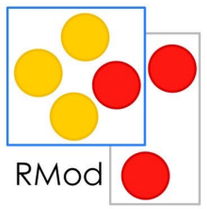
Esug 2018: A Pharo story on blockchain technology

by Santiago Bragagnolo - ESUG Cagliari - 2018
santiago.bragagnolo@inria.fr
santiago.bragagnolo@gmail.com
skype:santiago.bragagnolo
@sbragagnolo

inventeurs du monde numérique

1967 >> 2017 >> 2067 Imaginons notre futur

RMod



Who I am?

Santiago :)

RMod

A Pharo story on Blockchain technology

RMod

Much has been told about blockchain but, really:

What is blockchain?

inventeurs du monde numérique

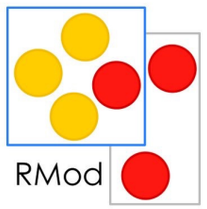
1967 ›› 2017 ›› 2067 Imaginons notre futur

RMod

BITCOIN

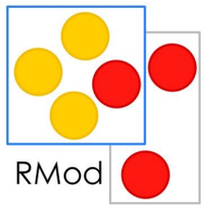
- **Be millionaire in a week**
- **Super fast transactions!**
- **Escape those tedious and uncomfortable taxes!**
- **Washing money like going to the laundry shop!**

Inria
inventeurs du monde numérique
50 ANS
1967 ›› 2017 ›› 2067
Imaginons notre futur



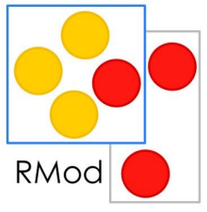
No, this is not a CryptoCurrency talk.

(you cannot leave, we already locked the door)



What is Blockchain?

- Distributed append only transaction log (database)
  - Immutable data
  - Verifiable record

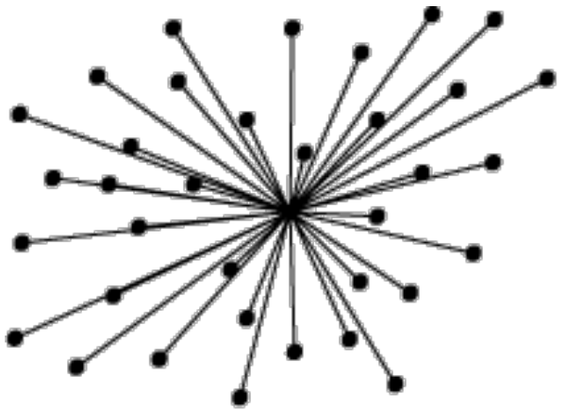


How does it works?

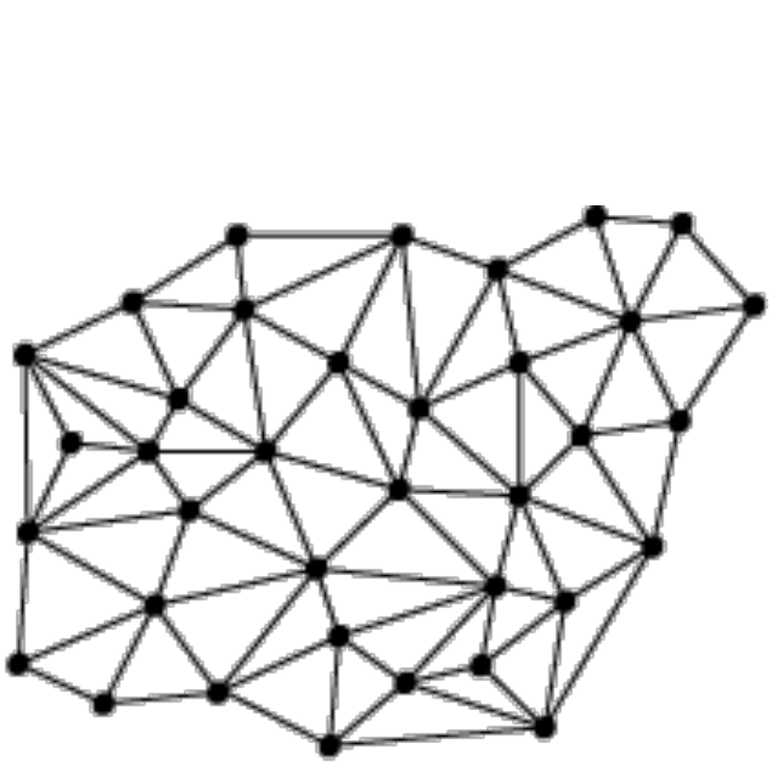
- Democratisation and incentivization of the surveillance
- Each participant of the network can verify the incoming transactions
- To participate into the surveillance is rewarded

