LINKSFOUNDATION.COM

FONDAZIONE links
PASSION FOR INNOVATION

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

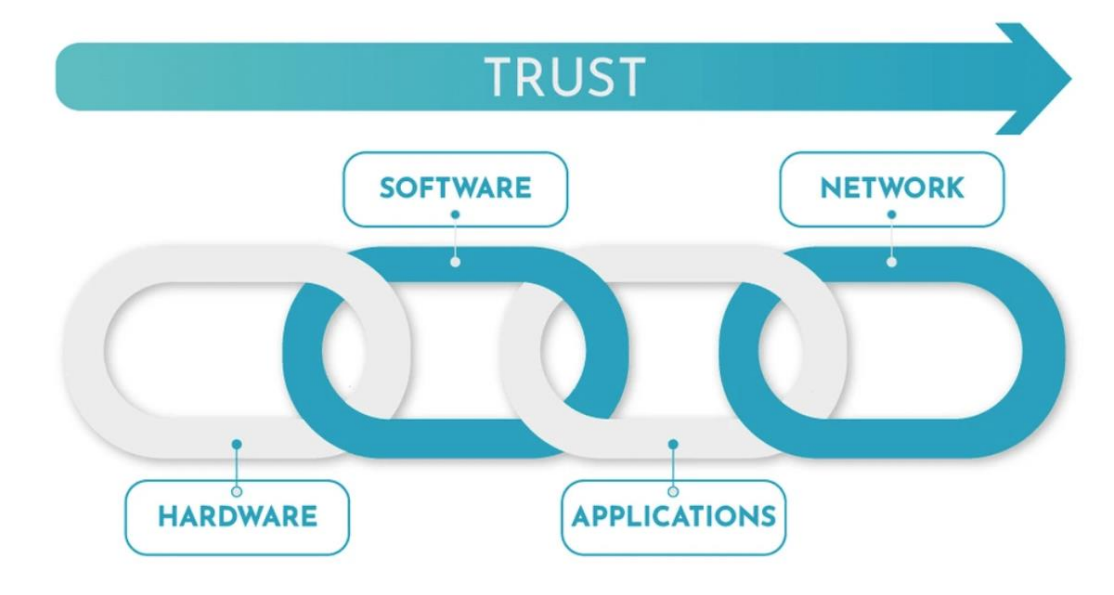
SPIRS project

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

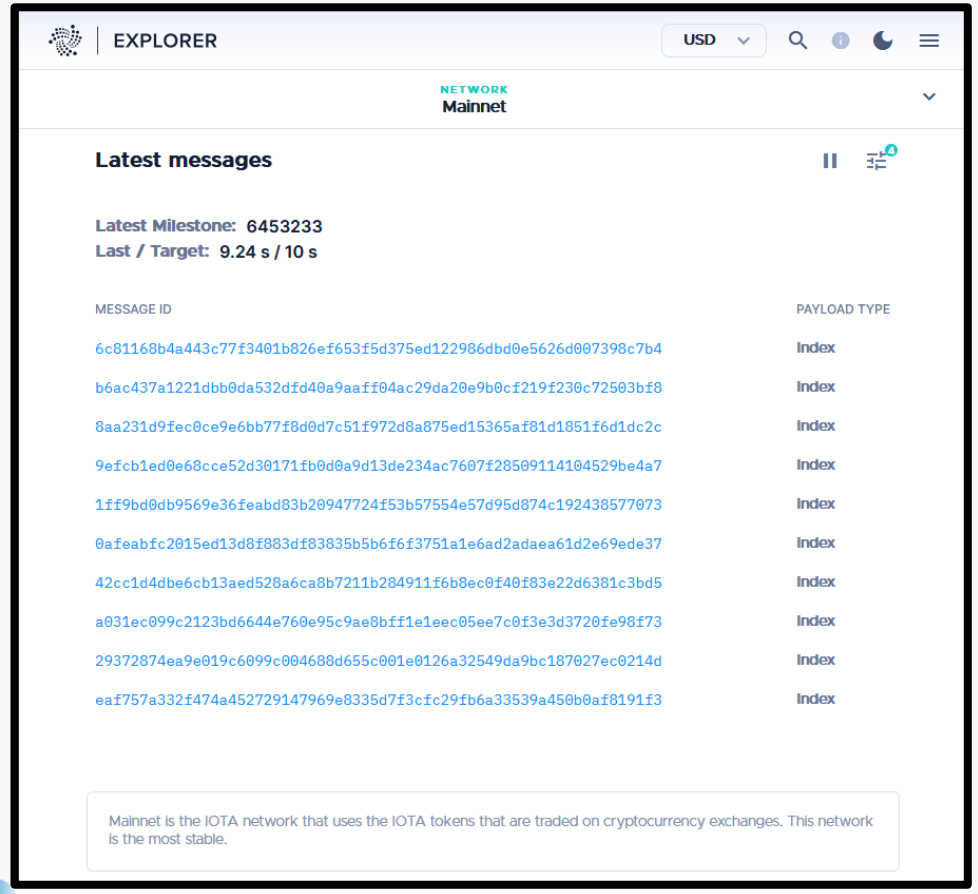
- **IOTA Tangle** advantages:
  - DLT as *Directed Acyclic Graph* (**DAG**)
  - Faster validation than Blockchain
  - Feeless data transaction
  - Storage (data exchange)

