Data Privacy and GDPR in Open Blockchains

Andreas Koidis

Programize, LLC.
&
(ISC)^2 Hellenic Chapter

Scope of this presentation

- Trustless,
- permissionless,
- open consensus networks.

ethereum

bitcoin

not in scope

- Trusted,
- permissioned,
- enterprise blockchains.

HYPERLEDGER
FABRIC

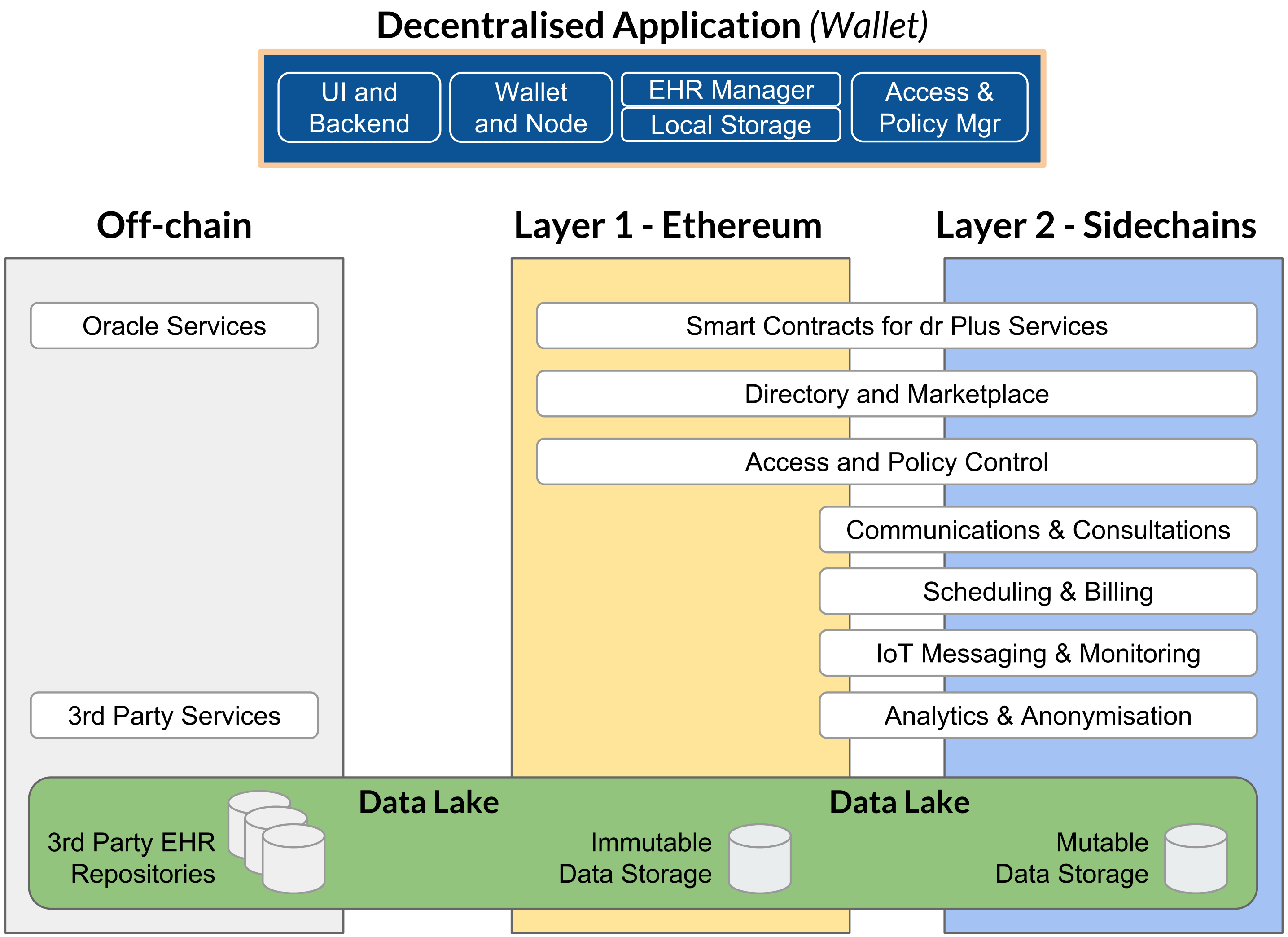
What the CRAB?