RMod

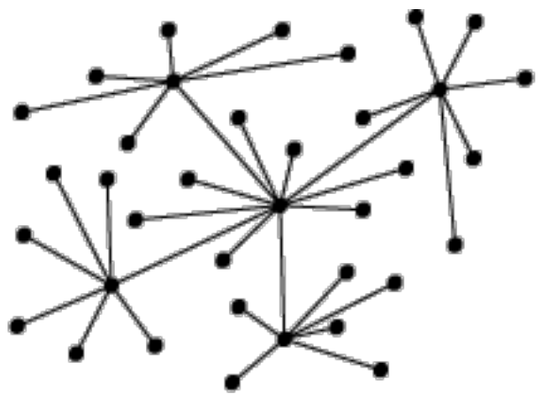
Distributed: High availability



centralised



distributed

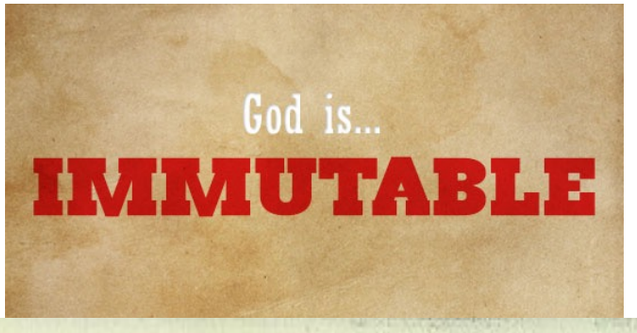


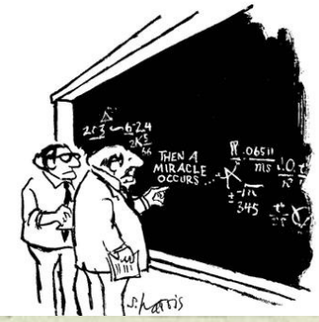
decentralised

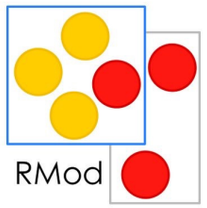
inventeurs du monde numérique

1967 › 2017 ›› 2067 Imaginons notre futur

Immutable & Verifiable: Trustable






RMod

Ok, so what?

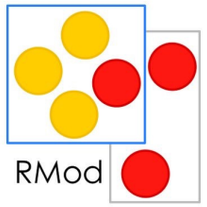

Inria
inventeurs du monde numérique
50 ANS
1967 › 2017 ›› 2067
Imaginons notre futur

RMod

Blockchain is about “democratising” the Trust business

inventeurs du monde numérique

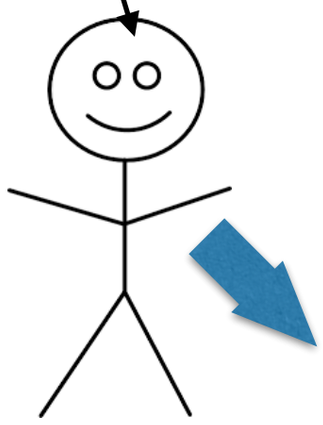
50 ANS 1967 › 2017 ›› 2067 Imaginons notre futur



What is a “Trust business”?

How do you lend money to a friend?

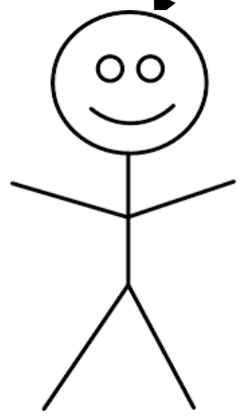
You



Your apple

The people you trust the most (?????)

Your friend



Your apple

They did not left even de leave :(

inventeurs du monde numérique

50 ANS
1967 / 2017 ›› 2067
Imaginons notre futur

RMod

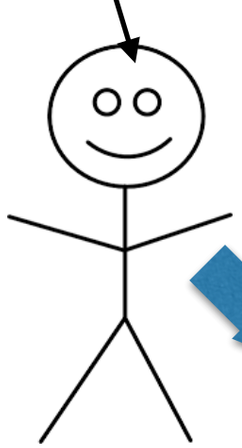
What can blockchain do for you in this case?

inventeurs du monde numérique

1967 › 2017 › 2067 Imaginons notre futur

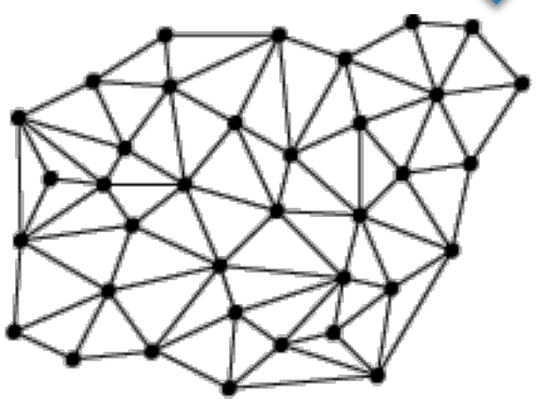
How could you lend money to a friend?

