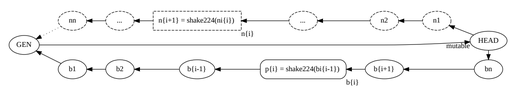
SELF HEALTH QUANTIFICATION BLOCKCHAIN

Michel Combes PhD[1] and Colleen F. Draper MS RD PhD[2]

[1] Blockchain consultant and CEO GC-Bank, Lausanne, Switzerland
[2] Research Consultant, Personal projects, Lausanne, Switzerland
[V] email: m.combes@gc-bank.org



… nourishing research with data commons

Introduction

- With a dazzling number of quantification devices and infiltration of sensors everywhere, personal data is abundant; and opportunities for self health quantification are on the rise.
- Data are not available in consistent formats. Data need to be unified.
- Most health records are centrally managed and do not place the owner of data in control. These systems lead to data leaks, security threats, loss of privacy, and inefficiencies.
- Users do not own their data, and it is often not available when most needed. (walled garden") .
- Block chain technology may offer a reliable, consistent solution to catalogue and share research and personal health data.
- We present here a secure biomimethic system for data commons.

Solutions

- Consistent, private, reliable, easily accessed. Operates offline.
- Continuity of personal health.
- Near real time research data collection.
- Data owner provides real time informed consent with cryptographic keys.
- Removal of big data silos.
- Decentralized data.
- Transition to Internet of Everyone.
- Tightly coupled with living world.

Personal Health Record

Collect data on symptoms and responses to medications, nutritional therapies, and other lifestyle modifications. Record personal changes and analyze how they benefit your health resilience.

Graphs provide easy to read information on trends and changes over time; including a timeline chart that shows how events in your life correspond with changes in your health.

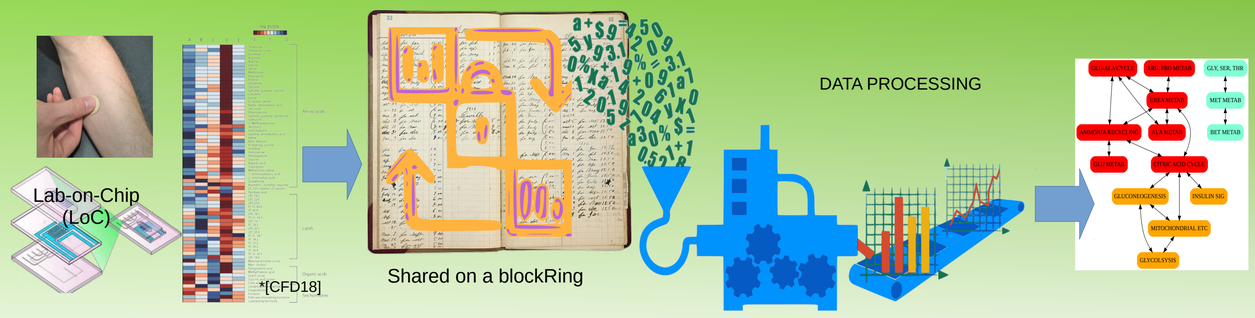
You can approve medical provider access to your information, which is easily downloadable and augmented by any practitioner.

SHQ BLOCKRING = BRINGING HEALTH TO TECHNOLOGY

Research data

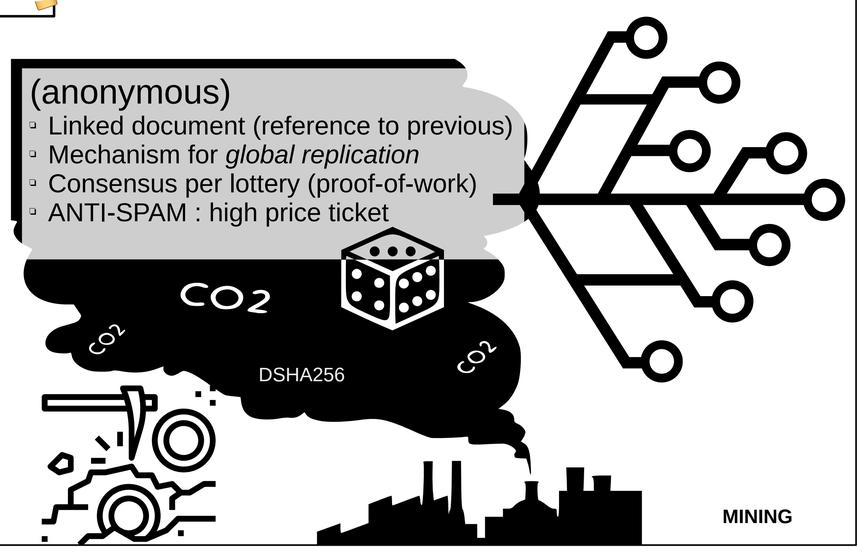
Hosted and distributed by users who control update and access.

