A Blockchain Based Architecture for Fulfilling the Needs of an E-Procurement Platform

Tahereh Nodehi[1], Aneesh Zutshi[2], Antonio Grilo[3]
UNIDEMI, Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa
Lisbon, Portugal
[1]t.nodehi@fct.unl.pt, [2]aneesh@fct.unl.pt, [3]acbg@fct.unl.pt

Abstract

E-Procurement platforms have emerged as the primary source of procurement procedure for large organizations, whether Public or Private, and thus form a principal driver for the economy. Since many vendors bid for procurement procedures, often for publicly managed funds, it is extremely vital that full transparency and accountability is ensured in the entire process. Ensuring that certain digital certification functions, such as timestamps are independent from e-procurements Platform Owners has been a challenge. Blockchain Technology has emerged as a promising solution for not only ensuring transparency and immutability of records, but also providing for interoperability across different platforms by acting as a trusted third-party. This paper identifies some of the core needs of an e-procurement platform that could be fulfilled by Blockchain Technology. Further it presents a Hyperledger based blockchain solution with some of the key architectural elements that could fulfil these needs while presenting the advantages of such a solution.

Keywords: e-Procurement Platform, Blockchain Technology, Hyperledger Fabric, Permissioned Network

1. Introduction

Online procurement has been established as one of the most important aspect of e-business operational excellence for companies (Mehrbod *et al.*, 2015). E-procurement platforms have made the bidding process easier, quicker, and more cost efficient by streamlining the procurement process. Most large companies and public entities use these commercial e-procurement platforms to manage their procurement procedures since these platforms are designed to fulfil bidding requirements of the procuring organizations (Baldus and Hatton, 2020). This translates to more business opportunities for suppliers, vendors and the organizations that are requesting these bids (Bag *et al.*, 2020). Due to the fact that E-procurement Platforms manage the interests of multiple stakeholders, and critical data that could determine the fairness of many of the bidding procedures, it is vital that the platforms not only maintain transparency but are seen to be completely transparent and impartial. That is why Digital Platforms are governed by many regulations, and interface with independent third-party agencies for issuing Digital Certifications and Timestamps for recording and validation of the bids. Also, many of the digital platforms are exploring cross platform interoperability where sellers on one platform are able to bid for procurement procedures in another platform (Zutshi and Grilo, 2019). This fulfils a key objective of cross border trade within the European Union and was the basis of some of the EU Projects like Interplat. Such cross border cross platform interactions require an even greater level of trust and transparency (Grilo *et al.*, 2017)(Nodehi *et al.*, 2015)(Jardim-Goncalves *et al.*, 2013).

With the emergence of the Blockchain Technology, there is a big opportunity for e-procurement platforms, to address many aspects for making their platforms more transparent and trustable. Blockchain is a decentralised ledger that can act as a trusted third party without being in the control and supervision of any one entity. This unique aspect of the technology makes it applicable for solving multiple issues faced by the E-Procurement Platforms. Many of the existing functions performed by third parties like issuance of time stamps, digital certificates can be effectively and cheaply performed over a Blockchain platform, while it can add new benefits such as immutability of events, identity management, and bring interoperability while acting as a trusted third party. In a blockchain based system, a verifiable copy of the ledger is stored across multiple nodes held by more than one entity (eg. Different Platform owners, Larger Clients, Public Bodies, Independent Certification Agencies) thus ensuring data immutability, and a greater trust in the stored records.

To present a Blockchain based architecture catering to the needs of an e-Procurement Platform, we worked very closely with the Vortal e-Procurement Platform to analyse its business needs while proposing the Blockchain Solution.

Vortal (https://vortal.biz) is the largest e-Procurement platform in Portugal and one of the major players in Europe and was a part of the Interplat EU Project for inter-platform Interoperability (Zutshi, Grilo, *et al.*, 2018). This paper identifies some of the core needs of an e-procurement platform that could be fulfilled by Blockchain Technology. Further it presents a Hyperledger based blockchain solution with some of the key architectural elements that could fulfil these needs while presenting the advantages of such a solution.

2. Defining the Business Requirements of an e-Procurement Platform

To characterise the functions of a Blockchain Based architecture, it is important to define the key processes within an e-Procurement platform. Some of the principal functions are shown in Figure 1. The Buyers create the tender procedure and send invitation to Sellers to bid for the tender. Subsequently the sellers prepare proposals and receive receipts for their bids. Following this, the buyers compare the bids and evaluate the proposals. Following the award, the contracts are signed by both the parties. Calls for tenders, requests for proposals and blind auctions are prevalent and essential procedures (Zutshi, Mota, *et al.*, 2018). However, the e-procurement platforms are still vulnerable to fraud and corruption (Dávid-Barrett and Fazekas, 2020). With blockchain technology, many of risks can be eliminated and the maximum transparency level of bidding processes can be achieved.

The platform requires mechanisms to ensure there won't be information leak to any bidders allowing them to outbid competitors using this inside information (Mehrbod *et al.*, 2017). Currently, third parties sell timestamps or trusted software solutions are utilized to secure the process. Third party timestamps are a guarantee of the bid that is recorded by the platform as well as the exact moment in which it took place. Blockchain technology is a new paradigm that can change the way of interaction with different stakeholders and institutions. Blockchain enables trust to be achieved through cryptography and remove the dependence on participant integrity from one side and third-party organisations from another side. It can automate and govern transactions and bring transparency as well as privacy for various members. The “block” is the key element of a blockchain that can immutably store any value representative of any set of data including the time of creation of a message. Moreover, this technology can provide a solution to guarantee auditability and cost-effectiveness without the need for third parties.