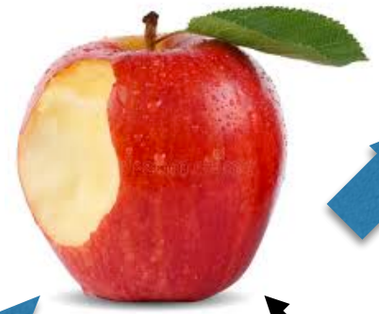
You



Your apple

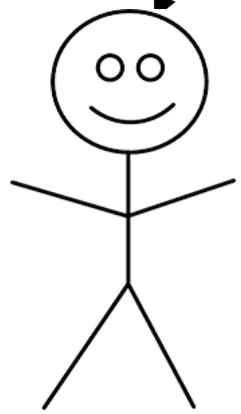
Blockchain



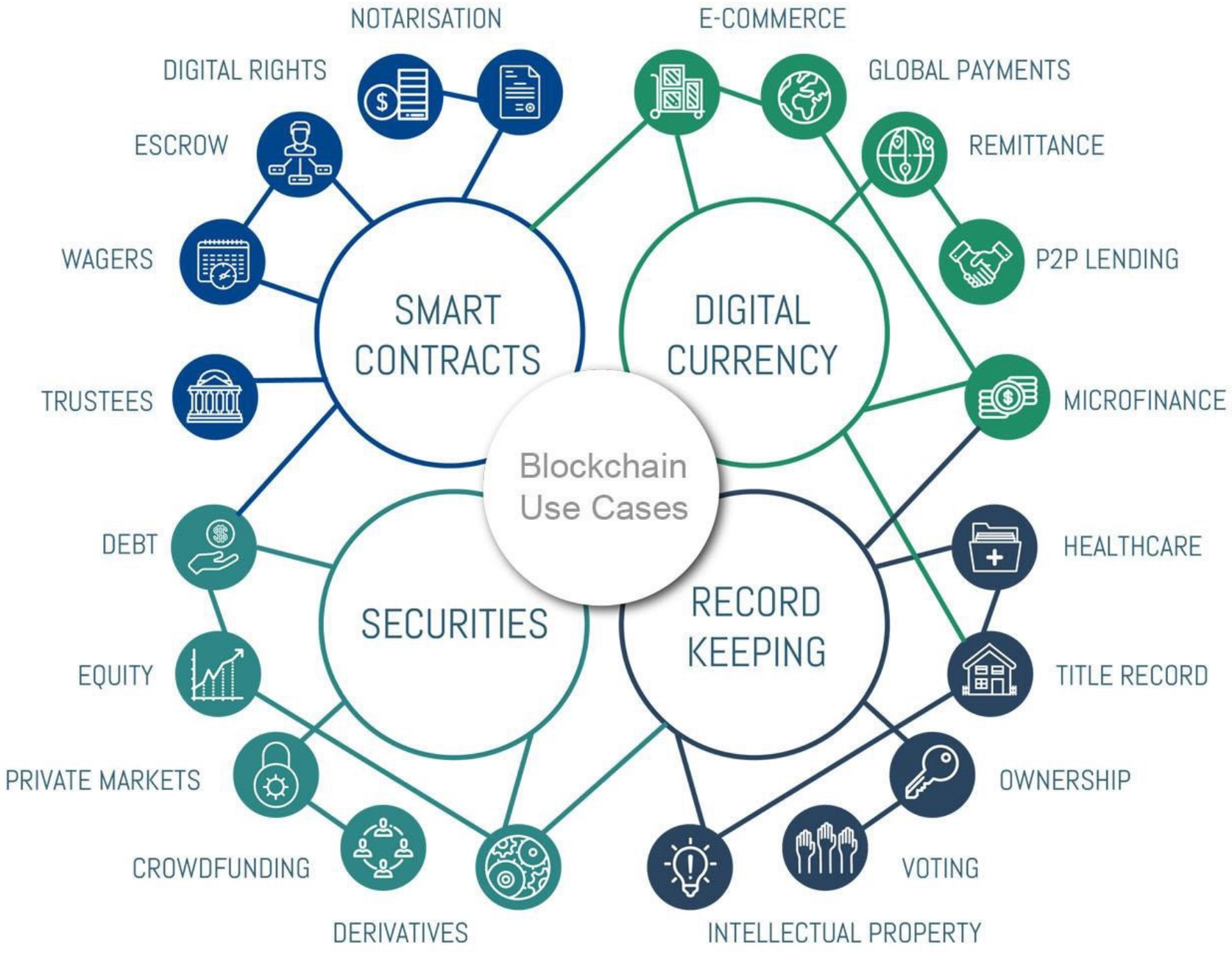


Your apple (still fresh)

Your friend



Domains of application



RMod

50+ BLOCKCHAIN
REAL WORLD USES CASES

GOVERNMENT
Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION
Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

uport

MOBILE PAYMENTS
The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

INSURANCE
A smart contract-based blockchain is being used by Insurer **American International Group Inc** as a means of saving costs and increasing transparency.

AIG

ENDANGERED SPECIES PROTECTION
The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS
IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

IBM HYPERLEDGER

ENTERPRISE
Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**

Microsoft Azure

BORDER CONTROL
Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS
IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

IBM Walmart

HEALTHCARE
A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

MEDREC

SHIPPING
Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

MÆRSK

REAL ESTATE
Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy**.

PROPY

ENERGY
Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY
Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

NATIONAL AGENCY of PUBLIC REGISTRY

COMPUTATION
Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

DIGITAL CURRENCY GROUP

ADVERTISING
New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

NYIAX

BORDER CONTROL
Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM
Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

CIVIL

WASTE MANAGEMENT
Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY
Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

LDC. Louis Dreyfus Company

DIAMONDS
The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

DE BEERS GROUP OF COMPANIES

FINE ART
By storing **certificates** of authenticity on the blockchain, it's possible to dramatically reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY
For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM
In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION
In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY
Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

CNE COMISIÓN NACIONAL DE ENERGÍA

RAILWAYS
Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock

ДРУЗОВАЯ КОМПАНИЯ НОВОТРАНС

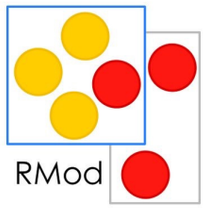
ENTERPRISE
Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

Google Alphabet

MUSIC
Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

arbit

FISHING
Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.



