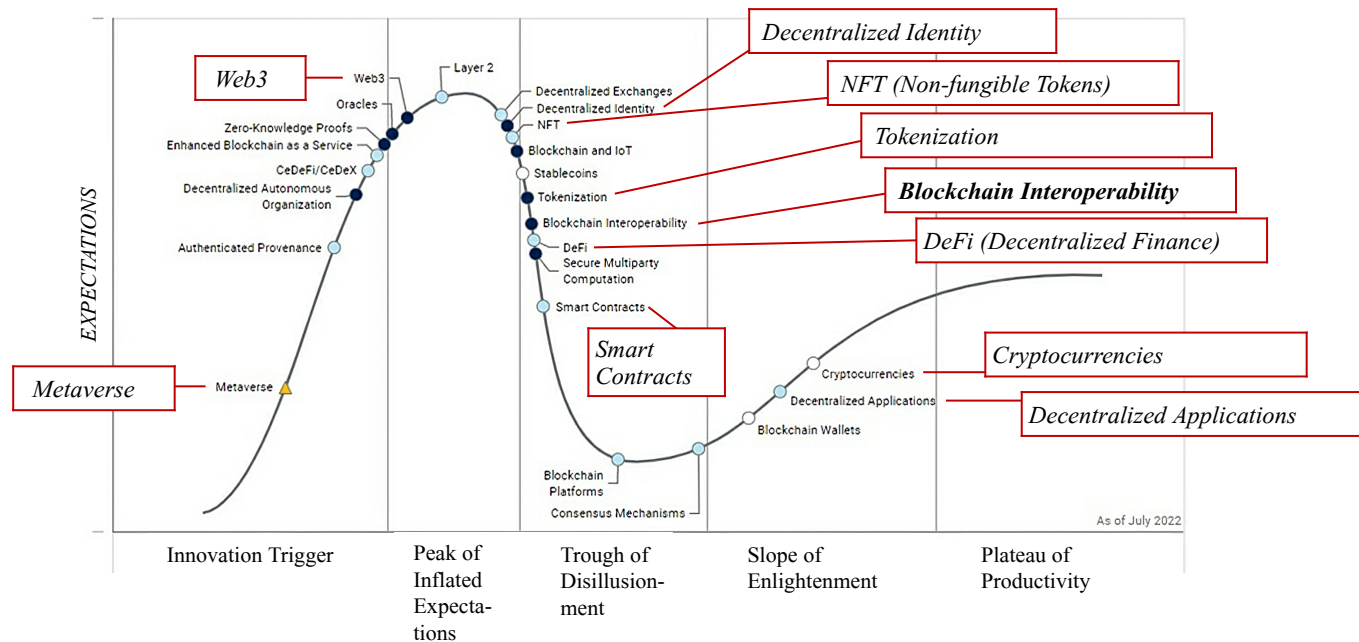
- SI Business Informatics Blockchain Forum (online)
unifr.ch/inf/digits/events
- 3rd International Workshop on Blockchain for Trusted Data Sharing, B4TDS @ BIR 2023, Ascoli Piceno, Italy
pros.unicam.it/B4TDS2023

Recent Publications

- Curty, S., Härer, F. & Fill, HG: Design of blockchain-based applications using model-driven engineering and low-code/no-code platforms: a structured literature review. *Softw Syst Model* (2023)
- Härer, F.: Towards Interoperability of Open and Permissionless Blockchains: A Cross-Chain Query Language, in: *Proceedings of the 2022 IEEE International Conference on E-Business Engineering (IEEE ICEBE 2022)*, 2022, Bournemouth, UK.

BLOCKCHAIN TRENDS

Blockchain Technology According to the "Hype Cycle for Blockchains and Web3, 2022" (Gartner)













July 2022

<https://blogs.gartner.com/avivah-litan/2022/07/22/gartner-hype-cycle-for-blockchain-and-web3-2022/>















BLOCKCHAIN AND CRYPTOCURRENCY

Cryptocurrency

#	Name	Price	1h %	24h %	7d %	Market Cap 
1	 Bitcoin BTC	\$26,074.20	▲ 0.33%	▲ 1.64%	▼ 4.21%	\$505,826,567,570
2	 Ethereum ETH	\$1,765.35	▲ 0.36%	▲ 1.40%	▼ 7.31%	\$212,243,796,012
3	 Tether USDT	\$1.00	▼ 0.01%	▼ 0.00%	▲ 0.03%	\$83,415,305,049
4	 BNB BNB	\$237.80	▲ 0.35%	▼ 0.07%	▼ 22.31%	\$37,062,041,317
5	 USD Coin USDC	\$1.00	▲ 0.00%	▲ 0.01%	▲ 0.03%	\$28,387,926,951
6	 XRP XRP	\$0.5274	▲ 1.21%	▲ 4.72%	▼ 1.79%	\$27,417,559,144
7	 Cardano ADA	\$0.2729	▲ 0.75%	▲ 3.36%	▼ 28.39%	\$9,526,493,528
8	 Dogecoin DOGE	\$0.06218	▲ 0.14%	▲ 1.95%	▼ 14.70%	\$8,687,740,868
9	 TRON TRX	\$0.07033	▲ 0.23%	▲ 1.37%	▼ 14.09%	\$6,337,870,651

