

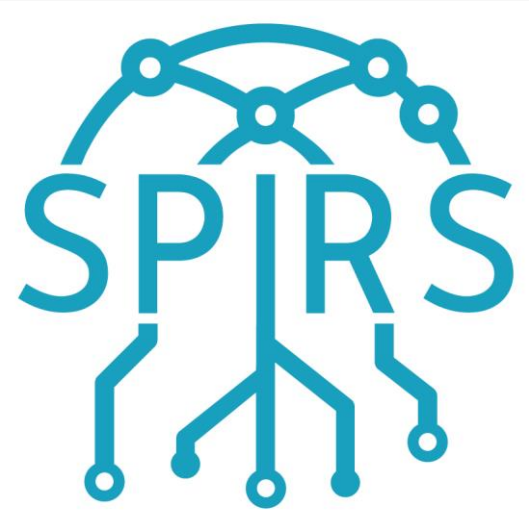
LINKSFOUNDATION.COM



Protocollo abilitante per la gestione sicura dei dati sul Tangle IOTA per processori RISC-V

DAVIDE MARGARIA, Senior Cybersecurity Researcher
Torino, 26 Maggio 2023





Acknowledgement

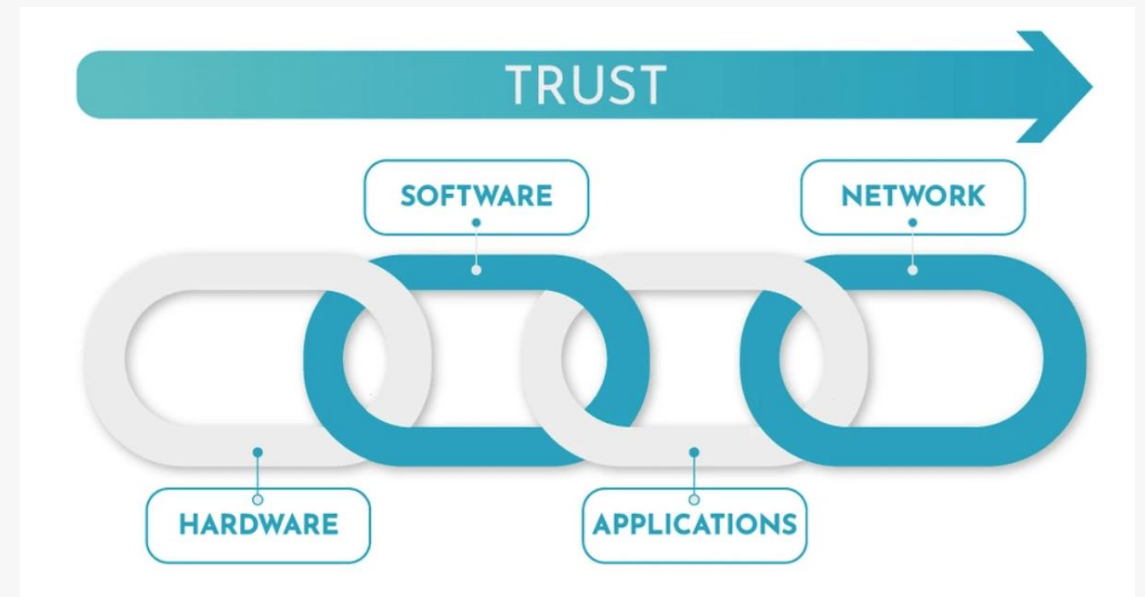
■ SPIRS project

This work was supported by the SPIRS (*Secure Platform for ICT systems Rooted at the Silicon manufacturing process*) Project with Grant Agreement No. 952622 under the EU H2020 research and innovation programme.

■ Main objective

Establish chains of trust rooted in the silicon manufacturing process for ICT systems, and apply them in improving the supply chain for networked infrastructures.

■ **Website:** www.spirs-project.eu





Outline

- **Context & Motivation**
 - DLT & IOTA Tangle
 - Data Storage & Encapsulation
- **WAM Protocol**
 - Message Encapsulation
 - Message Chaining
 - Index Generation
 - Chain Ownership
 - Message Structure
 - Authentication & Integrity
- **Open Source Project**

DLT & IOTA Tangle

- Distributed Ledger Technology (**DLT**)
 - Verifiability
 - Immutability
 - Persistence

- **IOTA Tangle** advantages:
 - DLT as *Directed Acyclic Graph (DAG)* (**DAG**)
 - Faster validation than Blockchain
 - Feeless data transaction
 - Storage (data exchange)



Source @Shutterstock



Source <https://www.iota.org/>

DLT & IOTA Tangle

- IOTA Tangle Explorer & Visualizer: <https://explorer.iota.org/mainnet/>

The screenshot shows the 'EXPLORER' interface for the 'Mainnet' network. The 'Latest messages' section is active, displaying a list of messages with their IDs and payload types. The latest milestone is 6453233, and the last target is 9.24 s / 10 s.

MESSAGE ID	PAYLOAD TYPE
6c81168b4a443c77f3401b826ef653f5d375ed122986dbd0e5626d007398c7b4	Index
b6ac437a1221dbb0da532dfd40a9aaff04ac29da20e9b0cf219f230c72503bf8	Index
8aa231d9fec0ce9e6bb77f8d0d7c51f972d8a875ed15365af81d1851f6d1dc2c	Index
9efcb1ed0e68cce52d30171fb0d0a9d13de234ac7607f28509114104529be4a7	Index
1ff9bd0db9569e36feabd83b20947724f53b57554e57d95d874c192438577073	Index
0afeabfc2015ed13d8f883df83835b5b6f6f3751a1e6ad2adaea61d2e69ede37	Index
42cc1d4dbe6cb13aed528a6ca8b7211b284911f6b8ec0f40f83e22d6381c3bd5	Index
a031ec099c2123bd6644e760e95c9ae8bff1e1eec05ee7c0f3e3d3720fe98f73	Index
29372874ea9e019c6099c004688d655c001e0126a32549da9bc187027ec0214d	Index
eaf757a332f474a452729147969e8335d7f3cfc29fb6a33539a450b0af8191f3	Index

Mainnet is the IOTA network that uses the IOTA tokens that are traded on cryptocurrency exchanges. This network is the most stable.