Blockchain

Basic structure

accounts

pablo (#234indp)
guille (#114cabj)
esteban (#24cabj)

RMod

Blockchain

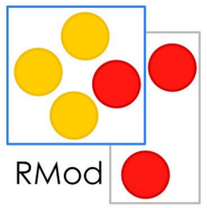
Basic structure

Transactions

#ID	from	to	$
#345..	pablo	guille	200
#425..	guille	pablo	220
#115..	esteban	pablo	100

inventeurs du monde numérique

50 ANS 1967 › 2017 ›› 2067 Imaginons notre futur



Blockchain

Basic structure

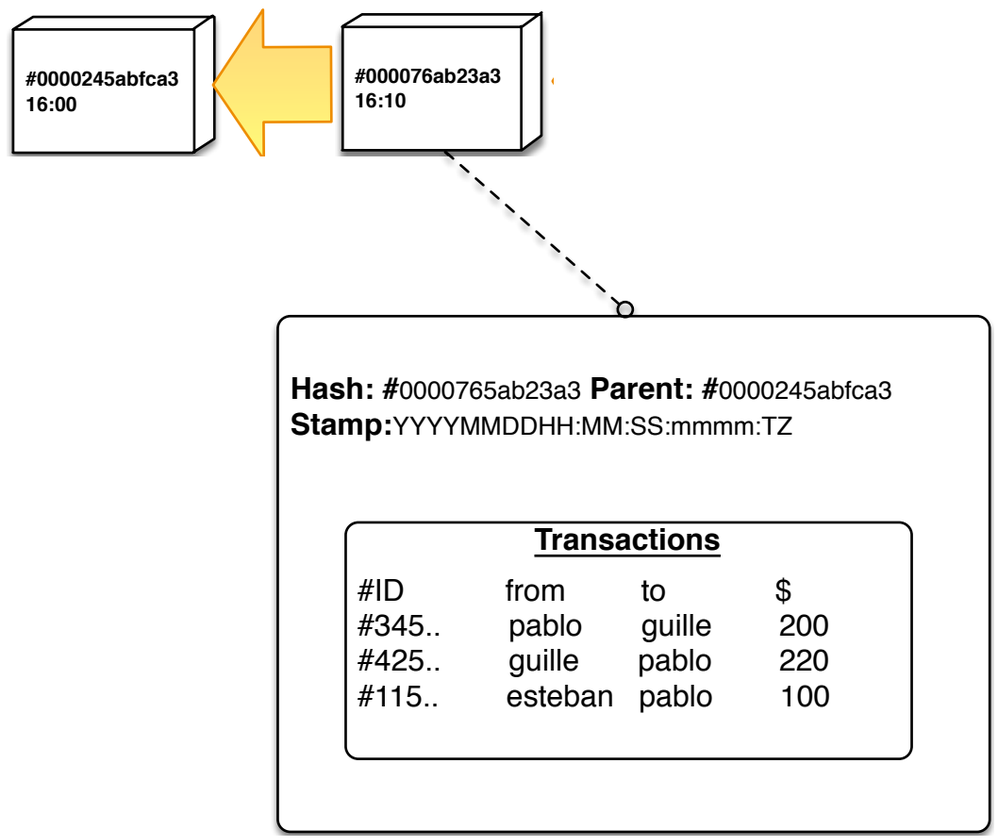
Hash: #0000765ab23a3 **Parent:** #0000245abfca3
Stamp:YYYYMMDDHH:MM:SS:mmmm:TZ

Transactions

#ID	from	to	$
#345..	pablo	guille	200
#425..	guille	pablo	220
#115..	esteban	pablo	100

Blockchain

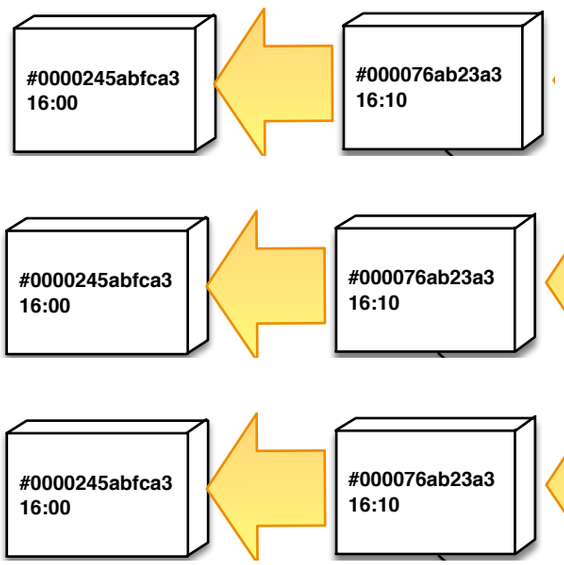
Basic structure



RMod

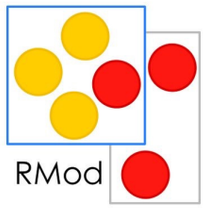
Blockchain

Basic structure



inventeurs du monde numérique

50 ANS 1967 › 2017 › 2067 Imaginons notre futur



Smart contracts

- A contract is a remote object
  - It reinforces rules
  - It means to automise the impact of it application
  - It allows to give different semantic to transactions

RMod

Example

A sale (specially obvious online) is a contract in between two parts.
How do I sell an item online?

