SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE
Finanziato dall'Unione europea
NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA
UNICAM
Università di Camerino
1336
Università di Camerino

Analyzing DApps: from Extraction to Visualization

Andrea Morichetta

University of Camerino, Camerino, Italy

Context

Decentralized Applications (DApps) expanded among several domains and they use **smart contracts to encode and execute business logic**

Ensuring the **correctness of smart contract behaviour is crucial** as logical flaws or undesired situations may occur

Many approaches focus on **verifying the implementation of smart contracts** by analysing data obtained before their deployment, such as source code or bytecode

Smart Contract Execution Analysis

Smart contracts have been the subject of many **high-profile exploitation** that differently from code vulnerabilities, **cannot be detected during the development**

Logical Flaws in Design

- Incorrect assumptions
- Unhandled edge cases

Behavioral Analysis

- Centralization
- Token velocity

Exploits

- Flash loans
- Market manipulation

Smart contract execution generates **on-chain data** can reveal novel perspectives during **analysis and monitoring activities**

Contribution

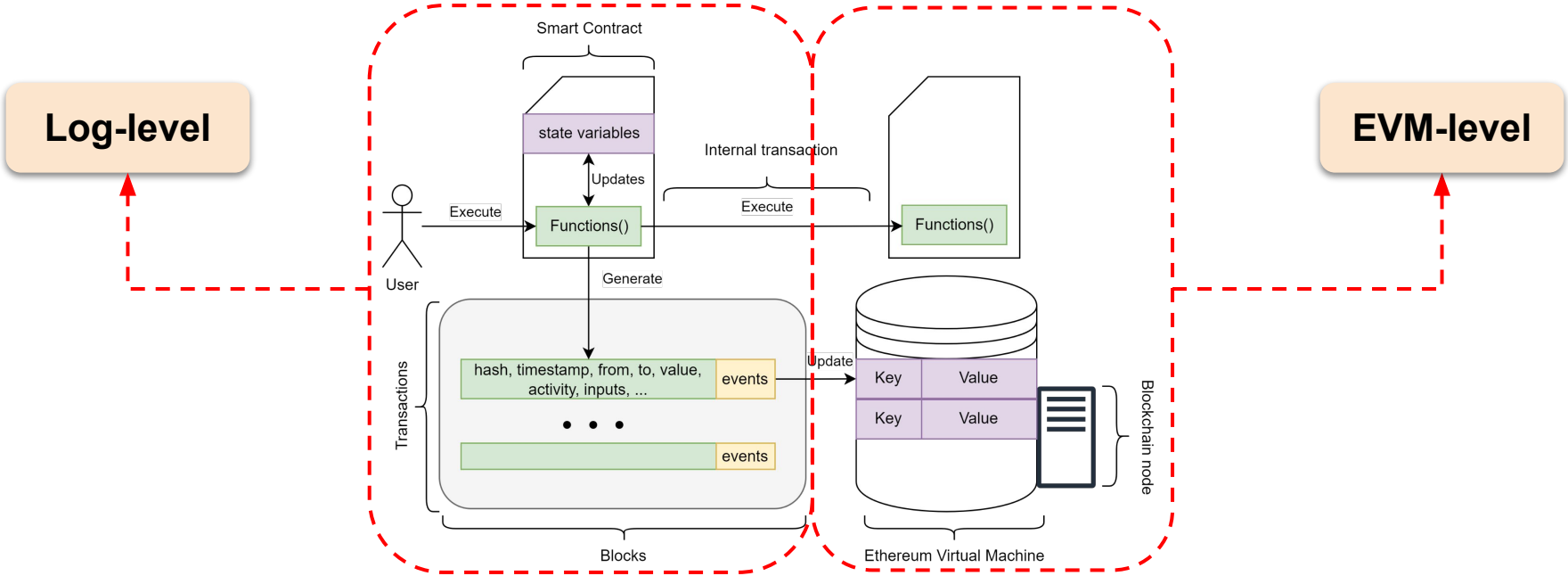
We propose a **framework supporting the analysis of decentralized applications** leveraging execution data [1]

