Point to me, then I'll point back!

@henkvancann

Never ever forget…

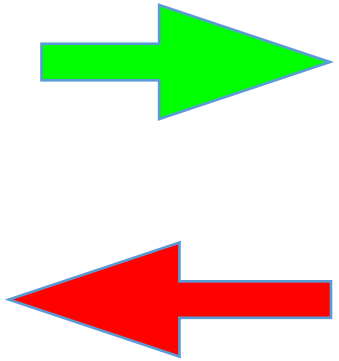
Only pointers on the blockchain!

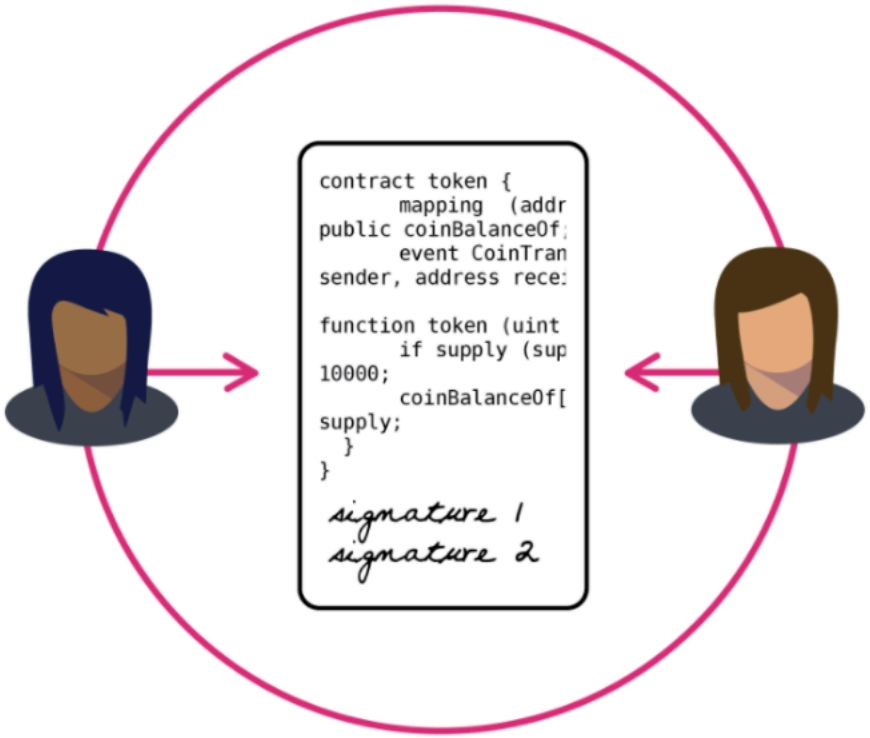
What is ON the blockchain?!

CONTENT

POINTERS

SCRIPTS / PROGRAM CODE

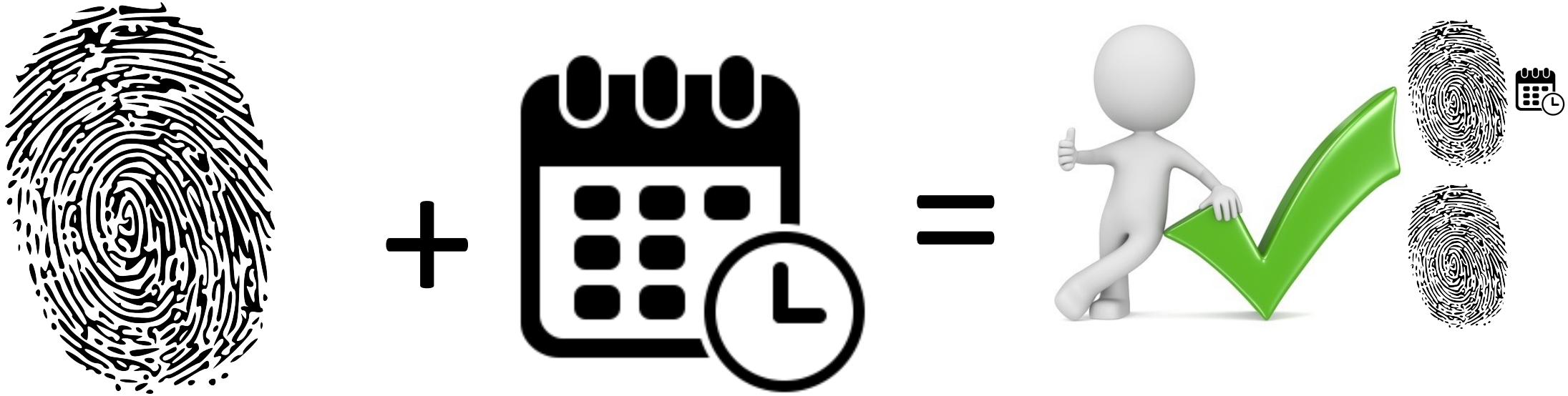




NO

YES

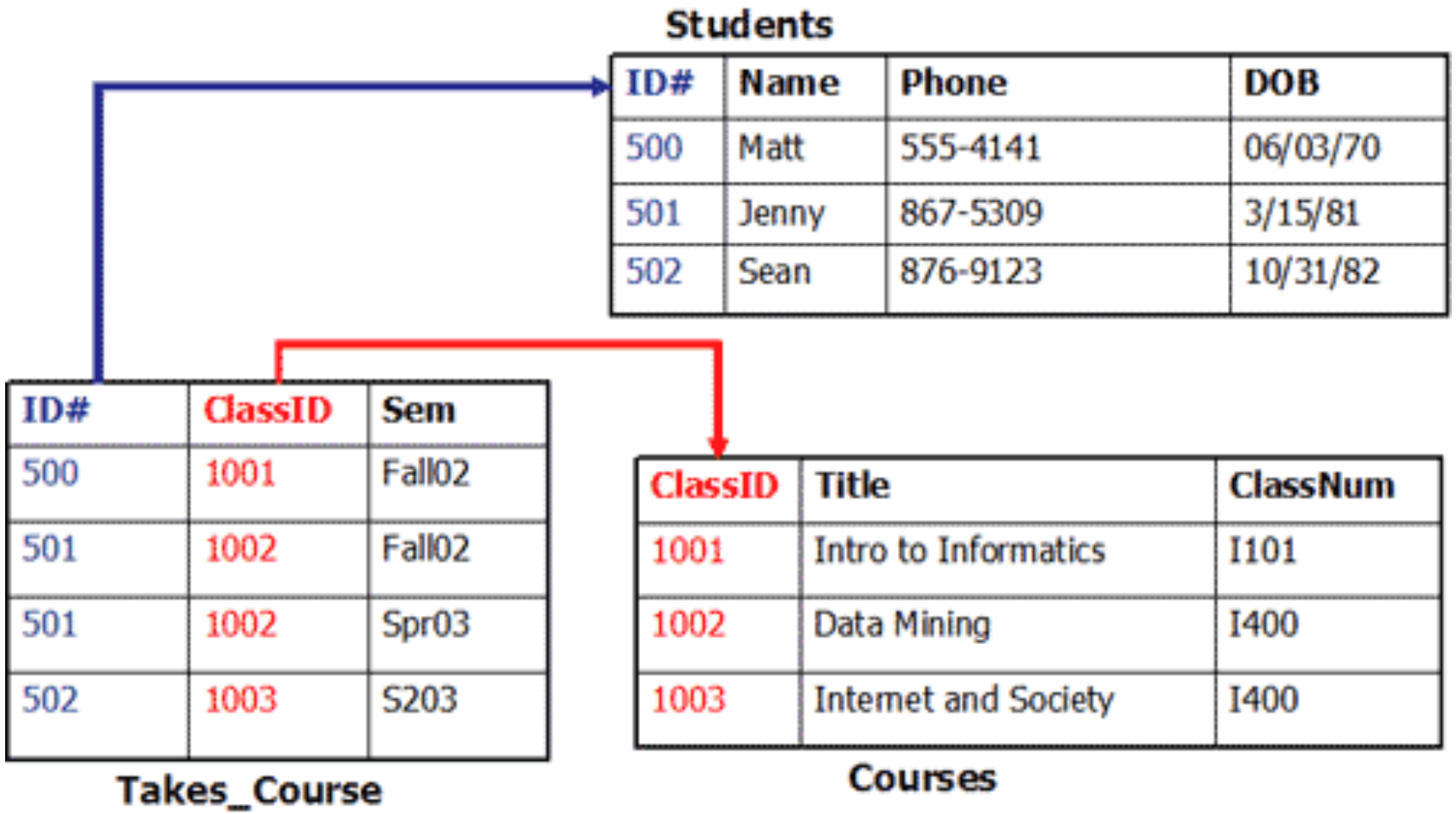
YES



Example SHA-256 HASH:

ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb

Tables - Pointers and keys



Students

ID#	Name	Phone	DOB
500	Matt	555-4141	06/03/70
501	Jenny	867-5309	3/15/81
502	Sean	876-9123	10/31/82