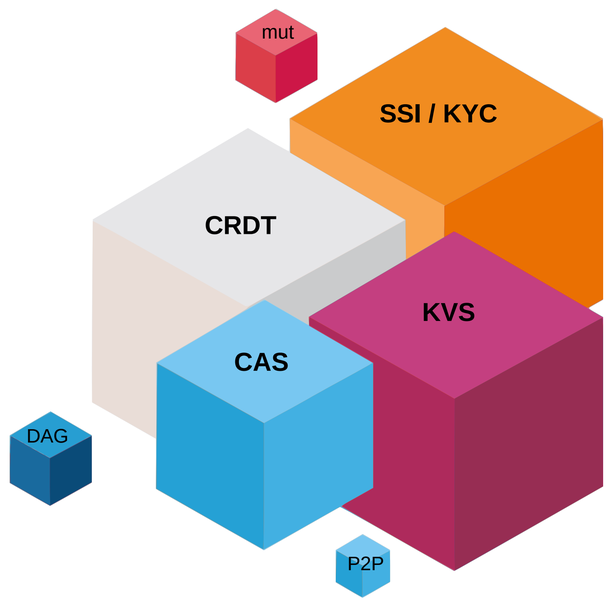
Consistency in data collection and categorization allows everyone to participate in retrospective and prospective research programs.



BLOCKCHAIN ?

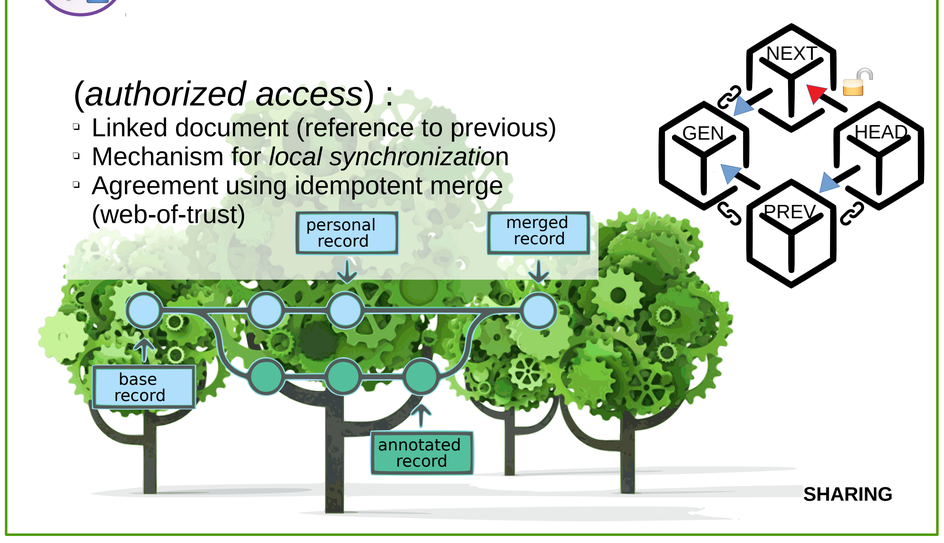
(anonymous)
- Linked document (reference to previous)
- Mechanism for *global replication*
- Consensus per lottery (proof-of-work)
- ANTI-SPAM : high price ticket