Key benefits:

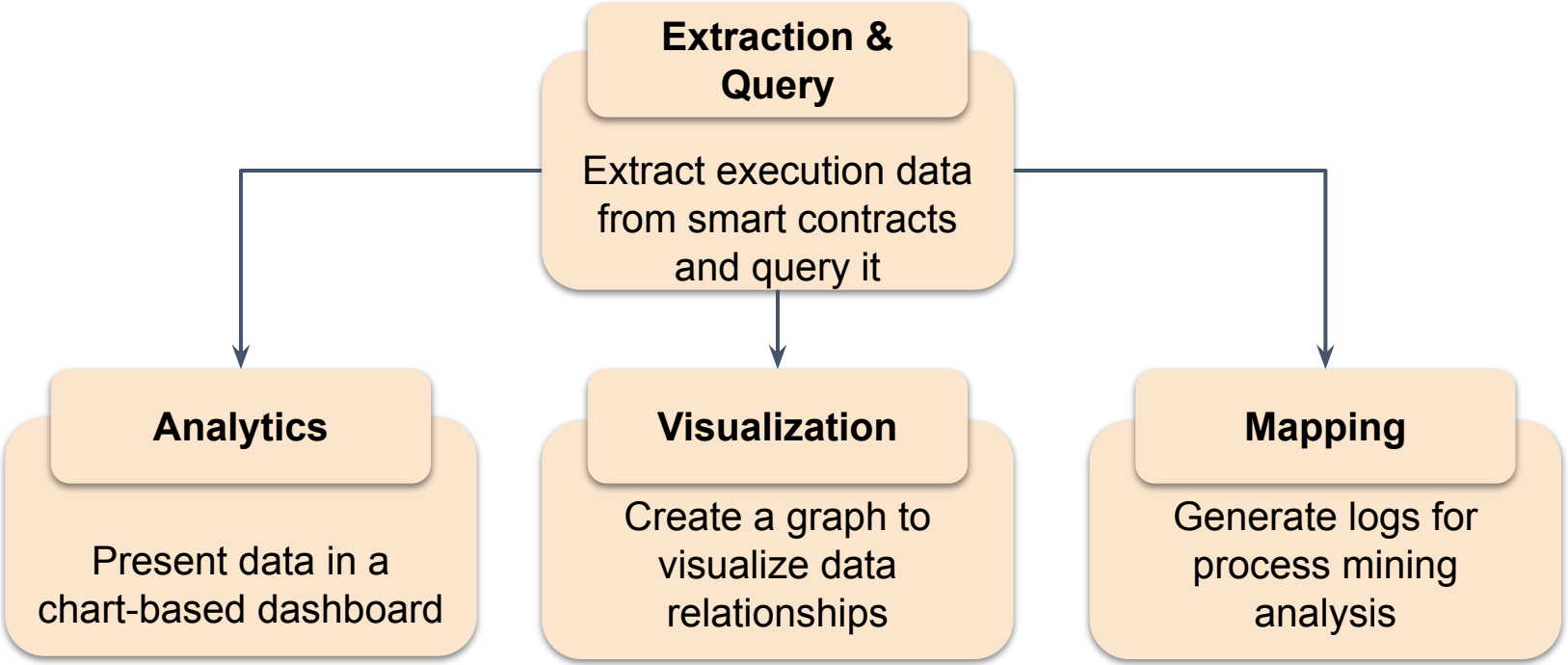
1. **extraction** of **execution data**
2. clear and intuitive **understanding of interactions** among dapps smart contracts
3. **All-in-one tool** accessible without requiring technical skills

[1] F. Corradini, A. Marcelletti, A. Morichetta, B. Re, L. verducci. A Mapping Methodology Enabling Object-Centric Process Mining on Blockchain Applications, Blockchain: Research and Applications (2025)