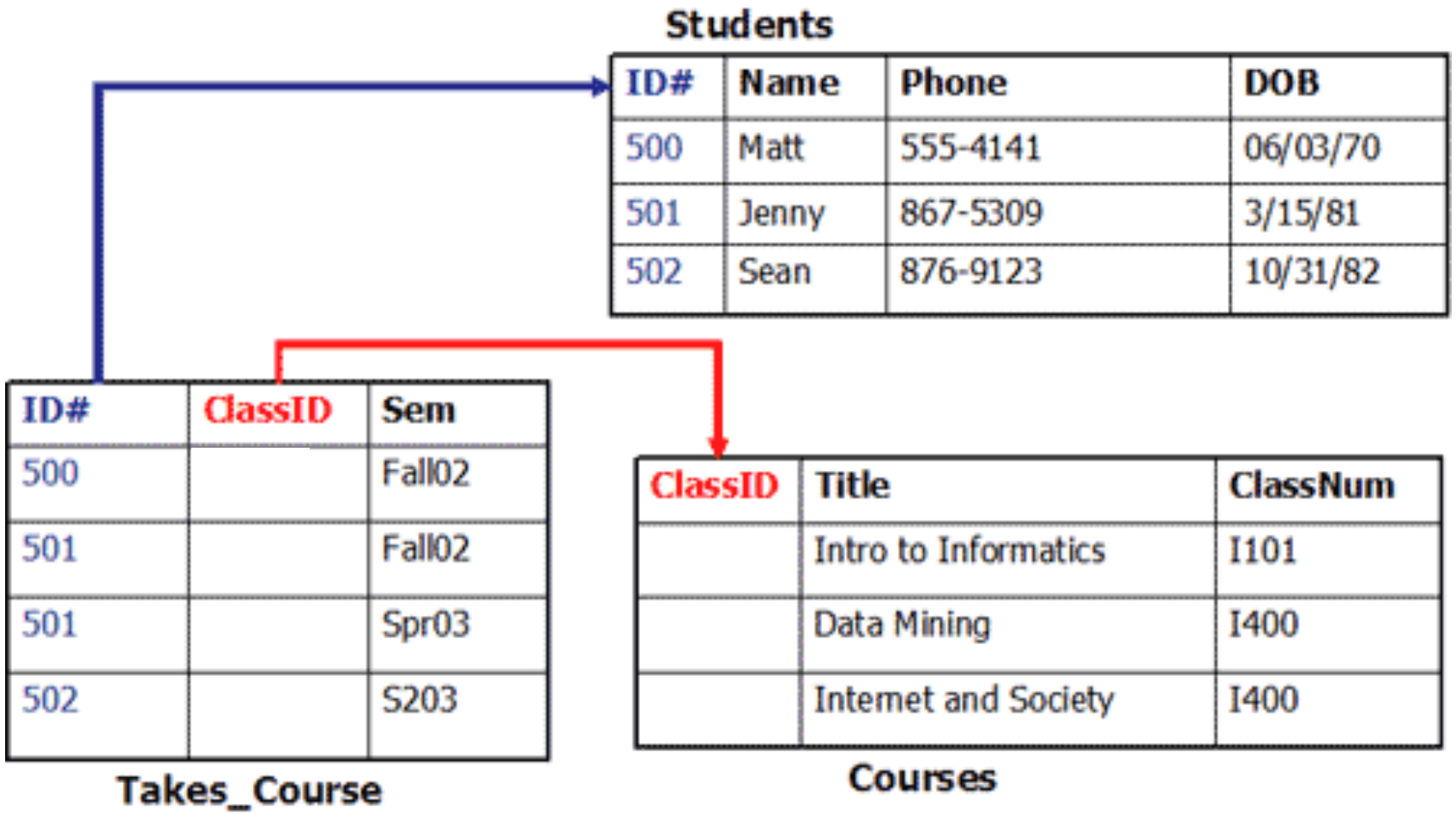
Takes_Course

ID#	ClassID	Sem
500	1001	Fall02
501	1002	Fall02
501	1002	Spr03
502	1003	S203

Courses

ClassID	Title	ClassNum
1001	Intro to Informatics	I101
1002	Data Mining	I400
1003	Internet and Society	I400

Tables - Pointers and keys



Students

ID#	Name	Phone	DOB
500	Matt	555-4141	06/03/70
501	Jenny	867-5309	3/15/81
502	Sean	876-9123	10/31/82

