MODULE:

2.4

Oracles, Data, GDPR

BESIDE
Blockchain usE caSes In Digital financE

Blockchain usE caSes In Digital financE – BESIDE – 2022-1-DE02-KA220-VET-000089587 is funded by Erasmus+.
The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by
the European Union

OUTLINE

BESIDE
Blockchain usE caSes
In Digital financE

1.	Personal Data	3
2.	GDPR	9
3.	GDPR Issues in Blockchains	13
4.	Data Connectivity & Oracles	20
5.	Conclusions	26

Co-funded by
the European Union

CHAPTER:

1.

Personal Data

BESIDE
Blockchain usE caSes In Digital financE

Co-funded by
the European Union

PERSONAL DATA

PERSONAL DATA

Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, particularly through an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (art. 4 GDPR).

DEFINITIONS	Natural Person	The data is related to a living individual, not a company. Some exceptions apply.
	Any Information	Objective information, not limited to any particular format.
	Data Processing	Any action performed on data, whether automated or manual. (collecting, recording, organising, storing, using, erasing,…)

Co-funded by
the European Union

PERSONAL DATA

EXAMPLES OF PERSONAL DATA

- NAME
- ADDRESS
- ID / PASSPORT NUMBER
- CULTURAL PROFILE
- IP ADDRESS
- ETHNICITY
- POLITICAL OPINIONS
- RELIGION
- GENETIC, BIOMETRIC, HEALTH DATA

Co-funded by
the European Union

DATA PROTECTION IN THE EU

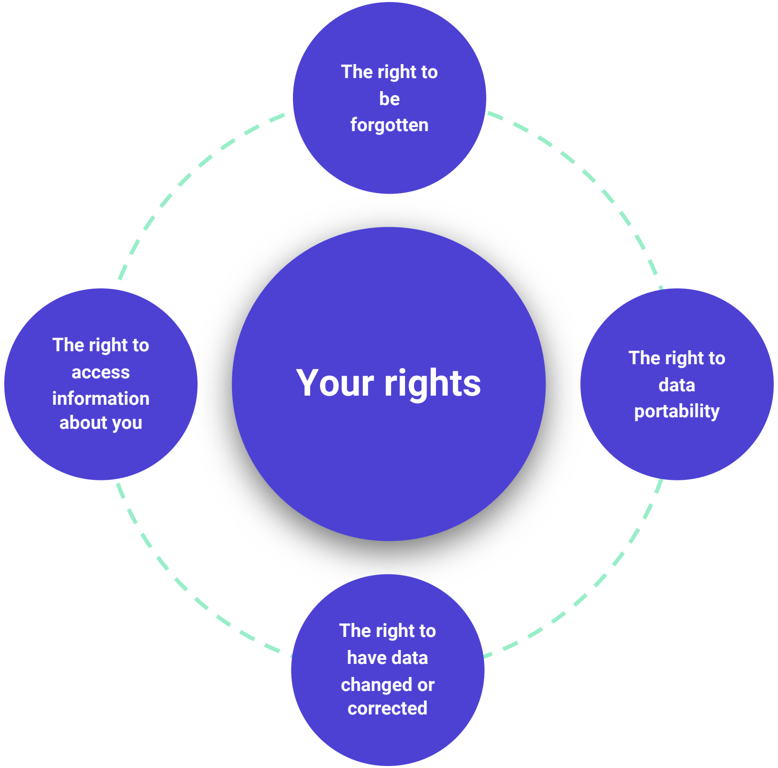
In the European Union, data protection has the status of a fundamental right. Article 8 of the Charter of Fundamental Rights states that everyone has the right to the protection of personal data concerning them.

As a consequence, personal data 'must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law' under Article 8(2) of the Charter. The Charter furthermore ensures that everyone has the right to access personal data relating to them, as well as the right to have such data rectified or deleted.

