MakoLab

Digital Solutions company with strong R&D activity

MakoLab UK MakoLab USA

For Blockspaces – February 2019

GraphChain presented to Tampa
Blockspaces Community
Thursday, Feb 21, 2019

MakoLab

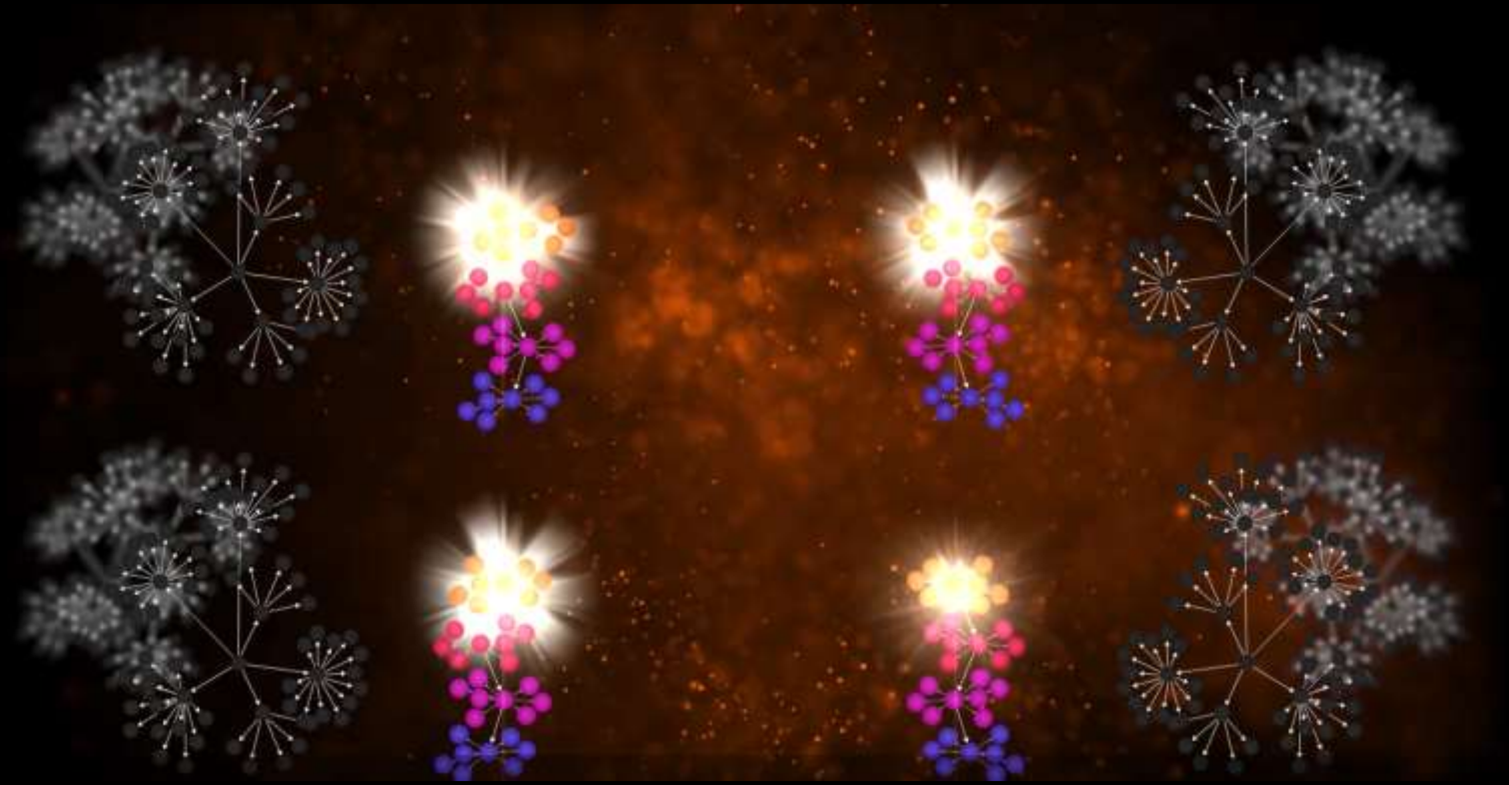
MakoLab

5

OFFICES

MakoLab

GraphChain



MakoLab

The Motivation

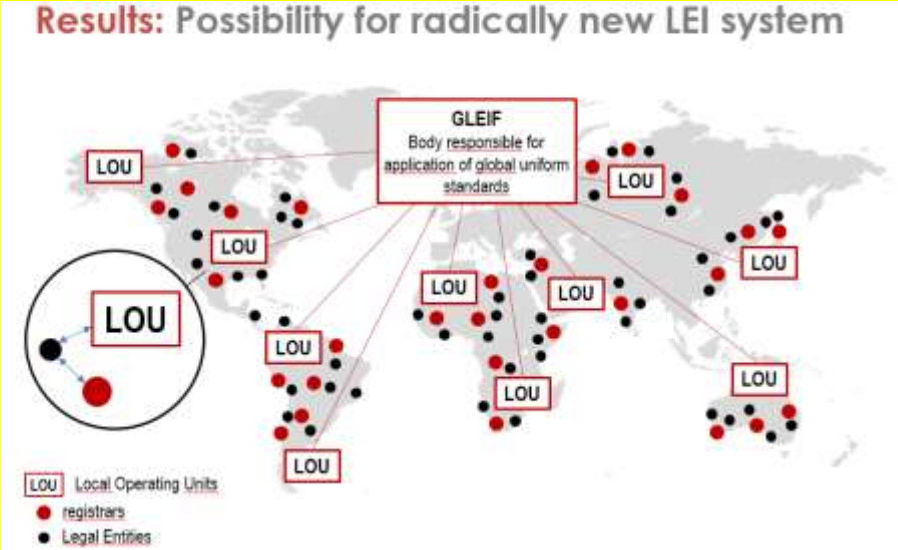
Why did we invent GraphChain?

Digital Identification systems need not just Blockchain.

They need GraphChain.

Standard digital ID systems shortcomings ...