Stakeholder		Process Steps
Buyers	1	Create the Tender procedure and invitation to Tender
Buyers	2	Publicise the Tender (including Contract Notice and Documents)
Suppliers	3	Prepare Proposals and receive online Submissions with Receipts
Buyers	4	Compare Bids automatically and evaluate Proposals
Buyers and Suppliers	5	Hold an e-Auction
Suppliers	6	Award Bid, create Contract and send Notifications
Suppliers	7	Creation of the Contract
Buyers and Suppliers	8	Digitally sign the Contract

Figure 1. e-Procurement Process (Source: Vortal platform).

3. Selection of the Appropriate Blockchain Technology for e-Procurement Platform

3.1. Key advantages of Using Blockchain Technology

In the blockchain context, **smart contract** is a computer code with responsibility of reading and updating the ledger (Zheng *et al.*, 2020). A smart contract is set based on business logic which is like a self-operating computer program that automatically executes when certain conditions are met. Blockchain technology has applicability in the situations where the following characteristics are required:

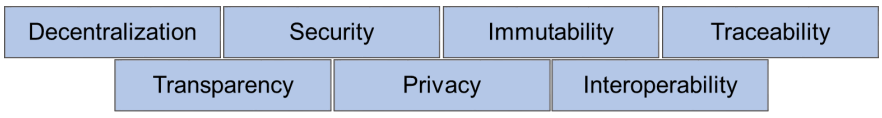

Figure 2. Key characteristics of blockchain technology (Nodehi *et al.*, 2018).

a. **Decentralization:** Blockchain is a public ledger of all transactions on the network which is maintained by different decentralized nodes. There is no need for a trusted third party or intermediary for interacting with each other to validate transactions; instead, a consensus mechanism is used to agree on the validity of transactions. It means technology provides distributed trust among different actors in the system.

b. **Transparency:** In the blockchain network, all data are shared, and everyone can see what is on the blockchain and the holdings and transactions of each public address are open to viewing. This allows the system to be transparent and as a result trust is established through technology. Anyone in a public/ permissioned blockchain network can have full traceability of events, actions, and measurements, leading to protection of markets and adherence to legal and regulatory obligations. For example, in the Supply Chains where the conditions of storage and product source and quality can be transparently monitored (Alvarez-Rodríguez, Labra-Gayo and De Pablos, 2014). In Hyperledger Fabric (HF) based enterprise blockchain network, there is a possibility to create channels, permitting a group of participants to create a private ledger for the transactions based on their business logic. This feature in the HF based networks is valuable specially where some members are competitors and not want every transaction they make known to all participant (Lu *et al.*, 2020).

c. **Security:** All transactions in a blockchain network are cryptographically secured and provide integrity. The blockchain itself is an immutable and durable ledger. Once the transactions are recorded on the blockchain after a consensus among the peers, they cannot be altered or deleted (Khan, Arshad and Khan, 2020). In the fight against poor security and identity theft, blockchain can be used to improve security and grant users more granular control over data.

d. **Privacy:** Despite the transparent nature of blockchain, this technology can enable different entities (e.g. IoT devices (Ghimire *et al.*, 2016), humans, workers) to communicate with each other and do transactions autonomously. It means each transaction is between two public addresses, at the same time it is not linked to the actual names. Economic agents, whether natural persons or legal entities, have the right to choose and consent to the information that is stored and shared about them. As above, blockchain and DLT has the capability to give agents the access and control of their data so that they can chose the level of privacy they wish to adopt.

e. **Traceability:** In the traditional models, each operation involves a central third party and requires a considerable long process for verification, reconciliation, and clearance involving paperwork and bureaucracy. Blockchain can play a significant role by enabling a quicker settlement of trades or interactions because a single version of agreed upon data is available on a distributed ledger between organisations (Mirabelli and Solina, 2020). Thus, it can help bring about full traceability.

f. **Immutability:** Blockchain is an excellent record keeper, ensuring that the original data cannot be tampered with.

g. **Interoperability:** Since the Blockchain is accepted by a large number of nodes, it can offer an intrinsic degree of Interoperability for several applications.

3.2. Key components of Blockchain Technology

Using blockchain, bitcoin became the first cryptocurrency that avoids double-spending without requiring a central authority and has been the inspiration for many further applications (Nakamoto, 2008). Blockchain as a distributed ledger tracks various assets, other than cryptocurrencies. The transactions are grouped into blocks, and there can be any number of transactions per block. The process of blockchains syncing up have to do with a concept of consensus - an agreement among the network peers (Bamakan, Motavali and Babaei Bondarti, 2020). So, eventually, each machine has an exact copy of the blockchain throughout the network. A block refers to a set of transactions that are bundled together and added to the chain at the same time. Figure 3 depicts the main components of blockchain.

Ledger	Contains the current world state of ledge and a Blockchain of transaction invocations
Smart Contract	Encapsulates business network transactions in code. Transaction invocations result in gets and sets of ledger state
Consensus Network	A collection of network data and processing peers forming a Blockchain network. Responsible for maintaining a consistently replicated ledger
Membership	Manages identity and transaction certificates, as well as other aspects of permissioned access
Event	Creates notifications of significant operations on the blockchain, as well as notifications related to smart contracts. Does not include event distribution
System Management	Provides the ability to create, change and monitor blockchain components

Figure 3. Key Components of blockchain technology.