Co-funded by the European Union

DATA PROTECTION RIGHTS

BESIDE
Blockchain usE caSes
In Digital financE



Your rights

The right to be forgotten

The right to access information about you

The right to data portability

The right to have data changed or corrected

Co-funded by the European Union

DATA PROTECTION BASICS

1	**Lawfulness, fairness and transparency**	Processing of data must be lawful, fair, and transparent to the data subject.
2	**Purpose limitation**	You must process data for the legitimate purposes specified explicitly to the data subject during the collection process.
3	**Data minimisation**	Data minimisation — You should collect and process only as much data as absolutely necessary for the purposes specified.
4	**Accuracy**	You must keep personal data accurate and up to date.
5	**Storage limitation**	You may only store personally identifying data for as long as necessary for the specified purpose.
6	**Integrity and confidentiality**	Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7	**Accountability**	The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

CHAPTER:

2.

GDPR

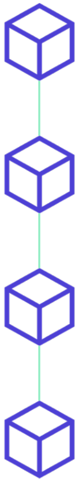
Co-funded by
the European Union

GDPR

The General Data Protection Regulation (GDPR) is regarded as the most stringent data protection regulations globally. It limits the uses of personal data by companies and improves individuals' access to information about themselves. The GDPR's full text is a detailed document made up of 99 separate articles.

The GDPR applies to all companies either located, operating, or serving customers in the European Union. Many companies chose to adhere to the GDPR as it can be seen as one standardised privacy protection policy.

How does this apply to blockchain?



A blockchain permanently and immutably stores all transactions.

These transactions may in some form include personal data, which is an issue.

Co-funded by
the European Union

GDPR: DATA STORAGE

> “ The storage period shall take into consideration the reason(s) why you process the data and any legal obligations
> (e.g.: tax laws, product warranty, national labour law, etc.). ”

✅ Data should be stored for the shortest period of time possible.

✅ Stored data must be accurate and kept up-to-date.

✅ Companies which store data must set time limits of erasure/review of stored data.

Co-funded by the European Union

GDPR: DATA STORAGE

EXAMPLE

You manage a recruitment office that collects CVs of people looking for a placement in exchange of a fee for your intermediary service. You plan to keep the data for 20 years and you take no measures for updating the CV archive.

Unfortunately, the storage period does not reflect the purpose of finding people a work placement in the short/medium term.

Furthermore, it is clear that after some time such CVs become useless to seek a workplace if they are not updated (one of cases could be that the person has gained experience or has got new qualifications).

❌

This would not be GDPR compliant.

Co-funded by
the European Union

CHAPTER:

3.

GDPR Issues in Blockchains

Co-funded by
the European Union

STORAGE OF DATA: BLOCKCHAINS

Blockchains store data in a decentralised way by using a dispersed network of computers around the globe rather than in a single location. In doing so, it is possible to safely and permanently store a wide range of data which remains unaltered.

While this is not an issue for non-personal data, some issues may arise with respect to personal information:

1. **Identification and Obligations of Data Controllers and Processors**
2. **The Anonymisation of Personal Data**
3. **Exercise of some Data subjects rights**

Co-funded by the European Union

1. Right to Erasure and Rectification

GDPR grants individuals the right to have their personal data erased under certain circumstances (Article 17). This is challenging for blockchains, as they are inherently designed to be immutable, meaning once data is added, it cannot be altered or deleted.

Immutability: The foundational principle of blockchain is its immutable ledger, ensuring data integrity and trust. However, this clashes with the GDPR's requirement to allow data erasure.

Decentralisation: In decentralised blockchains, no single entity has control over the entire network, making it difficult to enforce data erasure across all nodes.

Co-funded by
the European Union

2. Right to Erasure and Rectification

GDPR requires that personal data be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing (Article 5 and Article 32). It also has strict rules around the processing of personal data, requiring consent or another legal basis for processing.

Pseudonymization vs. Anonymization: While blockchains often use pseudonymization (replacing private identifiers with fake identifiers), in some cases GDPR requires anonymization (completely stripping away personal identifiers). Achieving true anonymization on a blockchain is challenging due to its transparent and permanent nature.

Data Control and Access: In public blockchains, data is visible to all participants, raising concerns about data privacy and unauthorised access.