- Lack of **explicit data semantics**
- While **many systems are distributed in nature**, the technology used to support them is of **old style and inherently unsecured**
- So, using LEI.INFO as the starting point, we have created a concept of **Blockchained LEI system** and we have made a number of POCs demonstrating its usefulness.



WHY **GraphChain?**

However, despite our efforts ...

- It was very hard to combine the three features the Digital ID systems required:
  - Explicit data semantics
  - Linked Open Data/SW data model and
  - Blockchain security model
- In our early Blockchain based POCs (using Ethereum), the extensibility of Legal Entity data was poor
- The queries across the entire LEI dataset were impossible or very hard

→ **What we really needed was a standard RDF Graph database protected by a Blockchain.**

Related works:

Marrying **Blockchain** to legacy **databases**

- **BigchainDB –** Blockchain database build using MongoDB

  „Rather than trying to enhance blockchain technology, BigchainDB starts with a big data distributed database and then adds Blockchain characteristics - decentralized control, immutability and the transfer of digital assets."
  (https://www.bigchaindb.com/features/)

- **MongoDB Blockchained** – is essentially the same development but from MongoDB perspective:

  "A blockchain-enabled MongoDB that wraps the core database (MongoDB) and implements the three blockchain characteristics of decentralization, immutability, and assets." ("Building Enterprise-Grade Blockchain Databases with MongoDB", A MongoDB White Paper)

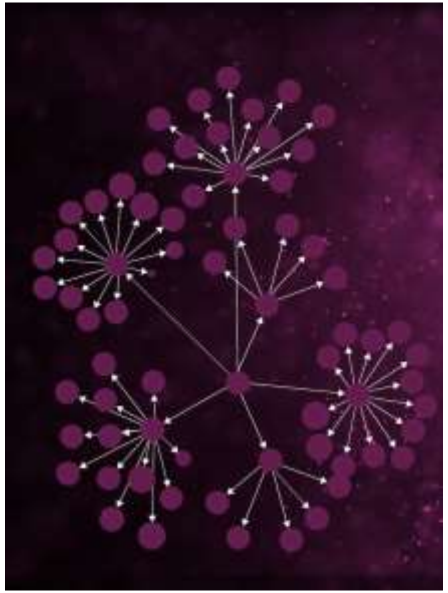
→**In both cases the essence is in the ability of the distributed database to use legacy access methods (and guarantee Querying, good Scalability and Operationalizability)**

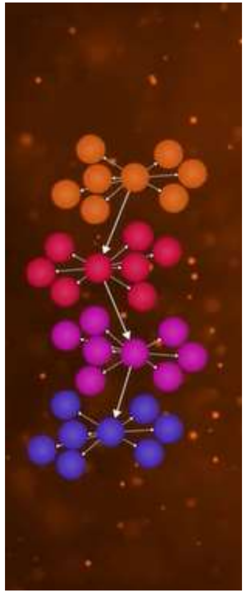
- An interesting extension of **Blockchain concept in IOTA's Tangle** (https://www.iota.org) – going away **from the sequence of blocks**
- Many Blockchains with consensus based on **DAGs** are coming close

The birth of GraphChain

Rather than trying to add Graphs and Ontologies to Blockchain, GraphChain starts with RDF database and then adds Blockchain features to the system.

GraphChain defined

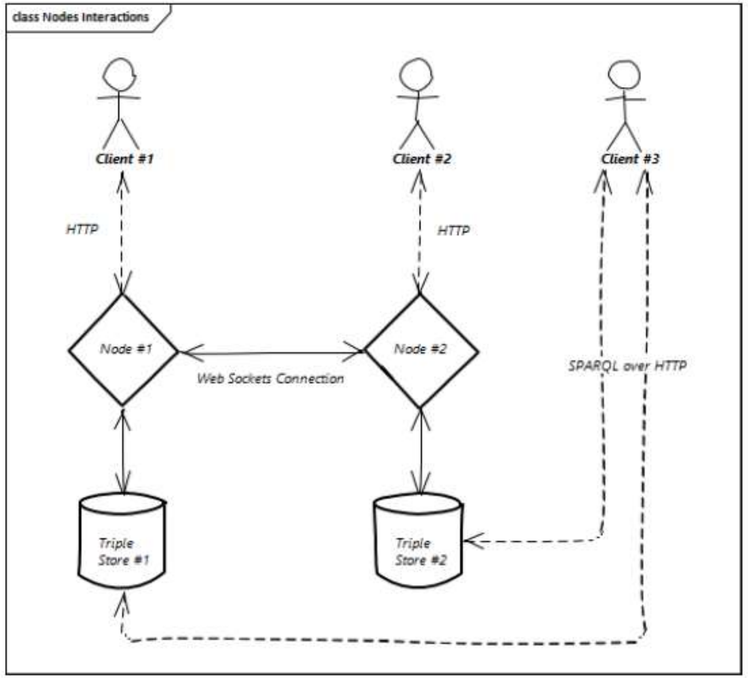




The main idea behind GraphChain is to use Blockchain mechanisms on top of an abstract RDF graph data model.

- An RDF graph is an unordered set of triples (atoms of data of the shape: object→property→value) and a named RDF graph is an RDF graph which is assigned a name in the form of a URI
- GraphChain is thus defined as:
  - A linked chain of named RDF graphs specified by the GraphChain ontology and an ontology for data graph part of the GraphChain.
  - A set of general mechanisms for calculating a digest of the named RDF graphs.
  - A set of network mechanisms that are responsible for the distribution of the named RDF graphs among the distributed peers and the for achieving the consensus.

The GraphChain **Architecture**



A single node perspective

- A single node of the GraphChain consists of several parts:
  - a web interface for communication with clients (via the HTTP protocol),
  - a web socket endpoint for communication with others nodes,
  - a cryptography module for handling of digest calculation,
  - a triple store repository manager for storing blocks as sets of triples and obtaining blocks from the repository,
  - and services which bind all these parts together.