3.3. Selection of Consensus Mechanism

The consensus mechanism in the blockchain network is the key factor to establish a decentralized peer-to-peer system with no authoritative entity. There are various consensus protocols with the same goal to ensure the new records on the ledger are original and accurate (Cao *et al.*, 2020). The difference is the way the consensus is reached. Here three main consensus mechanisms are mentioned (Zhang and Lee, 2019):

- **Proof-of-Work** (PoW): Bitcoin and Ethereum (Buterin, 2015), the two famous and trustable blockchain networks use PoW consensus mechanism. In PoW, data transactions are stored in blocks validated by nodes solving a complicated math problem. PoW is slow and consumes huge amount of energy. A reward in the form of a cryptocurrency is issued to the first miner who cracks the problem.
- **Proof-of-Stake** (PoS): In PoS the creator of a new block - validator - is randomly chosen based on how much stake they commit to the network. Hence, the higher the stake placed, the higher the chance to be selected as a validator which give more power to a single node. Blockchain protocols like Cardano and EOS adopt the PoS consensus.
- **Proof-of-Authority** (PoA): A modified form of Proof-of-Stake where only approved parties selected based on their reputation can become validators. There are various algorithms that can be based on PoA.

In the enterprise, the companies need to have some control over that network. They require to know what members and nodes are on the network who has the authority to influence the change on the network. Hence, enterprise blockchain usually uses PoA consensus protocol. Various industries are often interested in having a pluggable consensus models in which the network can be configured based on appropriate consensus protocol. Hence, Proof of Authority would be a more appropriate consensus mechanism for the e-procurement use case.

3.4. Enterprise blockchain solutions

As mentioned previously (Figure 2), Blockchain has some inherent properties beneficial for many companies. It is wildly versatile and can be used to increase security efficiency and transparency across many industries. Hence, various industries across the world are showing interest in leading the movement towards blockchain technology. It is essential for them to stay relevant and choose the right technology. There are two types of blockchain network, *permissionless* or public blockchain and *permissioned* or private blockchain (Putz, Menges and Pernul, 2019):

- In a **permissionless** blockchains like Bitcoin or Ethereum, anyone can access to the ledger or issue a transaction, publish a smart contract or run a node. In this type of network, there is full transparency and a relatively high level of anonymity. However, the performance is slow and scaling is a massive challenge in the permissionless blockchain. In these networks, there are monetary incentives for those running nodes. In Bitcoin or Ethereum network, there is proof of work consensus algorithm which consumes an immense amount of energy.
- **Permissioned** blockchain networks are closed ecosystems where all participants are well defined through membership identity services. Only pre-approved entities can run nodes. The degrees of decentralization and transparency are dependent on the configuration set by the consortium members. Validation of the transactions does not require mining. Moreover, in validation of a transaction does not require a crypto economic incentive or tokens for the running nodes. Consensus mechanisms are computationally inexpensive allowing permission blockchains to perform and scale much better than permissionless.

Permissioned blockchain is the appropriate network for e-Procurement case. The reason is the network requires a high scalability and efficiency as well as the possibility for membership management. Currently, there exists few permissioned enterprise blockchain platforms. Table 1 presents the comparison between the some of the current enterprise blockchain platforms. Quorum is the software fork of the public Ethereum blockchain developed by American investment bank and financial services company, J.P. Morgan. Hyperledger. Or Hyperledger is an open source project with a modular design under the Linux Foundation (Androulaki *et al.*, 2018). Corda is another project, developed by R3 (r3.com), specifically aimed towards the financial world. An open-source collaborative software development approach can ensure the transparency, longevity, interoperability, and support required to bring blockchain technologies forward to mainstream commercial adoption. All of these platforms are an open-source blockchain. Hyperledger is hosted by Linux, the world's leading open source community. Moreover, the Hyperledger has a modular design which means that businesses can plug in different functionalities to suit their particular needs. Hyperledger is not focused on a specific industry and already has been deployed in various industries, such as supply chain traceability, e-Government, insurance, copyright protection and real estate (hyperledger.org/learn/blockchain-showcase). This paper is using Hyperledger Fabric blockchain solution.

Table 1. Comparison between permissioned enterprise blockchain platforms.

	Quorum	Hyperledger	Corda	Openchain	MultiChain	EoS
Code type	Open-source	Open-source	Open-source	Open-source	Open-source	Open-source
Industry focus	Financial services	Cross-industry	Financial services	Digital Asset Management	Financial services	Cross-industry
Language	Solidity	Java, Golang, NodeJS	Kotlin, Java	JavaScript	C++	C++
Consensus	Pluggable (PoA) (Istanbul BFT, Raft)	Pluggable (PoA) (Kafka, RBFT, Sumeragi, PoET)	Pluggable (PoA) (RBFT, Raft)	Pluggable	PoA (PBFT)	Delegated PoS
Webpage	goquorum.com	hyperledger.org	corda.net	openchain.org	multichain.com	eos.io

3.5. Selection of Hyperledger for the E-Procurement use case

Hyperledger is an open source project established to assist enterprises around the world deliver on the promise of blockchain for more secure, more reliable, and more streamlined interactions. It is a global collaboration, hosted by The Linux Foundation, and includes leaders in finance, logistics, Internet of Things, manufacturing, and technology. Hyperledger provides all the capabilities of the blockchain architecture - data privacy, information sharing, immutability, with a full stack of security protocols - all for the enterprise. Hyperledger aims to advance cross-industry blockchain technologies. So far, it has one of the largest blockchain developer communities and allows them to utilize the technology for designing data-sharing networks, micro-currencies, operating systems for marketplaces, and decentralized digital communities.