Co-funded by
the European Union

BLOCKCHAIN GDPR ISSUES

Storing personal data on a blockchain, even when encrypted, is not advisable due to the inherent risks and challenges mentioned previously.

Encryption, while providing a layer of security, is not foolproof and can be vulnerable to advances in decryption techniques and computational power over time, potentially exposing the personal data.

Co-funded by
the European Union

GDPR COMPLIANT TECHNIQUES

There are 4 main GDPR compliant techniques to utilise personal data in the context of Blockchain systems:

HASHING

Instead of storing the actual personal data, a cryptographic hash of the data can be stored on the blockchain. This ensures data integrity without exposing the actual information.

OFF-CHAIN STORAGE

Personal data can be stored off the blockchain, with only a reference or hash of the data stored on-chain. This approach maintains the integrity and verifiability benefits of blockchain while keeping the personal data mutable and more secure.

PERMISSIONED CHAINS

These types of blockchains restrict access to approved participants only, providing a higher level of privacy and control compared to public blockchains.

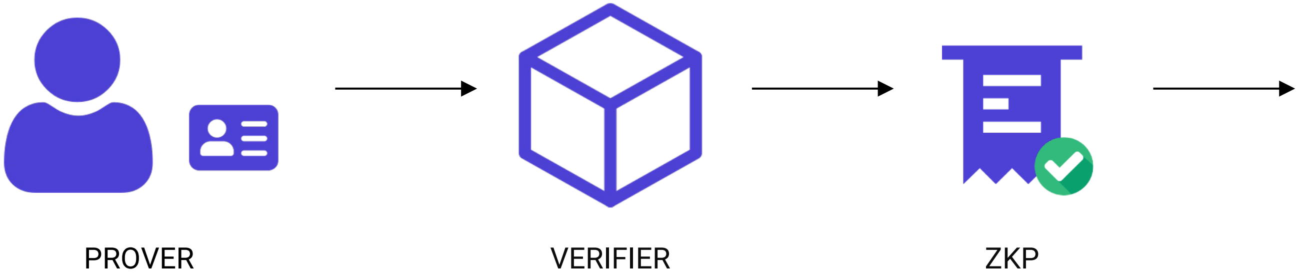
ZERO-KNOWLEDGE PROOFS

This cryptographic technique allows for the verification of certain properties of the data without revealing the data itself, ensuring privacy while leveraging blockchain for data integrity.

Co-funded by the European Union

ZERO KNOWLEDGE PROOFS

Zero Knowledge Proofs (ZKPs) are cryptographic techniques that enable one party (the prover) to prove to another party (the verifier) that a certain statement is true, without revealing any information about the statement itself.



Using ZKPs, personal data is not recorded onto the blockchain.

The only information recorded is that the prover successfully proved some data to a verifier.

Co-funded by the European Union

CHAPTER:

4.

Data Connectivity & Oracles

BESIDE
Blockchain usE caSes In Digital financE

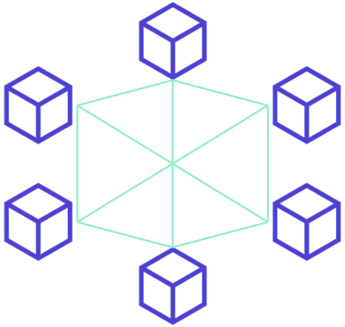
Co-funded by the European Union

DATA CONNECTIVITY

Blockchains are inherently closed networks with no native connection to external systems or data.

This is inherent to the security and integrity of blockchains, however it severely restricts the usefulness of the technology.

There are several ways of bringing real-world data into blockchain systems. All with their own pros and cons regarding efficiency, GDPR compliance, and more.