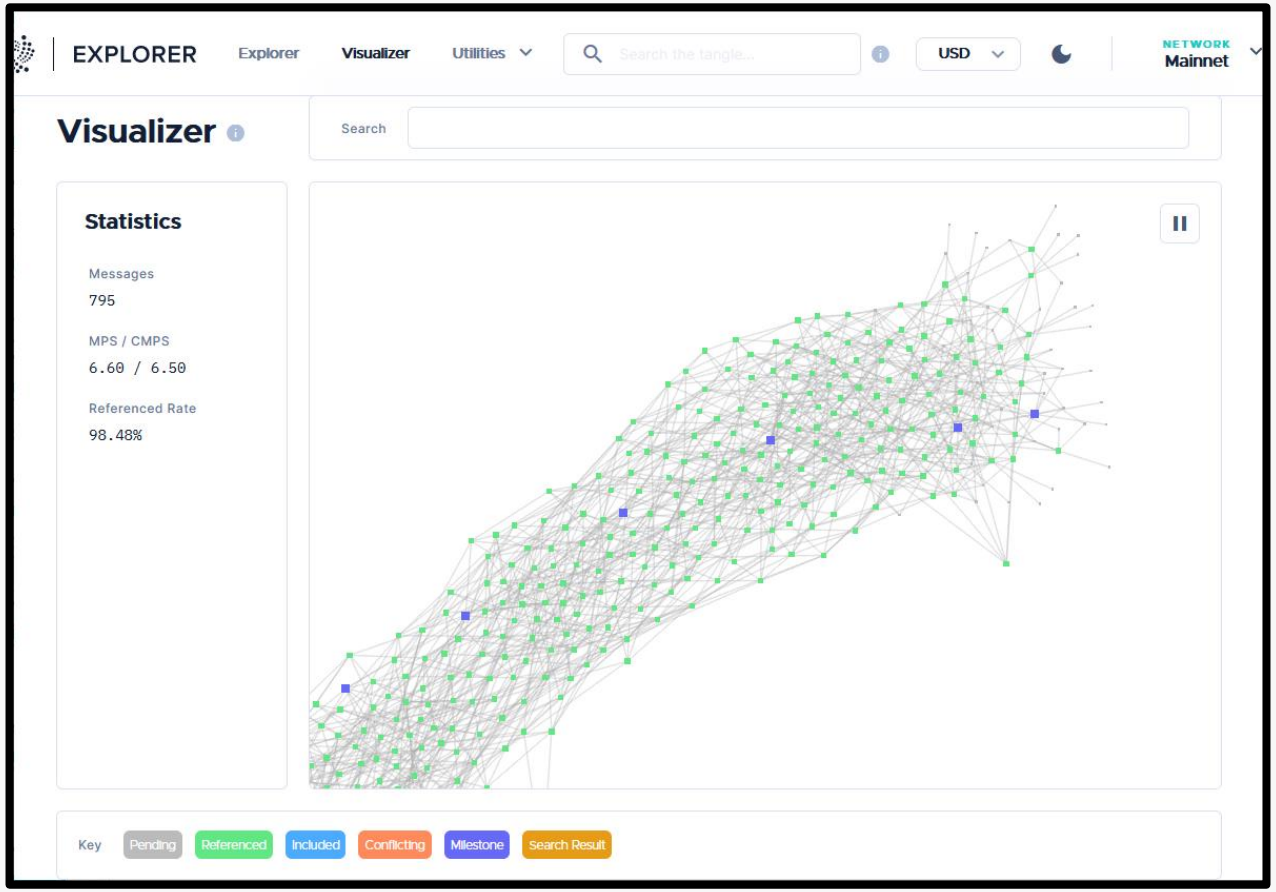
Source @Shutterstock

Source https://www.iota.org/

DLT & IOTA Tangle

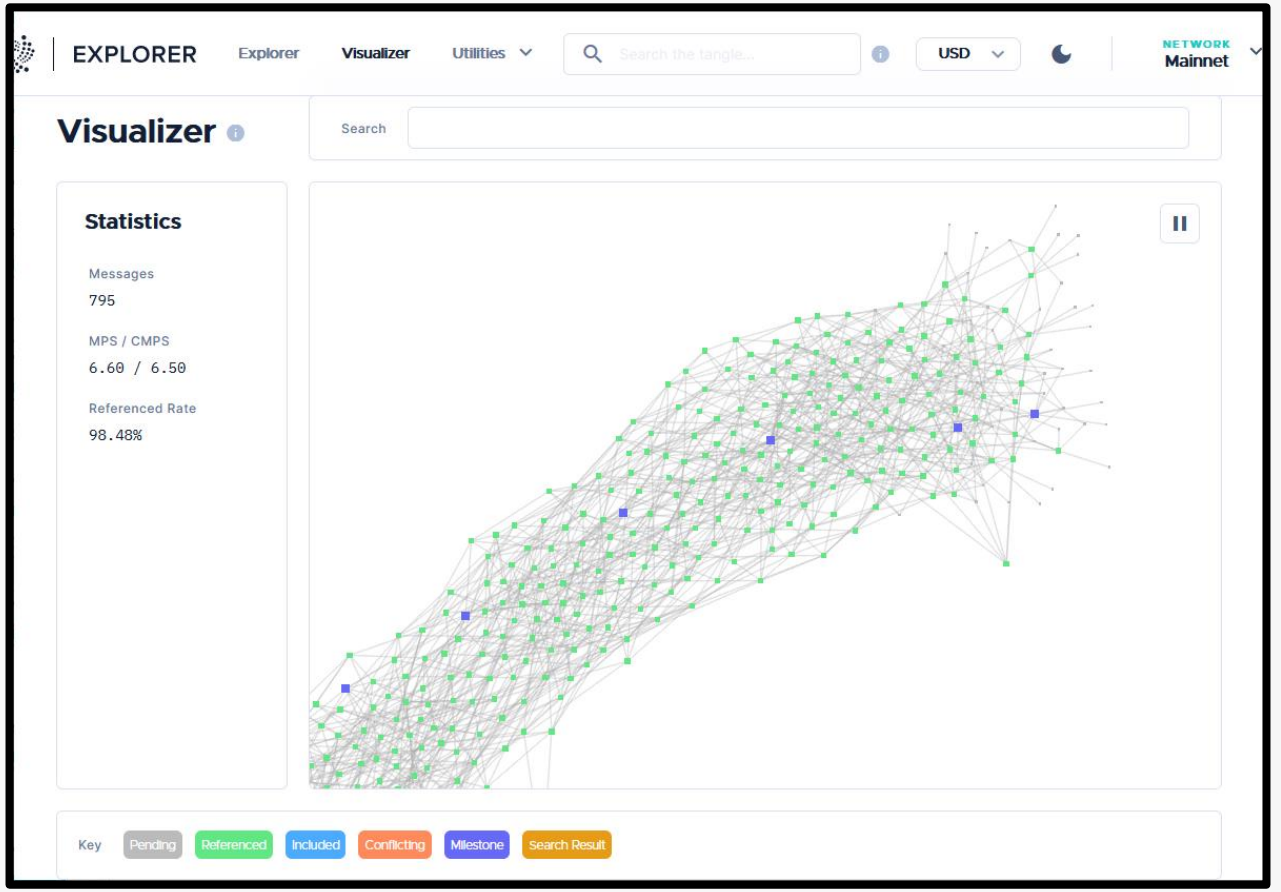
- IOTA Tangle Explorer & Visualizer: https://explorer.iota.org/mainnet/