Hyperledger blockchains are generally permissioned blockchains, which means that the parties that join the network are authenticated and authorized to participate on the network. Hyperledger incubates and promotes a range of business blockchain technologies, including distributed ledger frameworks, smart contract engines, client libraries, graphical interfaces, utility libraries and sample applications. The Hyperledger umbrella strategy incubates and promotes a range of business blockchain technologies and encourages the re-use of common building blocks and enables rapid innovation of DLT components. As of May 2020, there are 6 types of distributed ledgers, 4 libraries, 5 tools, and 2 domain-specific within the Hyperledger ecosystem. This paper is using the Hyperledger Fabric framework.

Hyperledger Fabric (HF) (Androulaki *et al.*, 2018) is a blockchain framework implementation and one of the Hyperledger projects hosted by The Linux Foundation. Intended as a foundation for developing applications or solutions with a modular architecture, Hyperledger Fabric allows components, such as consensus and membership services, to be plug-and-play. Hyperledger Fabric leverages container technology to host smart contracts called "**chaincode**" that comprise the application logic of the system. The chaincode executes when the term and conditions in the smart contract are met. Assets are added, updated, and transferred using chaincode. Fabric has five main functionalities as shown in Figure 4.

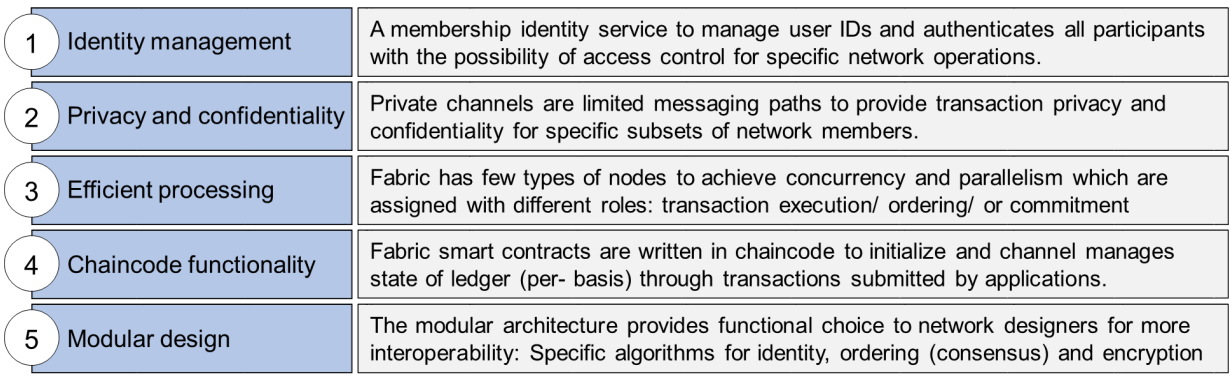

Figure 4. Hyperledger functionalities.

A HF network contains a set of nodes which are the primary foundation of the blockchain network for communication. Each node requires permission and valid certificate to communicated with the network. In Fabric network there are three types of nodes:

1- **Client node:** It initiates a transaction using application SDK and has an identity.

2- **Peer node:** Peer nodes can host ledgers and run smart contracts. There are 4 types of peer nodes:
- Committing Peer: Every peer of a channel is a committing peer. The committing peer holds a ledger for each channel that engaged in. It is not necessary to install a chaincode on this kind of peer. The peers validate ordered blocks of transactions and then commits (writes/appends) the blocks to its copy of the channel Ledger. The peers and mark all transactions of each block as valid or invalid.
- Endorsing Peer: Any peer that has a chaincode installed is an endorsing peer. An endorsing peer executes the requested smart contract code and return a proposal response to the client application. Once a transaction is endorsed, it can be accepted onto a committing peer´s copy of ledger.
- Leading Peer: In an organisation while there are multiple peers subscribed for various channels, at least one peer should serve as the leading or admin peer for the channel with the responsibility of communicating with the network ordering service on behalf of the organisation.
- Anchor Peer: It is defined in channel configuration of an organisation for cross-organisation communication scenarios depends on gossip. Anchor peers increase the availability and redundancy in the network.

3- **Ordering node:** An Orderer receives endorsed transactions from application SDK, package them into blocks as based on channel configuration file and send them to all other peers to validate those transaction and update their ledgers. Ordering service keeps track of all transactions in their ledger including valid transactions and invalid transactions. It is not necessarily run by every organisation in the network but at least one of the organisations must run it. Instead of proof-of-work consensus mechanism in Bitcoin network where all nodes independently trying to come to consensus on the state of the blockchain, the ordering service node will interact with the peers who are validating the transactions and then will order the blocks and send it out back out to the peers. Different configuration options for the ordering service includes (Sousa, Bessani and Vukolic, 2018):

- **SOLO:** single node for development
- **Kafka:** Crash fault tolerant consensus with minimum 3 nodes (Odd number of nodes are recommended).