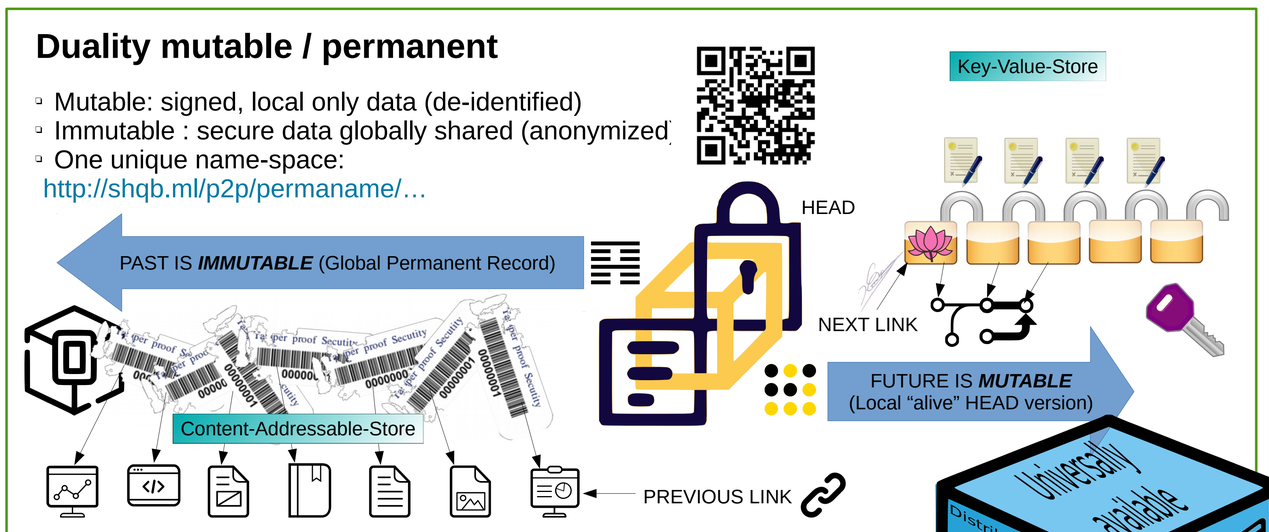
SHQ BLOCKRING ?

(*authorized access*) :
- Linked document (reference to previous)
- Mechanism for *local synchronization*
- Agreement using idempotent merge (web-of-trust)



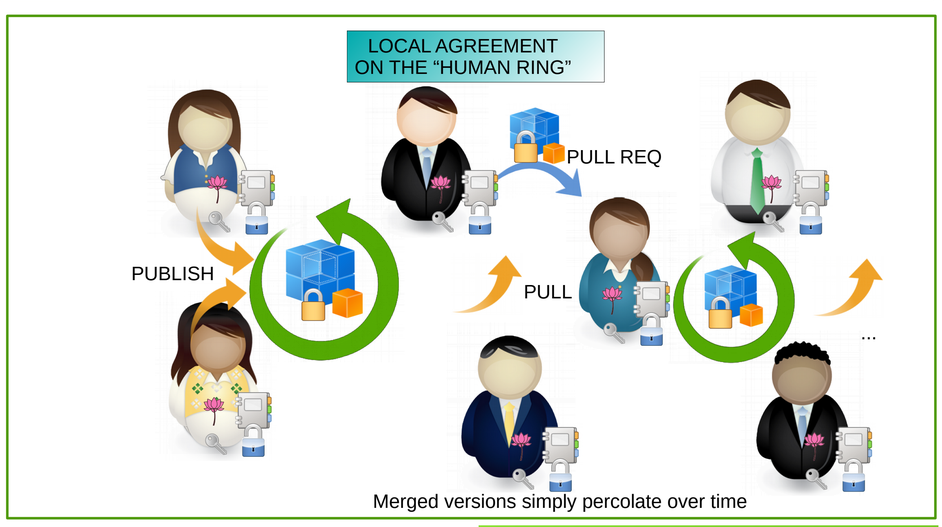
Duality mutable / permanent

- Mutable: signed, local only data (de-identified)
- Immutable : secure data globally shared (anonymized)
- One unique name-space:
  http://shqb.ml/p2p/permaname/…



RULES TO BE ON THE SHQ BLOCK !