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

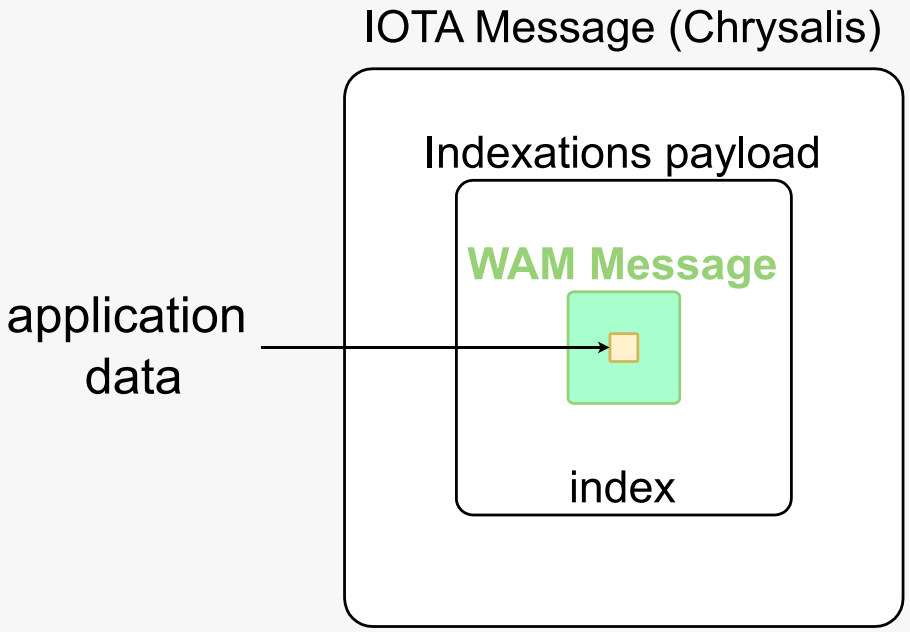
- ***Wrapped Authenticated Message*** **(WAM)**
  - Secure protocol for writing & reading data onto the IOTA Tangle
  - Suitable to IoT and resource-constrained devices
  - Also compatible with RISC-V microprocessors

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)

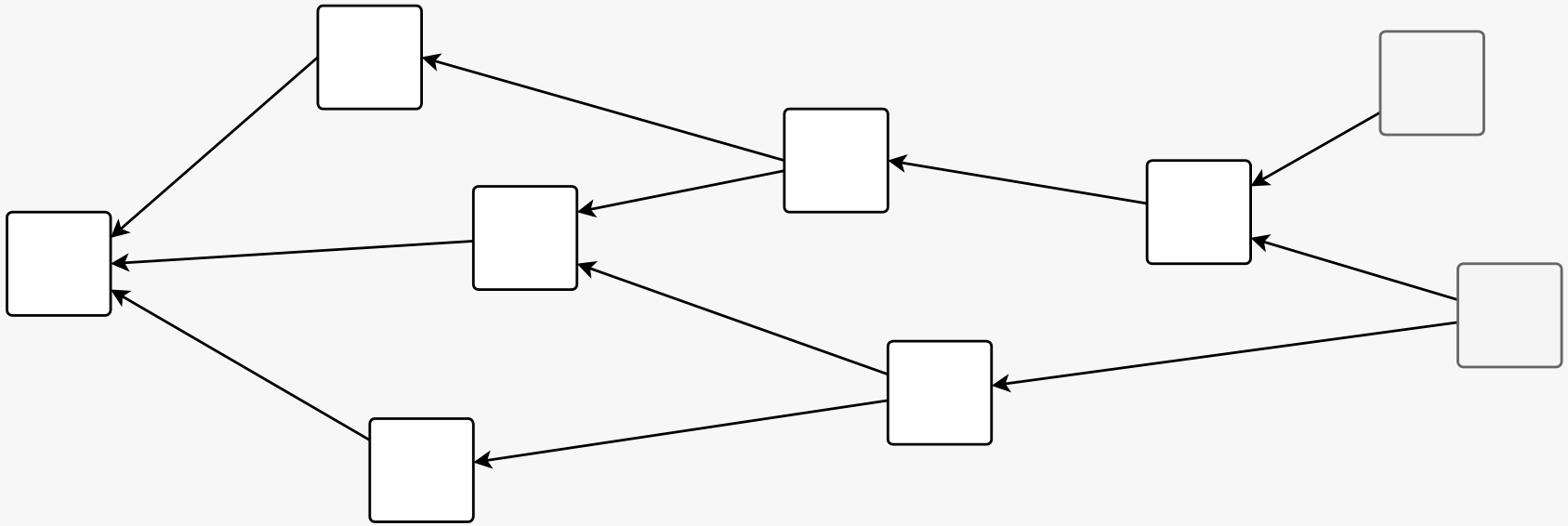
WAM – Encapsulation

- **Message Encapsulation**
  - Application data into a WAM message
  - WAM message into an Indexation Payload