Example

Create an account in:





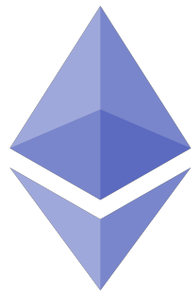

Publish your product

send your product

receive your money

Example

Create an account in:

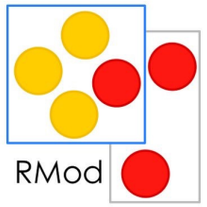


Publish a contract for the sale

promote your item

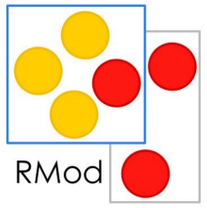
send the product

receive your money



Ethereum

- Blockchain based technology
- Open source & public network
- Smart contracts
  - State stored in a blockchain
  - Byte-code executed in the turing complete EVM
  - Many development languages (solidity, serpent, etc)



Smart contracts

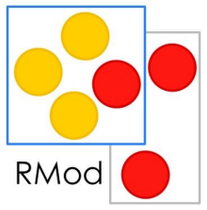
- A contract is a remote program

```
contract Sell {

    enum State { ON_SALE, WAITING_SEND, SENT, FINISH }

    address _owner;
    address buyer;
    uint payed;
    uint price;

    State state;

    constructor () public {
        _owner = msg.sender;
          state = State.ON_SALE;
    }

    function buy() payable public {
        if (state == State.ON_SALE) { return ; }
        if( price != msg.value ) revert();
        state = State.WAITING_SEND;
        payed = msg.value;
        buyer = msg.sender;
    }

    function informItemReceived  () public {
        if ( buyer == msg.sender && state == State.WAITING_SEND ) {
            state = State.SENT;
        }
    }

    function withdrawMoneyTo  (address toAddress) public{
        if ( _owner == msg.sender && state == State.SENT) {
            toAddress.transfer(price);
            state = State.FINISH;
        }
    }
}
```

Smart contracts

- Reinforce rules

```
contract Sell {

    enum State { ON_SALE, WAITING_SEND, SENT, FINISH }

    address _owner;
    address buyer;
    uint payed;
    uint price;

    State state;

    constructor () public {
        _owner = msg.sender;
          state = State.ON_SALE;
    }

    function buy() payable public {
        if (state == State.ON_SALE) { return ; }
        if( price != msg.value ) revert();
        state = State.WAITING_SEND;
        payed = msg.value;
        buyer = msg.sender;
    }

    function informItemReceived  () public {
        if ( buyer == msg.sender && state == State.WAITING_SEND ) {
            state = State.SENT;
        }
    }

    function withdrawMoneyTo  (address toAddress) public{
        if ( _owner == msg.sender && state == State.SENT) {
            toAddress.transfer(price);
            state = State.FINISH;
        }
    }
}
```



Fog DEMO

https://github.com/smartshackle/Fog

What are the Challenges on Fog?

Ethereum

- Highly immature documentation
- Language definition still mutating
- Deployed contracts are pieces of byte code with no reference to original “class”
- Contracts have only a very low-level API for data access and method invocation
- Contract inspection can help developer & companies

Fog

- Connection to GETH
- SmaCC solidity parser
- Type marshalling
- Object reification
- Pluggable remote mirror for contracts
- Contracts Proxy generator
- Keccak crypto algorithm implementation (32 bits only so far)
- Clear API