4. Application scenario for e-Procurement

Membership Management	In HF, Membership Service Provider authenticates, authorizes, and manages identities on a permissioned blockchain network.
ID Management /Digital Signature	The identities have the form of cryptographically validated digital certificates that comply with X.509 standard and are issued by a Fabric-CA or an external CA. MSP manages a set of identities within a Fabric network, provides identity for all nodes, client applications, and organizations' administrators.
Audit tracker	In HF, the ordering service is responsible for ordering a sequence of transactions into immutable blocks and deliver to all the pears in the network. All events and audit records and communication of decisions can be automatically track to provide more security and traceability.
Timestamps	The blockchain is used as permanent digital ledger's that can record immutably any transactions in real time which includes details such as the transaction time, transaction ID and the signed documents hash value.
Immutable Tender Document	The hash of a tender document can be stored on the distributed ledger of blockchain network which is immutable.
Contract Management	HF network can create parallel channels that authorize a group of stakeholders to create a private ledger for the transactions based on their business logic which can be programmed by chaincode as a legal contract. Each contract can be signed through digital signature.
Micro-Payment/ Payment	HF blockchain can create a trusted and transparent environment for automating finance processes and settlement of micropayment.
Internal Data Management	Blockchain enables data storage to be more secure and robust against attacks, hence, it can be a credible solution for management of internal sensitive data.
Interoperability	The modular and pluggable architecture of HF can play a significant role by enabling interoperability between organizations within the network as well as external organization with distinct blockchain solutions.
Security	All transactions in the network are secure, since they are authenticated and verifiable.

HF: Hyperledger Fabric, MSP: Membership Service Provider, CA: Certificate Authority

Figure 5. Identifying blockchain application scenarios for the e-Procurement platforms.

Procurement is a business function that's constantly evolving. Today an e-Procurement platform positions itself as a strategic function and a value contributor. Procurement not only adds support to the business relationships, it also drives them. It is the interface between organisations and the supply market. In the e-Procurement process, the requests for quotations or sealed bid auctions are often used to collect competing proposals from several bidders. However, e-Procurement platforms are still vulnerable to fraud and corruption. Traditionally, third parties or trusted software solutions are employed to protect the bids. These forms of trust are still relevant and important, but they have their own limitations and cost. Blockchain is a new structure that can provide a trust mechanism through technology. The blockchain network is built based on cryptography in a way that organisations can trust the information without a central point of trust and removing the reliance on participant integrity. As shown in Figure 5, the possible application scenarios of employing blockchain technology in an e-Procurement platform are identified.

5. Hyperledger Fabric based solution architecture

To present an enterprise blockchain architecture providing to the needs of an e-Procurement Platform, there was collaboration with the Vortal e-Procurement platform to analyse the business needs while proposing the blockchain solution. As identified in previous section, there are many possible application scenarios that can employ blockchain. Following scenarios are identified based on Vortal platform requirement where blockchain can provide a solution:

- **Audit Tracker**

An audit reviews the procurement process to reduce fraud and offer suggestions for improvement. One of the possible application scenarios in our case study is using blockchain technology for automatically track events and internal audit record and communication of decisions to provide more security and traceability. The blockchain technology can provide solution related to audit tracker in following ways:

- Automatic and trustable creation of procedures and submission of Bids

The blockchain technology can maintain a record of every event such as creation of new procedures by buyers or submissions of bids by sellers. Thus, an audit trail can be maintained on the distributed ledger and can be independently verified by different peers from various entity. There is a fundamental concept inside Hyperlarger Fabric called "**channel**" that provides confidential transactions between authorized members of a (business) group. A Fabric blockchain network can run discrete channels which are completely independent. Each channel can define a different set of rules, business policies, and chaincode smart contract. There can exists only one distributed ledger per channel which every member has access to it. However, each channel can run multiple smart contract based on the consortium requirement. In a channel, the members of a business can specify asset types for ordering transactions. This can ensure that all participants for a specific call can receive same information and can automate some processes like closing and bid analysis.

- Automation of internal process review

Moreover, audit procedures include an evaluation of employee functions during the purchasing process. Traditionally, auditors might, for example, check if a list and samples of authorized signatures exists and if employees are using the list when verifying purchase orders. Review steps in the formal bidding process to make sure they are being followed. Ask if accounts payable and receiving checklists are being implemented. Determine if conflict-of-interest policies and opportunities for training and purchasing certification are available for employees. Blockchain technology provides a transparent and automatic solution for reviewing these internal processes and track each process from the point of origin to the final step.

- Increasing the efficiency to the procurement process

Audits provide an opportunity for organisations to assess the effectiveness and efficiency of their procurement process. Traditionally, if an organisation has contracted with a firm specializing in audits, a common end-of-audit procedure is to offer suggestions for improvement to correct the purchasing performance, reduce fraud and enable cost savings. Blockchain can automate the procurement process while it can give a transparent and immutable solution during procurement steps. For example, the identity and validity of the source and destination of each transaction in the platform is recorded in the distributed ledger, hence, nothing can be lost or misfiled which can provide new suggestions and insight as well as opportunity for automation of the process. The HF solution can also provide efficient processing through segregating of consensus and chaincode execution.