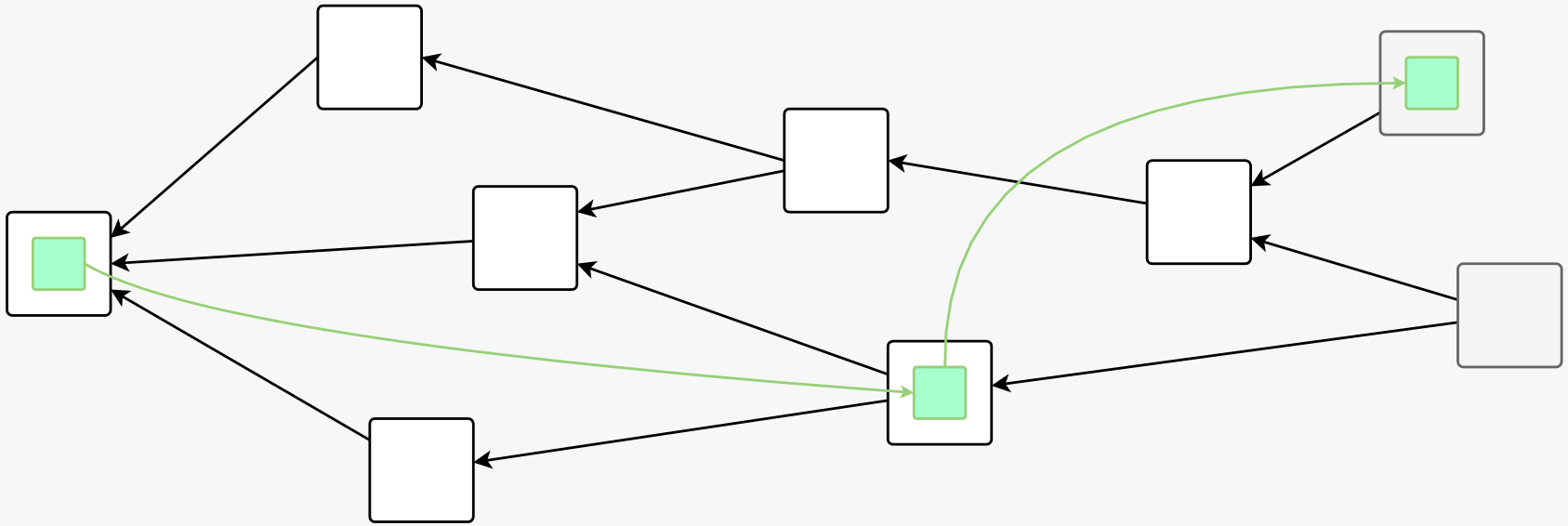
WAM – Chaining

- **Physical Tangle** vs **WAM channel**



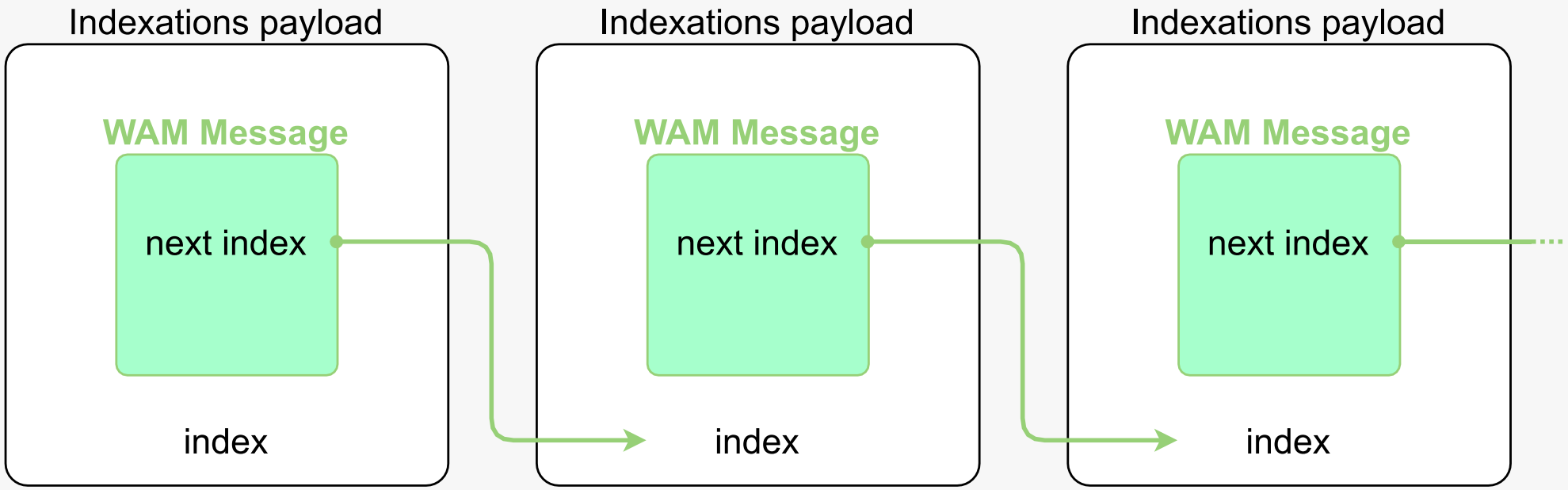
WAM – Chaining

- **Physical Tangle** vs **WAM channel**

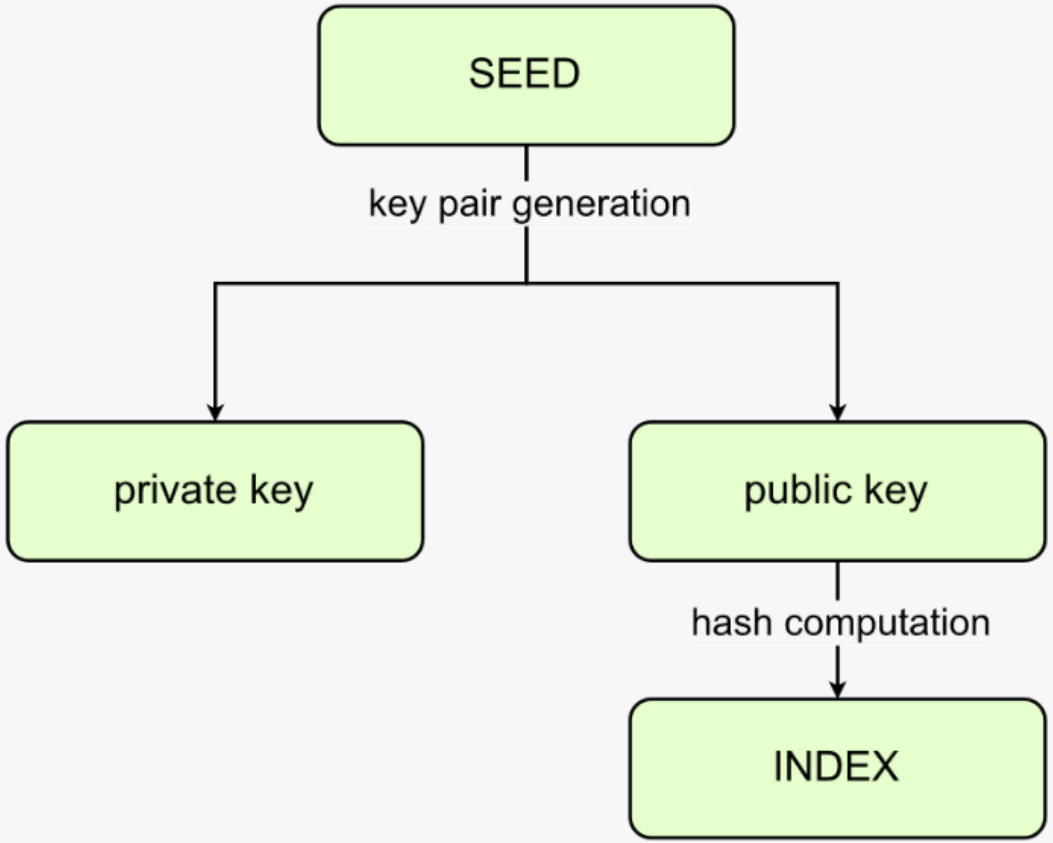


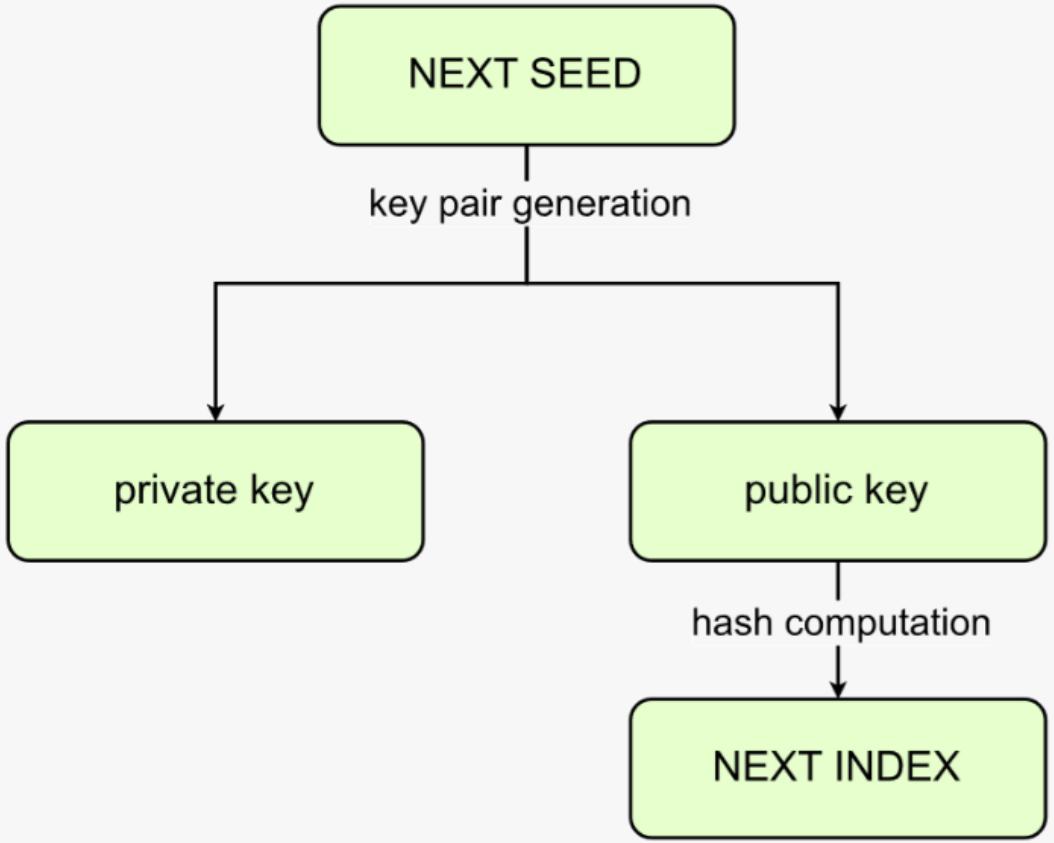