Smart Contract Execution Data

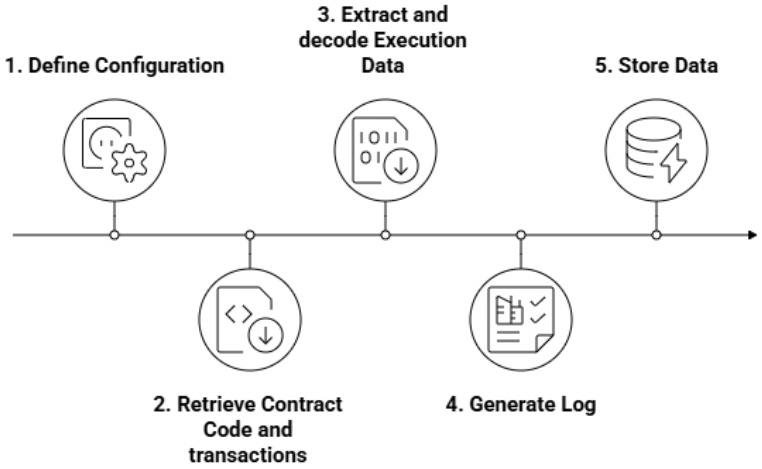


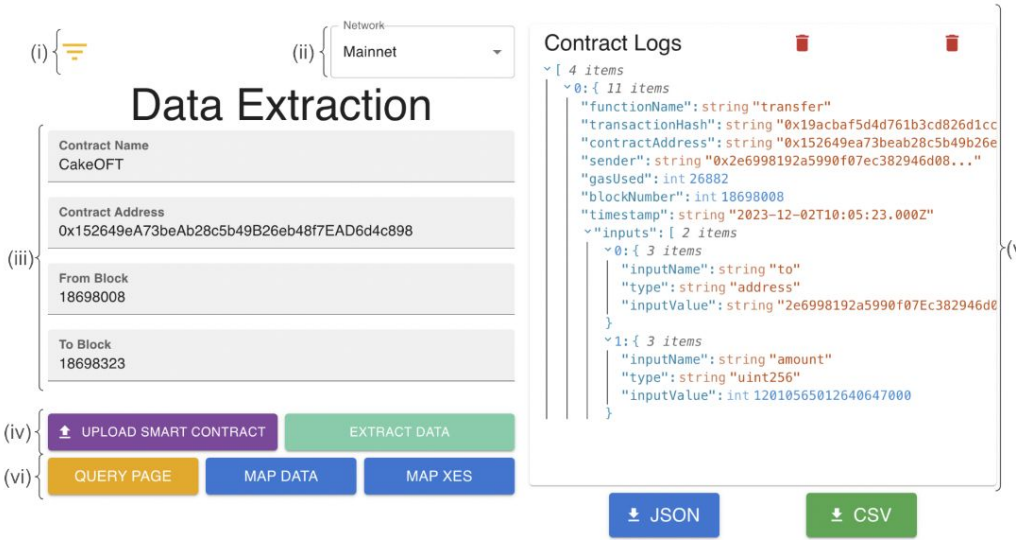
The Framework Modules



Extraction and Query Modules

The modules [2] automates the collection, decoding, and storage of smart contract execution data, making it accessible for analysis



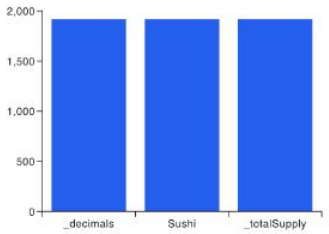


[2] F. Corradini, A. Marcelletti, A. Morichetta, B. Re, A methodology for extracting and decoding smart contracts data, Computer Communications (2025)

Analytics Module

Chart-based dashboard that visualizes and explores data from multiple smart contracts