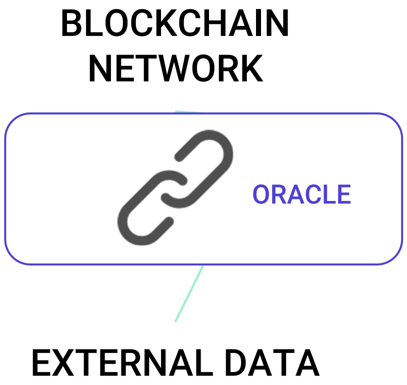


Co-funded by the European Union

ORACLES

An oracle in a blockchain network is a type of middleware that connects smart contracts with external data sources, allowing them to securely interact with real-world information.

This bridge is essential for executing smart contracts based on off-chain events and data. Almost any type of data can be brought on-chain by using an oracle.



BLOCKCHAIN NETWORK

ORACLE

EXTERNAL DATA

Co-funded by
the European Union

ORACLES

Oracles can be used to make many types of data available on chain.

MARKET
DATA

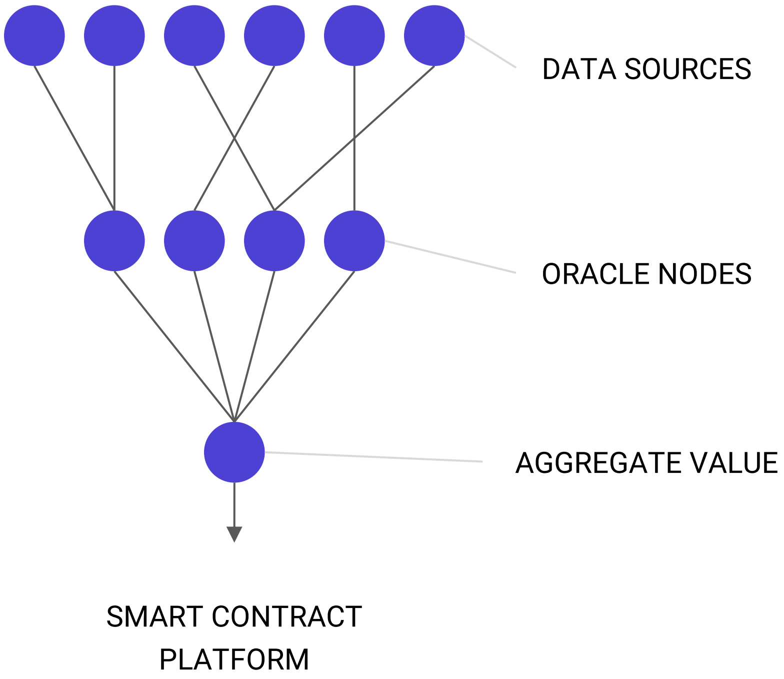
EVENT
DATA

WEATHER
DATA

… and many more.

Co-funded by
the European Union

DECENTRALISED ORACLE NETWORKS



Execution of smart contracts is guaranteed to happen as written.

Smart contracts that rely on external data may be susceptible to manipulation of that data.