WAM – Chaining

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

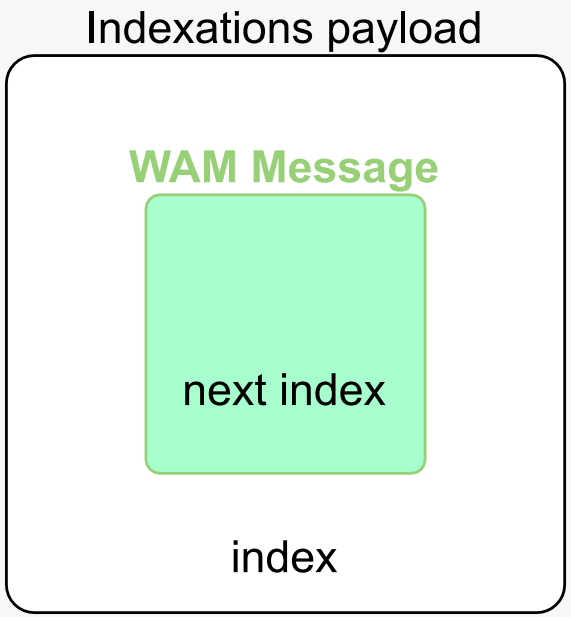


WAM – Index Generation

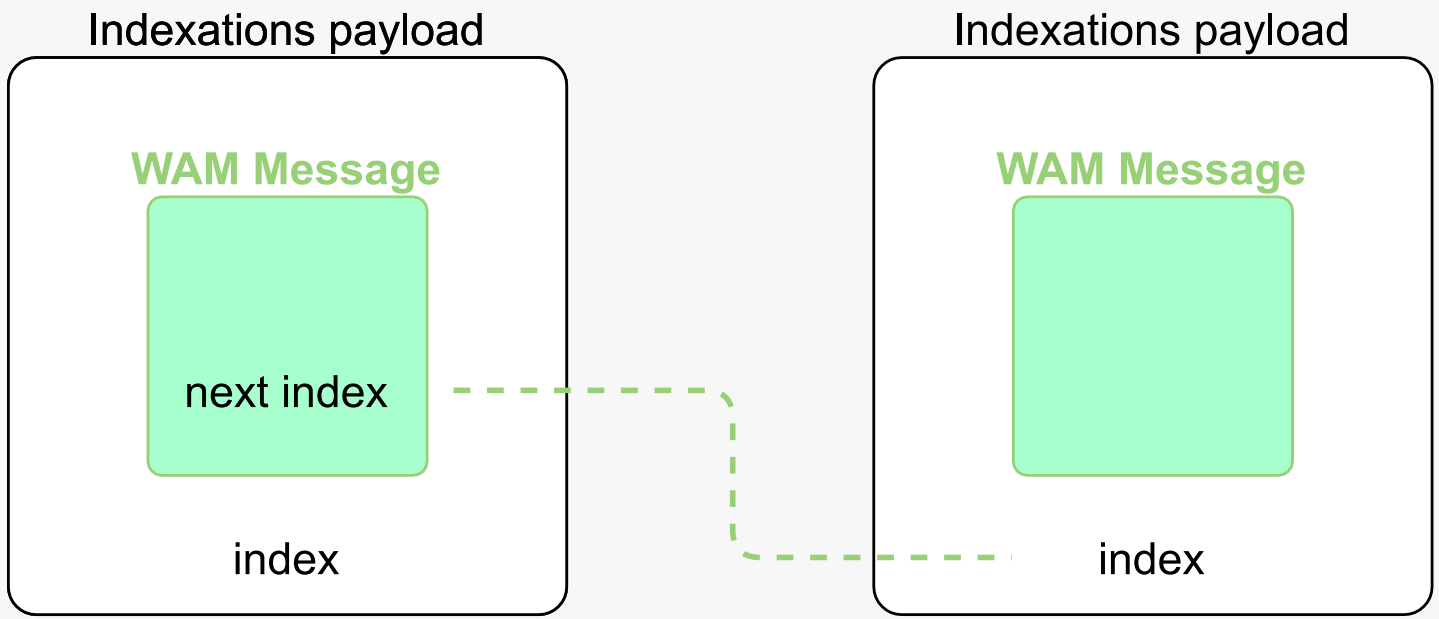




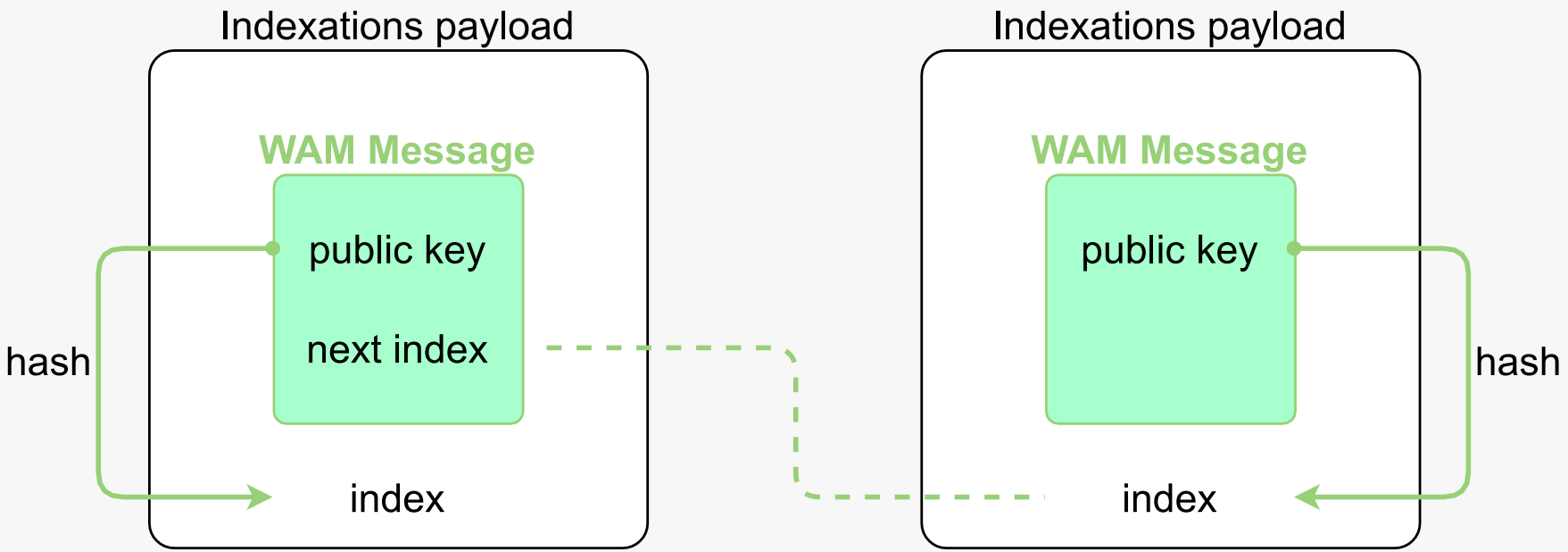
WAM – Chain Ownership