The screenshot shows the 'EXPLORER' interface for the 'Mainnet' network, specifically the 'Visualizer' section. The 'Statistics' panel shows the following data:

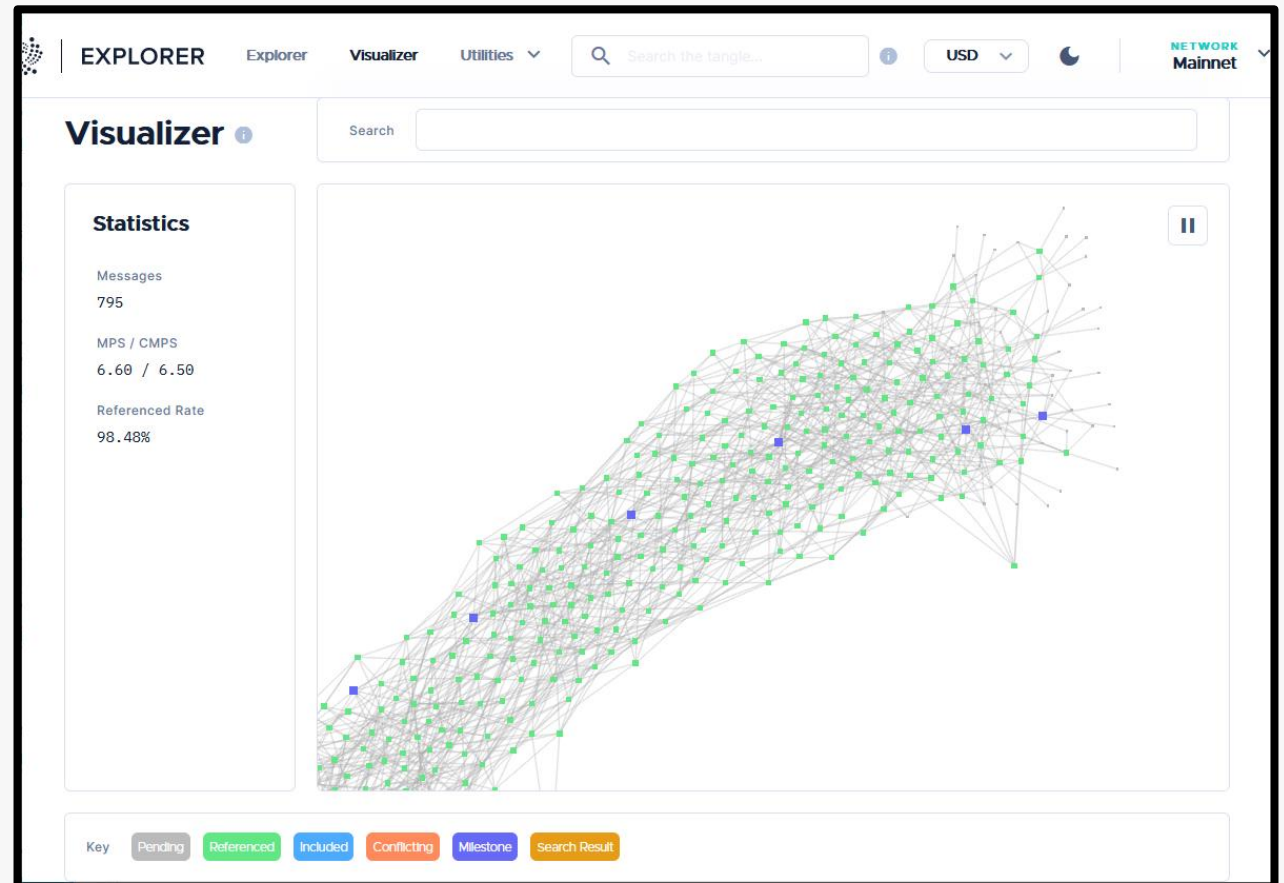
- Messages: 795
- MPS / CMPS: 6.60 / 6.50
- Referenced Rate: 98.48%

The main area displays a network graph with nodes and edges, representing the Tangle structure. A search bar is visible at the top right of the visualizer.

Key: Pending, Referenced, Included, Conflicting, Milestone, Search Result

Data Storage & Encapsulation

- **IOTA (Chrysalis) messages**
 - Value message
 - Data message
- **Indexation Payload**
 - Allow raw data
 - Read/Write operations by index
- **However:**
 - How to store data of arbitrary size?
 - Confidentiality? (Data is public)



WAM Protocol

- ***Wrapped Authenticated Message (WAM)***

- Secure protocol for writing & reading data onto the IOTA Tangle
- Suitable to IoT and resource-constrained devices
- Also compatible with RISC-V microprocessors