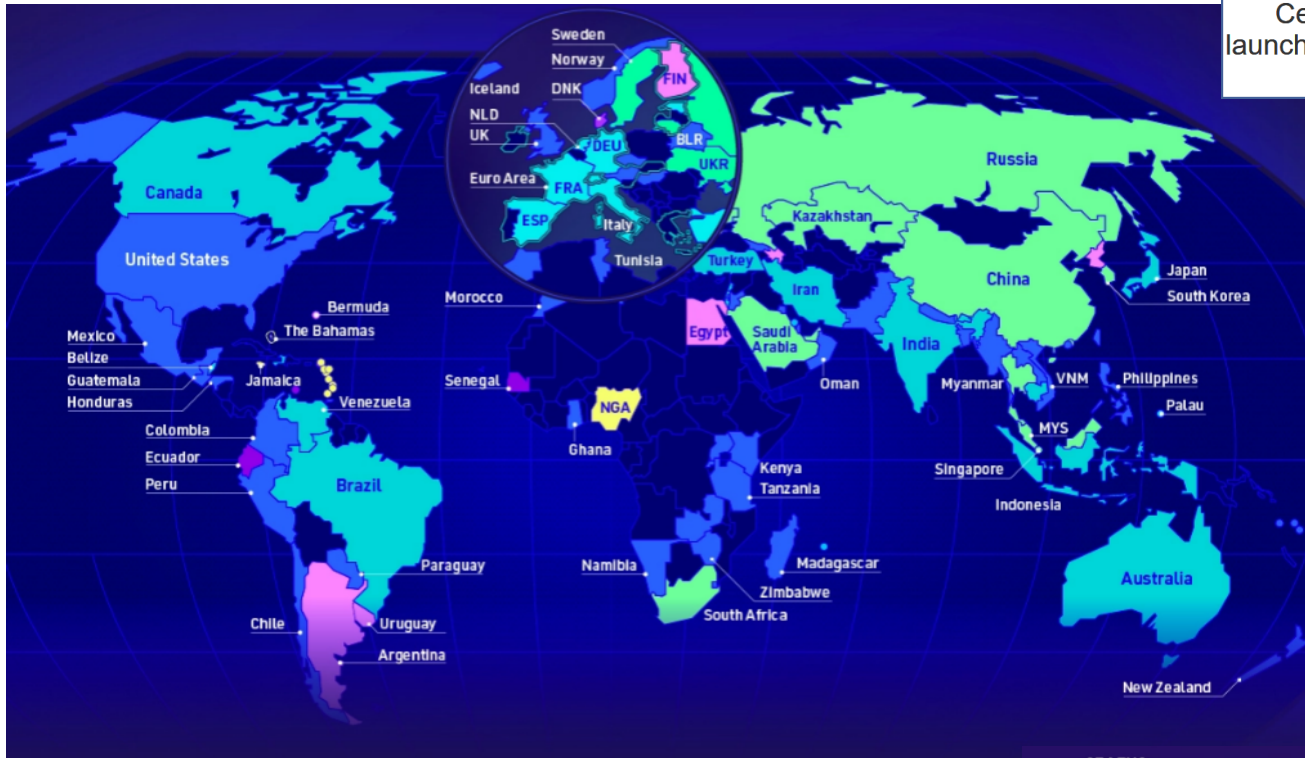
coinmarketcap.com

Companies

Rank	 Name	 Market Cap
1	 Apple AAPL	\$2.846 T
2	 Microsoft MSFT	\$2.429 T
3	 Saudi Aramco 2222.SR	\$2.097 T
4	 Alphabet (Google) GOOG	\$1.622 T
5	 Amazon AMZN	\$1.274 T
6	 NVIDIA NVDA	\$957.61 B
7	 Tesla TSLA	\$774.62 B
8	 Berkshire Hathaway BRK-B	\$733.77 B
9	 Meta Platforms (Facebook) META	\$695.77 B
10	 TSMC TSM	\$533.16 B
11	 Visa V	\$479.07 B
12	 UnitedHealth UNH	\$459.57 B

companies-
marketcap.com

CENTRAL BANK DIGITAL CURRENCIES (CBDC)

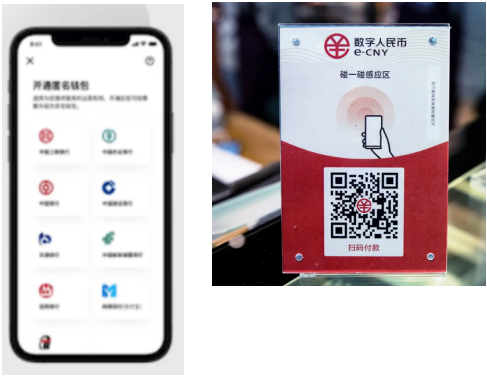




Ministry of Finance

Central Bank Digital Currency (CBDC) pilot launched by RBI in retail segment has components based on blockchain technology

<https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882883>









eCNY

<https://www.chinainternetwatch.com/33050/cbdc-ecny/>
<https://www.nytimes.com/2021/03/01/technology/china-national-digital-currency.html>

Data: Atlantic Council, CBDC Tracker (2022). Visualization: <https://www.visualcapitalist.com/visualized-the-state-of-central-bank-digital-currencies/>

SNB: https://www.snb.ch/de/ifor/research/conf/other_academic_conferences/id/sem_2022_06_03

ECB Report August 2022: <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2713~91ddff9e7c.en.pdf>

STATUS			
	Launched Issued a CBDC for widespread retail and/or wholesale use.		Pilot Initiated small-scale testing of a CBDC in the real world with a limited number of participants.
	Development Initiated technical build and early testing of a CBDC in a controlled environment.		Research Started exploring the use cases, impact and feasibility of a CBDC.
	Inactive CBDC initiative is on hold.		Canceled CBDC initiative decommissioned.

TOKENIZATION

Framework

	Currency				Token		
Unit	Fungible Coins				Fungible / Non-fungible Tokens		Non-fungible Tokens
Representation	Crypto-currency	Stablecoin <i>algorithmic</i>	<i>private</i>	Central Bank Digital C.	Asset / Security / Equity	Utility	Art / Collectible / Avatar (Virtual) Object / (Virtual) Land
Issuance and Supply	Decentralized and algorithmic		Private Firm(s)	Central Bank(s)	Asset Management and Investment Firms	Decentralized and algorithmic	Decentralized and algorithmic, issuance often centralized
Technology	Blockchain	Blockchain w/ Smart Contracts		Blockchain / other IT	Blockchain w/ Smart Contracts operate accounts, transfer fees, shares of ownership, interest etc.		
Examples	Bitcoin, Ether	DAI	USDC USDT	₹-W ₹-R eCNY	SEBA Security Tokens PAXG (Gold-backed token)	Link (provides data on-chain), Graph , Golem (computation)	artèQ, OpenSea (tokenized art), Decentraland, Sandbox (avatars, land, objects in virtual worlds (“metaverse”))

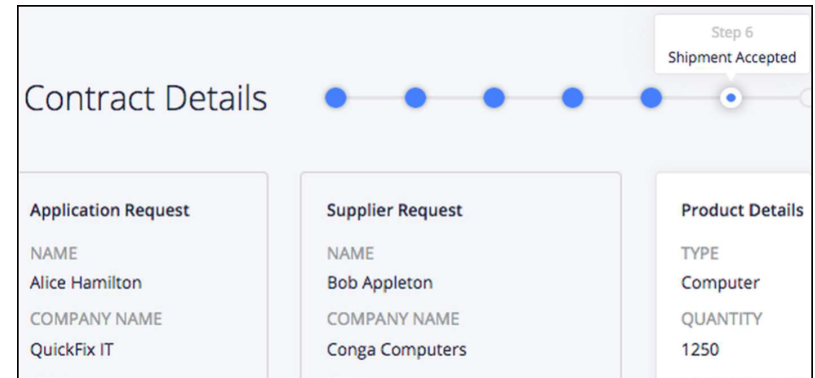
Adapted in 01/2023 from
"Kryptowährungen" (Härer, 2019) in:
Blockchain Kompakt, Springer (2019)

₹-W:
Digital Rupee – Wholesale
₹-R: Digital Rupee - Retail
<https://pib.gov.in/PressReleaselframePage.aspx?PRID=1882883>

SMART CONTRACT AND DECENTRALIZED APPS (DAPPS)

Example Applications

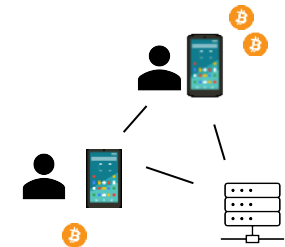
- **Attestation of Documents and Identities, Notarization**
- **Decentralized Web / web3**
- **Business Process Management**
- **Supply chain tracking**
- **IoT**
- **Healthcare and Pharma**



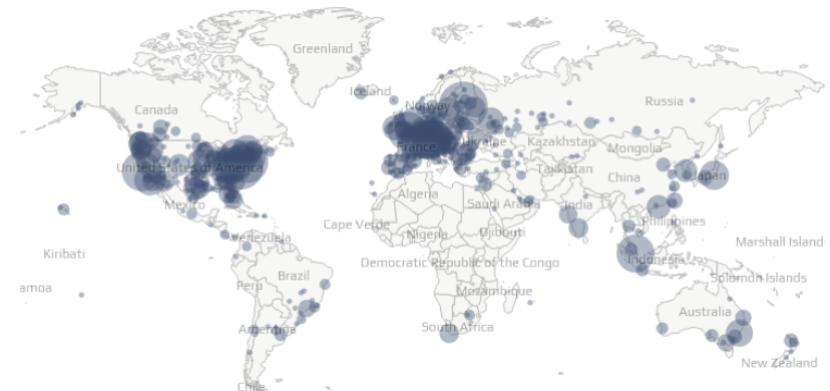
Example of Supply Chain Tracking using Hyperledger

DISTRIBUTED SYSTEMS

- Today, open and public blockchains are emerging as globally distributed systems
- Largest open and permissionless blockchains by approx. number of network nodes



— Bitcoin		15 000
— Ethereum		6 000
— Cardano		3 000
— Solana		1 600
— Avalanche		1 300