- **Timestamps**

In e-Procurement, timestamping technique enables stakeholders to be sure about the creation and modification time of any document such as a bid proposal. Since security is an important factor and no entity should be able to change

a submitted document, currently, third party trusted companies provide timestamps. Blockchain technology can provide timestamps at the exact time of submission of any document with tamper proof records.

- **Identity Management**

To avoid frauds and risks in e-Procurement processes, each stakeholder needs to have a certified identity in order to participate in each process. As an example, a fraudulent bidder could prepare multiple bids, all of them digitally signed and timestamped. Then, after the deadline and in collusion with auctioneer's database administrator, see competitors' proposals and set the bid that better fits his requirements. Hence, trusted digital signatures and a permissioned blockchain network can help achieving stakeholder authentication, documents integrity and non-repudiation of tender proposals. Fabric network is a private blockchain and each member only through Membership Service Provider (**MSP**) can be part of the blockchain network. The HF architecture uses x.509 certificates through a public key infrastructure for the MSP or the Certificate Authority (CA). each member or each organisation within a business network will run their own certificate authority. Additionally, as mentioned before, using multi-channel HF network, each consortium can define permissions on who can join the network and what type of access each membership can grant.

Vortal-Interdata is considering providing digital identity and validate permissions for stakeholders using HF blockchain technology. This can provide trusted identity of bidders and the bidding entity.

- **Internal Data Management**

Data on the centralized servers are vulnerable to hacking, data loss, and human error. Using blockchain enables data storage to be more secure and robust against attacks (Meng *et al.*, 2018). One of the obvious use cases is deploying blockchain technology for sensitive data security and management in organisations. Furthermore, through permissioned blockchain technology, it is possible to manage data access and sharing data with the authorized employees (Guo *et al.*, 2018). This will improve data security and privacy.

Another use case can be supporting digital copies of valuable artworks, creative media and entertainment contents from incorrect propaganda over social media.

5.1. Hyperledger Fabric based solution

Previously, we identified and explained the four main application scenarios for Vortal blockchain and how HF can provide solution for each scenario. Here, we are presenting the proposed HF based solution. The Vortal-Interdata blockchain solution has following characteristics:

- Vortal-Interdata blockchain is using Hyperledger Fabric (HF) framework which is one of the available open source blockchain solutions as described earlier.
- Based on the organisation requirement, the blockchain solution is a permissioned blockchain network.
- The network includes peer nodes to host ledgers and chaincode smart contracts.
- A ledger immutably records all the transactions generated by smart contracts. Smart contracts and ledgers are used to encapsulate the shared processes and shared information in a network, respectively.
- There will be different channels in the network as subnet of communication between two or more specific network members. Each channel can define the smart contract and consensus algorithms independently for the purpose of conducting private and confidential transactions. This characteristic is going to be useful for audit tracker application scenario as well as membership management for each specific call, since it provides privacy and confidentiality through defined channels.
- The consensus algorithms will be based on Proof of Authority to avoid unnecessary power consumption. HF offers a pluggable architecture where a consortium can define their own algorithm. **Consensus** mechanism in HF comprise of three separate steps:
  1. Transaction endorsement
  2. Ordering
  3. Validation and commitment
- To incentivise the node in the Vortal-Interdata blockchain ecosystem, Vortal-Interdata is defining a token called VIT (Vortal Interdata Token). Vortal promises to exchange VIT with fiat currency if it is needed. So external private and public entity can host the node by receiving VIT based on their contributions.
- There would not be any security issue for storing the ledgers in hosting nodes outside of Vortal platform, since only the cryptographic hash of various information will be stores on the blockchain. Moreover, based on privacy requirement always it is possible to add or remove a (external/ internal) peer to the business channel configuration.

- As explained at the beginning of section 5, the proposed HF based solution provides solution for the four identified application scenarios.

Each of the organizations are running in their own Docker container virtual networks. These virtual networks are going to interface between each other and that's how the different organizations will interact.