Source <https://riscv.org/>

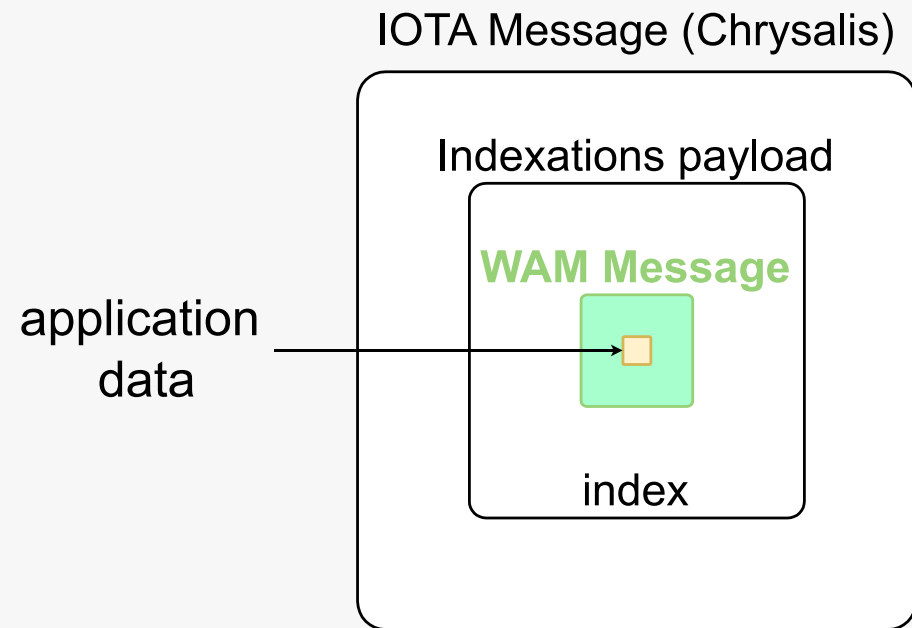
- **Targets**

- Support writing & reading operations
- Abstract complexities and peculiarities of the Tangle (size, link, fetch)
- Ease of use
- Portability (x86_64 and riscv64 architectures)