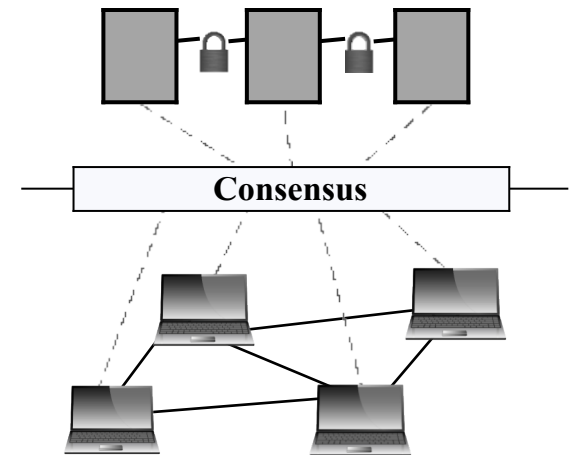
Data collected in August 2022

Distribution of Bitcoin nodes (bitnodes.io)

OPEN AND PERMISSIONLESS BLOCKCHAINS

Blockchain System Components

- **Data Structure:**
Ledger of transactions
- **Consensus:**
Mechanisms and algorithms, at least for distribution, security, scalability, incentivization
- **Network Nodes:**
Participants executing consensus








Terminology

- Distribution: distribution across the network
- Decentralized: without centralized coordination
- Blockchain: the data structure component, in practice also used for the system

OPEN AND PERMISSIONLESS BLOCKCHAINS

Open and Permissionless Blockchain Platforms in 2023

by Number of Participants / Network Nodes

	Blockchain	Data Structure	Network	Consensus Protocol	Smart Contract Features
	[1] Bitcoin ^a	Blocks, UTXO data model	Bitcoin, approx. 15000 nodes	Nakamoto Consensus, Proof-of-Work	Stack-based script execution, monetary transactions
	[2] Ethereum ^b	Blocks, account state storage in tree data structures	Ethereum Mainnet, approx. 6000 nodes	Proof-of-Stake	Ethereum Virtual Machine, general-purpose programs
	[3] Cardano ^c	Blocks, extended UTXO model	Cardano, approx. 3000 nodes	Ouroboros, Proof-of-Stake	General-purpose programs, functional
	[4] Solana ^d	Block and graph data structures over different time spans	Solana Mainnet Beta, approx. 1600 nodes	Graph-based (proof-of-history), Proof-of-Stake	General-purpose programs
	[5] Avalanche ^e	Block and graph data structures over different networks	Platform/Exchange/Contract (P/X/C) chain, approx. 1300 nodes	Avalanche (P Chain) Snowman (X/C Chain), Proof-of-Stake	Ethereum Virtual Machine (C Chain), general-purpose programs

^a <https://bitnodes.io/>

^b <https://ethereum.org/en/developers/docs/>, <https://ethernodes.org/>

^c <https://adastat.net/pools/>

^d <https://docs.solana.com>, <https://solanabeach.io/validators/>

^e <https://stats.avax.network/dashboard/network-status/>

Table: Adapted from Härer (2022): Towards Interoperability of Open and Permissionless Blockchains: A Cross-Chain Query Language. In publication.