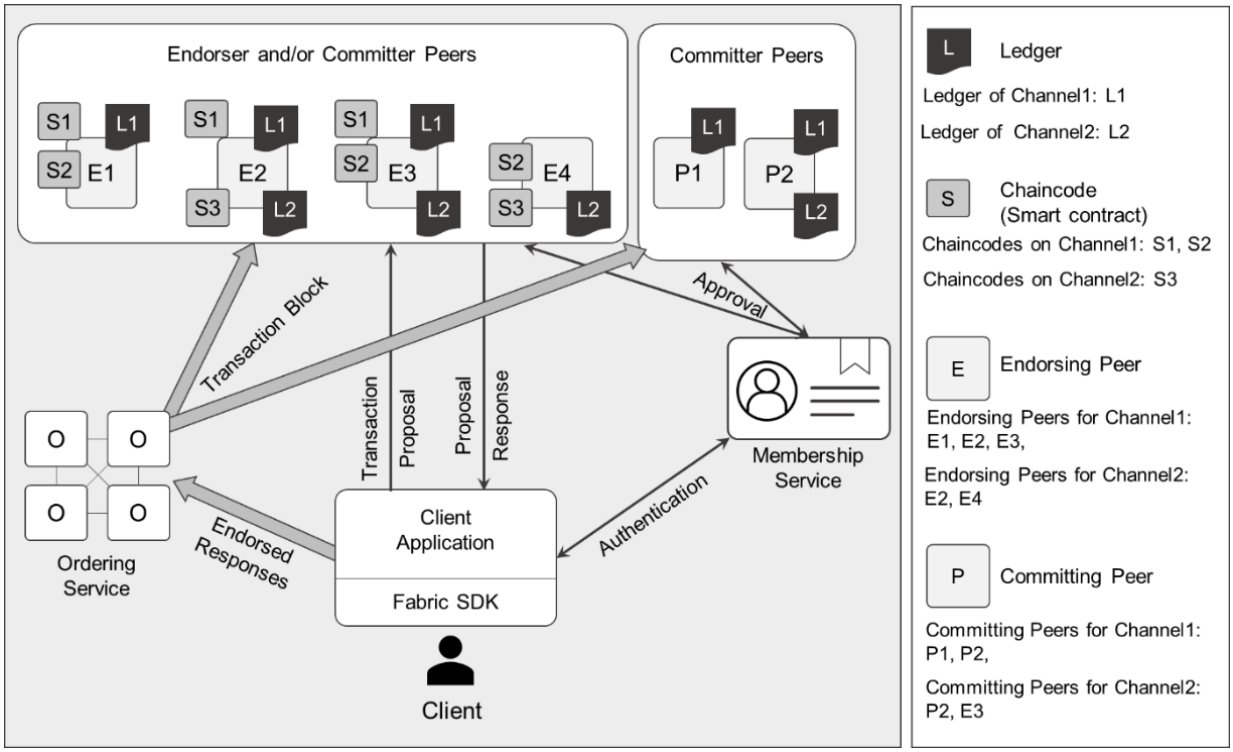

Figure 6. Blockchain Network Components and Transaction Flow.

In Figure 6, we provide an example of blockchain solution with following components:

- **Membership Service:** In the proposed framework, every node had an identity and holds set of permissions and valid certificate to communicated with the network. Based on the business requirement the permission can dynamically modified by organisation's administrator(s). One of the important characteristics of provided solution is all capabilities of this solution are modular and pluggable. Hence, Vortal can plug in parts of its existing systems to the blockchain solution. One of them is its current identity management system and certificate authority. Furthermore, in proposed solution, any authorized external entities can host a blockchain node and each member or each entity within a business network can run their own certificate authority.
- **Ledger**: Distributed ledger is the primary component of any blockchain network. In proposed solution, as shown in Figure 7 a ledger consists of two data structures:
  1. Blockchain or log of transactions: which is an immutable linked list of blocks (a hashchain) with new block always added to the end. Each block contains zero or more transactions and some additional metadata. The first block is known as "genesis" block and has zero transactions. It includes details about configuration of network which contains certificates of all the organizations and peers in the network and information on how to bootstrap the blockchain network for the case study. The Genesis block is downloaded primarily on the ordering service node.
  2. World State: which stores the last state of smart contracts and output of transactions. World State is stored in a traditional database where data elements can be added, modified, deleted. Each of the peers in the network can run an external state database. CouchDB is the most important externally supported World State database.

  The blockchain component of ledger stores immutable log of all activities and transactions occurred in each channel and can enable audit tracking and as general traceability for our use case. Each transaction can be defined as shown in Figure 7. Each transaction can be any message or document produced by any stakeholder in the procurement network. Either it is valid or not, it gets a transaction ID at the time of creation and has a creator ID. The time of

creation gets recorded in the Timestamp field. The timestamp provides an additional level of verification for any document or event (transaction) created by stakeholders in the procurement process. Transaction proposal or its hashtag depending on the type and size of transaction gets recorded in another filed. The other fields will be described later in this section.

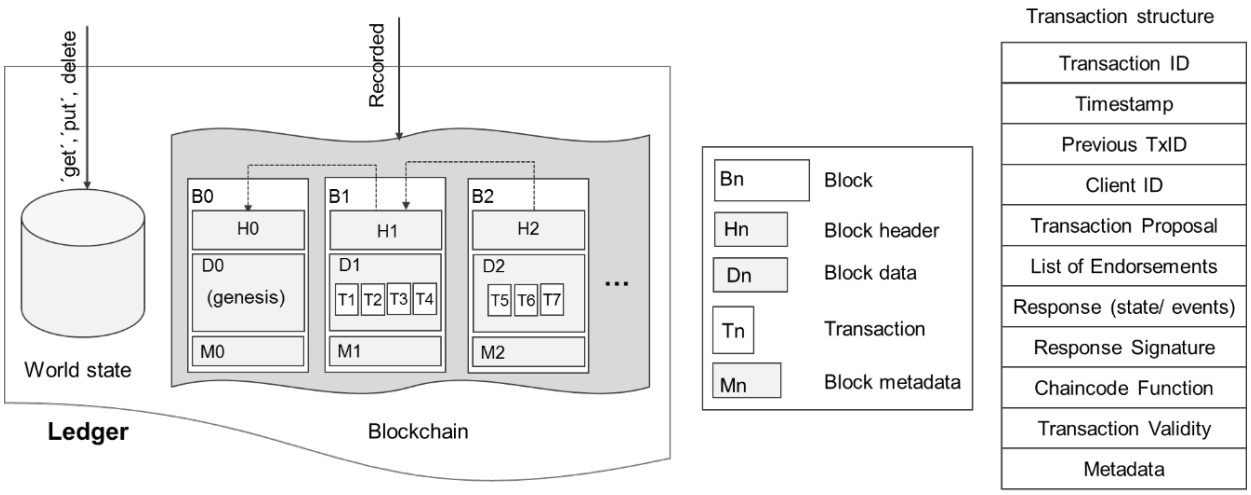

Figure 7. Ledger structure.