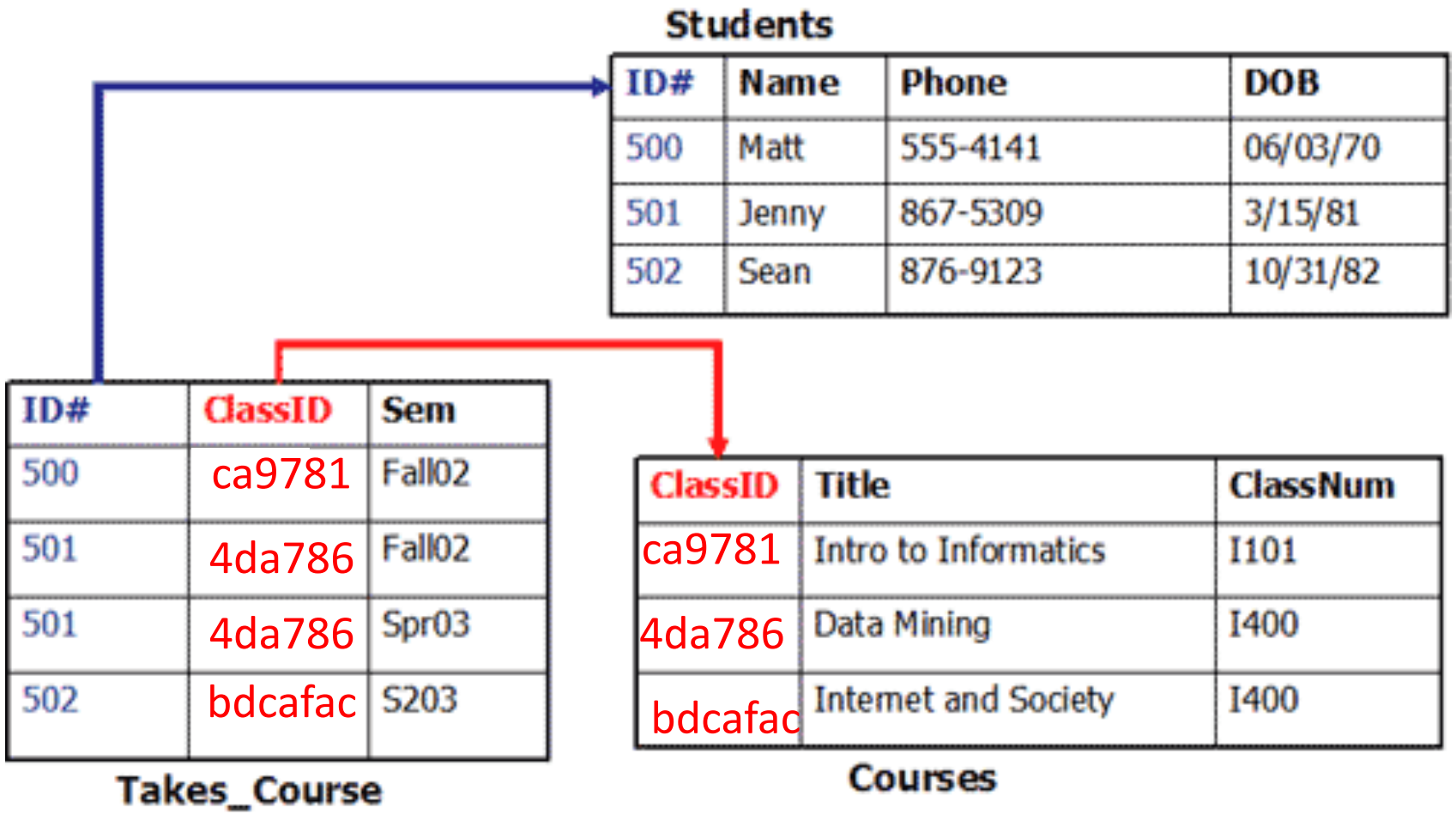
Takes_Course

ID#	ClassID	Sem
500		Fall02
501		Fall02
501		Spr03
502		S203

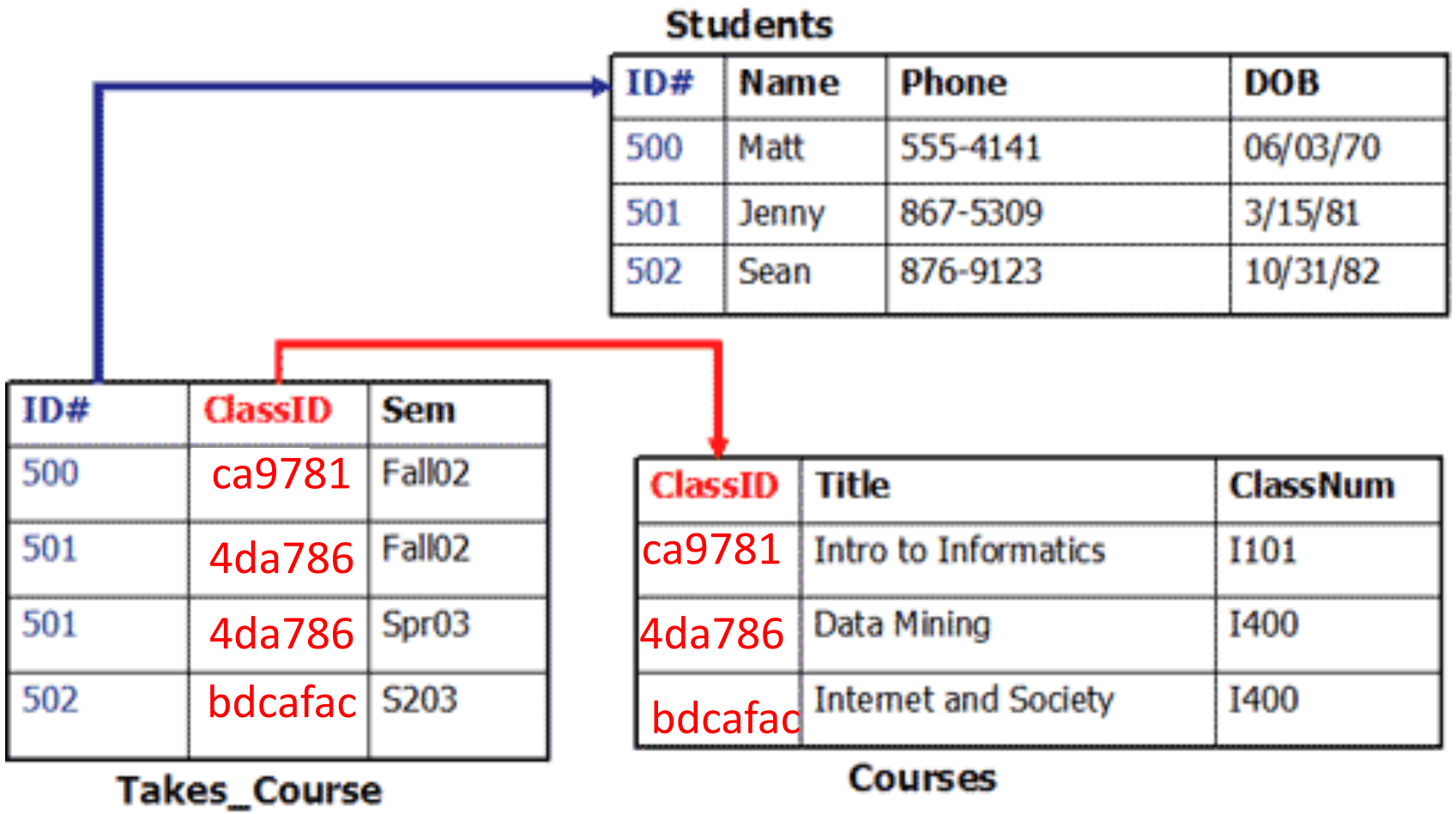
Courses

ClassID	Title	ClassNum
	Intro to Informatics	I101
	Data Mining	I400
	Internet and Society	I400

Tables - Pointers and keys

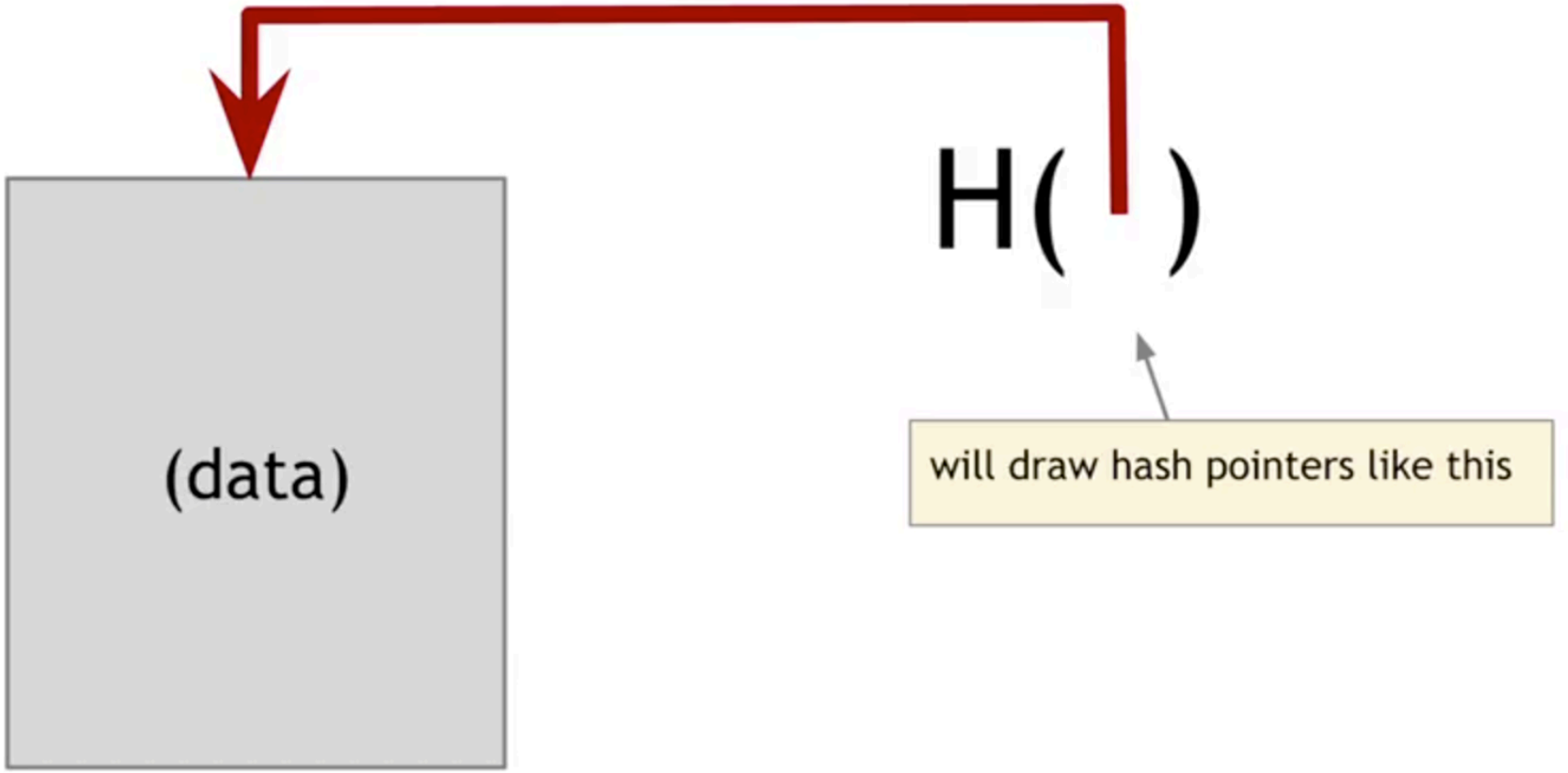


Tables - Pointers and keys



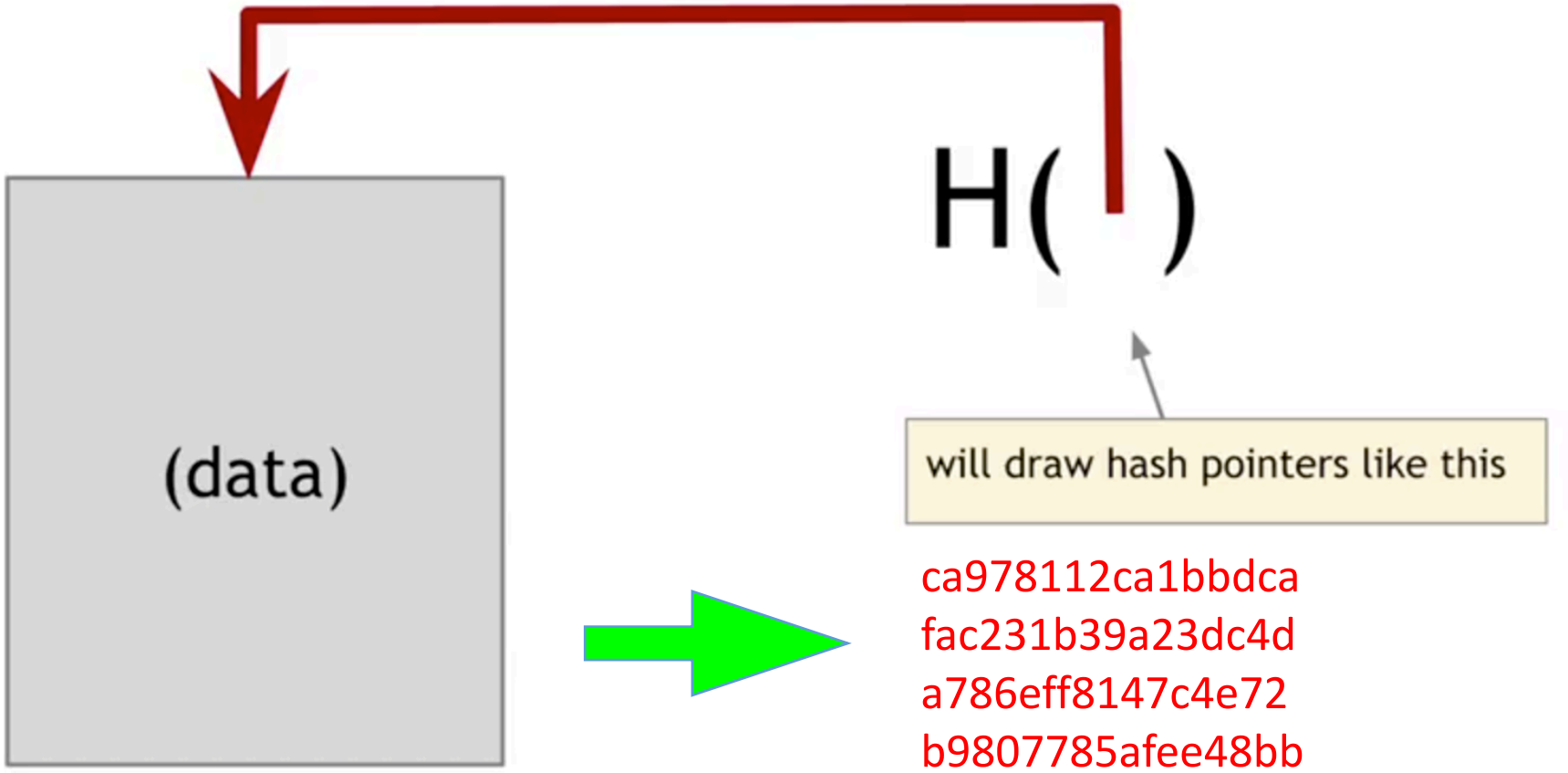
ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb

Hashpointer
ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb



Source: Princeton University / Coursera: Introduction to Crypto and Cryptocurrencies

Hashpointer
ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb



Source: Princeton University / Coursera: Introduction to Crypto and Cryptocurrencies

http://www.xorbin.com/tools/sha256-hash-calculator

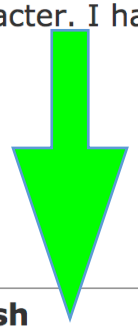
SHA-256 hash calculator

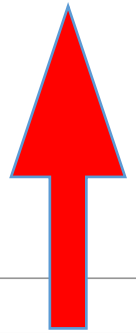
Like 404 Tweet Pin it Share 6.2K

SHA-256 produces a 256-bit (32-byte) hash value.

Data

I have a dream that one day this nation will rise up and live out the true meaning of its creed: "We hold these truths to be self-evident: that all men are created equal." I have a dream that one day on the red hills of Georgia the sons of former slaves and the sons of former slave owners will be able to sit down together at a table of brotherhood. I have a dream that one day even the state of Mississippi, a state, sweltering with the heat of injustice and sweltering with the heat of oppression, will be transformed into an oasis of freedom and justice. I have a dream that my four little children will one day live in a nation where they will not be judged by the color of their skin but by the content of their character. I have a dream today.





SHA-256 hash

3384a4722da6b6df0e84cbd86c862035c094e8dbd6e36bdcadb0b241088c68c2

Calculate SHA256 hash

http://www.xorbin.com/tools/sha256-hash-calculator

SHA-256 hash calculator

Like 404 Tweet Pin it Share 6.2K

SHA-256 produces a 256-bit (32-byte) hash value.

Data

I have a dream that one day this nation will rise up and live out the true meaning of its creed: "We hold these tru
to be self-evident: that all men are created equal." I have a dream that one day on the red hills of Georgia the so
of former slaves and the sons of former slave owners will be able to sit down together at a table of brotherhood.
have a dream that one day even the state of Mississippi, a state, sweltering with the heat of injustice and swelt
with the heat of oppression, will be transformed into an oasis of freedom and justice. I have a dream that my f
little children will one day live in a nation where they will not be judged by the color of their skin but by the co
of their character. I have a dream today.