OPEN AND PERMISSIONLESS BLOCKCHAINS

Decentralization - Bitcoin

Bitcoin Mining

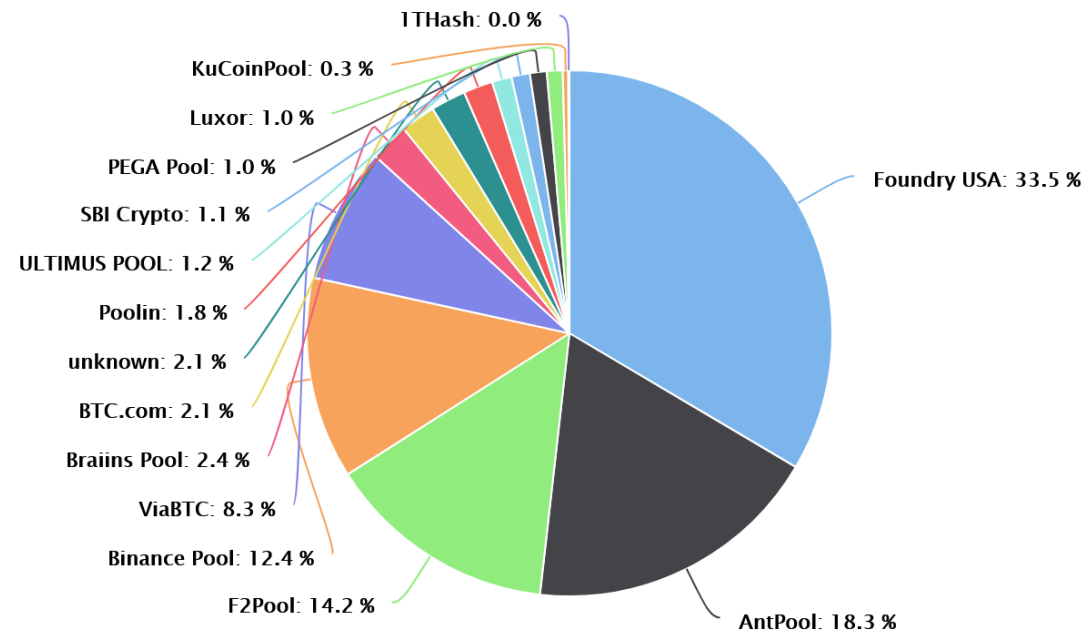


Nodes
Specialized
ASIC
Miner
Hardware



Distribution

Nodes operating in mining pools



https://btc.com/stats/pool?pool_mode=month

Feb 2023, Timespan: 1 Month

OPEN AND PERMISSIONLESS BLOCKCHAINS

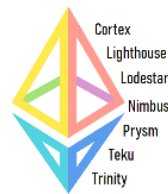
Decentralization - Ethereum

Ethereum Staking

Nodes



Low-power PCs



Node Software
in multiple
implementations



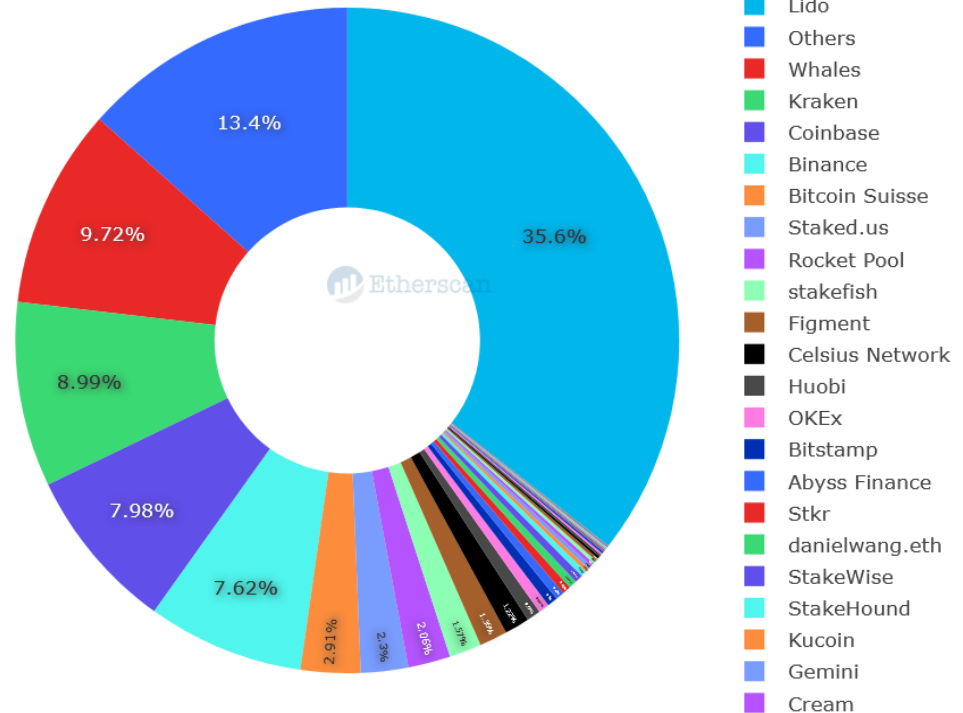
Cloud
Servers



Virtual Machine
Nodes

Distribution of Nodes

Nodes with deposits (staking) on Ethereum



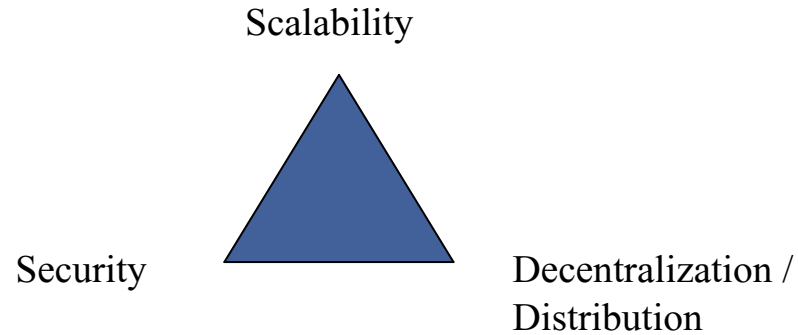
https://bi.etherscan.io/public/dashboards/KH9jbP687szqlAnHiNEfNictwNhvdOEQI0PwB6m?org_slug=default

Feb 2023

OPEN AND PERMISSIONLESS BLOCKCHAINS

Blockchain Properties

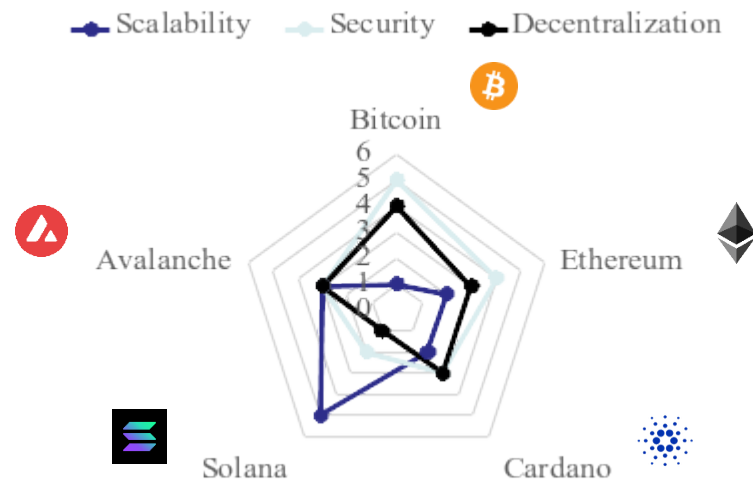
Blockchains *internally* guarantee certain properties to varying degrees



Blockchain trilemma and variants suggested by Zooko Wilcox and others

OPEN AND PERMISSIONLESS BLOCKCHAINS

Blockchain Properties



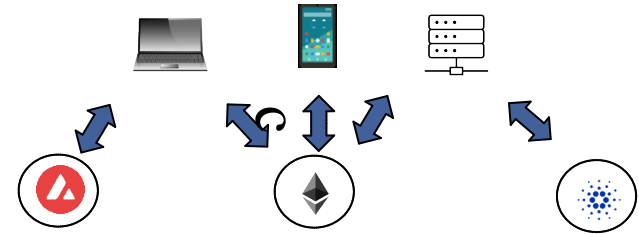
Estimation of factors for well-known blockchains

Based on factors from Härer (2022): Towards Interoperability of Open and Permissionless Blockchains: A Cross-Chain Query Language. In publication.

INTEROPERABILITY CHALLENGE

The Ultimate Application Platform?

- Open and permissionless blockchains provide unique properties on a technical level
 - Novel consensus and incentivization mechanisms
 - Transactions with a-priori unknown parties
 - Transactions without Trusted Third Parties
 - Verifiability and transparency
 - Guarantees: varying degrees of decentralization, security, scalability
- Properties, features, trade-offs differ considerably



INTEROPERABILITY CHALLENGE

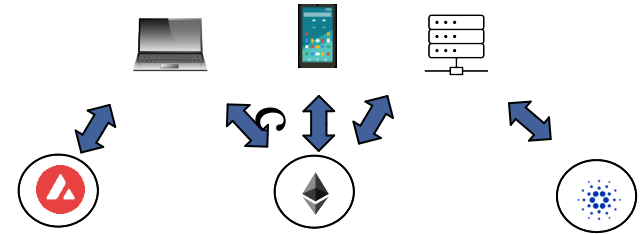
Interoperability Challenge

1. No interoperability on a technical level

=> Cross-Chain Interoperability?

2. No interoperability beyond blockchains

=> Real-World Applications?

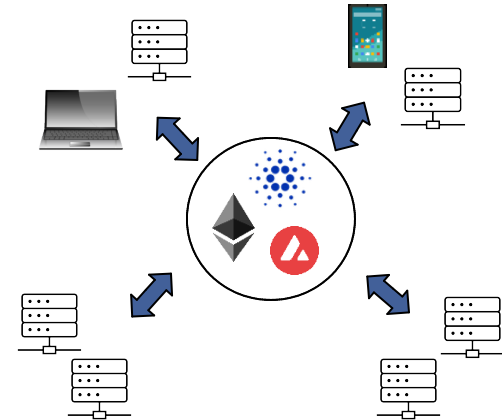


Blockchains as universal application platforms for storage and computation?

CROSS-CHAIN INTEROPERABILITY

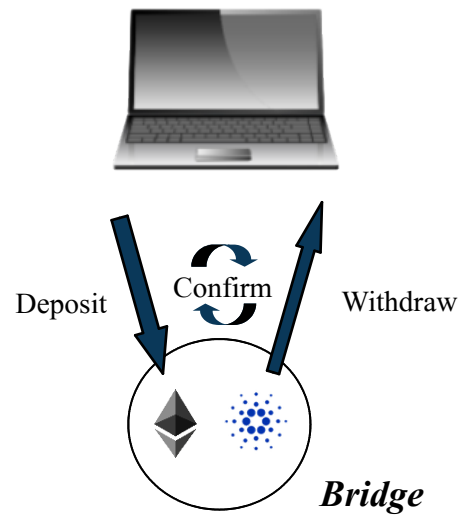
Bridges

- Connection of isolated networks
- Transfer of standardized tokens, data, function calls for smart contracts
- Adapter paradigm, n-to-n complexity
- Applied for blockchains, sidechains, layer 2 (Channels, Roll-Ups, Zero-Knowledge)























CROSS-CHAIN INTEROPERABILITY

Bridges



CROSS-CHAIN INTEROPERABILITY

Bridges in Practice

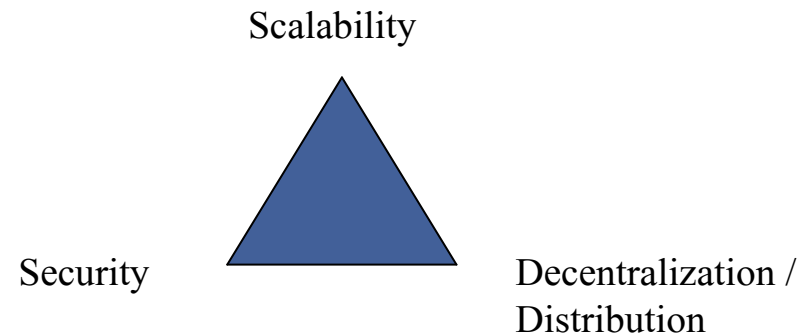
#	NAME	TVL ⓘ	7D CHANGE ⓘ	BREAKDOWN ⓘ	MKT SHARE ⓘ
1	 Polygon PoS	\$2.07B	▼ 5.13%		42.22%
2	 Polygon "Plasma"	\$614M	▼ 26.88%		12.49%
3	 Ronin V2	\$521M	▼ 27.35%		10.60%
4	 Avalanche Bridge	\$377M	▼ 5.46%		7.67%
5	 Rainbow Bridge	\$200M	▼ 7.52%		4.07%
6	 Portal (Wormhole)	\$158M	▼ 8.89%		3.22%
7	 Multichain ⚠️	\$154M	▼ 25.34%		3.15%
8	 PulseChain	\$127M	▼ 5.07%		2.60%
9	 Orbit Bridge ⚠️	\$102M	▼ 4.17%		2.09%
10	 Satellite (Axelar)	\$94.89M	▲ 6.20%		1.93%