CRUD	CRAB
CREATE	CREATE
READ	RETRIEVE
UPDATE*	_APPEND*_
DELETE*	_BURN*_

https://tutorials.bigchaindb.com/crab

Architecture
(eg. Healthcare)

- ➢ Layer 1 Ethereum
- ➢ Layer 2 Sidechains
- ➢ Off-chain APIs
- ➢ Data Storage Mgmt
- ➢ Wallet app (fat client)

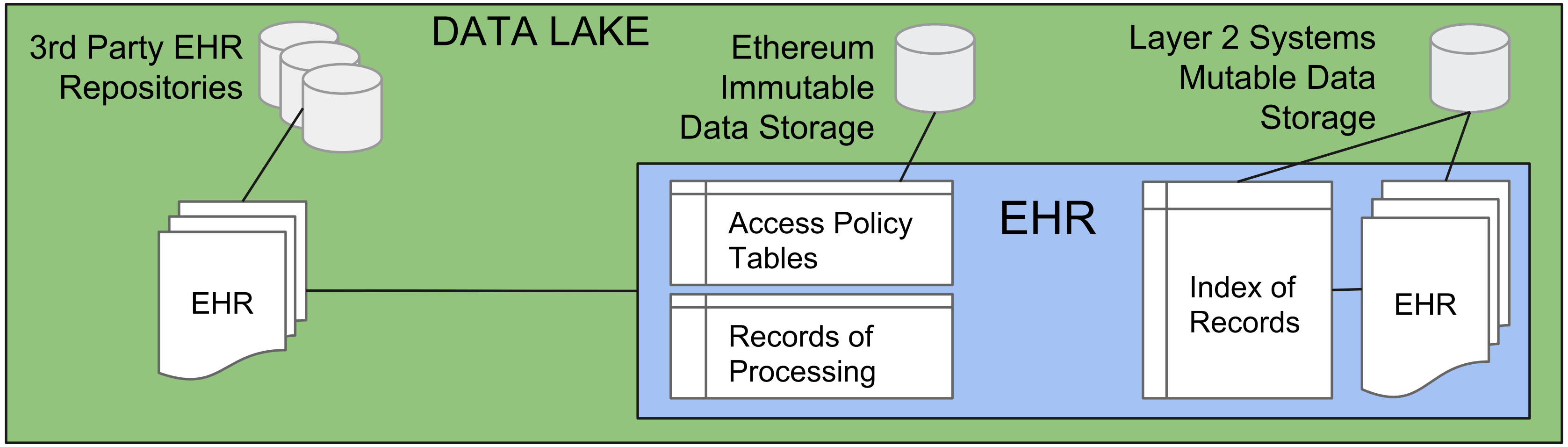


Programize, LLC.

Mutability and immutability

- Immutable storage: Access policies hash & links, Audit trails
- Mutable storage: Access policy operands, Indexes, Metadata, Data
- Mutable storage can be personal (Offline, Dropbox, Provider, etc.)