The **artistic visualization** of the GraphChain

https://youtu.be/1D9jFjh4Y1g

MakoLab

The implementation challenges

The implementation of GraphChain brings a number of challenges that must be addressed before production-grade alternative to the existing Blockchain implementations is offered.

MakoLab

The implementation **challenges**

The most important challenges

- Performance of the programmatic access to RDF graphs.
- Performance and quality of the RDF graphs serialization used for the broadcast of the named graphs to other nodes.
- **Computation of the RDF digests.**

The computation of the **RDF digests**

The proposed solutions

- "Canonicalization" — calculation of the digest as the hash of the canonical graph serialization
- "DotHash" — calculation of the digest as the result of the combining operation on the hashes of the individual triples

$$\mathcal{D}(S) = \bigodot_{i=1}^{N} h(serialisation(t_i))$$

- **"Interwoven DotHash"** — calculation of the digest as the result of the combining operation on the hashes of the individual triples and the triples linked by blank nodes.

The GraphChain Ontology

The GraphChain ontology is an OWL ontology of the chained, named RDF graphs

MakoLab

An OWL ontology of chained

The Gra

Ontolog

ally

original

CIT

graphs, it

all data

```
@prefix owl: <http://www.w3.org/2002/07/owl#> .
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix xml: <http://www.w3.org/XML/1998/namespace> .
@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix gc: <http://ontologies.makolab.com/bc/> .

gc:b0 a gc:GenesisBlock ;
  gc:hasDataGraphIRI  "http://ontologies.makolab.com/bc"^^xsd:anyURI ;
  gc:hasDataHash "7dc25665a24a48dca4c89e9ba0fe053009d1dc85eaf1fd5c8f5126aa13e3c217" ;
  gc:hasHash "27f9ac0be5bd0fb1a84e74247cb6e5cbe9d49d1692e37a481d4710617cf871c6" ;
  gc:hasIndex "0"^^xsd:decimal ;
  gc:hasPreviousBlock gc:b0 ;
  gc:hasPreviousHash "0" ;
  gc:hasTimeStamp "1502269780"^^xsd:decimal .

gc:b1 a gc:Block ;
  gc:hasDataGraphIRI "http://makolab.com/foo"^^xsd:anyURI ;
  gc:hasDataHash "ea8ea1a9dade4880445bea3e7efe505276a3a0cf14b0fcddf4b5e105012d0edf" ;
  gc:hasHash "d50f6fa69a7ff6e1b6cb20ecf87dfff360190c1f9b4fc7ad7f3724bc17f85664" ;
  gc:hasIndex "1"^^xsd:decimal ;
  gc:hasPreviousBlock gc:b0;
  gc:hasPreviousHash "27f9ac0be5bd0fb1a84e74247cb6e5cbe9d49d1692e37a481d4710617cf871c6" ;
  gc:hasTimeStamp "1515745336"^^xsd:decimal .
```

The implementations

So far, GraphChain has three simple, exemplary implementations and one production grade (in progress)

Simple implementations of **the GraphChain**

https://github.com/MakoLab/GraphChain

- **.NET/C#**
  The C# implementation uses .NET Core platform. The node itself is an ASP.NET Core web application with REST API for a client - node communication and WebSocket layer for Peer to Peer transmission
- **Java**

  The Java implementation was created as a Spring-managed web application. It uses the RDF4J library for handling semantic-related operations. Can store RDF graphs in both the RDF4J triple store and the AllegroGraph triple store. Adding a new storage method is easy.
- **JavaScript/node.js**

  We have also developed a third, illustrative and simple implementation of the node: a JavaScript implementation which is based on Naivechain. It offers HTTP API and P2P communication between nodes. There are some differences between our implementation and Naivechain, though.

Web interface for the GraphChain

http://binsem.makolab.pl/indy/
http://binsem.makolab.pl/indy/GET_TXN/785

- Uses YasUI client (http://about.ayasgui.org)
- Allows for SPARQL querying both GraphChain ledger and data graphs
- Connects to multiple nodes of the GraphChain

Agent name	Blockchain				
	index	timestamp	dataGraphIri	previousHash	hash
	13	1524309684	http://lei.info/254900UIZS15MTA7H075	769a241332927f9beecf977fb9f591c419c07b4c8a23dfc5c26238cce933a923	3f9779a9d9ee808b52d8f7641
	12	1524306633	http://lei.info/52990060MW19AH86UT03	89414e59d625e571d696b5dc7f115d0e266870b1f4aeb5c15fc9b99e5209cb75	769a241332927f9beecf977fb
	11	1524142739	graph://lei.info/213600VBL21SHWTVFI73	31796c17e4fcdf145f6d8e126238d3ada54d8065263bdc22d7b80088972dbcc1	89414e59d625e571d696b5dc
	10	1524140812	http://lei.info/213800GP6ZQTAL4TTY44	543fb7879b05802e93cef00e90d9e95ecbcb514c5b6624cd9b5872b62b4acd90	31796c17e4fcdf145f6d8e126
	9	1520172216	http://lei.info/5493000C01ZX7D35SD85	96ae8ddb1751494b5ec0d16afa5ff5c61b1216b9cda8414a855ea112ff153df0	543fb7879b05802e93cef00e
	8	1520171734	http://lei.info/549300NCY2P2FLJT9D42	b8652eee7af392eb33d83230ba07b6c04a6f1c172392249acd703eebbd34a467	96ae8ddb1751494b5ec0d16a
binsem:8881/mammoth/	7	1519723889	http://lei.info/6SHGI4ZSSLCXXQSBB395	f5e9811aacf5575df4997ae0e1d58aa1acb2d64afbada4f8923f341d5ae4d7a3	b8652eee7af392eb33d83230
	6	1517398832	http://lei.info/PBLD0EJDB5FWOLXP3876	0f3af827baf5c02049ef5f58f92b94607ddf2c9ddb50b587c44c5ddebf228ba1	f5e9811aacf5575df4997ae0e
	5	1517395205	http://lei.info/8I5DZWZKVSZI1NUHU748	86acdb0d782134fceb63cfcc15c9e7a0802bdc6ab3bed46d064c6540dc8f91e4	0f3af827baf5c02049ef5f58f92
	4	1517395019	http://lei.info/F5WCUMTUM4RKZ1MAIE39	117232d272f0eacef9e31442257e3319fde98e0f77e0c14a86206fcf22b059af	86acdb0d782134fceb63cfcc1
	3	1516614502	http://lei.info/PBLD0EJDB5FWOLXP3876	0b5c8a81f892dc4c609303204e969dc603fc3e1a720e45f4119bf22776dd7983	117232d272f0eacef9e31442
	2	1516613042	http://lei.info/MLU0ZO3ML4LN2LL2TL39	3ecc0180a4d7a4a1a7af94f6d575a55a68fe45db975688453113109258 2c1f6a	0b5c8a81f892dc4c60930320
	1	1516379147	http://lei.info/2594007XIACKNMUAW223	f4e5f8d34e03c109ae98f6a57cf36fcd6bcf028e1a8362006c1d3bb1500a9c06	3ecc0180a4d7a4a1a7af94f8c
	0	1502269780	http://www.ontologies.makolab.com/bc	0	f4e5f8d34e03c109ae98f6a57