- EVERY BLOCK IS ADDRESSED WITH ITS "SPONGE" VALUE
- EVERY BLOCK CONTAIN TWO LINKS :
  - A REFERENCE TO THE PREVIOUS BLOCK AND
  - AN ADDRESS WHERE THE NEXT ONE WILL BE POSTED
- EVERY NEXT ADDRESS IS SIGNED BY ITS AUTHOR
- EVERY GENESIS BLOCK, POINTS TO THE HEAD OF THE CHAIN
- EVERY BLOCK IS IN A FORMAT SUCH THAT IT CAN BE AUTOMATICALLY MERGED



Permanent links (secure hash):

Data integrity guaranteed by one-way hash :
sponge function SHAKE-224(data)

Used in Content-Addressable-Store
Data change → key change (i.e. link broken)

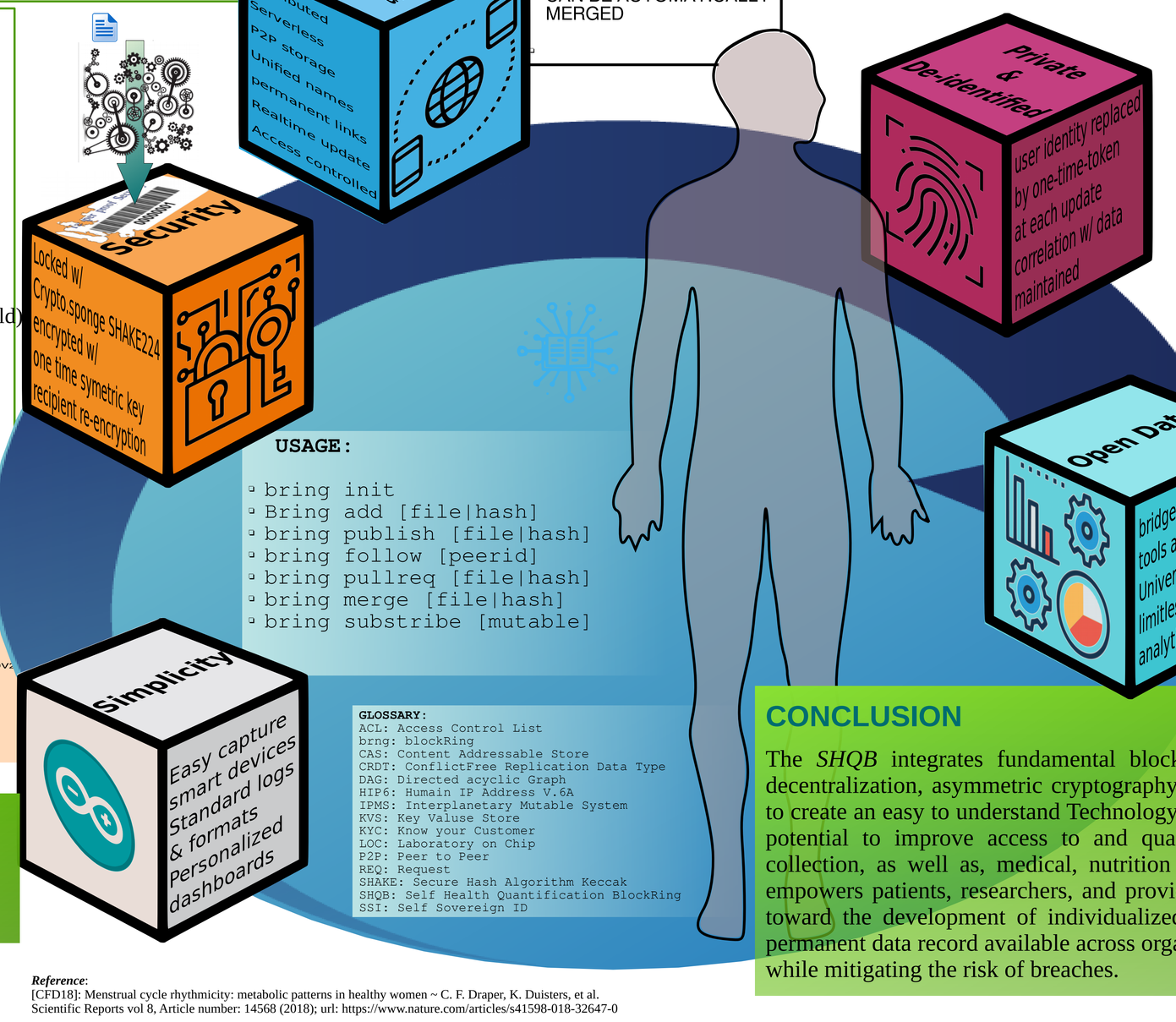
Open locks (colliding hash) :