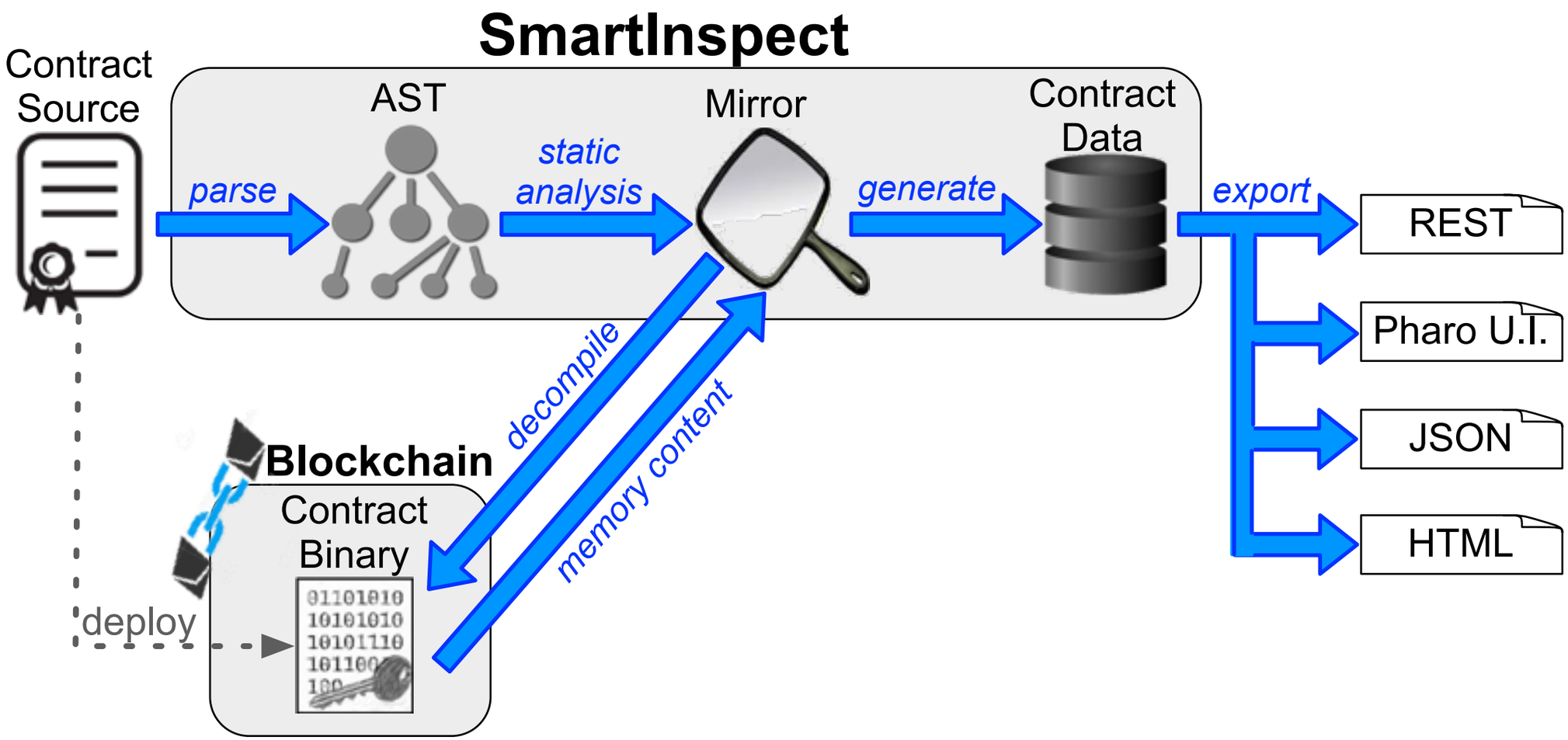
Fog includes a Contract Inspector

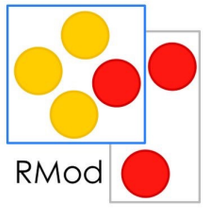
[SmartInspect, IWBOSE/SANER 2018]

- Deployed Smart Contracts are opaque
- Debugging contracts is very tedious and time-consuming.
- Contract inspection can help developer & companies

Fog includes a Contract Inspector

[SmartInspect, IWBOSE/SANER 2018]





Once we started having contracts, we find new needs

Need

Where is the contract of the pen I sold last week?

It is my application using my ethereum account as I expect?

RMod

Solution (?)

Lets navigate the blockchain!

inventeurs du monde numérique

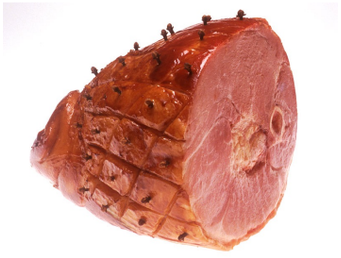
50 ANS 1967 › 2017 ›› 2067 Imaginons notre futur

Ethereum

- Hash Access Memory (HAM)
- Massive data
- Data opaqueness
- Lowlevel API for access to the important content

RMod

HAM



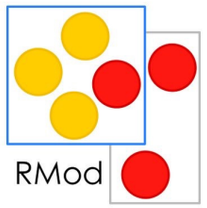
Hash access memory
(or god save the hash)

Objects are only accessed by hash

- Secondary database mixed with remote hashes
  - redundant contract related data
  - security exploit point

inventeurs du monde numérique

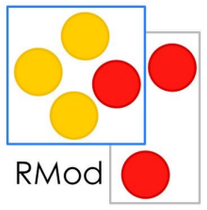
50 ANS
1967 › 2017 ›› 2067
Imaginons notre futur



Massive data

Looking for a hash in a blockchain (or a needle in a haystack)

- Blockchain is always-growing-db
- Ethereum has 856k transactions per day
  - Older information get overwhelmed in time

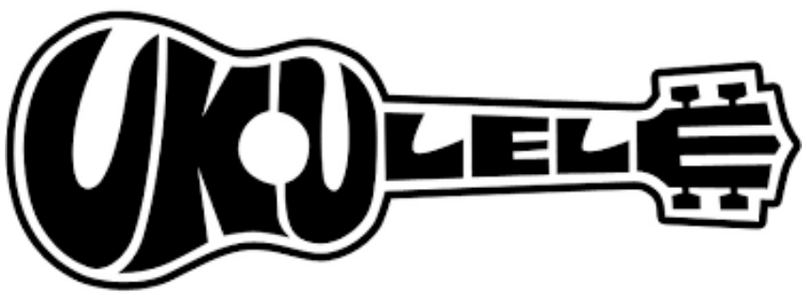


Data opaqueness

- Semantic abstract data structure
- the smart contracts storage is related with arbitrary hashes on the code structure
- no meta-data is stored within the smart contract

RMod

[EQL, ICSE2018]