Product
impleme
GraphC

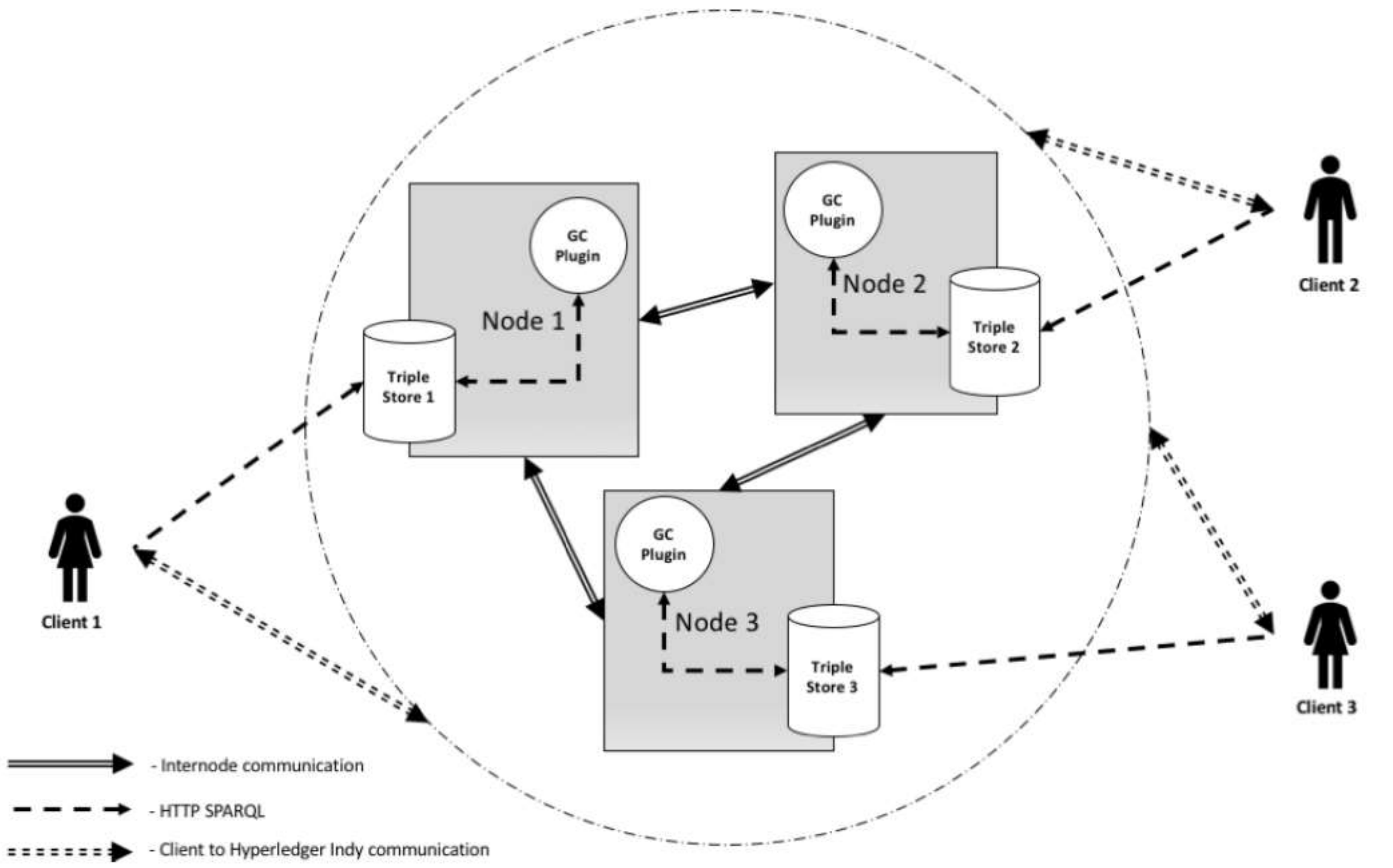


Fig. 4. The architecture of Hyperledger Indy with Triple Store

ledger, purpose-

://sovrin.org/) for

ions
alf of 2018
ur POC on the use
ger Indy and are
m.