Section	Chart content	Table content
Gas Used	Total percentage of gas consumed by each function	Smart contract information, function name, total gas consumed by each function
Function	Occurrence of executed function by each function	Smart contract information, function name, occurrences of executed function
Sender	✗	Sender address, occurrences of transaction performed, average gas used
Time	Time interval of sent transaction	✗
Input	Occurrences of each input variable	Smart contract information, input name, input type, occurrences of each input variable
Event	Occurrences of each emitted event	Smart contract information, event name, occurrences of each emitted event
Internal transaction	Occurrences of each internal transaction	Smart contract information, internal call type, occurrences of each internal transaction
Storage state	Occurrences of each updated state variable	Smart contract information, variable name, occurrences of each update state variable

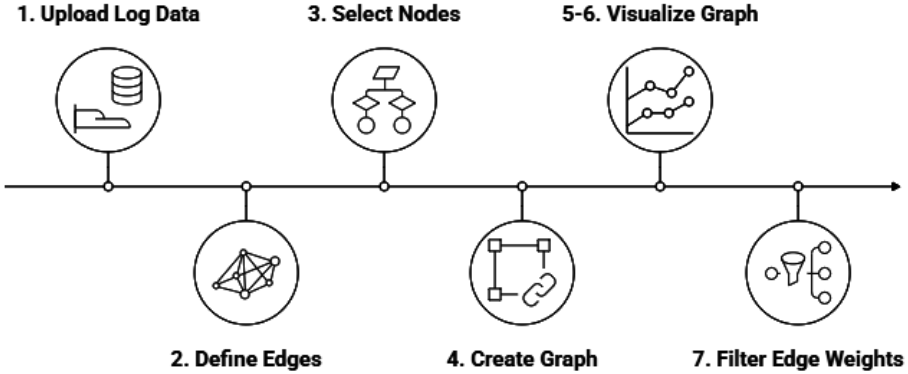


Smart Contract	Variable Name	Occurrences
0x2662e8407673927826...	_decimals	1916
0x2662e8407673927826...	Sushi	1916
0x2662e8407673927826...	_totalSupply	1916

Rows per page: 100 1–3 of 3

Visualisation Module

Extracted data can be visualized as **undirected graphs to reveal complex relationships**

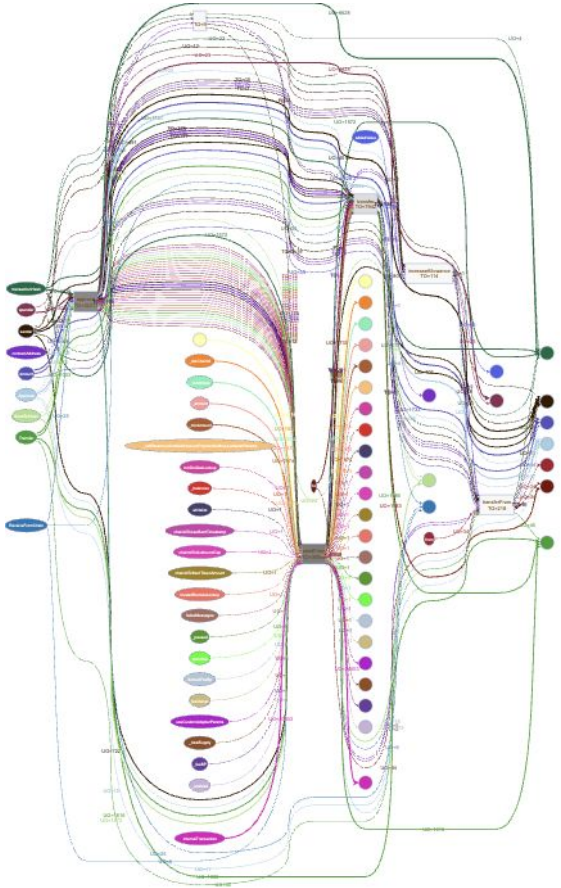


Mapping Module

This module enables **process mining analysis** on blockchain applications [3] by:

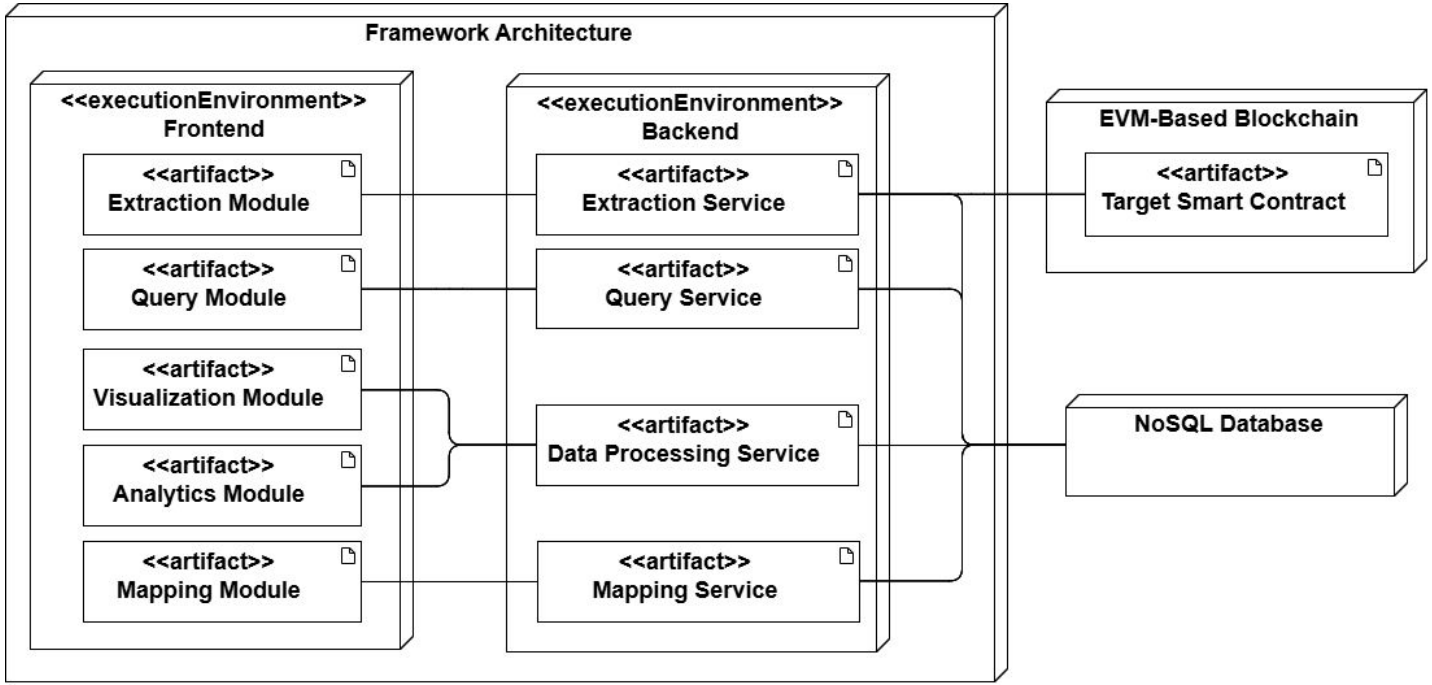
- **Automatically mapping** executed smart contract functions to process mining **events**
- **Manually selecting** of which blockchain data should be mapped as an **object**

As a result, an OCEL2.0 log is generated, usable in current available tools



[3] F. Corradini, A. Marcelletti, A. Morichetta, B. Re, L. verducci. A Mapping Methodology Enabling Object-Centric Process Mining on Blockchain Applications, Blockchain: Research and Applications (2025)

Implementation



To Wrap Up

Conclusion

Analysing DApps is crucial to ensure their correct behavior and detect issues

Smart contract execution data enables the analysis of the actual behavior

We propose a framework for supporting DApps Analysis, **integrating from data extraction to its visualization**

Future Works

Apply **monitoring techniques** to detect specific behaviors

Enhance graph functionalities with custom aggregation or clustering

Provide an **open source dataset** of extracted smart contracts

Thank you for your attention

Andrea Morichetta

andrea.morichetta@unicam.it