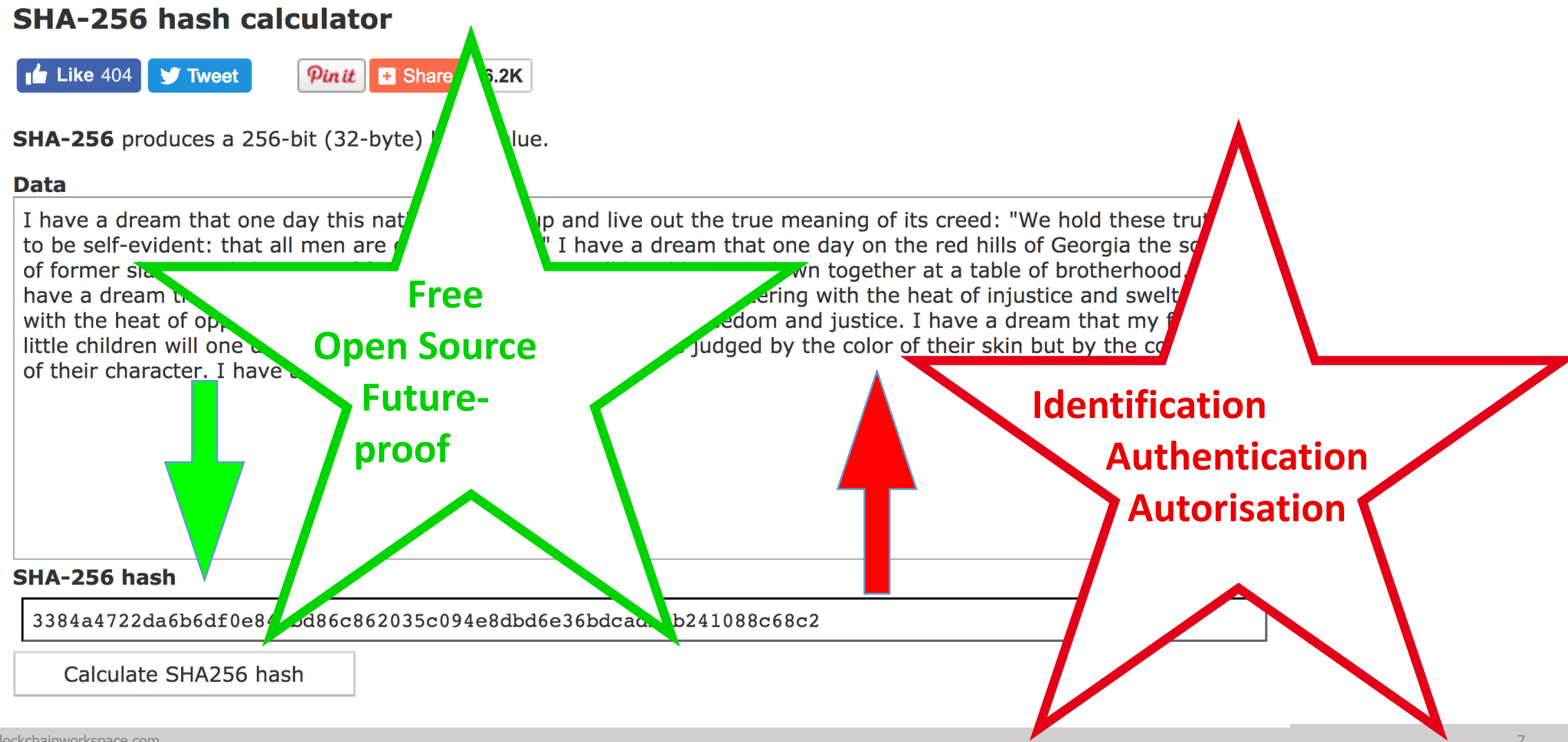
SHA-256 hash

3384a4722da6b6df0e84cbd86c862035c094e8dbd6e36bdcadb0b241088c68c2

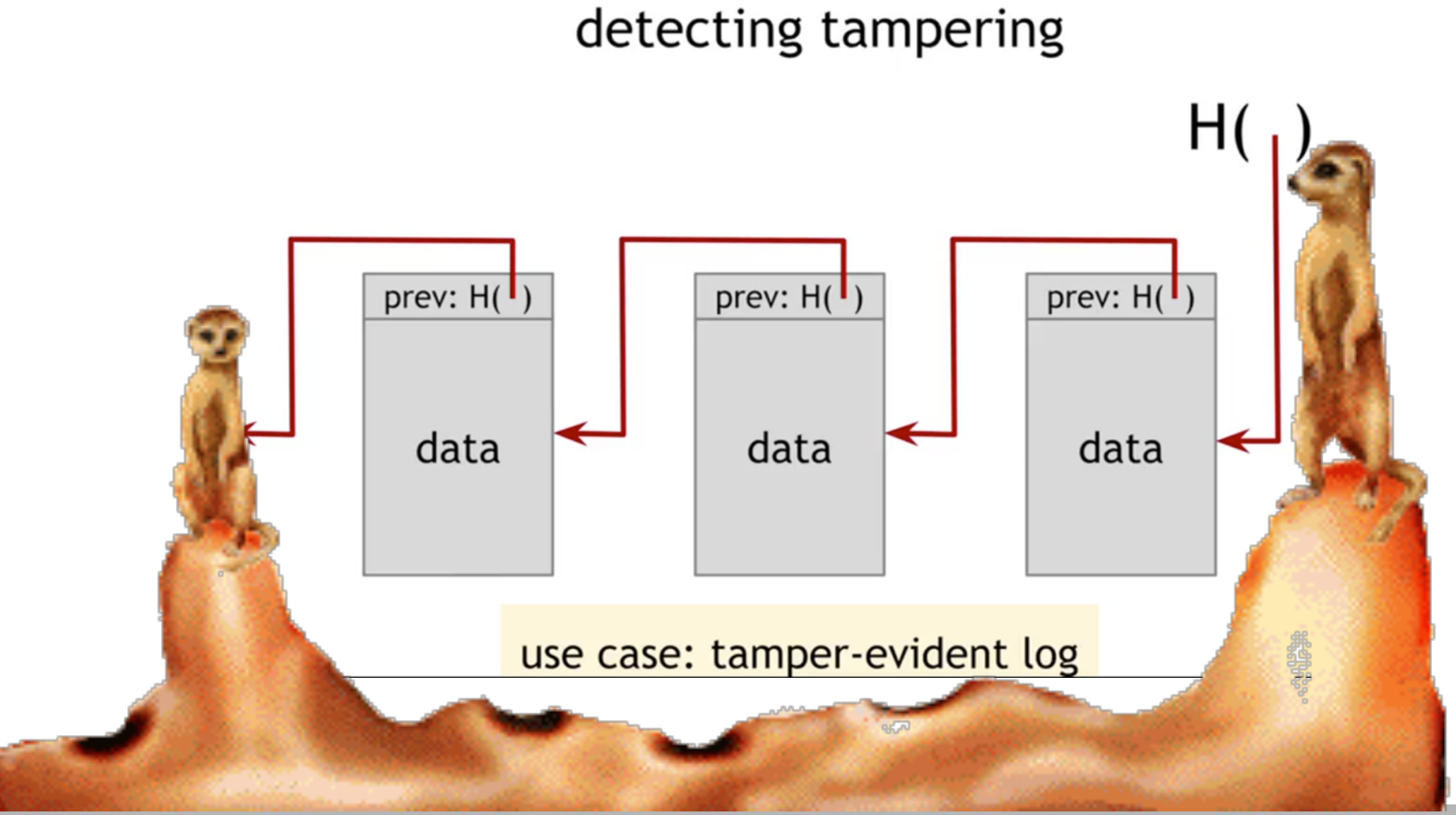
Calculate SHA256 hash

Identification
Authentication
Autorisation

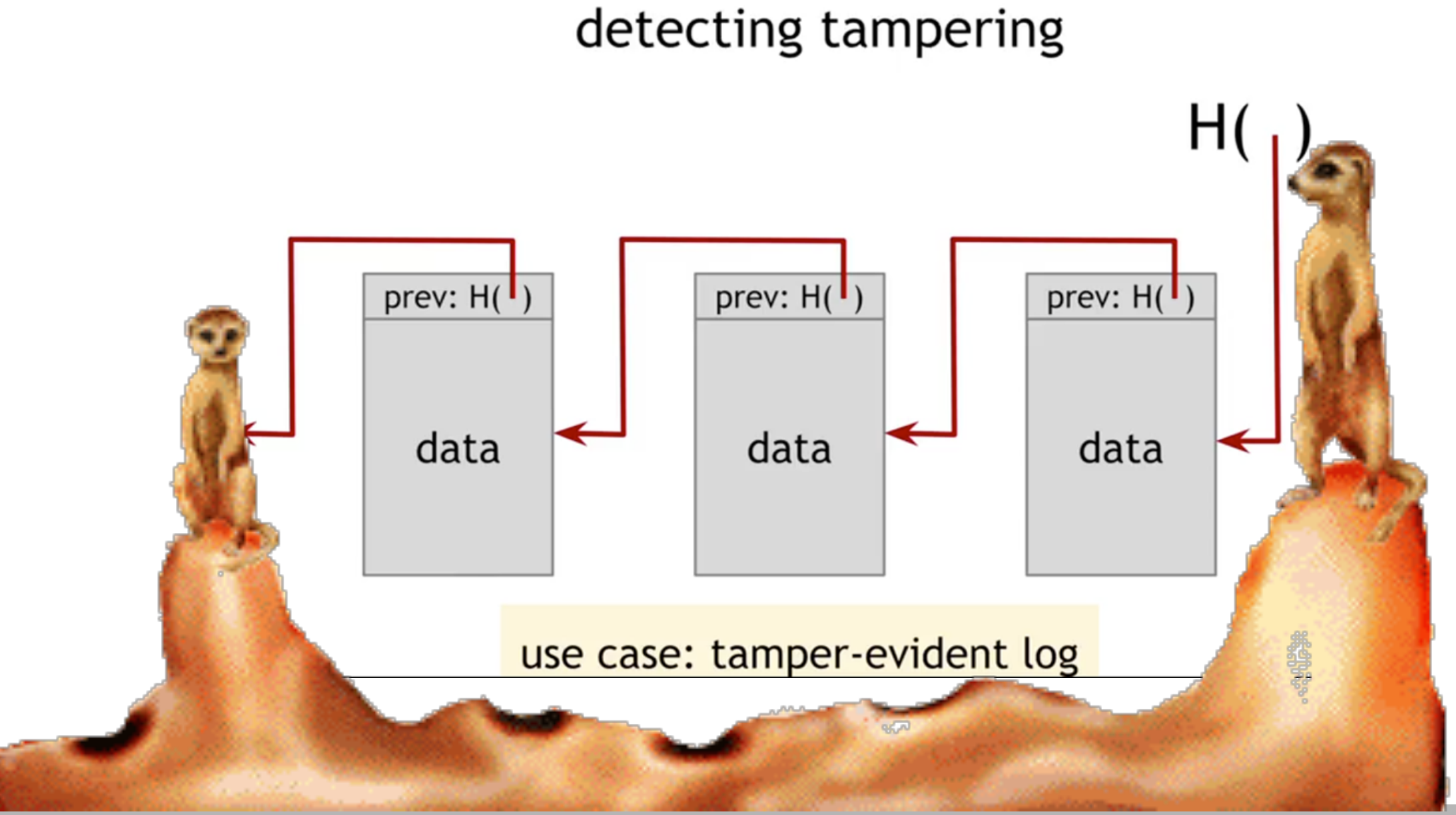
http://www.xorbin.com/tools/sha256-hash-calculator



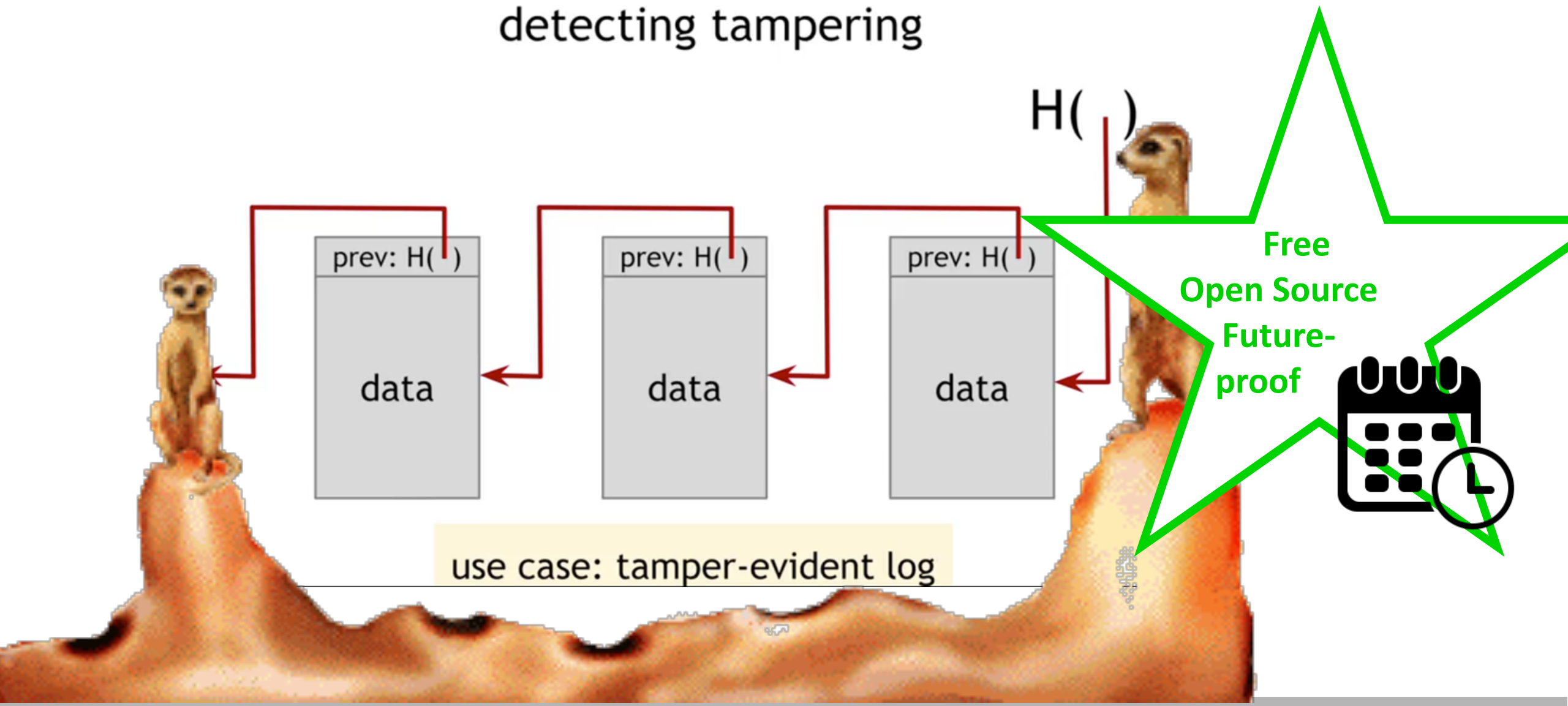
Chain of hashes (pointers): Tamper evident!