Production grade implementation of the GraphChain

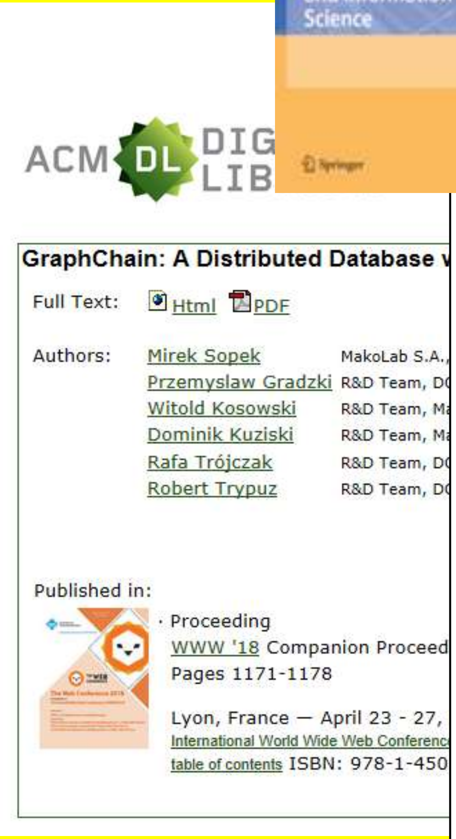
http://wisem.makolab.pl/leigc/

Validation OK:

http://wisem.makolab.pl/leigc/254900UIZS15MTA7H075

Validation KO:

http://wisem.makolab.pl/leigc/G30CO71KTT9JDYJESN22



ACM DL DIG LIB

GraphChain: A Distributed Database w

Full Text: Html PDF

Authors: Mirek Sopek MakoLab S.A.,
Przemyslaw Gradzki R&D Team, DC
Witold Kosowski R&D Team, Ma
Dominik Kuziski R&D Team, Ma
Rafa Trójczak R&D Team, DC
Robert Trypuz R&D Team, DC

Published in:
· Proceeding
WWW '18 Companion Proceed
Pages 1171-1178

Lyon, France — April 23 - 27,
International World Wide Web Conferenc
table of contents ISBN: 978-1-450

Legal Entity Identifier blockchained by a Hyperledger Indy implementation of GraphChain

Mirek Sopek[1], Przemysław Grądzki[1], Dominik Kuziński[1], Rafał Trójczak[1,2], and Robert Trypuz[1,2]

[1] R&D Team, MakoLab S.A.
ul. Demokratyczna 46
93-430 Łódź, Poland
sopek@makolab.com
[2] The John Paul II Catholic University of Lublin,
Faculty of Philosophy
Al. Racławickie 14,
20-950 Lublin, Poland

Abstract. The main idea behind GraphChain is to use blockchain mechanisms on top of an abstract RDF graphs. This paper presents an implementation of GraphChain in the Hyperledger Indy framework. The whole setting is shown to be applied to the RDF graphs containing information about Legal Entity Identifiers (LEIs).

Keywords: Hyperledger, Hyperledger Indy, GraphChain, semantic blockchain, LEI, GLEIS

1 Introduction

In this paper are presenting the idea and propose the implementation of Blockchain based data management system that could be used for the Global LEI system (GLEIS). The system preserves all the benefits of using RDF graph data model for the representation of LEI system reference data, including the powerful querying mechanisms, explicit semantics and data model extensibility with the security and non-repudiation of LEI as the digital identifiers for legal entities. To achieve such features we combined the solutions previously invented for the GraphChain[6] with one of the frameworks of the Hyperledger project, namely Hyperledger Indy.

The idea of combining blockchain technology with the Semantic Web principles has been proposed in [2,9,3]. An approach similar to the presented in this paper, albeit not for LEI system, can be found in [4], where Flex Ledger – a graph data model and a protocol for decentralised ledgers – was presented.

We will first introduce the basics of the Legal Entity Identifier (LEI) and the basics of GLEIS - Global LEI System and an ontology we have developed for the LEI system called GLEIO[8,]. Then, after short introduction to Blockchain technology we will explain the rationale of using Blockchain for LEI system and why the idea of GraphChain is important for the goals of our work. Finally, we will present how the use Hyperledger Indy helps to achieve the goals and present some implementation details behind the proposal.

The future of the GraphChain

MakoLab

Future applications of GraphChain

What's next ?

- P**erfecting the LEI.INFO** implementation
- Working towards GraphChain use for Global LEI system (**GLEIF**)
- Storage of LEGAL documents (working with **EU Commission on regulatory documents**) – adding ML to the GraphChain (http://ml.ms/fisma)
- Building infrastructure for **Electronic Lab Notebooks** (first PoC starts in March)
- Storing **business reports for regulatory purposes**

Quantum Blockchain

A very preliminary proposal

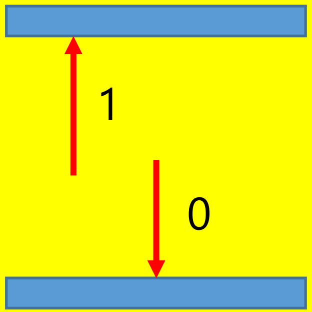
MakoLab

Quantum Computers …

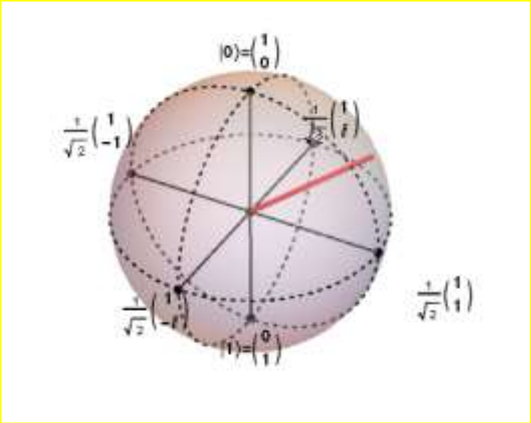
Quantum computer is a device that is using quantum-mechanical phenomena, such as superposition and entanglement.

Quantum computer is completely different from our common binary digital computers.

While common digital computer require that the data be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1), quantum computation uses quantum bits or qubits, which can be in a superposition of states.



Bit



Qubit

MakoLab

Quantum Computers …

IBM’s Q System One …

… still an experimental device, despite its polished looks.

"IT'S MORE LIKE A STEPPING STONE THAN A PRACTICAL QUANTUM COMPUTER."

MakoLab

Quantum Compute

DESIGNLINES | MCU DESIGNLINE

Is D-Wave a Quantum Computer?