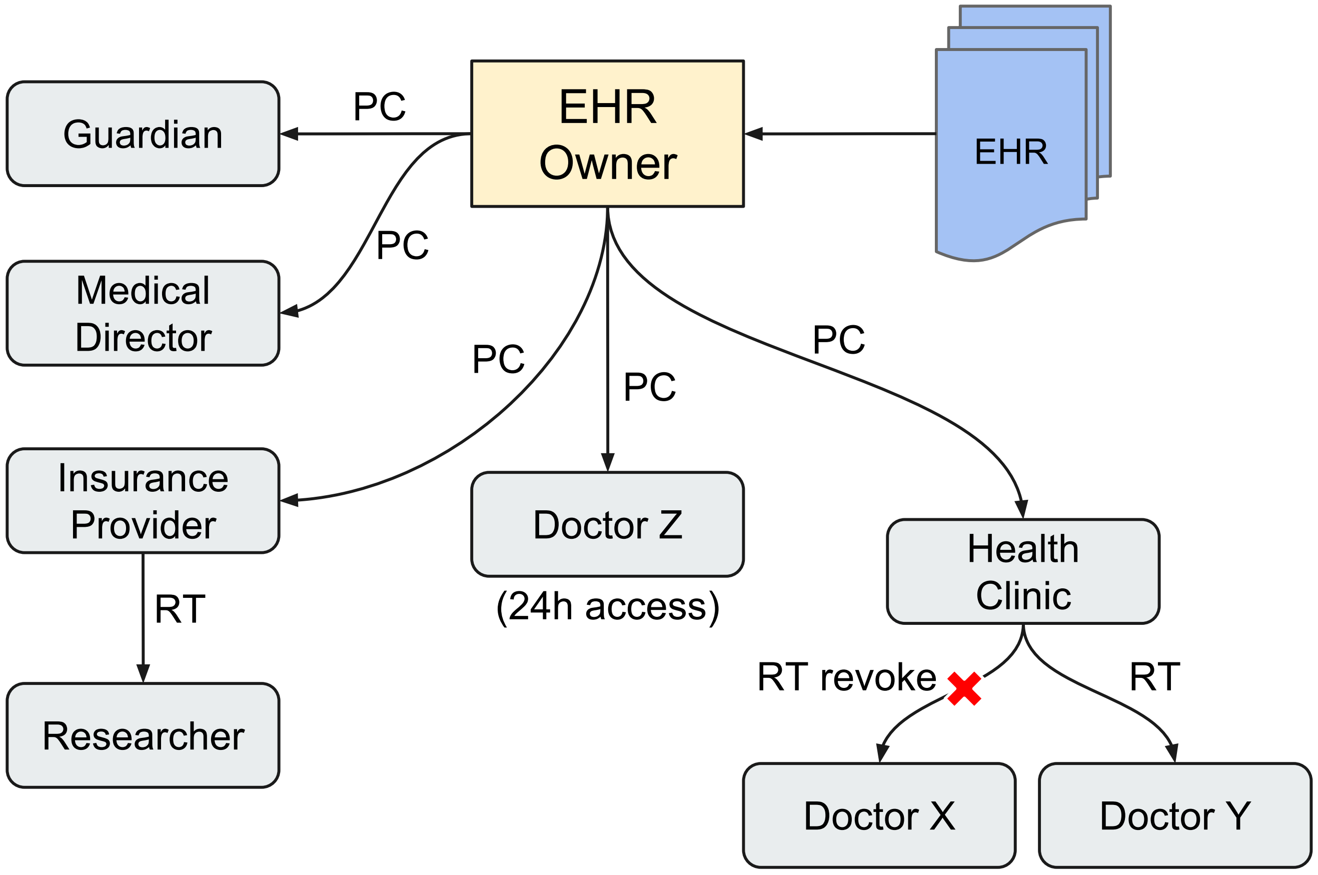
Logical structure of an EHR


DATA LAKE
3rd Party EHR Repositories
Ethereum Immutable Data Storage
Layer 2 Systems Mutable Data Storage
EHR
EHR
Access Policy Tables
Records of Processing
Index of Records
EHR

Programize, LLC.

RBAC → ABAC

- Data centric security
- From role-base to attribute-based
- Enables security in hostile environments
- Opt-in, opt-out, consent
- Rights transfer propagation
- Audit trails
- Revocation

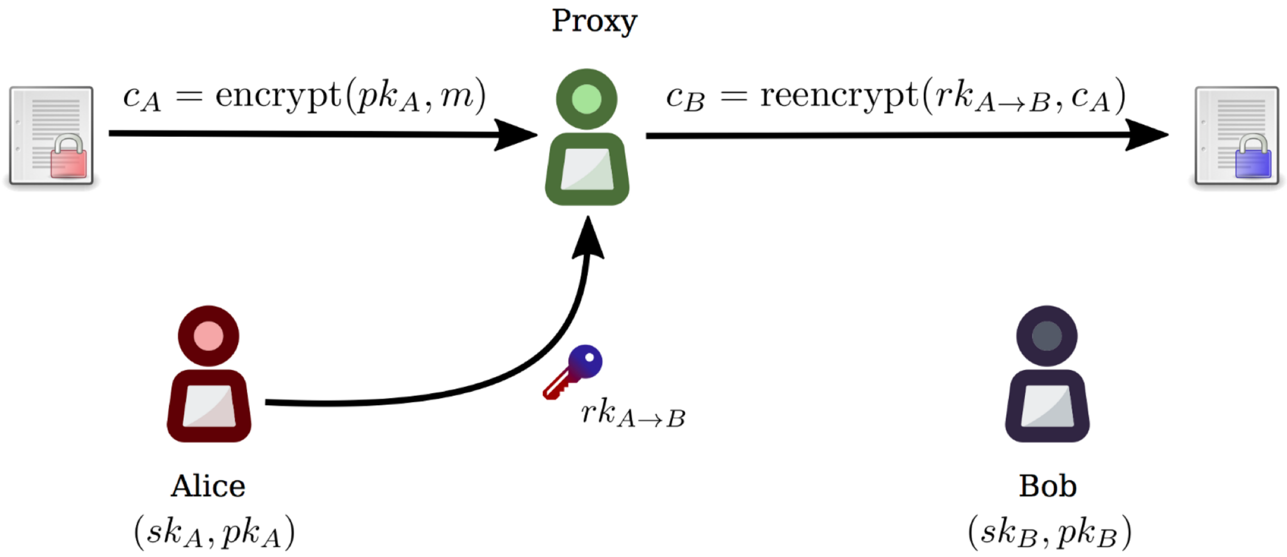


Policy Creation (PC), Rights Transfer (RT)

Programize, LLC.

Proxy re-encryption

- Essentially an access control for blockchains
- Operates via smart contracts to manage keys (zk proofs)
- Allows a third-party proxy to transform ciphertexts from one public key to another (using re-encryption keys)
- Without learning anything about the underlying message



Proxy
$c_A = \text{encrypt}(pk_A, m)$
$c_B = \text{reencrypt}(rk_{A\to B}, c_A)$
$rk_{A\to B}$
Alice
(sk_A, pk_A)
Bob
(sk_B, pk_B)

Umbral, NuCypher

Benefits

- Better privacy
- Data ownership
- Social scalability
- Anonymity

So, which path will you follow?

Thank you

Andreas Koidis

@koidis