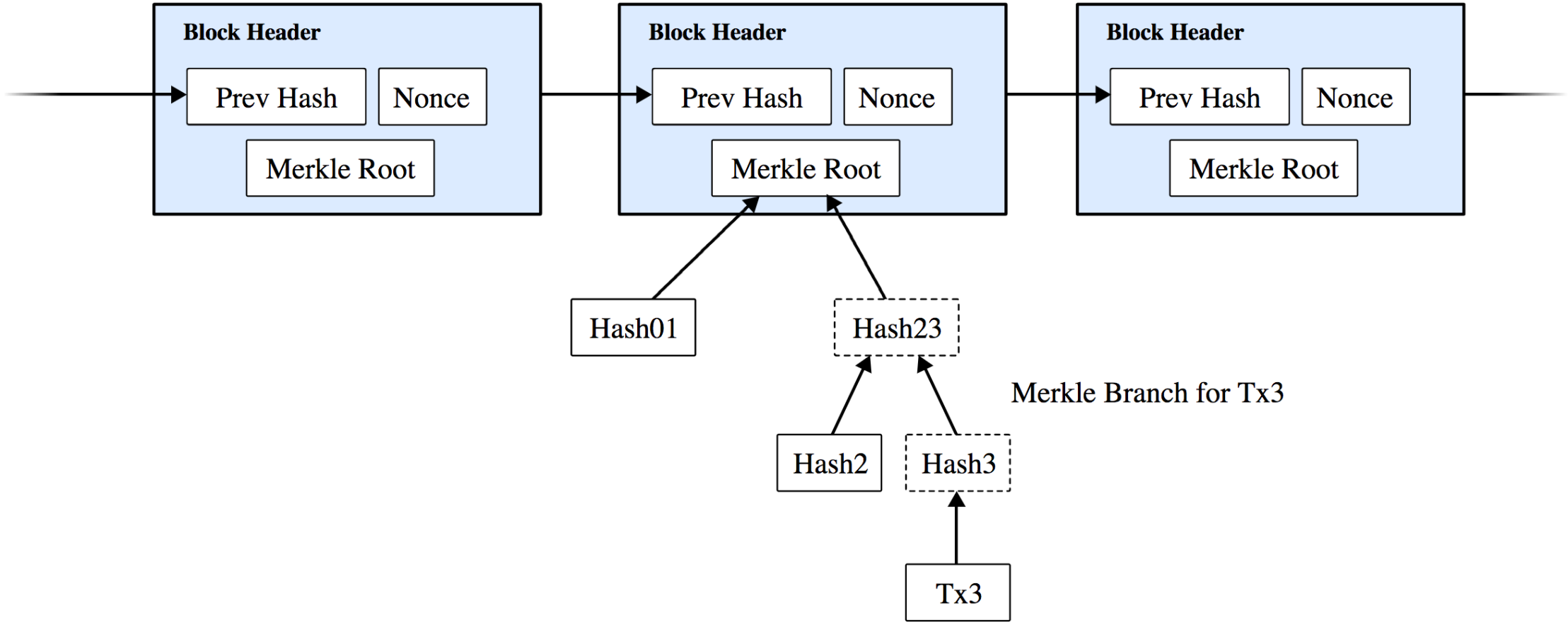
Chain of hashes (pointers): Tamper evident!



Chain of hashes (pointers): Tamper evident!

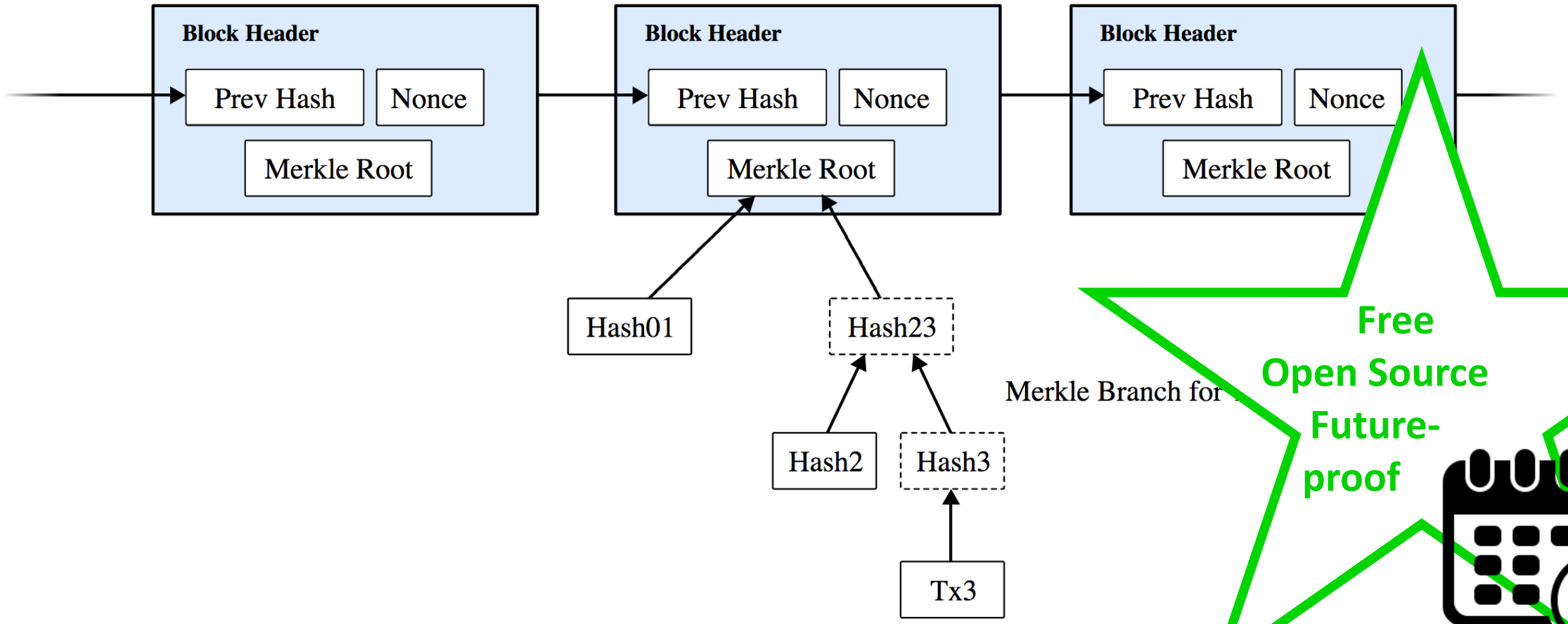


SPV wallet / Merkle tree



Source: http://nakamotoinstitute.org/bitcoin/#selection-229.4-232.0

SPV wallet / Merkle tree



Source: http://nakamotoinstitute.org/bitcoin/#selection-229.4-232.0

Point to me, then I might point back…

Only pointers to content on the blockchain!