Critics charge its not a "real" QC

By R. Colin Johnson, 05.14.15 9

Share Post Share on Facebook Share on Twitter in

PORTLAND, Ore.—Recently I had to explain to a reader why critics say that D-Wave's so-called quantum computer was not a "real" quantum computer, the answer for which he accepted on my authority. However, the question kept nagging me in the back on my mind "why" D-Wave markets what it calls a quantum computer if it is not for real. To get to the bottom of it, I asked Jeremy Hilton, vice president of processor development of D-Wave Systems, Inc. (Burnaby, British Columbia, Canada) about why critics keep saying its quantum computer is not for real. He also revealed details about D-Wave's next generation quantum computer.

MakoLab

Quantum Computers … and risk for Blockchain

MakoLab

MENU nature International journal of science

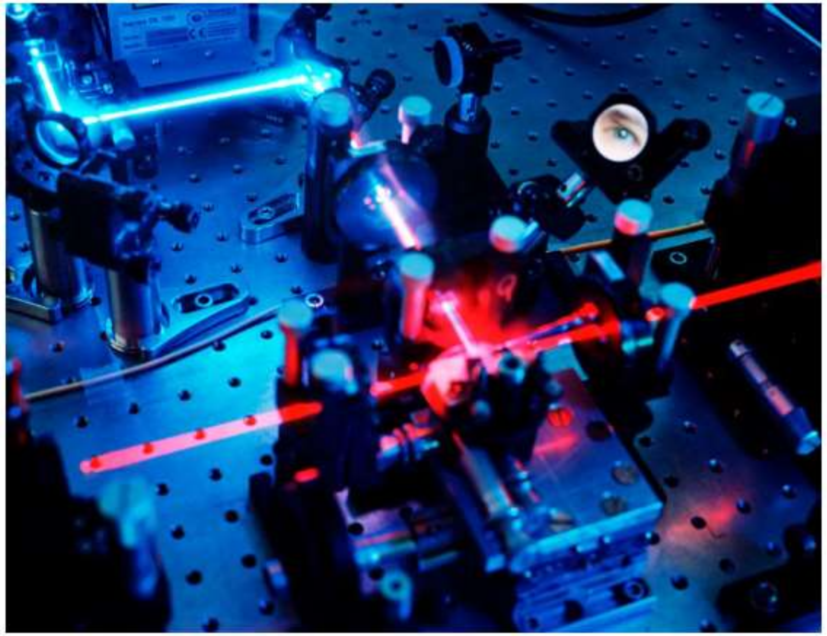
Search E-alert Submit Login

COMMENT · 19 NOVEMBER 2018

Quantum computers put blockchain security at risk

Bitcoin and other cryptocurrencies will founder unless they integrate quantum technologies, warn Aleksey K. Fedorov, Evgeniy O. Kiktenko and Alexander I. Lvovsky.

Aleksey K. Fedorov, Evgeniy O. Kiktenko & Alexander I. Lvovsky



PDF version

RELATED ARTICLES

The environment needs cryptogovernance

Here's what the quantum internet has in store

First quantum computers need smart software

Commercialize quantum technologies in five years

https://www.nature.com/articles/d41586-018-07449-z

The problem

- While the Blockchain technology is **currently secure** (within its own specific paradigm of security) it will no longer be secure when the **quantum computers become available**.
- Some of the foundational Blockchain technologies (like the **asymmetric cryptography**) can **almost certainly be broken.**

The existing solutions

MakoLab

The first natural solution to mitigate the risk posed by Quantum Computers is to use the upgraded cryptographic protocols from the family known as **POST QUANTUM CRYPOTOGRAPHY**

This was achieved by the company QRL and their product www.TheQRL.org which uses Quantum resistant algorithms (including XMSS) to deliver **Quantum Resistant Ledger**

Our work

Let's imagine PROVABLY SECURED Blockchain

MakoLab

Quantum Blockchain, a Simplified Framework (Extended Abstract)

Xin Sun[1,3], Mirek Sopek[2], Quanlong Wang[3], Piotr Kulicki[1], Robert Trypuz[1,2]

[1]*The John Paul II Catholic University of Lublin, Lublin, Poland*
[2]*MakoLab S A, Lodz, Poland*
[3]*University of Oxford, Oxford, UK*
xin.sun.logic@gmail.com

Abstract:
We develop Quantum Logical Ledger (QLL) as a simplified framework of quantum blockchain. We adopt a new scheme of quantum signature for transaction authentication and a simple vote-based consensus algorithm to achieve consensus on the blockchain. The cost of quantum resources is reduced in QLL compared to existing quantum blockchains. QLL is unconditional secure and can be realized by the current technology.

OCIS codes: 000.0000, 999.9999.

1. Introduction

A blockchain is a distributed ledger which enables achieving consensus in a large decentralized network of agents who do not trust each other. It is a ledger in the sense that data stored on a blockchain is transactions like "Alice sends 1 bitcoin to Bob". It is distributed in the sense that every miner (the agents who are in charge of updating the ledger) has a same copy of the database. One of the most prominent application of blockchain is cryptocurrencies, such as Bitcoin [1]. Another important application of blockchain is the implementation of self-executable smart contracts [2].

The power of quantum computers is a thread to most existing public key cryptographic systems. To react to the thread of quantum computers, Kiktenko *et al.* [3] developed quantum-secured blockchain (QB). Due to the application of quantum technologies, QB is more secure than classical blockchain in the sense that it is immune from attacks of quantum computers, while classical blockchain is not.

In QB [3], the authors use the classical Byzantine agreement protocol [4] to achieve consensus of the distributed ledger. They notice that a shortcoming of the classical Byzantine agreement protocol is that it becomes exponentially data-intensive if a large number of cheating agents are present. Therefore, further research on developing an efficient consensus protocol is required. This limitation of QB is fixed by our previous work [5]. In [5] we introduce a quantum honest-success Byzantine agreement (QHSB) protocol to replace the classical Byzantine agreement protocol in QB. While QHSB is scalable on the number of cheating agents, there is still room for improvement.