WAM – Encapsulation

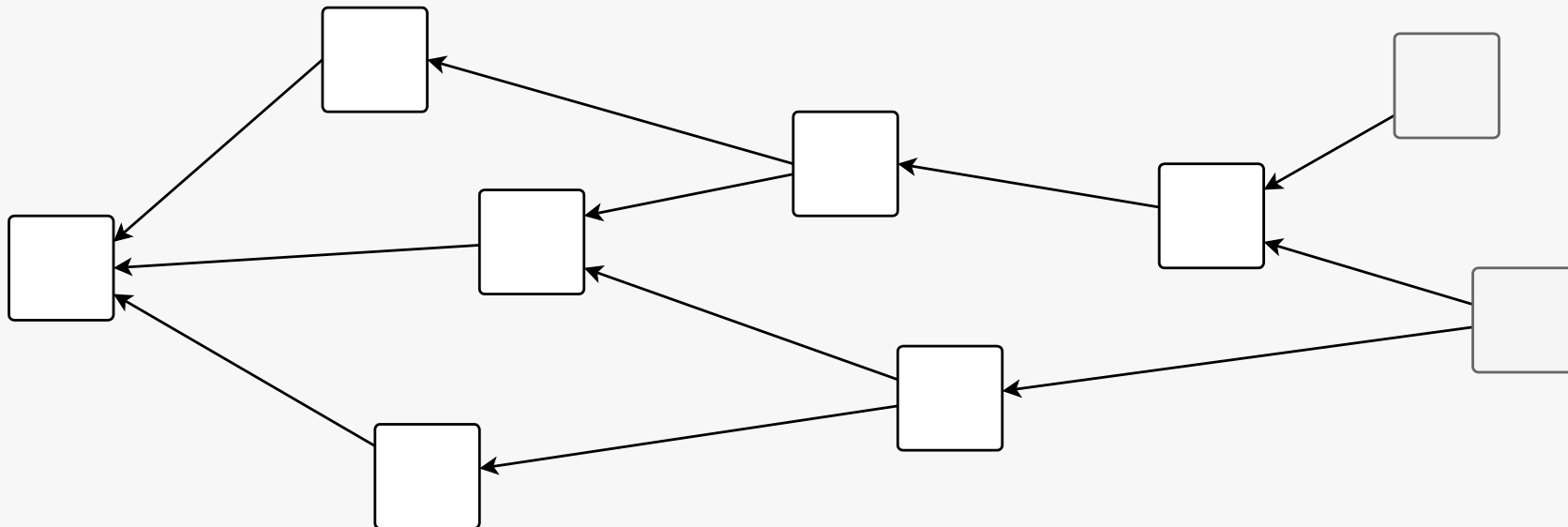
- **Message Encapsulation**

- Application data into a WAM message
- WAM message into an Indexation Payload



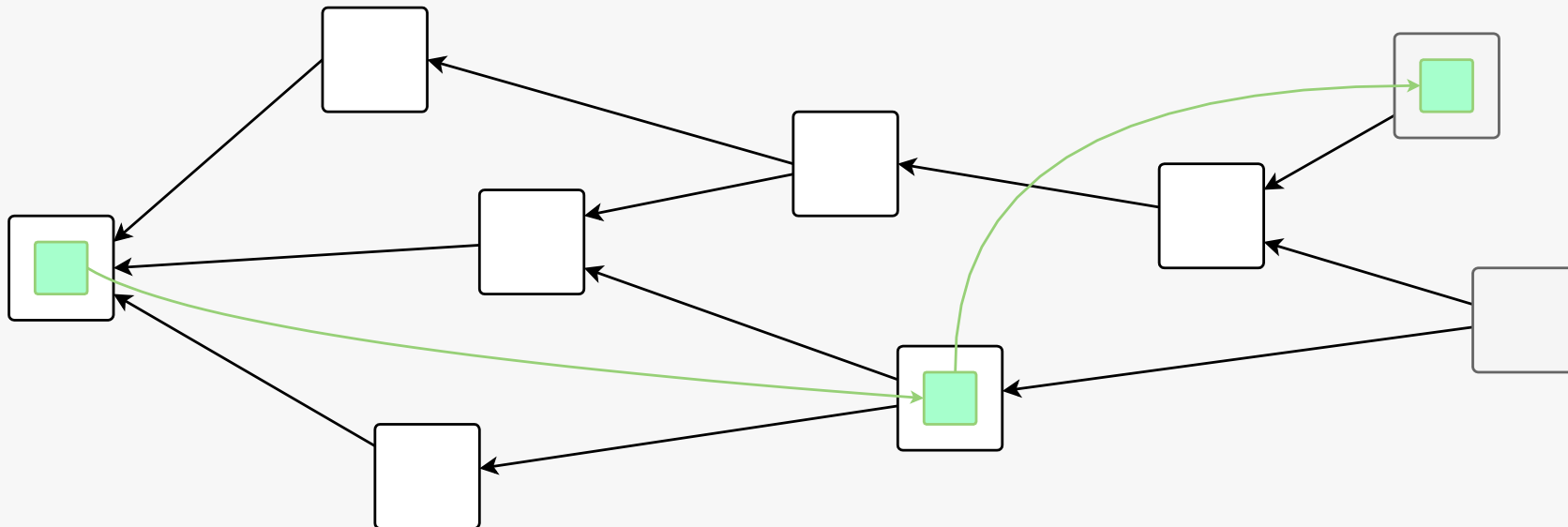
WAM – Chaining

- Physical Tangle vs WAM channel



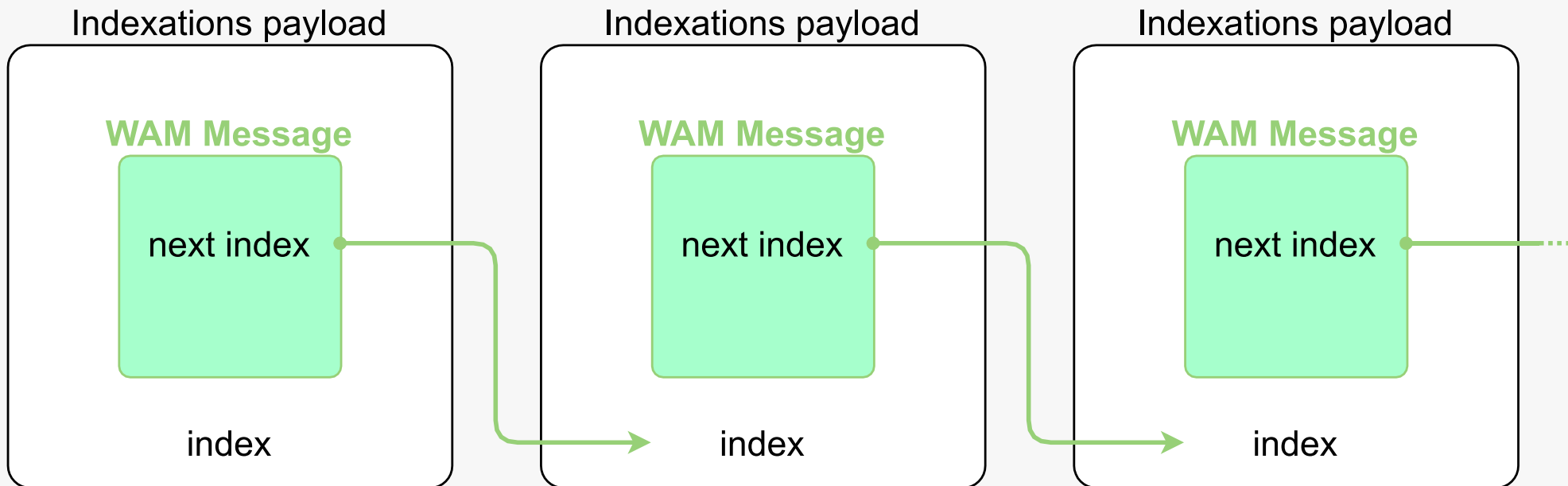