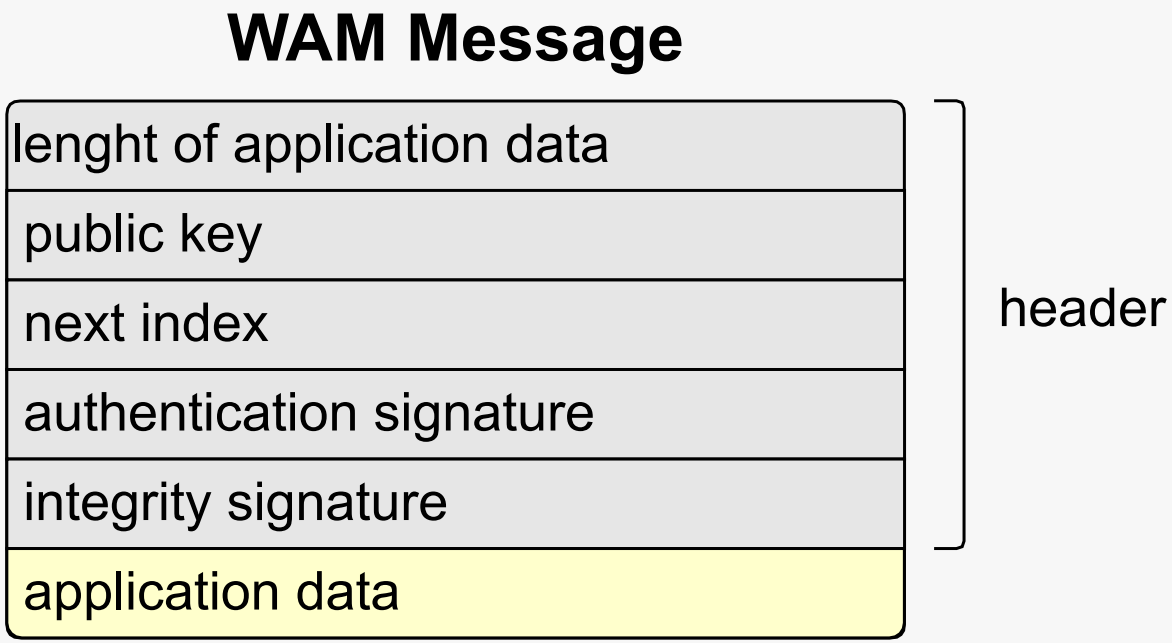
WAM – Chain Ownership



WAM – Chain Ownership

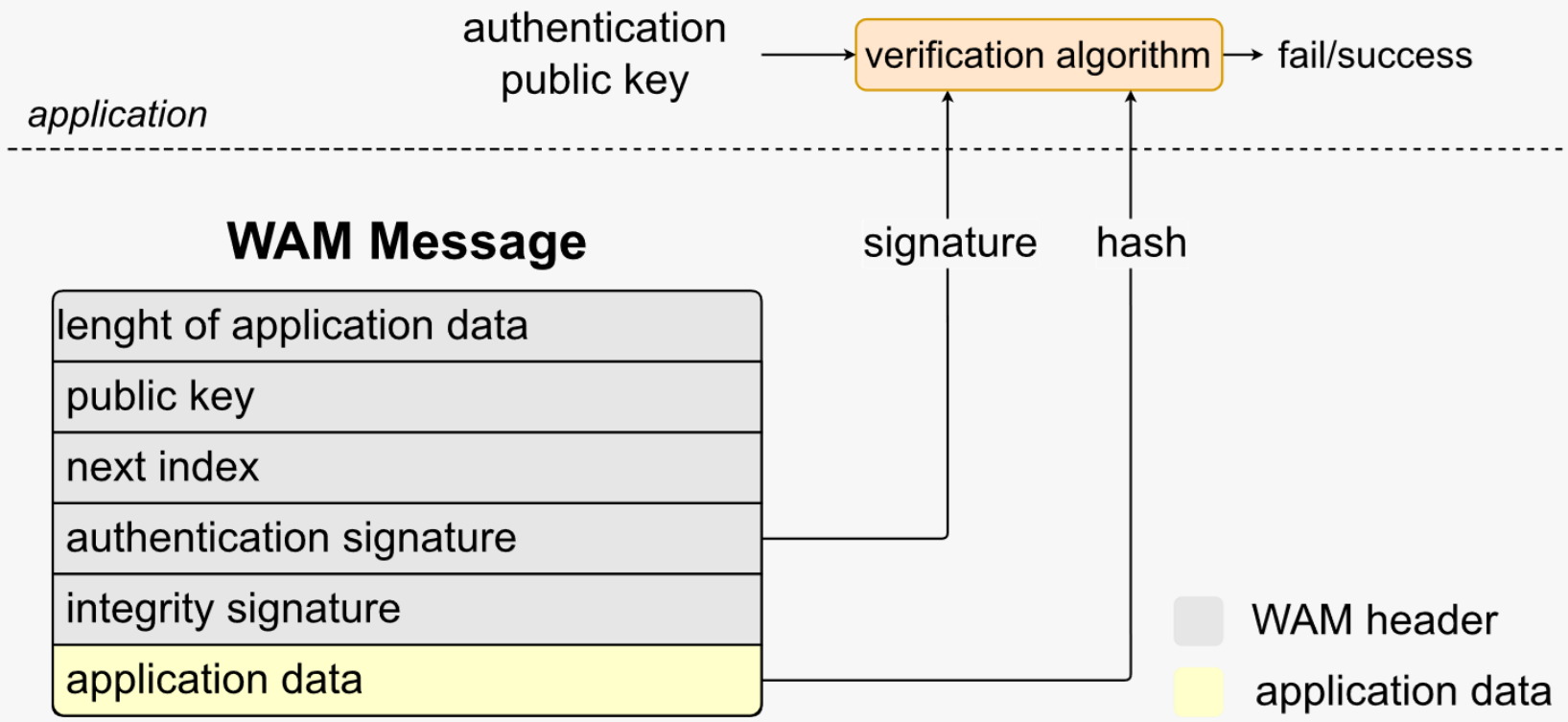


WAM – Message Structure

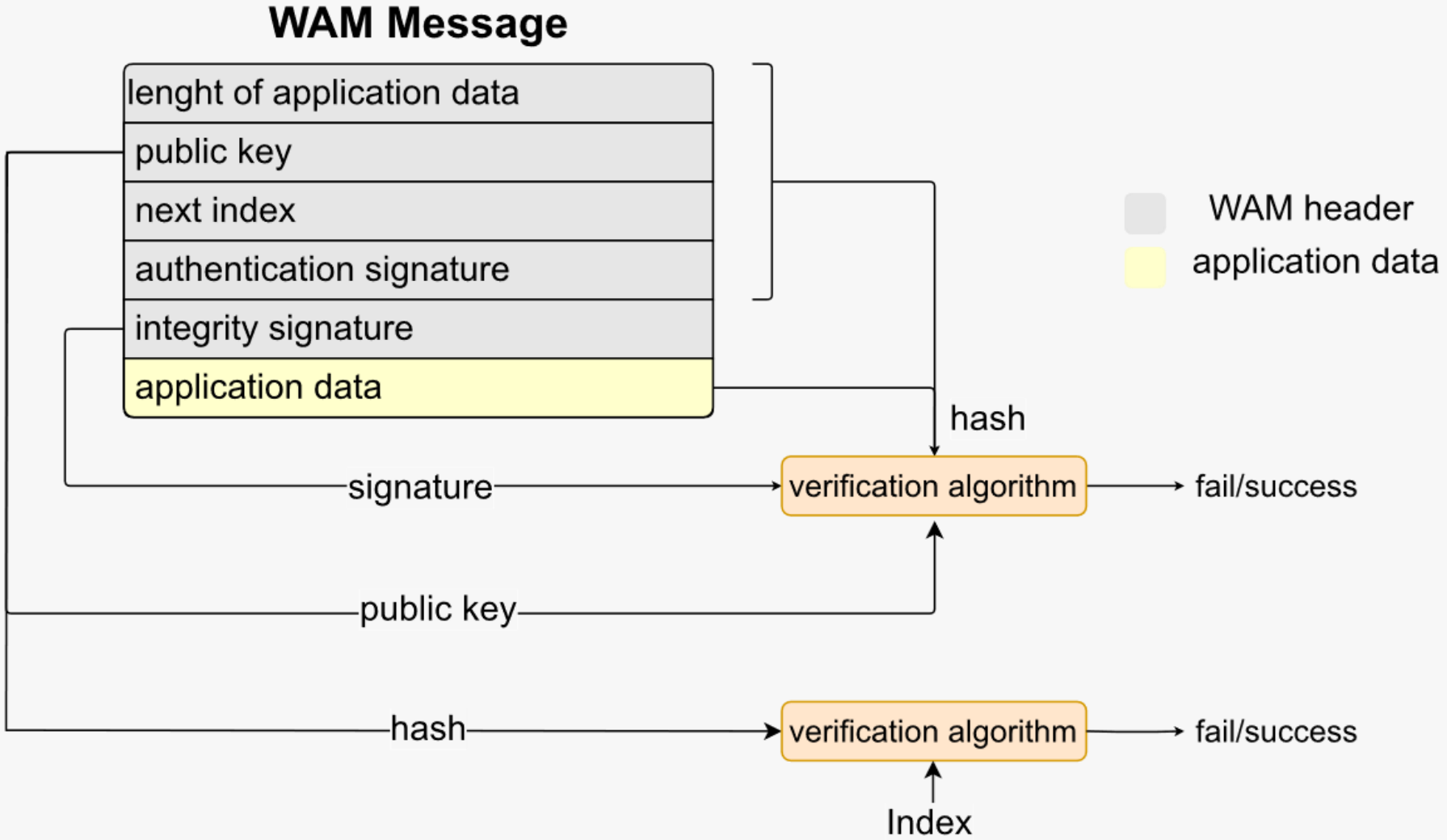


- The whole message can also be **encrypted**

WAM – Authentication

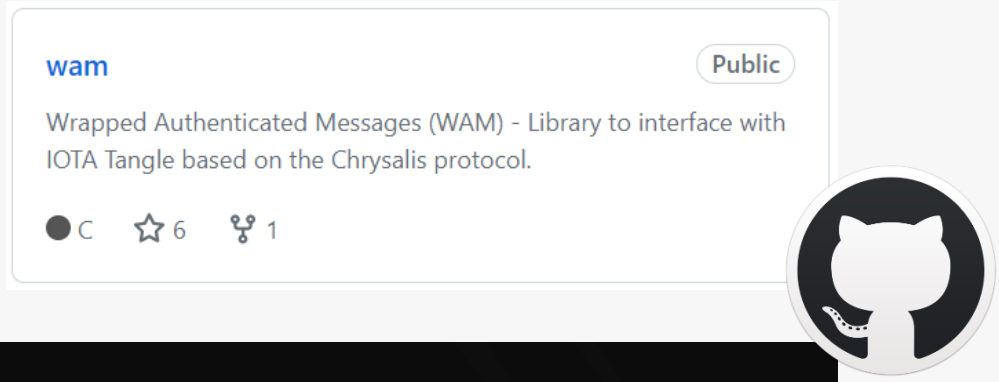


WAM – Integrity & Ownership



Open Source Project

- **Public Repository** on GitHub at:
  - https://github.com/Cybersecurity-LINKS/WAM




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

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

- **Authors** & **Contributors**:

– Alberto Carelli alberto.carelli@linksfoundation.com
– Luca Giorgino luca.giorgino@linksfoundation.com
– Andrea Vesco andrea.vesco@linksfoundation.com

Thank you for your attention.

Questions?

Davide Margaria davide.margaria@linksfoundation.com