Quantum Information and Measurement, QIM 2019, Rome

Our work

Let’s imagine PROVABLY SECURED Blockchain

MakoLab

International Journal of Theoretical Physics
January 2019, Volume 58, Issue 1, pp 275–281 | Cite as

A Simple Voting Protocol on Quantum Blockchain

Authors | Authors and affiliations

Xin Sun, Quanlong Wang, Piotr Kulicki, Mirek Sopek

Open Access | Article
First Online: 18 October 2018

Abstract

Keywords

Electronic voting

International Journal of Theoretical Physics (2019) 58: 275–281
https://doi.org/10.1007/s10773-018-3929-6

CrossMark

A Simple Voting Protocol on Quantum Blockchain

Xin Sun[1] · Quanlong Wang[2] · Piotr Kulicki[1] · Mirek Sopek[3]

Received: 4 June 2018 / Accepted: 10 October 2018 / Published online: 18 October 2018

Abstract
This paper proposes a simple voting protocol based on Quantum Blockchain. Despite its simplicity, our protocol satisfies the most important properties of secure voting protocols: is anonymous, binding, non-reusable, verifiable, eligible, fair and self-tallying. The protocol could also be implemented using presently available technology.

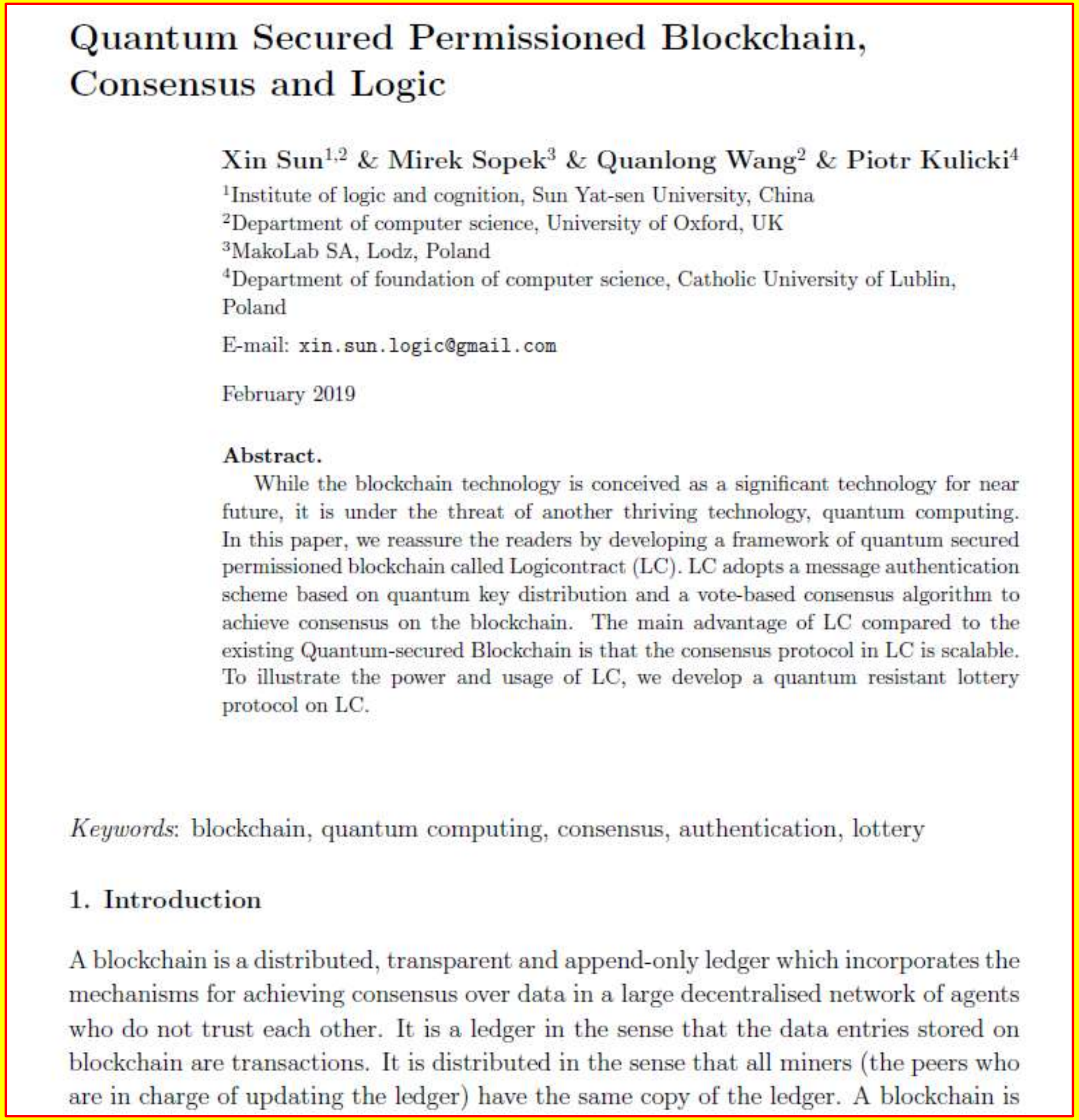
Keywords Electronic voting · Quantum computation · Blockchain

1 Introduction

Many voting protocols based on classical cryptography have been developed and successfully applied since Chaum et al. [9]. However, the security of protocols based on classical cryptography is based on the unproven complexity of some computational algorithms, such as the factoring of large numbers. The research in quantum computation shows that quantum computers are able to factor large numbers in a short time, which means that classical protocols based on such algorithms are already insecure. To react to the risk posed by forthcoming quantum computers, a number of quantum voting protocols have been developed in the last decade [3, 15, 16, 18, 24, 25, 38, 40, 41, 43].

Our work

Let's imagine PROVABLY SECURED Blockchain



Quantum Secured Permissioned Blockchain, Consensus and Logic

Xin Sun[1,2] & Mirek Sopek[3] & Quanlong Wang[2] & Piotr Kulicki[4]

[1]Institute of logic and cognition, Sun Yat-sen University, China
[2]Department of computer science, University of Oxford, UK
[3]MakoLab SA, Lodz, Poland
[4]Department of foundation of computer science, Catholic University of Lublin, Poland

E-mail: `xin.sun.logic@gmail.com`

February 2019

Abstract.
While the blockchain technology is conceived as a significant technology for near future, it is under the threat of another thriving technology, quantum computing. In this paper, we reassure the readers by developing a framework of quantum secured permissioned blockchain called Logicontract (LC). LC adopts a message authentication scheme based on quantum key distribution and a vote-based consensus algorithm to achieve consensus on the blockchain. The main advantage of LC compared to the existing Quantum-secured Blockchain is that the consensus protocol in LC is scalable. To illustrate the power and usage of LC, we develop a quantum resistant lottery protocol on LC.