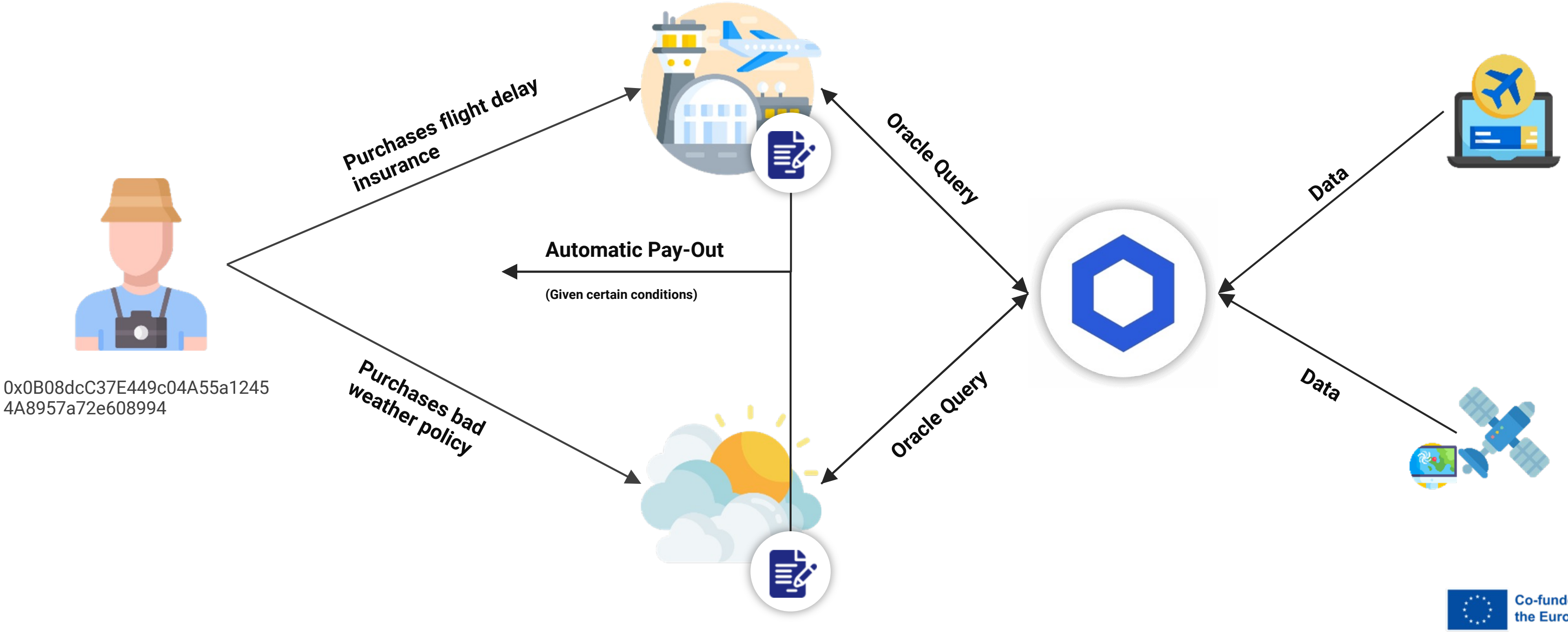
Decentralised Oracle Networks gather data from various sources and transmit an aggregate value to the smart contract.

Co-funded by the European Union

ORACLES: EXAMPLE USE CASE

BESIDE
Blockchain usE caSes
In Digital financE

Automated Parametric Insurance using Oracles & Smart Contracts


Purchases flight delay insurance
Automatic Pay-Out
(Given certain conditions)
Purchases bad weather policy
0x0B08dcC37E449c04A55a1245
4A8957a72e608994
Oracle Query
Oracle Query
Data
Data

Co-funded by the European Union

CHAPTER:

5.

Conclusions

Co-funded by
the European Union

CONCLUSIONS

GDPR Personal data should never be recorded on public blockchains.

Data Blockchains are not natively able to access real-world data.

Oracles Oracles are a type of middleware that bring data on-chain while aiming to minimise the need for trust in a single party.

Co-funded by
the European Union

BIBLIOGRAPHY

- https://gdpr.eu/
- https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm
- https://gdpr-info.eu/
- https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en
- https://www.ibm.com/topics/data-storage#:~:text=Data%20can%20be%20recorded%20and,block%20storage%20and%20object%20storage.&text=File%20storage%2C%20also%20called%20file,to%20organize%20and%20store%20data
- https://www.techtarget.com/searchstorage/definition/blockchain-storage
- https://academy.binance.com/en/articles/what-is-decentralized-storage
- https://medium.com/@backpacinc/blockchain-data-connectivity-vs-traditional-telecom-carriers-1ddbda2e6a98
- https://icommunity.io/en/blockchain-and-gdpr/
- https://gdpr-info.eu/
- https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Co-funded by
the European Union

CONTACTS

BESIDE

Blockchain usE caSes In Digital financE

e-mail: info@besideproject.eu

website: www.besideproject.eu

LinkedIn: https://www.linkedin.com/company/besideproject/

Blockchain usE caSes In Digital financE – BESIDE – 2022-1-DE02-KA220-VET-000089587 is funded by Erasmus+.
The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union