DEMO

inventeurs du monde numérique

50 ANS
1967 | 2017 ›› 2067
Imaginons notre futur

Challenges

- UQLL is SmaCC interpreted SQL like language for querying Ethereum
- UQLL indexes have two flavours
  - Memory
  - Index
- UQLL allows the creation of arbitrary indexes
- UQLL allows the querying of existing contracts
- UQLL allows the creation of arbitrary environments
- UQLL allows the creation of views over data

RMod

UQLL

The language implementation

UQLL Runtime

UQLL Parser

UQLL Interpreter

UQLL Stream

UQLL Namespace

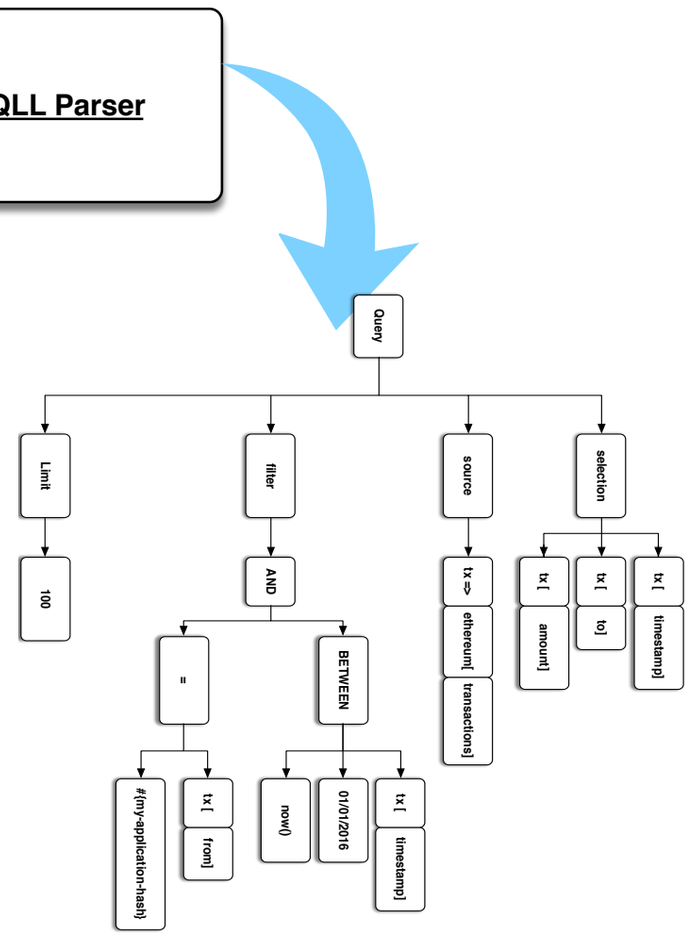
Fog Schema (ethereum)

Collections	**Blocks**	**Tx**	**Contract**	**etc**
Indexes	**Timestamp => Block Hash**			**etc**
Cache	**Previously fetched objects**			

Parsing

```
SELECT   tx.timestamp, tx.to, tx.amount
FROM     ethereum.transactions AS tx
WHERE    tx.timestamp
         BETWEEN date('2016-01-01) AND now()
         AND tx.from = #{my-application-hash}
LIMIT    100;
```

