QUANT-X SECURITY & CODING

Distinct Data Protection and Post-Quantum Security for Blockchain Applications

https://quant-x-sec.com/ | xb@quant-x-sec.com

Architectural Components

Ledger

- actual database, chain of data blocks
- distributed all over a blockchain network

Nodes/Pools of Nodes

- machines or collections of machines
- determine the order of entries in ledger

Accounts

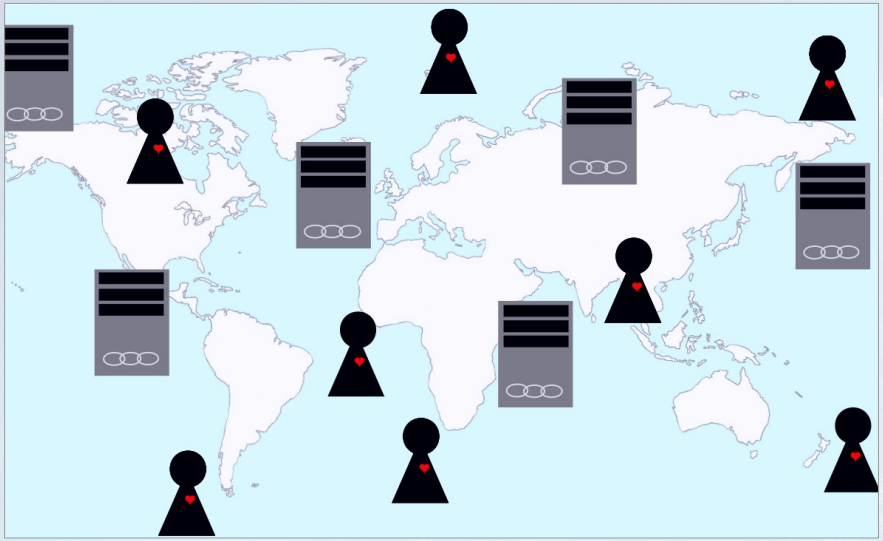
- represent members of the network
- can send or receive transactions
- located on devices such as PC's or mobile phones

Other instances (e.g. webservers)

- serve information about the ledger to accounts
- act as controlling instances for network communication

Public, Consortium and Private Blockchain

.

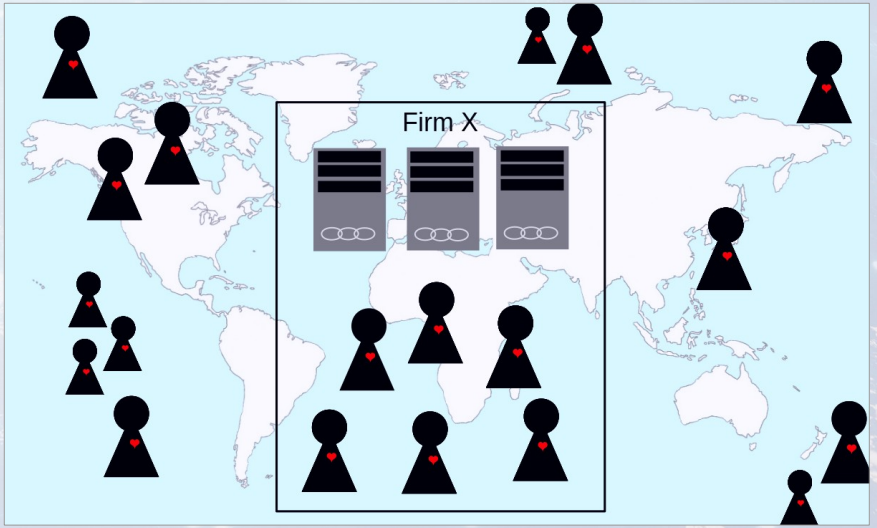


Independent of Architecture

- GDPR regarding data on ledger
- Platform depending access mechanisms
- Validity of crypto algorithms

Depending on Architecture

- Choice and control of consensus mechanism
- GDPR regarding nodes
- Other data protection laws



xb@quant-x-sec.com

Crypto Currencies and Blockchain Applications without Currency

The first Blockchain application was Bitcoin, an alternative financial value system.

xb@quant-x-sec.com

Crypto Currencies and Blockchains without Crypto Values

First Blockchain Application was Bitcoin, an alternative financial value system.