<https://12beat.com/bridges/tvl#active>

CROSS-CHAIN INTEROPERABILITY

Bridges - Limitations

- Tokens need to be defined in both chains, minting or reserves needed
- Smart contracts need to exist with well-known addresses in both chains
- Centralization risk
- Security risk
- Usually no distribution (e.g. multi-signature)
- N-to-n complexity
- Usually no atomic cross-chain swaps (locking of tokens, e.g. HTLC)



CROSS-CHAIN INTEROPERABILITY

Bridges - Limitations

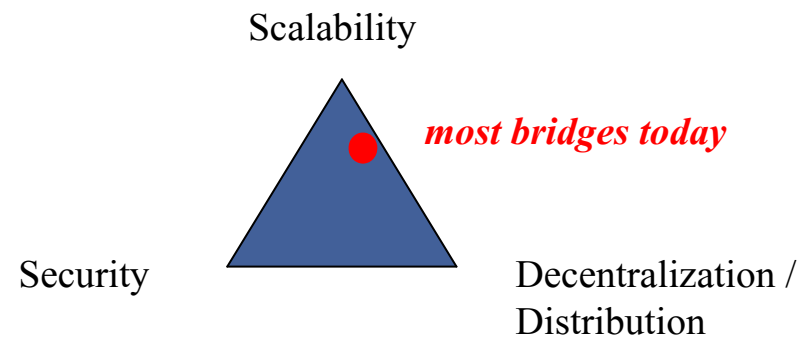
Bridge exploits account for ~50% of exploited funds in decentralized finance

(A. Fletcher, beamerbridge.com)

Recent Examples

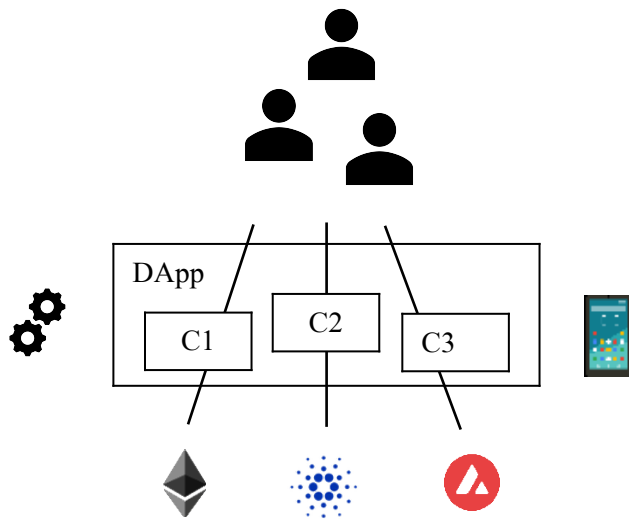
- Harmony Bridge: ~100M USD
- Ronin Bridge: ~600M USD
- Poly Network: ~600M USD

(Zamyatin, Imperial College London)



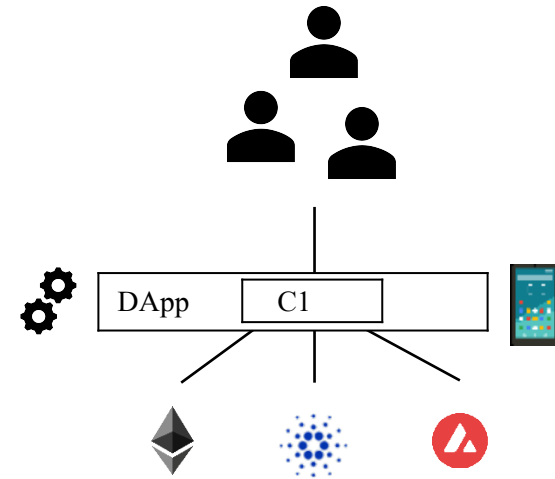
CROSS-CHAIN QUERY LANGUAGE

Application Level Interoperability



Current Architecture

Components (C) in n-to-n relationships



Integrated Architecture

Components (C) in 1-to-n relationship

CROSS-CHAIN QUERY LANGUAGE

Research Design of a Cross-Chain Query Language

Common data model

- Portability, compatibility, and migration advantages for software using blockchains

Standardized Syntax

- Abstract from implementation

Processing architecture

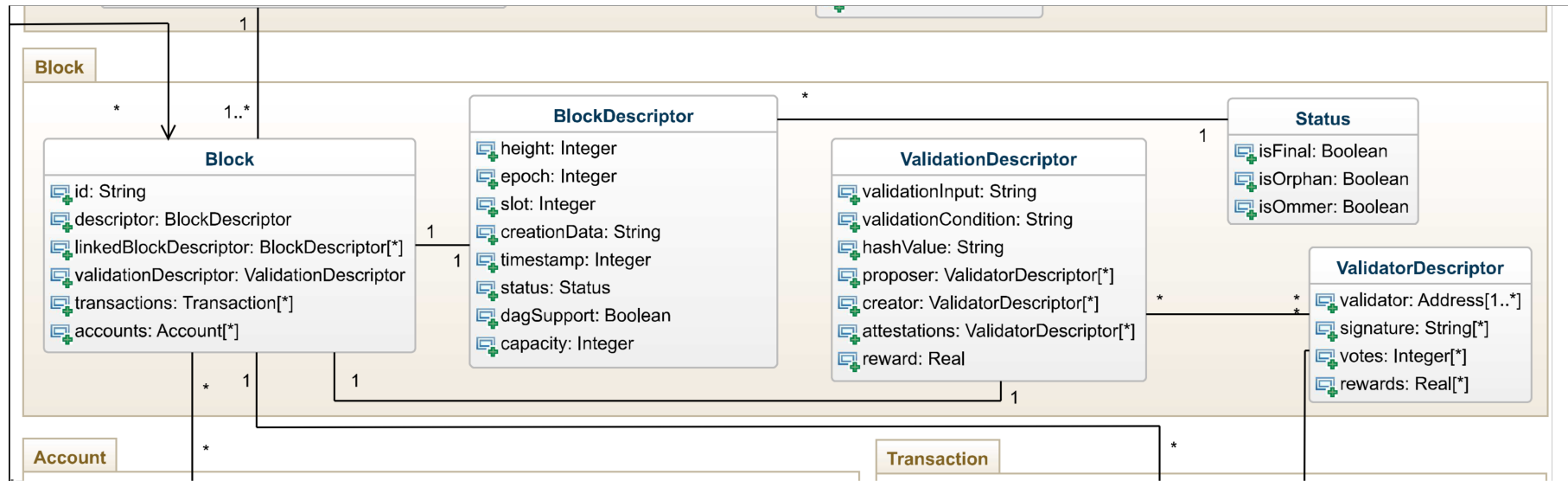
- Simultaneous access to multiple blockchains in individual query statements
- Utilization of the properties provided by blockchains

Related Publication:

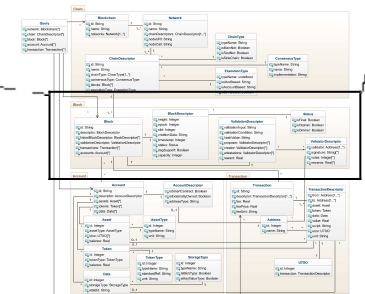
Härer, Felix (2022): **Towards Interoperability of Open and Permissionless Blockchains: A Cross-Chain Query Language**, in: Proceedings of the 2022 IEEE International Conference on E-Business Engineering (IEEE ICEBE 2022), October 14-16, 2022, Bournemouth, UK. *[Preprint arXiv:2209.07224 \[cs.DC\]](#)*

CROSS-CHAIN QUERY LANGUAGE – DATA MODEL

Data model derived from the blockchain concepts



Excerpt: Block Classes



C.f. Figure 1

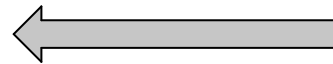
CROSS-CHAIN QUERY LANGUAGE – SYNTAX

Syntax definition based on Query-Source-Filter blocks using data model classes

Syntax

```
<QueryStatement> =  
  Q <AttrSpec>(, <AttrSpec>)*  
  S <SourceSpec>(, <SourceSpec>)*  
  [F <FilterSpec>(, <FilterSpec>)*];
```

Syntax derivation



Example

```
Q T.id, TDesc.value, TDesc.unit, TDesc.data  
S eth:main:1:Transaction.0xf50fc4bece6589655cc  
366ff2638de0e2ed61e01b500c138d5d3cd5450327334,  
avax:main:c:Transaction.0xb6b05f59ba6b69a082e6  
a8828d2afbf83a8847854fC56F3cC26a32e929104cef  
F TDesc.value == 0.0
```

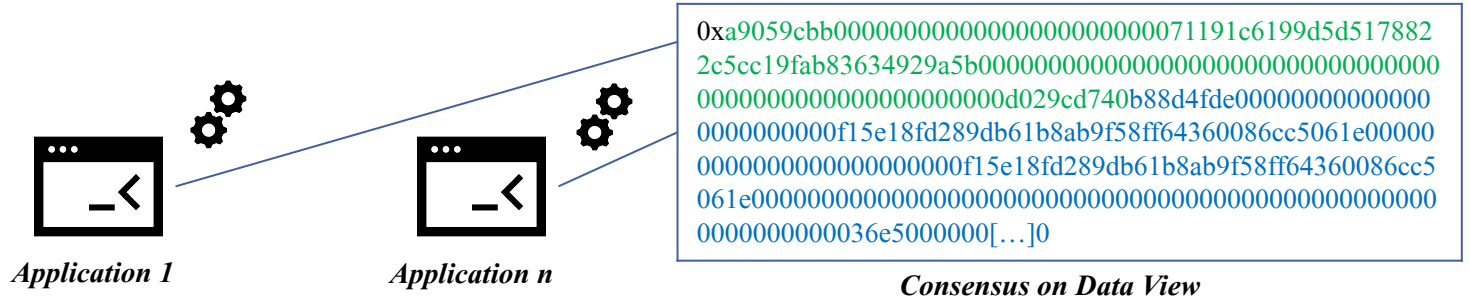
EBNF Grammar Specification

```
1 QueryStatement ::=
2   QueryAttrClause
3   SourceClause
4   FilterClause? ";"
5
6 QueryAttrClause ::=
7   'Q' AttrSpec ( ',' AttrSpec )*
8 SourceClause ::=
9   'S' SourceSpec ( ',' SourceSpec )*
10 FilterClause ::=
11   'F' FilterSpec ( ',' FilterSpec )*
12
13 AttrSpec ::=
14   CCQLClass '.' AttrName
15 SourceSpec ::=
16   BlockchainI ':' NetI ':' ChainDescI
17   ( ':' ( BlockI | TxI | AccI ) )?
18 FilterSpec ::=
19   CCQLClass '.' AttrName ComparisonFunction IValue
20
21 CCQLClass ::=
22   ChainPkgClass | BlockPkgClass | TxPkgClass | AccPkgClass
```

[...]

CROSS-CHAIN QUERY LANGUAGE – APP. EXAMPLE

Application Layer

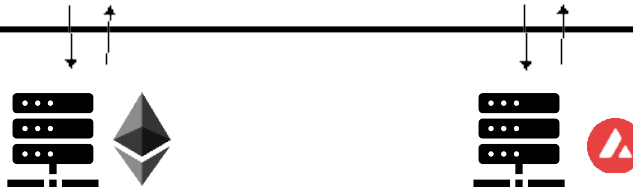


Data Layer

1:Transaction.id	1:TDesc.value	1:TDesc.unit
0xf50fc4bece65890		ETH
655cc366ff2638de		
0e2ed61e01b500c		
138d5d3cd545032		
7334		

1:TDesc.data	2:Transaction.id	2:TDesc.value	2:TDesc.unit	2:TDesc.data
0xa9059cbb00000000	0xb6b05f59ba6b6	0	AVAX	0xb88d4fde00000000
00000000000000000071	9a082e6a8828d2a			00000000000000000000
191c6199d5d5178822	fbf83a8847854fc5			f15e18fd289db61b8
c5cc19fab83634929a	6f3cc26a32e9291			ab9f58ff64360086cc
5b000000000000000000	04cef			5061e0000000000000
00000000000000000000				000000000000f15e1
00000000000000000000				8fd289db61b8ab9f5
000d029cd740				8ff64360086cc5061e
				00000000000000000000
				00000000000000000000
				00000000000000000000
				00000000036e50000
				00[...]0

Physical Layer



CROSS-CHAIN QUERY LANGUAGE – DISCUSSION

Cross-chain query language with data model, syntax, processing architecture

- Homogeneous data access
- Simultaneous access to one or more blockchains
- Standardized queries abstract from blockchain implementations

→ Software applications gain a shared view on data, secured by blockchain properties

Härer, Felix (2022): **Towards Interoperability of Open and Permissionless Blockchains: A Cross-Chain Query Language**, in: Proceedings of the 2022 IEEE International Conference on E-Business Engineering (IEEE ICEBE 2022), October 14-16, 2022, Bournemouth, UK. *[Preprint arXiv:2209.07224 \[cs.DC\]](#)*

INTEROPERABILITY BEYOND BLOCKCHAINS

Application Level Interoperability

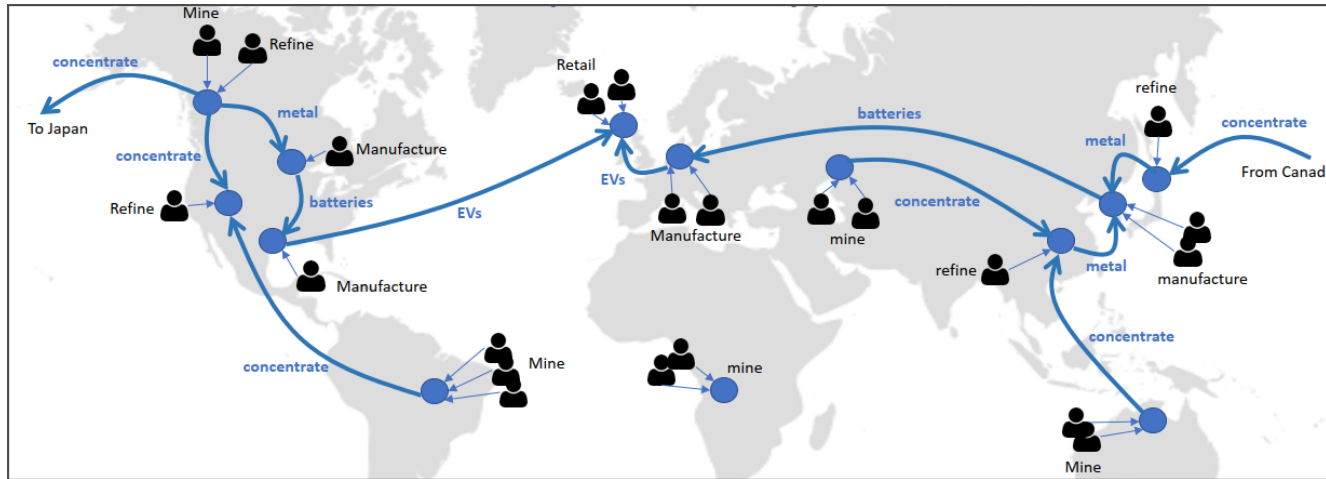
Interoperability of blockchains with, e.g.,

- Web and internet protocols
- IT architectures and the cloud
- Business Processes and Supply Chains

Interoperability with real-world applications deployed today?