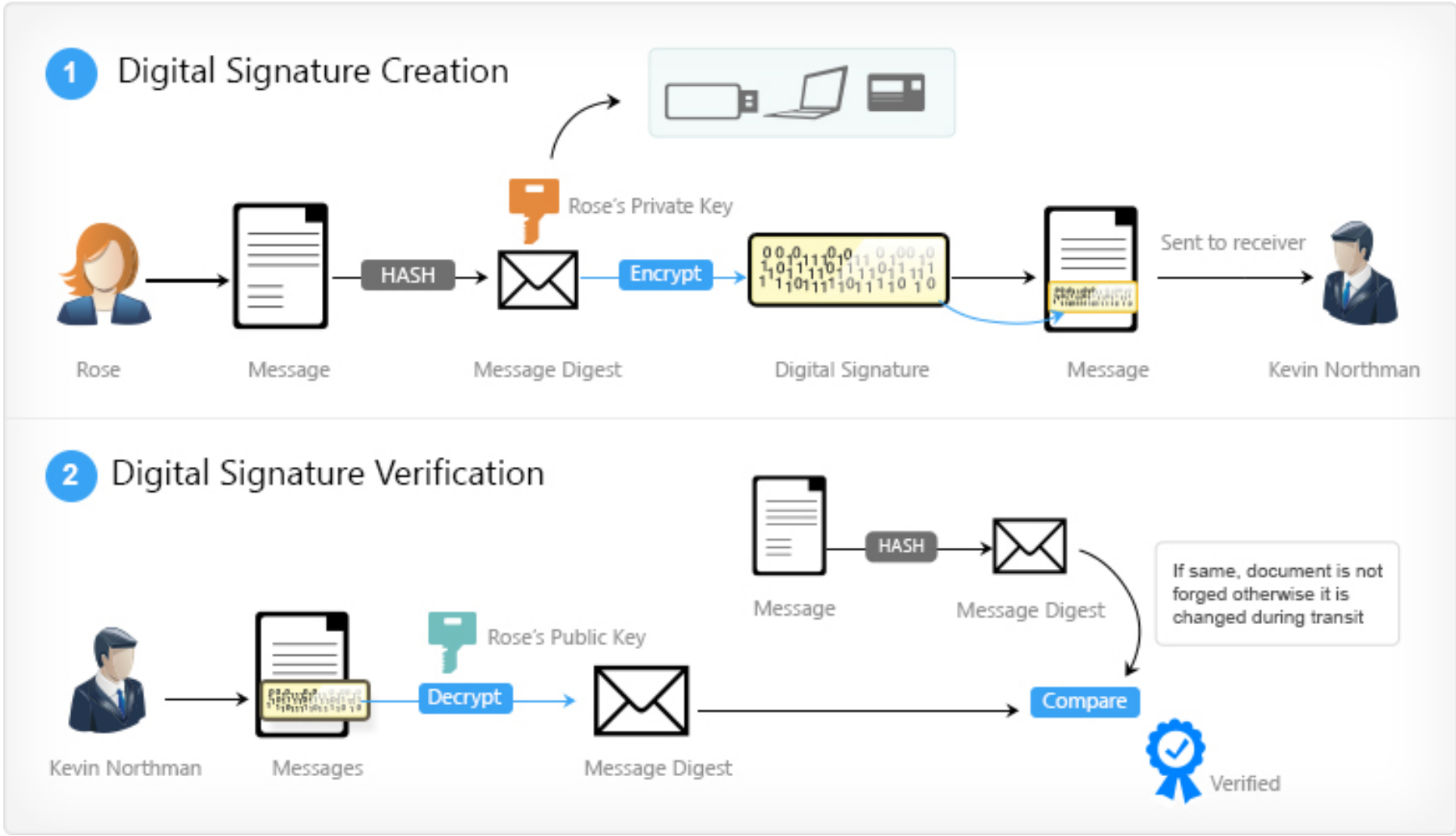
This is ON the blockchain!

Example 1. Alice's transaction, serialized and presented in hexadecimal notation

0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd73
4d2804fe65fa35779000000008b483045022100884d142d86652a3f47
ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039
ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813
01410484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade84
16ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc1
7b4a10fa336a8d752adfffffffff02**60e3160000000001976a914ab6**
8025513c3dbd2f7b92a94e0581f5d50f654e788acd0ef800000000000
1976a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac 00000000