WAM – Chaining

- Physical Tangle vs WAM channel

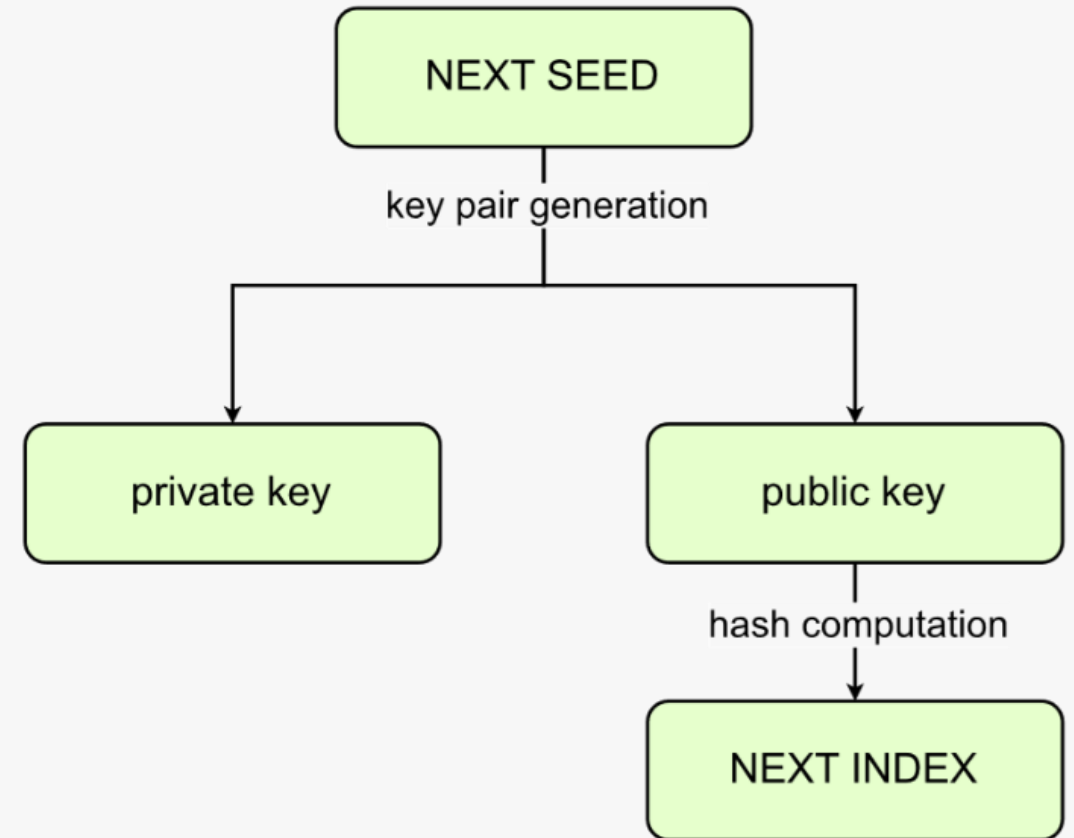
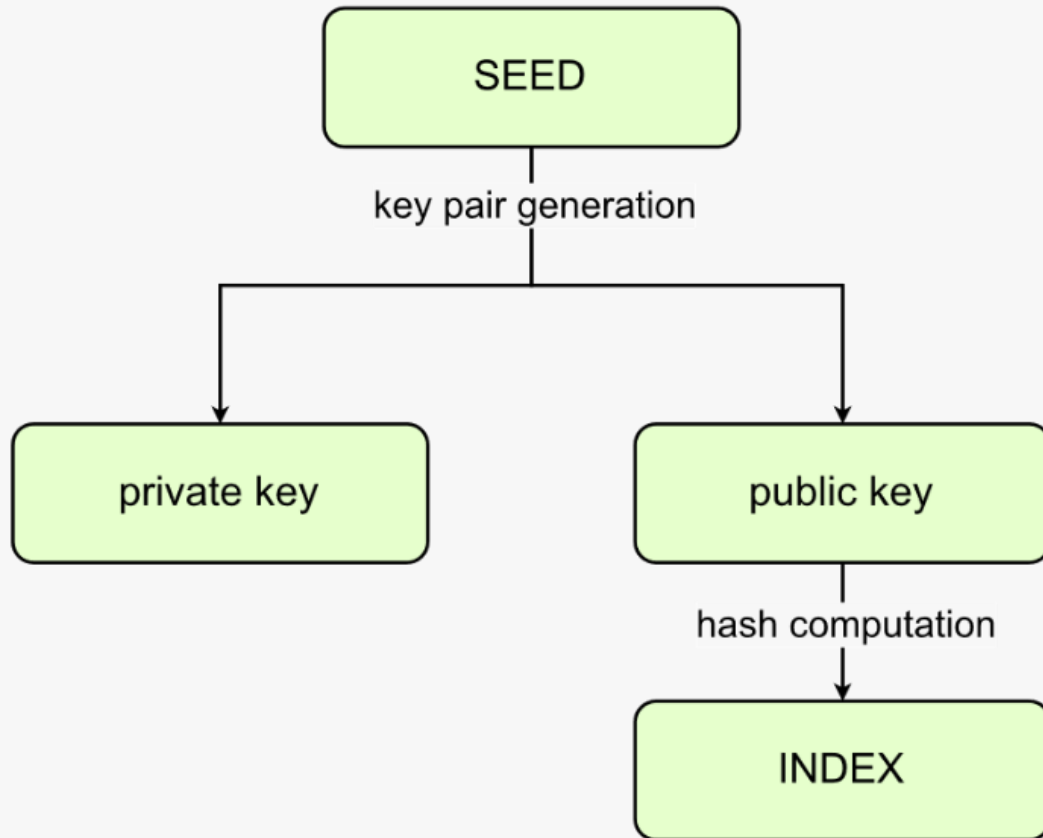


WAM – Chaining

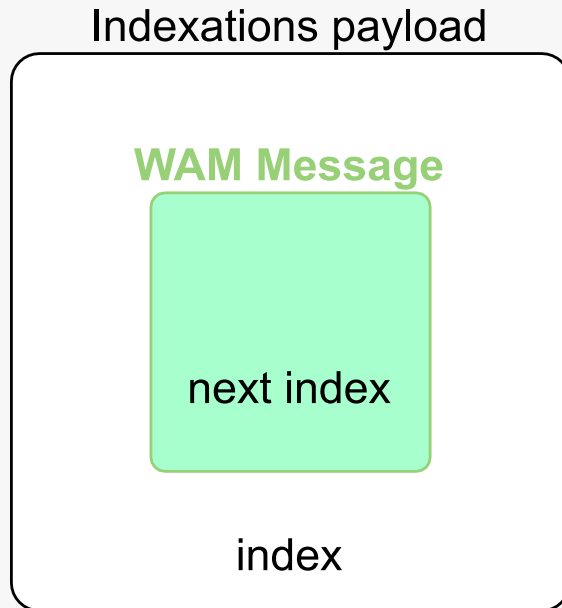
- Tangle messages are **constrained in size**
 - Link multiple messages together