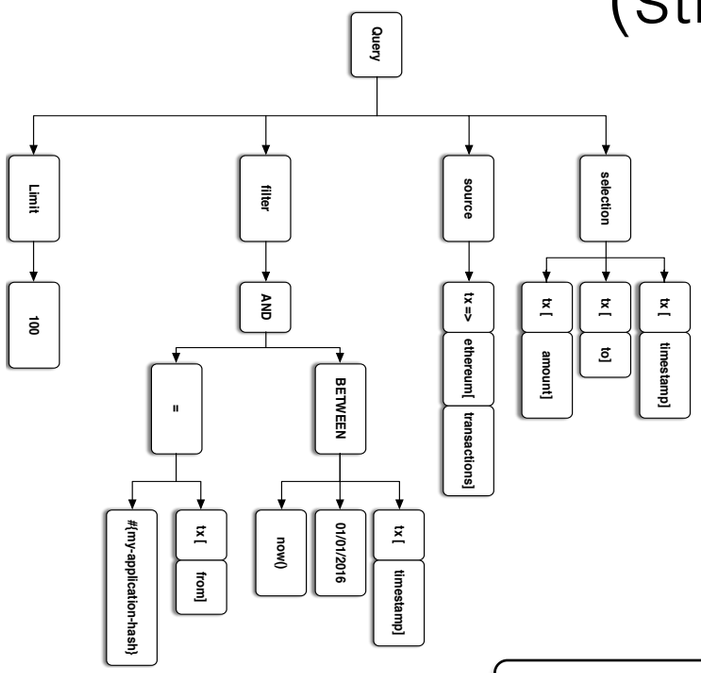
UQLL Parser

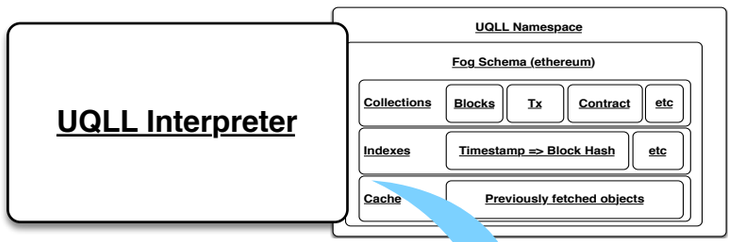


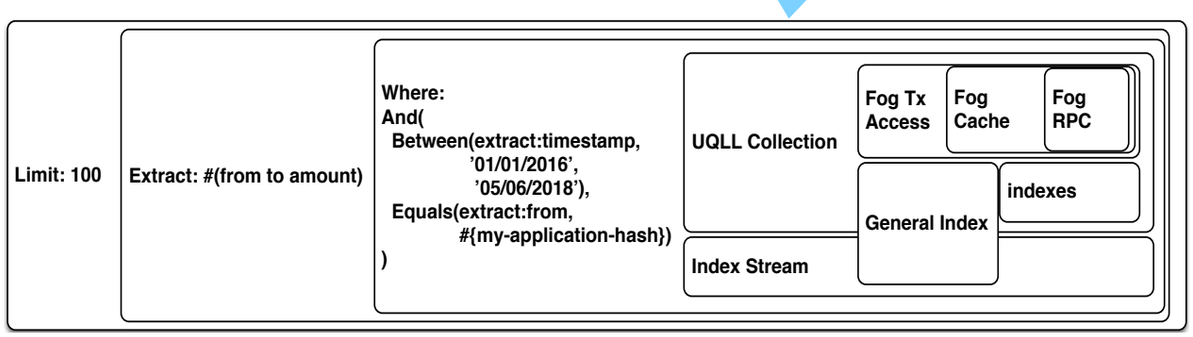
RMod

Interpretation

(stream compile)





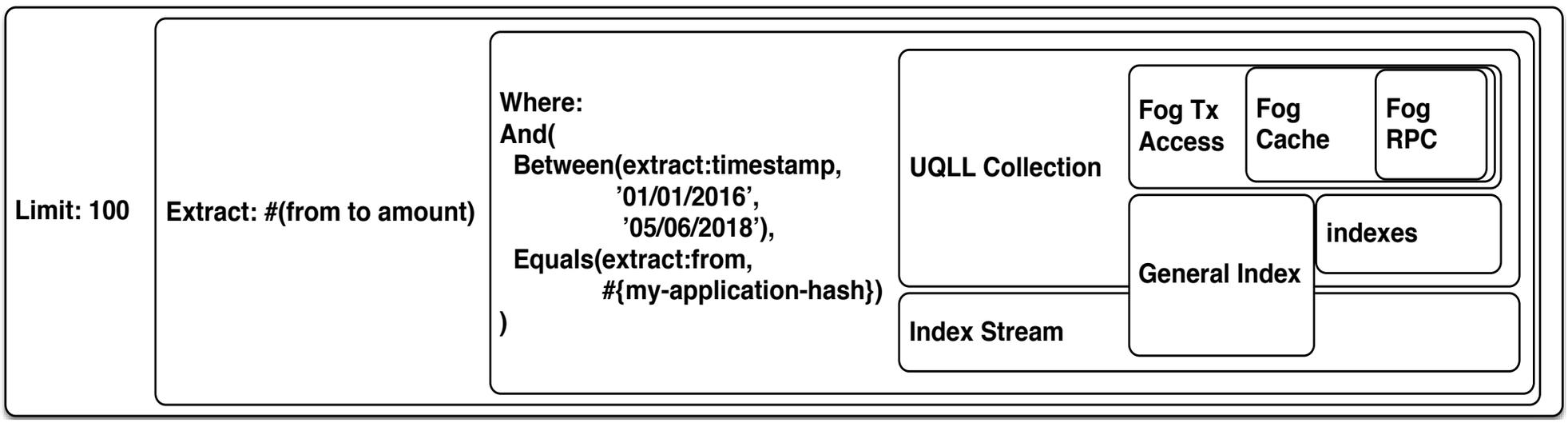


Inria inventeurs du monde numérique

50 ANS 1967 › 2017 ›› 2067 Imaginons notre futur

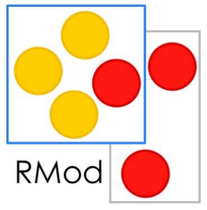
Stream

(ready to use :))



Available clauses so far

- CREATE SCHEME
- CREATE INDEX
- CREAT COLLECTION
- SELECT FROM WHERE
- ORDER BY
- LIMIT



So, now that we have now a nice known query language we need a nice way to visualise

Enma's Anvil Analyser

an anvil for hammering the chain

- Visualise transactions, blocks and contracts as tables

- Interact by clicking and scripting with the tracked values

RMod

DEMO

inventeurs du monde numérique

1967 / 2017 ›› 2067 Imaginons notre futur

Fog Future

- Documentation
- Implement a canonical example system
- Add more tests and benchmarks on top of large database of contracts
- Keep up with the sintaxis changes in solidity
- Reverse engineer the data in transactions

Ukulele Future

- Real implementation of order by
- Group by, Aggregation functions
- Joins
- Migrating the indexation process to map/reduce (Matteo Marra)
- Permanent-Indexation
- Adding new Schemes: Hyperledger fabric, mongoDB, RDBMS

Enma Future

- Stabilise and formalise the underlying architecture
- Implement a simple DSL (or nice pharo API) for plotting blockchain data
- Allow scripting to plots and plots to scripts for automating reports

Vision future

- Integrate other related projects
- Moose model
- Metrics extensions -
  Work done with UNICA.