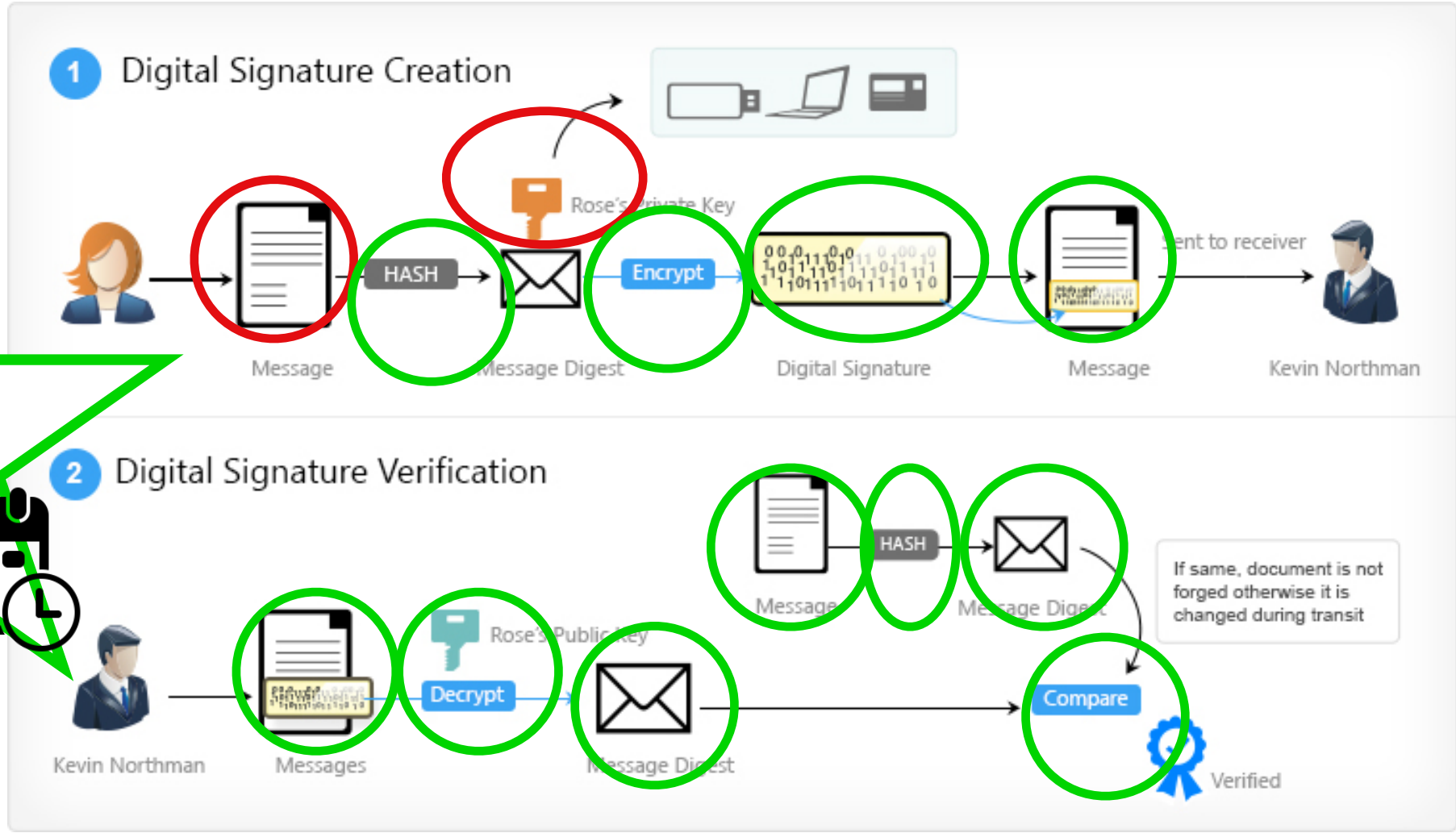
Receiving address creation

Digital Signatures - extended



Source picture: https://staging.signinghub.com/electronic-signatures/

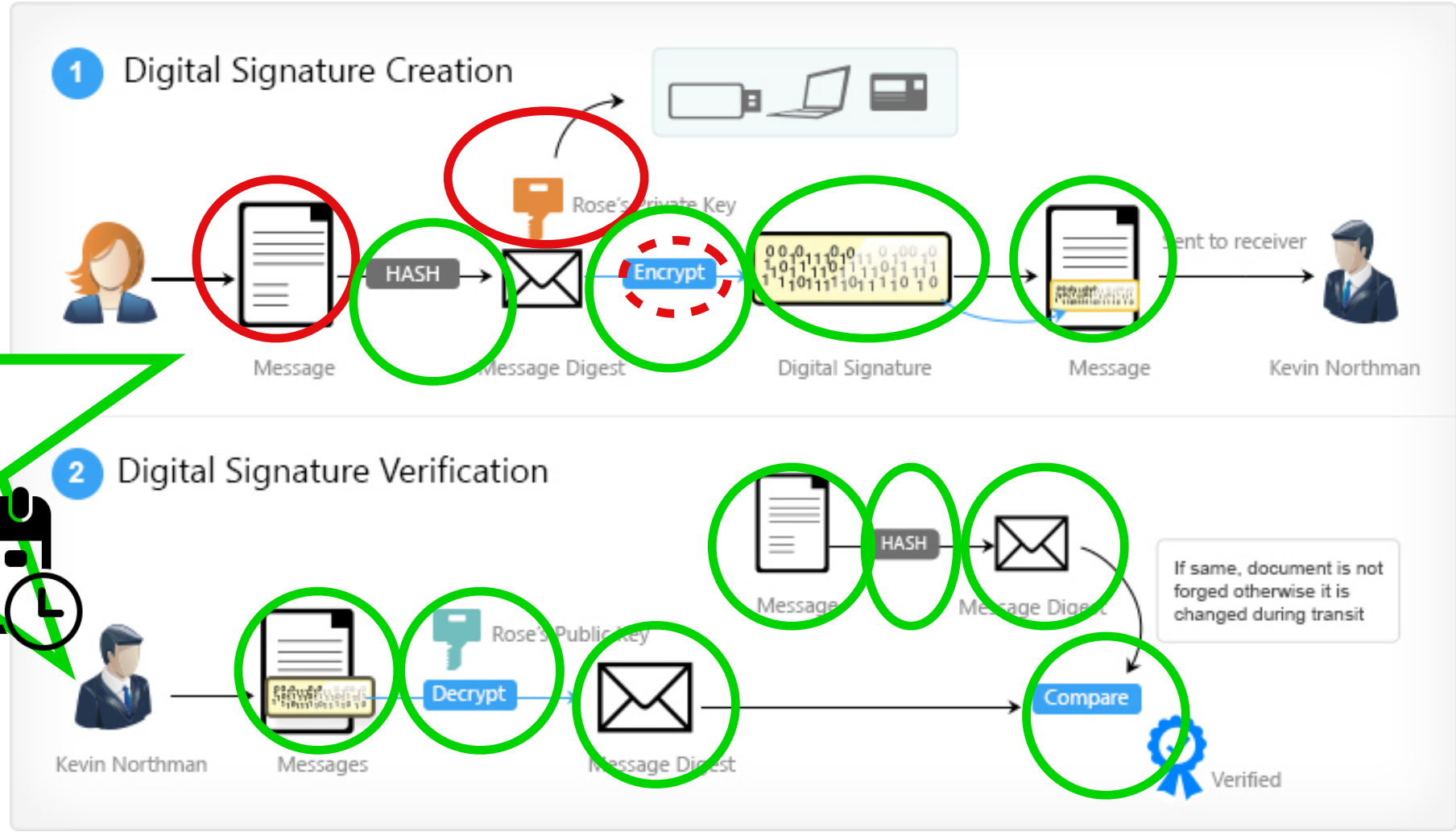
Digital Signatures - extended



Free Open Source

Source picture: https://staging.signinghub.com/electronic-signatures/

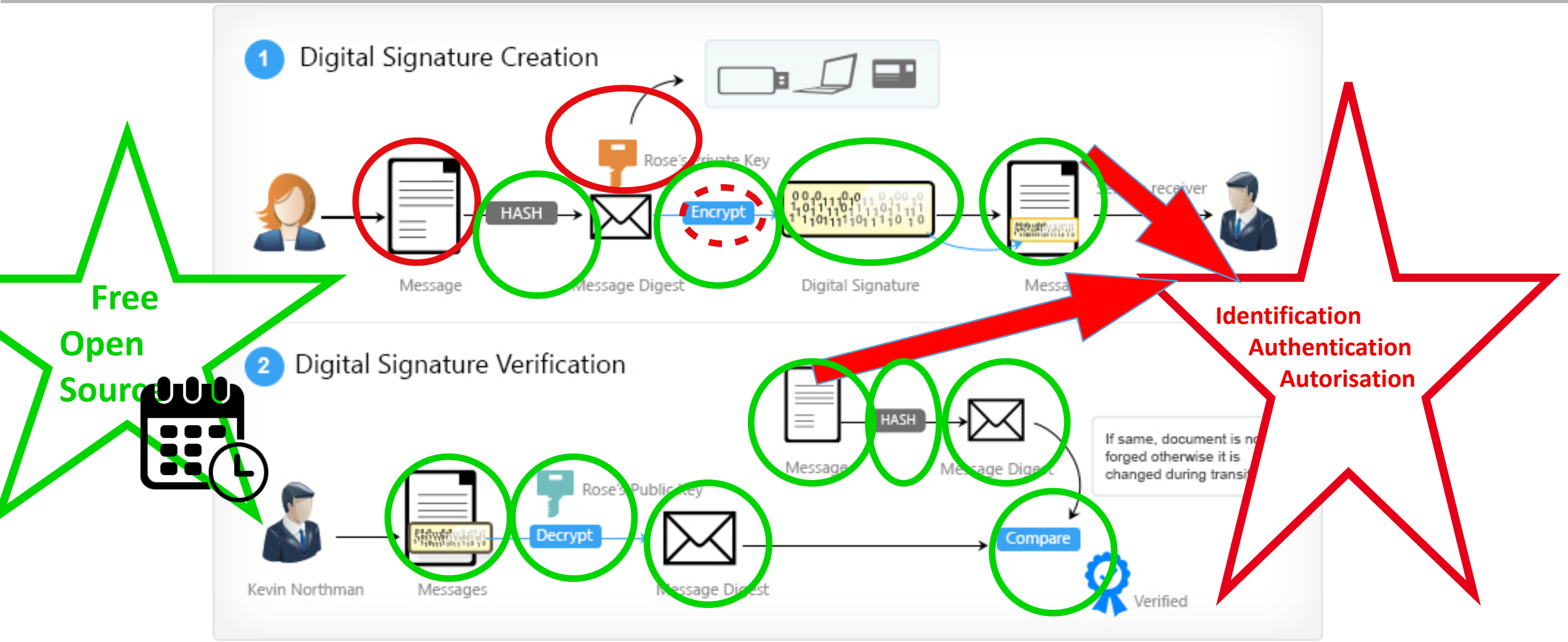
Digital Signatures - extended



Free
Open
Source

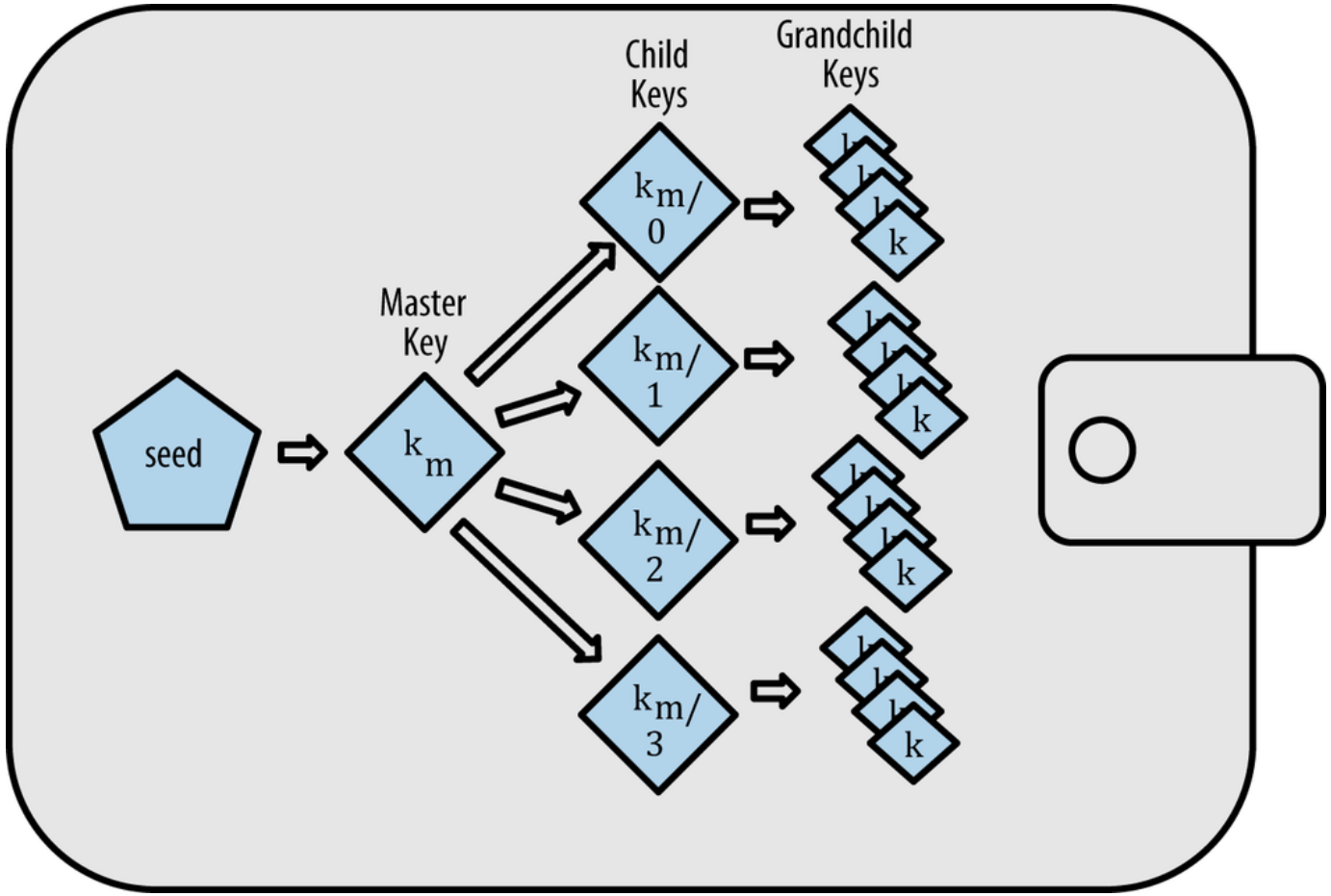
Source picture: https://staging.signinghub.com/electronic-signatures/

Digital Signatures - extended



Source picture: https://staging.signinghub.com/electronic-signatures/

Hierarchical Deterministic Keychains



Source: http://nakamotoinstitute.org/bitcoin/#selection-229.4-232.0

License

This work is licensed under a Creative Commons Attribution-Share Alike 4.0 license

https://creativecommons.org/licenses/by-sa/4.0/

Thank You

@henkvancann

Never ever forget…

Only pointers on the blockchain!

Never ever forget…

Only pointers on the blockchain!

…and a bit of program code, that we call smart contracts.