Keywords: blockchain, quantum computing, consensus, authentication, lottery

1. Introduction

A blockchain is a distributed, transparent and append-only ledger which incorporates the mechanisms for achieving consensus over data in a large decentralised network of agents who do not trust each other. It is a ledger in the sense that the data entries stored on blockchain are transactions. It is distributed in the sense that all miners (the peers who are in charge of updating the ledger) have the same copy of the ledger. A blockchain is

Third Symposium on Compositional Structures (SYCO 3)
University of Oxford, 2019

MakoLab

Planned PoC

MakoLab

Beyond scientific and R&D context

Together with the aforementioned authors we are now building purely theoretical ground for the first Proof-Of-Concept for the Quantum Blockchain.

It assumes the use of EXISTING and commercially available QKD (Quantum Key Distribution) infrastructure to build the POC.

The essence of the POC

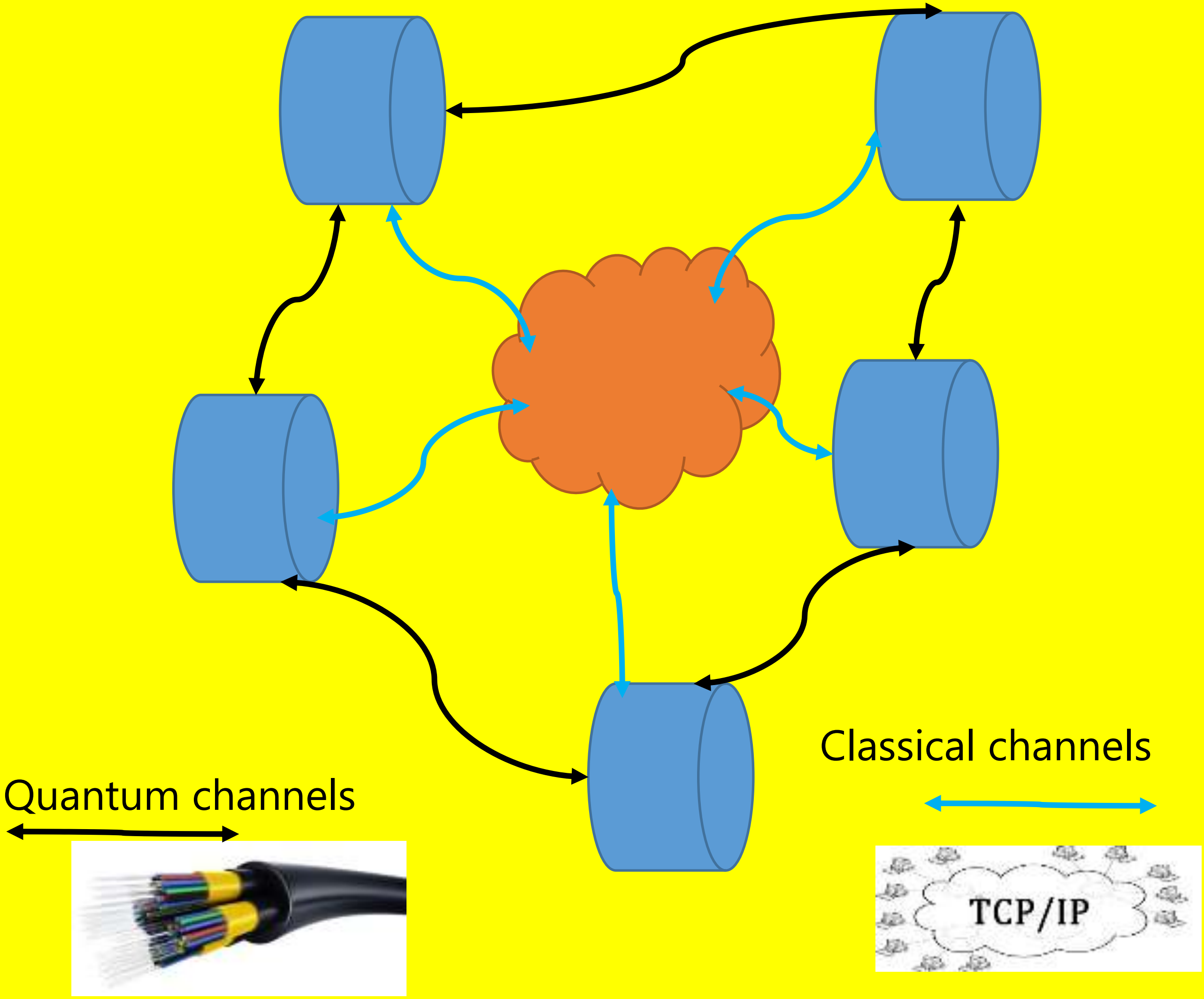
Beyond scientific and R&D context

Use QKD devices like ID-Quantique Clavis3 and/or Cerberis QKD Blade

Create dark-fiber based network between nodes.

Use the devices and the network for the highly secure communication between nodes.

The POC will create the hybrid model: the secure communication will assume the use of QKD devices and dark-fiber connections and standard peer-to-peer network over the clouds or public networks.



MakoLab

The current range of applicability

Because of the need to use dark-fiber connections between nodes, Quantum Blockchain can be best delivered for nodes located in **close geographical locations, e.g. banks in specific financial centers.**

This limitation will be lifted in the coming years when satellite based QKD channels become available.

There are also plans to run QKD over **FTTx (e.g. FTTO,FTTH) networks.**

This makes our idea even more realistic…

Contact us

MIREK SOPEK
PRESIDENT

sopek@makolab.com
+1 551 226 5488

MakoLab

Thank you!