INTEROPERABILITY BEYOND BLOCKCHAINS

Interoperability with real-world applications deployed today?



UPI Payments
in India

Textile Supply Chain



UN/CEFACT,
Capell

New York Times,
01.03.2023

INTEROPERABILITY BEYOND BLOCKCHAINS

Verifiable Credentials

"A verifiable credential is a tamper-evident credential that has authorship that can be cryptographically verified. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified. The claims in a credential can be about different subjects."

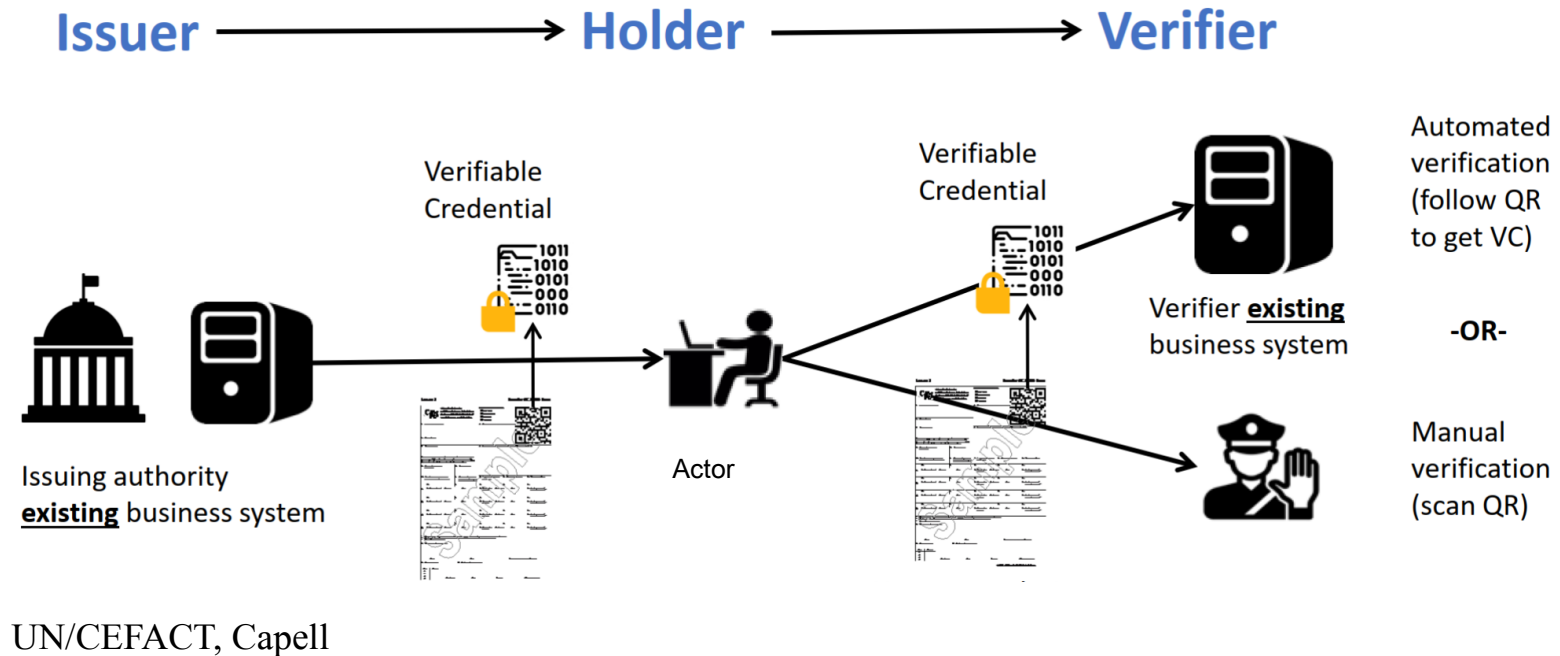


W3C Recommendation, Verifiable Credentials 1.1, 2022, VC Data Model

<https://www.w3.org/TR/vc-data-model/>

INTEROPERABILITY BEYOND BLOCKCHAINS

Verifiable Credentials - Application

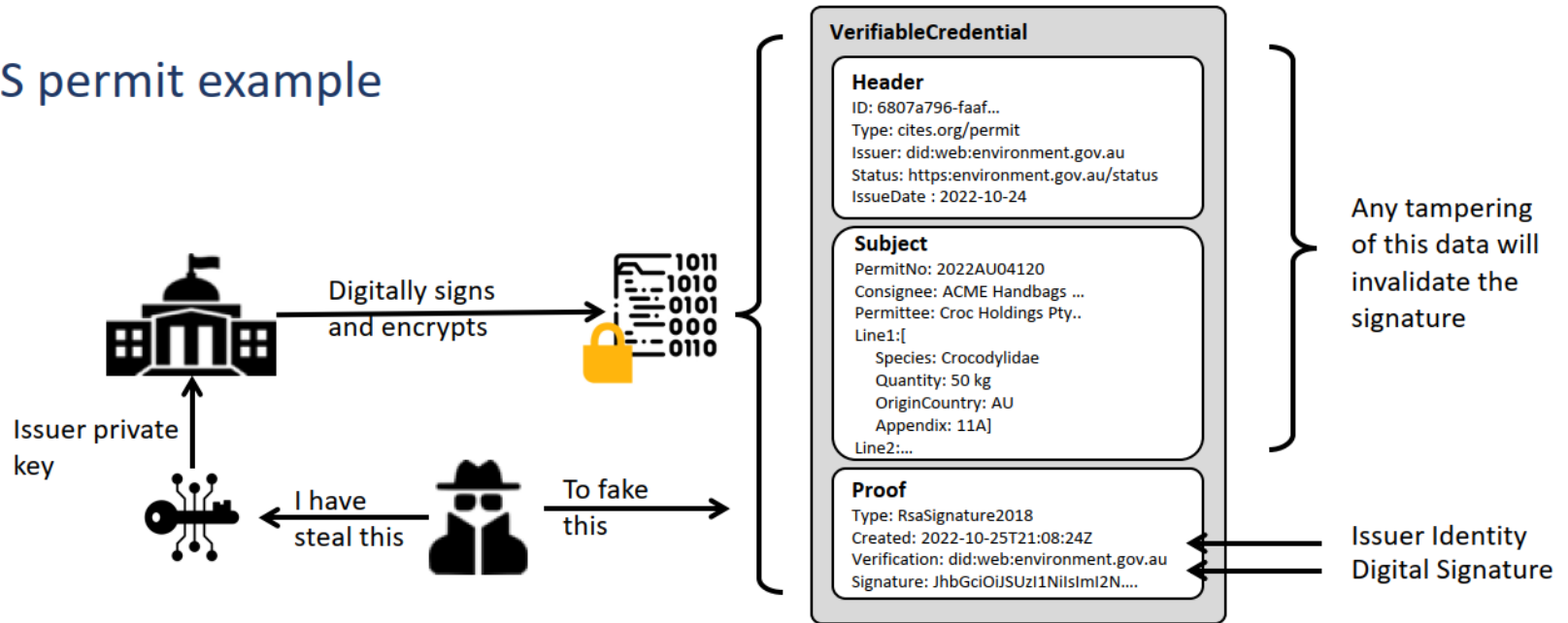


Verifiable by business systems and state authorities.