But there are many other Blockchain platforms without crypto currencies, e.g.:

- Hyperledger
- Corda

Why blockchain without crypto currencies?

- Immutable data on ledger
- Integrity of shared data in private and consortium blockchains*

* Not guaranteed in open blockchain network with malicious firewalls because of branching (no byzantine fault tolerance).

GDPR and other Regulations

Special security feature of Blockchain:

All data in ledger is immutable → Nothing which is written on the ledger can ever be changed!!!

Consequence of this fact & GDPR right to erasure & right to to rectification:

Storage of personal data* in ledger of common blockchains violates Art. 16 f. GDPR, Art. 16 LED

Furthermore risky for use of public blockchains:

Source: https://www.ait.ac.at/fileadmin//mc/digital_safety_security/downloads/Pesch_TransparencyLegal.pdf

- Transparency of blockchain data ≠ transparency of data processing (Art. 5 I a GDPR; Recital (26) LED)
- Data transparency runs counter to principle of data minimisation (Art. 5 I c GDPR)
- Other regulations as EU Directive PE CONS, FinCEN, governmental regulations are evolving.

* Defined as any information relating to an identified or identifiable natural person, e. g. addresses = pseudonyms

GDPR and other Regulations

Special security feature of Blockchain:

All data in ledger is immutable → Nothing which is written on the ledger can ever be changed!!!

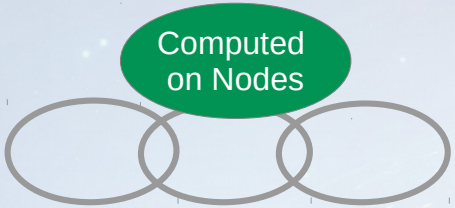
Consequence of this fact & GDPR right to erasure & right to to rectification:

Storage of personal data* in ledger of common blockchains violates Art. 16 f. GDPR, Art. 16 LED

Ongoing researches in order to solve the challenge:

- **Pruning** as a technical solution to make a blockchain forget data. The base for making this possible has to be implemented in the blockchain core technology.
- **Corresponding micro-transactions** on chain with offchain links. Obfuscate onchain data by deleting the offchain links.
- **Legal considerations**, such as outweighing the violation of right to erasure and rectification by the fact that blockchain technologies satisfy other articles of the GDPR, such as certification of user consent, better than other technologies. (protective circle - privacy by blockchain design)

Crypto Algorithms in the Context of Blockchain



Nodes
3) Asymmetric key pairs for identification
4) Password protected encryption of private key(s)
5) TLS and VPN crypto certificates

Ledger
1) Hashes for data integrity in blocks
2) DAGs, Merkle Trees and other proofs of work

Other Instances
6) TLS crypto certificates
7) VPN certificates

Accounts
8) Asymmetric key pairs for identification
9) Password protected encryption of private key(s)

xb@quant-x-sec.com

Crypto Algorithms in the Context of Blockchain

Problem

Currently used crypto algorithms are about to be replaced due to security threats by:

1) Technological improvements in performance
2) Newly discovered mathematical models for attacks on cryptographic algorithms
3) Rise of quantum technologies

NIST standardization for new crypto algorithms (Post-Quantum-Cryptography) is running until 2021/22. Most key pairs around blockchain platforms can be replaced in time. But:

Consequences

✗Encrypted data on public blockchains will not be confidential forever!

✗Confidential data sent via encrypted channels and being collected now together with the related key exchanges, can be decrypted sooner or later!

Conclusion

1) Blockchain technologies are highly complex regarding tech and legal questions.
2) The variety of blockchain platforms has become great, their properties very various.

Integrate legal, technical, algorithmic experts and consider second opinions in order to

1) Choose the right platform for your needs
2) Make wise decisions about architecture and data handling

Thank you!!!

X. Bogomolec | Quant-X Security & Coding GmbH | xb@quant-x-sec.com