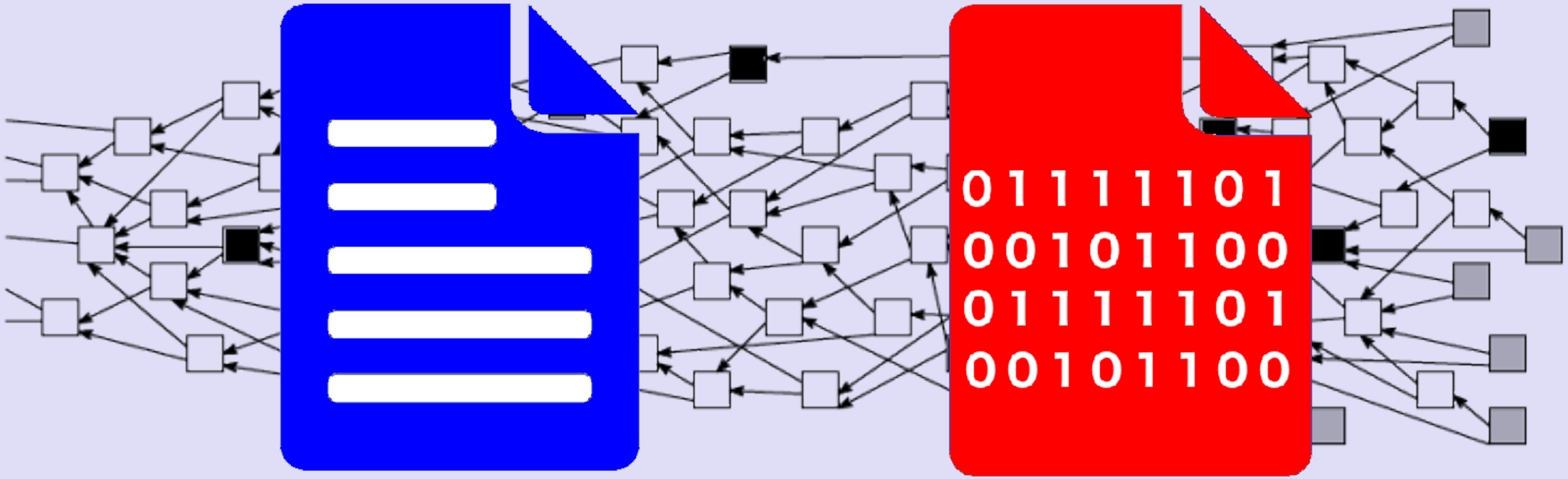
IOTA TUTORIAL 23

MAM Demo
Store file



INTRO

- In this video I will demonstrate that you can store files on the Tangle using Masked Authenticated Messaging.

BUG IN MAM.WEB.JS LIBRARY

- During making of this tutorial, I encountered a bug in the mam.web.js library (commit: feb 5, 2018; commit hash: a365e8f).

- The bug is in decode function in the Rust code which can only handle messages up to a certain size: https://github.com/iotaledger/MAM/blob/master/pascal/src/pascal.rs.

- Please note: This library is work in progress. A workaround this bug is to break up messages into chunks and upload a stream of MAM messages.

- If you have watched IOTA tutorial 19 and 22 and you are using my demo web applications be aware of this bug!
  https://www.mobilefish.com/services/cryptocurrency/mam.html
  https://www.mobilefish.com/services/cryptocurrency/mam_verifiable_claims.html

STORE FILE DEMO

- Two web applications are created to demonstrate storing files on the Tangle using Masked Authenticated Messaging.

- Demo 1: The uploaded file is not broken up in chunks. Due to the bug this web application only works for small files, 5 Kbytes or less, in any channel mode and security level.
  https://www.mobilefish.com/services/cryptocurrency/mam_store_file.html

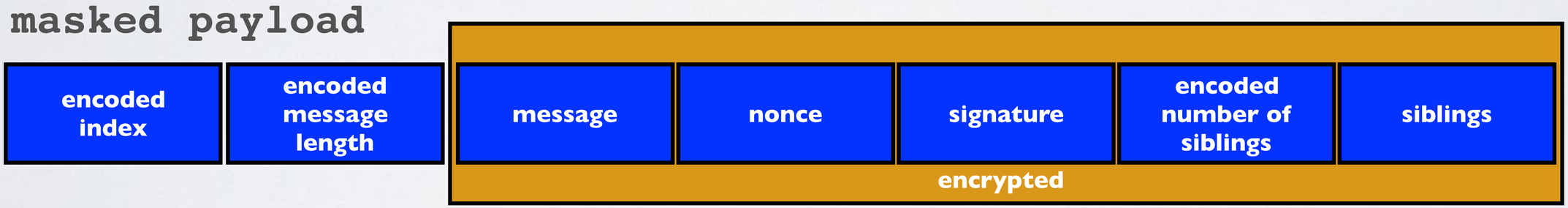
- Demo 2: The uploaded file is broken up in chunks. This web application works for any uploaded file size, channel mode and security level.
  https://www.mobilefish.com/services/cryptocurrency/mam_store_file_in_chunks.html

- Both web applications are created for educational purpose and can store any file types (text files or binary files) on the Tangle.

STORE FILE DEMO

- Please note: In this video a file is also considered to be a message.

- When using MAM, try to avoid breaking up a message in chunks. For each chunk a masked payload and therefor a transaction bundle is created. Creating a masked payload creates overhead: index, message length, nonce, signature, number of siblings and siblings.



STORE FILE DEMO

- Question: Can I use MAM to store a large message on the Tangle, for example a 1 MB pdf file?

- Answer: Yes, you can, but do you want to do this?
  Lets assume the bug is fixed and you do not have to break up the 1 MB pdf file in chunks.

- This file is stored on the Tangle by creating a transaction bundle containing multiple transaction objects. Each signatureMessageFragment field of these transaction objects contains part of the file. For each transaction object a Proof of Work needs to be done.

STORE FILE DEMO

- 1MB message equals ~1,764,208 trytes (not taking into account other masked payload overhead)

- The transaction bundle consists of 1764208 / 2187 = ~807 transaction objects

- The PoW takes ~19 sec per transaction object.
  I have done some non scientific measurements and came to this number.
  Please do your own measurements!

- Time spent for the PoW = 807 x 19 sec = ~4.25 hours

- To store a 1MB message on the Tangle takes ~4.25 hours.
  The main purpose of this calculation is to inform you that storing a large message size on the Tangle takes a lot of time.

REMEMBER

- After a snapshot all stored files are deleted from the Tangle.
  The stored files are still available, if the subscriber is connected to a permanode.

STORE FILE DEMO: SIMULATE SOFTWARE UPDATE

- Lets assume a software update (few kBytes in size) is stored on the Tangle.

- To simulate a software update, create a file: **mobilefish_change_color.txt**.
  This file must contain a single line containing a colour code, for example **#ff0000**
  https://www.mobilefish.com/services/cryptocurrency/mobilefish_change_color.txt

- Use one of the demo web applications to upload the mobilefish_change_color.txt to the Tangle.

- Use the same web application to retrieve the uploaded file.
  It will change the web application background colour simulating a software update.