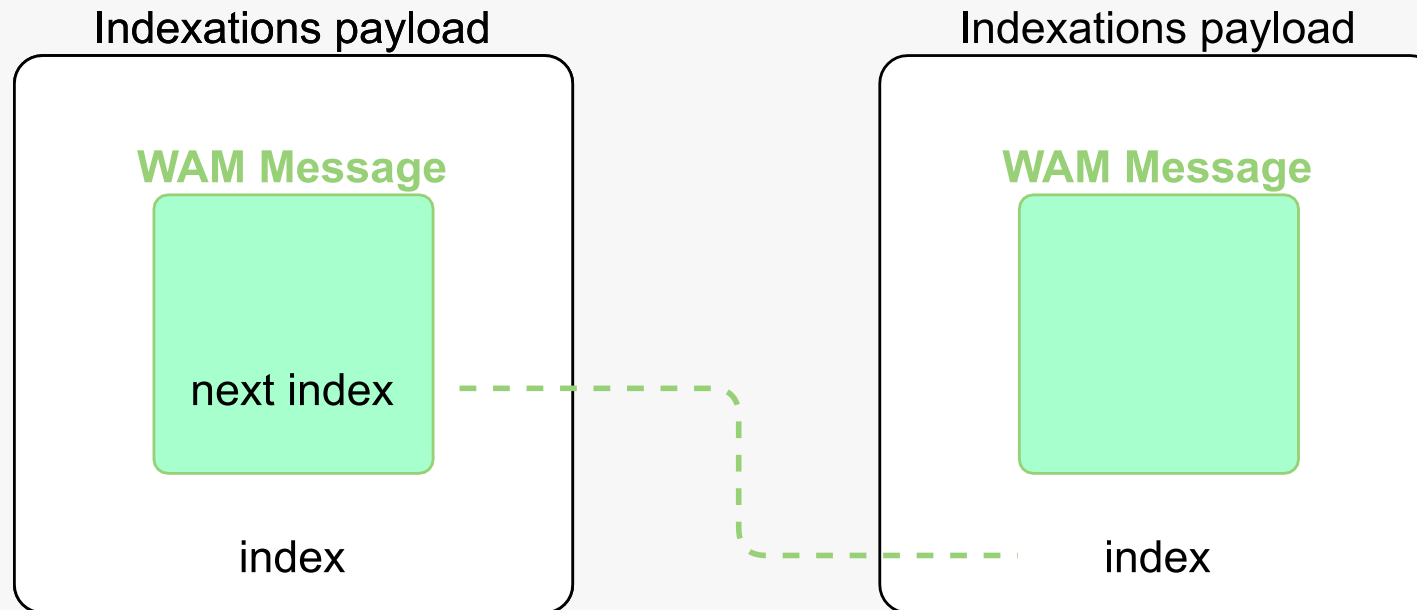
WAM – Index Generation



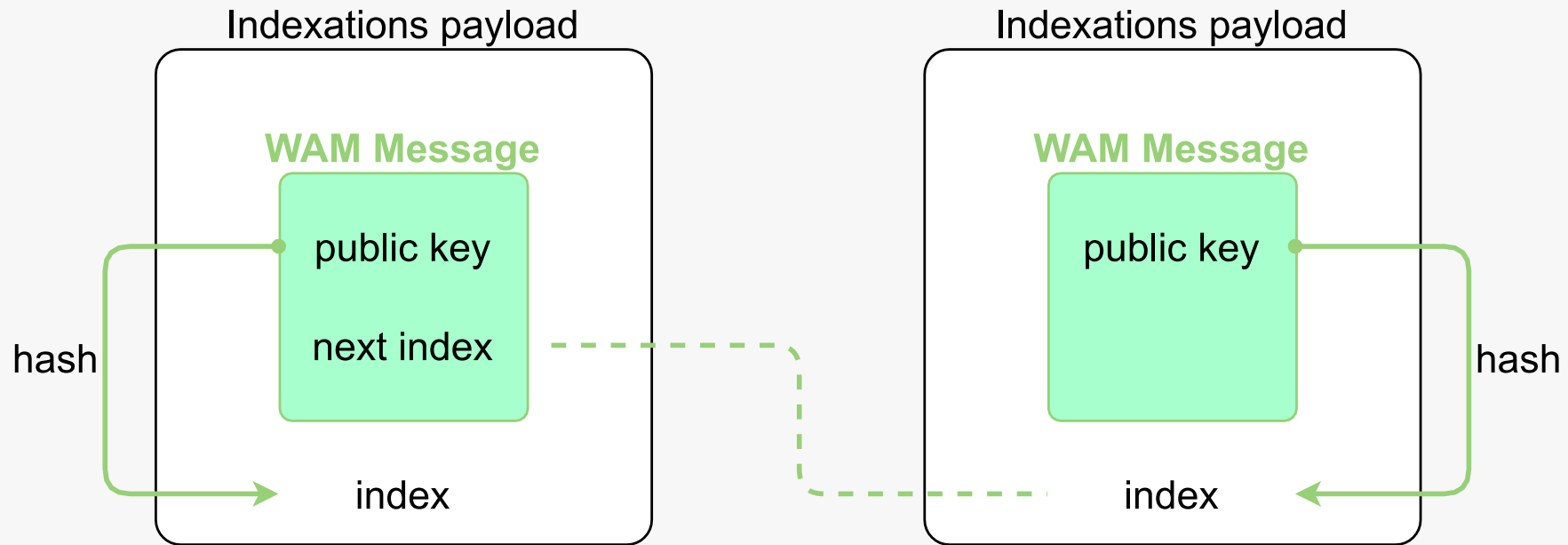
WAM – Chain Ownership



WAM – Chain Ownership

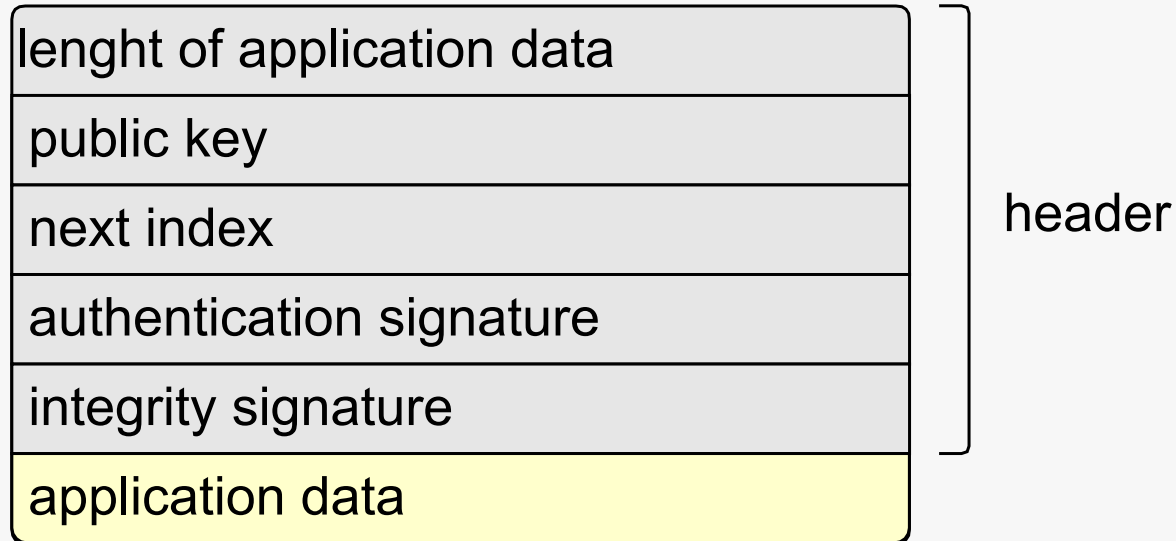


WAM – Chain Ownership



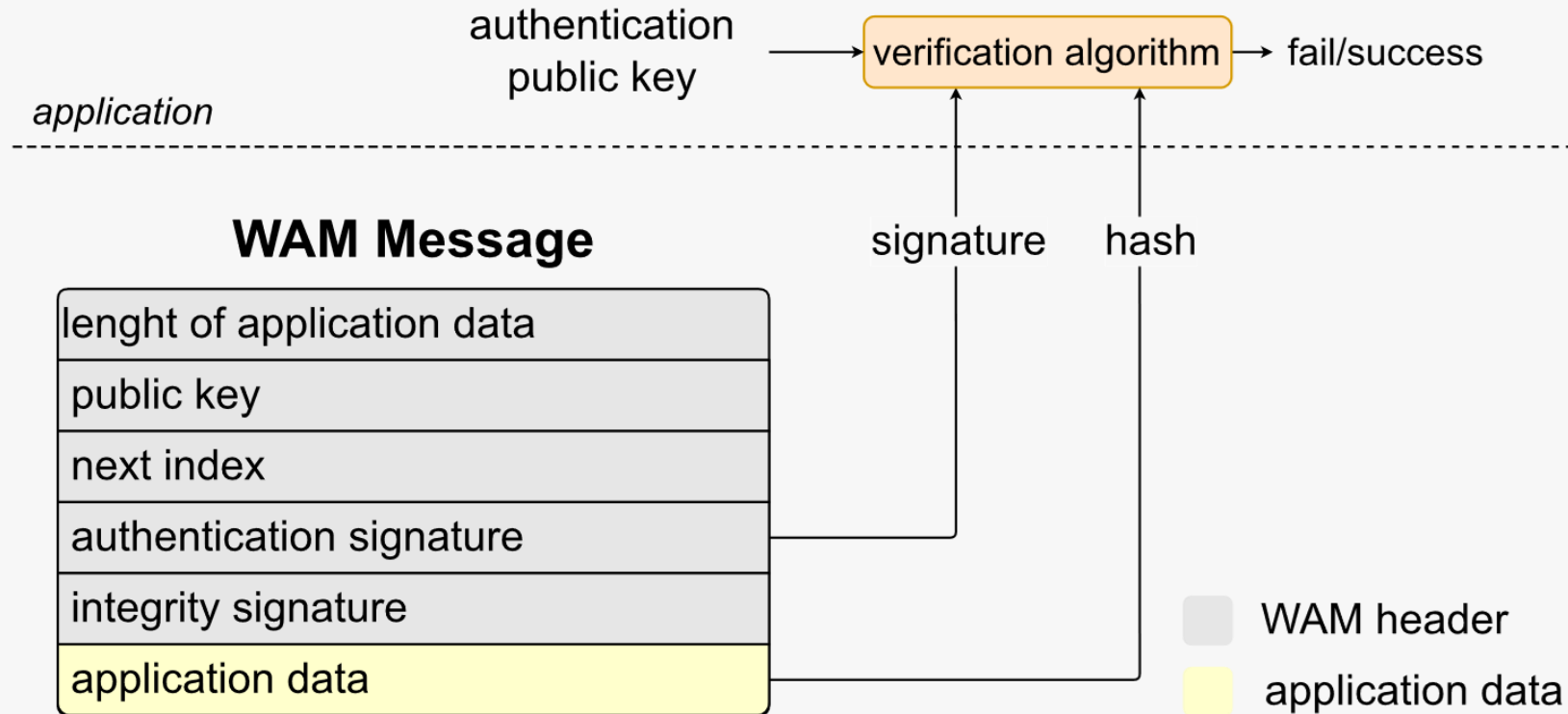
WAM – Message Structure

WAM Message

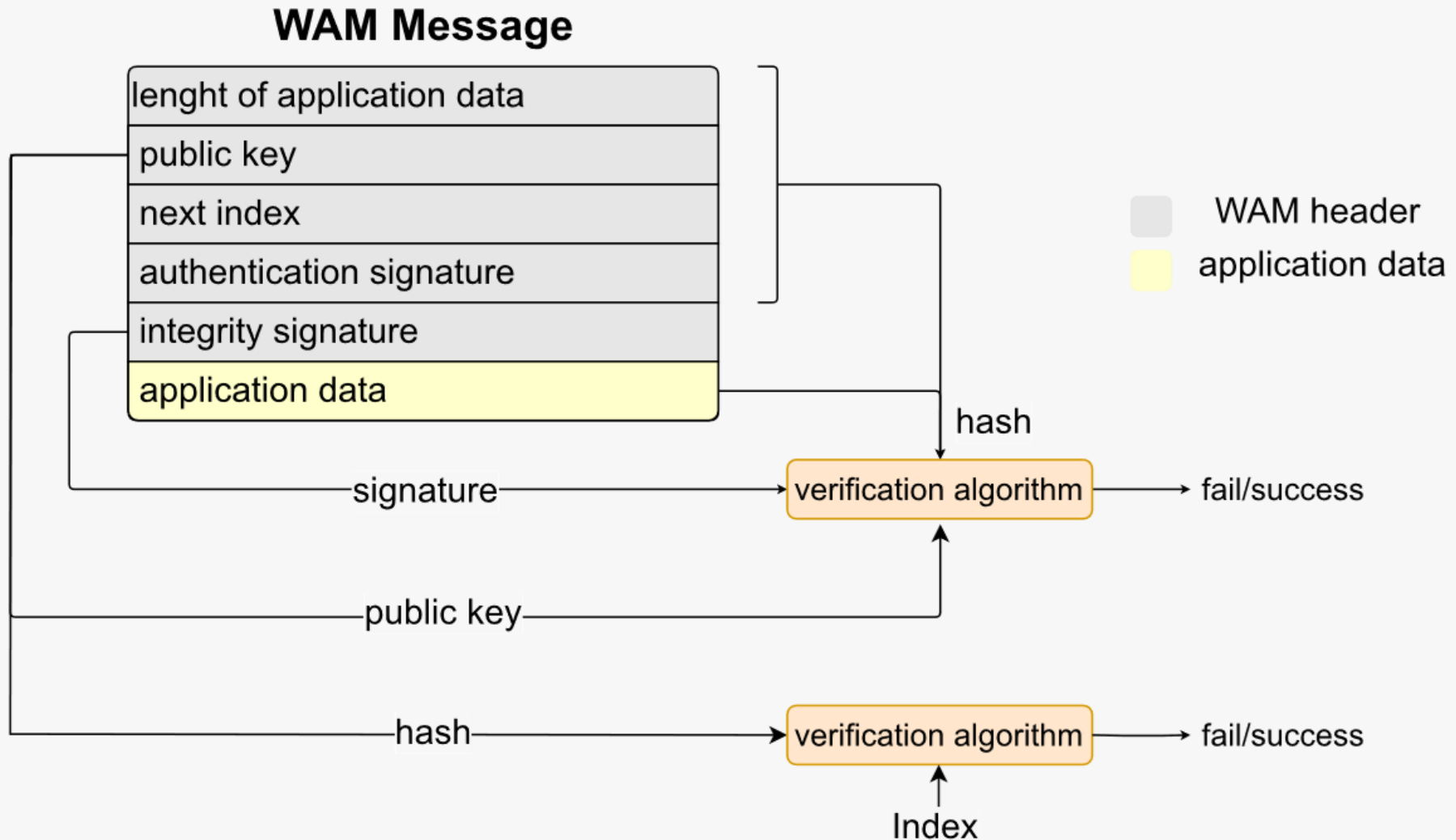


- The whole message can also be **encrypted**

WAM – Authentication



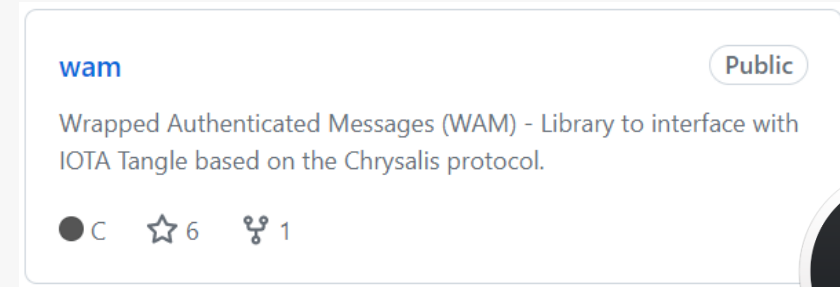
WAM – Integrity & Ownership



Open Source Project

- **Public Repository** on GitHub at:

➤ <https://github.com/Cybersecurity-LINKS/WAM>



The screenshot shows the GitHub repository page for 'wam'. The repository is public and is described as 'Wrapped Authenticated Messages (WAM) - Library to interface with IOTA Tangle based on the Chrysalis protocol.' It has 6 stars and 1 fork. The repository name 'wam' is in the top left, and the 'Public' label is in the top right. The description and statistics are in the middle. The GitHub logo is visible on the right side of the screenshot.

```
└─$ ./ExampleWAM
WAM_write "Hello world!"...
Sent message - index: 67E7FB418E4FC85DC3C732E3C2338765846CF1A287763EB57E9F67294F097724

WAM_read ...
bytes_read=13
msg_read=Hello world!
```

- **Authors & Contributors:**

- Alberto Carelli
- Luca Giorgino
- Andrea Vesco

alberto.carelli@linksfoundation.com

luca.giorgino@linksfoundation.com

andrea.vesco@linksfoundation.com



Thank you for your attention.

Questions?

Daide Margaria

davide.margaria@linksfoundation.com