INTEROPERABILITY BEYOND BLOCKCHAINS

Verifiable Credentials - Application

CITES permit example

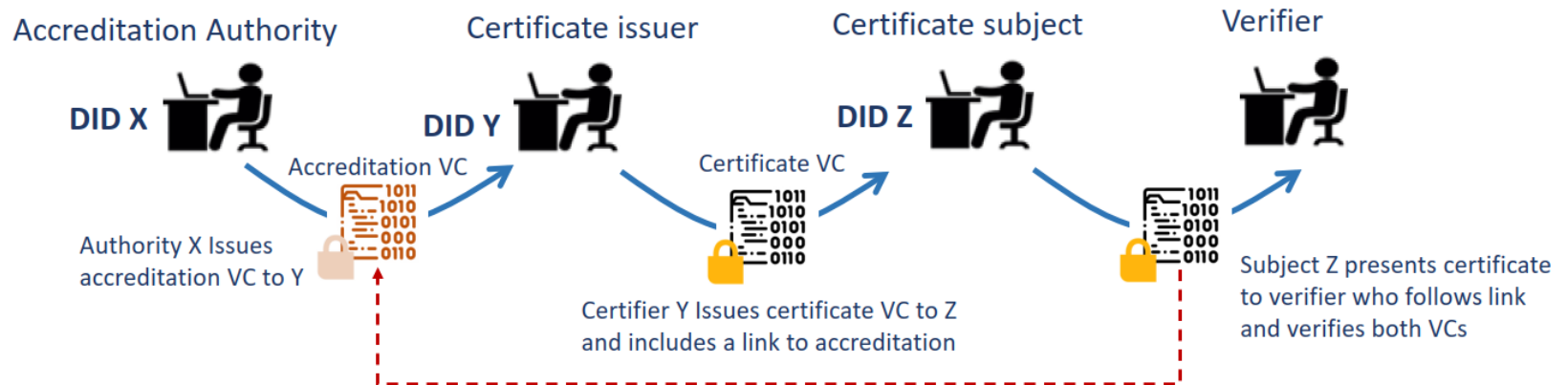


CITES:
Convention on International Trade in
Endangered Species of Wild Fauna
and Flora (CITES)

UN/CEFACT, Capell

INTEROPERABILITY BEYOND BLOCKCHAINS

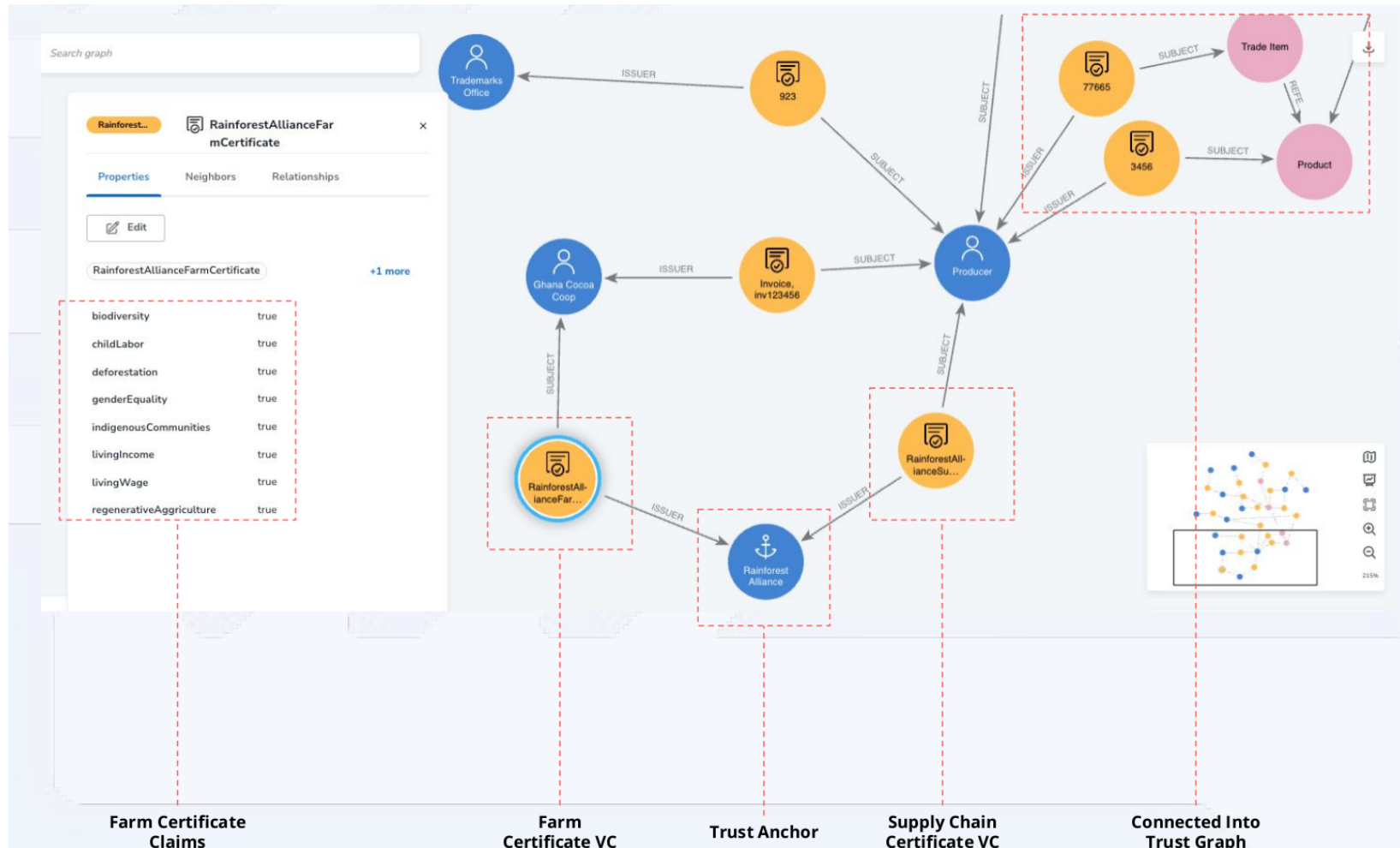
Outlook - Decentralized Identifiers (DID) and Trust Graphs



UN/CEFACT, Capell

INTEROPERABILITY BEYOND BLOCKCHAINS

Outlook - Decentralized Identifiers (DID) and Trust Graphs



UN/CEFACT, Jespersen

INTEROPERABILITY BEYOND BLOCKCHAINS

Verifiable Credentials - Conclusion

- Portable and self-contained packet
- Secured using digital signature standards
- Can include a human rendering
- Compatible to existing systems

Scalable, Decentralized, Secure.



UPI Payments in India

New York Times,
01.03.2023

Support and Adoption

- Standardized by W3C
- UN/CEFACT recommendation to policymakers (40th UN/CEFACT Forum May 2023)

BLOCKCHAIN FOR INFORMATION SYSTEMS

Conclusion

Verifiable Credentials, DID, UPI do not require blockchains.

We need standards on an application level.

We need systems compatible to real-world applications that are

- **open and permissionless,**
- **scalable,**
- **secure, and**
- **decentralized.**



UPI Payments in India

New York Times,
01.03.2023

What is a blockchain?

unifr.ch/inf/digits

Dr. Felix Härer
felix.haerer@unifr.ch