Mutability provided with "collision" prone hash function :
IDENT20:
Take the first 20 bytes of the document as a hash (magic field)

Wet Signature (MUT224 hash w/ limited life):

Take SHAKE-224(secret-key, permalink,
public-key(owner),
header(document),
time-to-live)
allow "update in the body part of the document" (KVS)

Dry signature = expired signature



You decide who you are for each recipient / data-set

Self Sovereign ID :
HIP6 = shake384(Civil-ID)
Derived IDs : {ID_1,ID_2,...}

ACL per recipient :
encrypt(DH(recipient),data)
Note: Symetric key for speed

PSEUDO -ANONYMOUS
Data published under ID_i for recipient$_i$

DE-IDENTIFCIATION
Data published under consistently random ID

```
--- # imfs blockRing™
name: imfs
peerid: QmRLZbRZcqdrM6L3rTFYFuz56vBoS1Z5dsu4V4X5yboZc1
mutable: '$Source: /imfs/root.yml $ '
tic: 1552211432
head: QmZx8RTB1L9jy3G1WCdQWvZc6yVm6UN8Bi2QFdQ3YzY737
gen: QmXJzfuS5P1KKsukh1Z92hQxaD2U3EWTaLn3GUPgpPfW9j
mut: zAEcm5EMaYRbvZfBk882tQuHFN5rSVNpPTLGWm51NWUpZwWrADaK5uQGRBYwGjR8ND9Vz
type: ring
qm:
  - QmNxUzcS1NukFdXkC7Du73vNnHVDX7yYJ9d78ApLrwYHMw
  - QmaVwK6P1m2Q17mYsJw8LtTSZQ9Cyr6fZ5jCZ1Av2Jng3a
  - QmS6jFEWfQAZ9fFTc2CJ6tD1UzyDEfqMiHLH6JA7KmMJBk
  - z3ZJxEVdjfFskSkhVTu6VUmghj1NM5FdtsYB
  - z3ZJxEVdkHGvxjFzKXv7ihodadBTEip4W1a5
  - zdj7WmmPuGAi7JCTCryfn4QTLvNv78DR9      /LyrqSSRtp
```

RESULTs
- First prototype code: 248 files, 17323 lines
- 6 blockRings : 24'796 Hashes Size: 13.32MB
- Data : 16'133 blocks gigSize: 150.9GB

GLOSSARY :
ACL: Access Control List
brng: blockRing
CAS: Content Addressable Store
CRDT: ConflictFree Replication Data Type
DAG: Directed acyclic Graph
HIP6: Humain IP Address V.6A
IPMS: Interplanetary Mutable System
KVS: Key Valuse Store
KYC: Know your Customer
LOC: Laboratory on Chip
P2P: Peer to Peer
REQ: Request
SHAKE: Secure Hash Algorithm Keccak
SHQB: Self Health Quantification BlockRing
SSI: Self Sovereign ID

CONCLUSION

The *SHQB* integrates fundamental blockchain concepts with decentralization, asymmetric cryptography and de-identification to create an easy to understand Technology. The *SHQB* holds the potential to improve access to and quality of research data collection, as well as, medical, nutrition and lifestyle care, It empowers patients, researchers, and providers to work together toward the development of individualized care, with a secure permanent data record available across organizations and borders while mitigating the risk of breaches.

Reference:
[CFD18]: Menstrual cycle rhythmicity: metabolic patterns in healthy women ~ C. F. Draper, K. Duisters, et al. Scientific Reports vol 8, Article number: 14568 (2018); url: https://www.nature.com/articles/s41598-018-32647-0