- **Client**: Each consultant, supplier, contractor, buyer, or even logistics system in the procurement network can be a client. As mentioned before, each client has an ID and it can initiate a transaction using application SDK.
- **Ordering Service:** The ordering service node is not necessarily run by every organization within network but at least one of the organizations including Vortal company has to run this node. Because this node is entirely responsible for ordering transactions and blocks in propagating those out to the peers in the network. The ordering service node will interact with the peers who are validating the transactions and then will order the blocks and send it out back out to the peers
- **Channels:** As described before, in this solution it is possible, within procurement network, to take two or more of the participants and put them in channels and have them sending blockchain transactions to each other without the rest of the network knowing about them. This can happen based on business requirements. All participants in each channel should be authorized and all have access to same ledger. Hence, each channel contains a distributed ledger. However, there can exist more than one smart contract defined for each channel. The segregating of consensus mechanism and the chaincode smart contract execution for each various channels can happen simultaneously. Other that privacy, that enables a very efficient model and it allows a high transaction throughput. One important channel is called "*Global Channel"* which is created by Vortal to include everyone in the network. All other organizations (which join to the blockchain network and provide different types nodes) can join the global channel. All the peers within each organization will find the global channel and join it using their Certificate Authority (CA). Since every peer is part of Global Channel, to simplify the example shown in Figure 6, we did not show the Global Channel.
- **Committing Peers:** Every peer of a channel is a committing peer. The committing peer holds a ledger for each channel that engaged in. They do not run any smart contract chaincode.
- **Endorser Peers:** The endorsing peers are the ones that run the chaincode on their machines to validate it. Once an endorsing peer receives a transaction proposal, it pursues a four step process to confirm the transaction is correct:

  1. It checks if the transaction proposal is well-formed with a correct syntax.
  2. It inspects if the transaction has been submitted in the past to avoid the double spending.
  3. It checks the identity that is submitted the transaction and confirms it has the correct digital signature. Each organization uses its own CA service to validate the transaction signature.
  4. Finally, it is important to confirm the authority and permission given to the identity who submitted the transaction.

Once these four steps at endorsing peers have been examined, the transaction proposal can be considered valid. Then, the endorsing peers send back the transaction proposal signatures to the original identity that submitted it. The

application SDK verifies the endorsing peer signature and compares the proposal response to determine if the proposal responses are the same. Then the Client combines all collected endorsements into a transaction. The SDK sends the transaction proposals and response within transaction message to the Ordering Service. Then, transaction block gets validated and committed. Finally, relevant ledger (based on the related chaincode) gets updated and the Client gets the notification.

6. Discussion and conclusion

Open Procurement Procedures and Cross Border Procurement is requiring new levels of trust and transparency from e-procurement platforms. Some of these requirements were being fulfilled by third parties who issue certifications, timestamps and conduct audits. However, these procedures are often cumbersome, expensive and still require trust in a particular entity or authority which could be prone to corruption or collusion. Blockchain Technology on the other hand provides a promising alternative, that is decentralised, immutable and secure thus can act as a multi-purpose trusted third party for several applications. In this paper we explored some of the key functionalities and use cases where Blockchain Technology that can be used to benefit e-procurement platforms. Based on some of the key requirements of an e-procurement platform Vortal, we developed an architecture based on the Hyperledger Blockchain Platform that can fulfil many of the identified requirements. Although we are not at a commercial implementation stage, such modelling has demonstrated the significant advantages that Blockchain Technologies can bring to the next generation of e-procurement infrastructure.

7. Acknowledgements

The research work of this paper has been partially funded by the project VORTAL INTER DATA (nº 038361), co-financed by Vortal and COMPETE Program P2020, and partially by Fundação para a Ciência e Tecnologia UIDB/00667/2020.

8. References

Alvarez-Rodríguez, J. M., Labra-Gayo, J. E. and De Pablos, P. O. (2014) 'New trends on e-Procurement applying semantic technologies: Current status and future challenges', *Computers in Industry*, 65(5), pp. 800–820. doi: 10.1016/j.compind.2014.04.005.

Androulaki, E. *et al.* (2018) 'Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains', *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, 2018-Janua. doi: 10.1145/3190508.3190538.

Bag, S. *et al.* (2020) 'Procurement 4.0 and its implications on business process performance in a circular economy', *Resources, Conservation and Recycling*. Elsevier, 152(September 2019), p. 104502. doi: 10.1016/j.resconrec.2019.104502.

Baldus, B. J. and Hatton, L. (2020) 'U.S. chief procurement officers' perspectives on public procurement', *Journal of Purchasing and Supply Management*. Elsevier Ltd, 26(1), p. 100538. doi: 10.1016/j.pursup.2019.05.003.

Bamakan, S. M. H., Motavali, A. and Babaei Bondarti, A. (2020) 'A survey of blockchain consensus algorithms performance evaluation criteria', *Expert Systems with Applications*. Elsevier Ltd, 154. doi: 10.1016/j.eswa.2020.113385.

Buterin, V. (2015) *A next-generation smart contract and decentralized application platform*. doi: 10.1016/j.jchromb.2013.02.015.

Cao, B. *et al.* (2020) 'Performance analysis and comparison of PoW, PoS and DAG based blockchains', *Digital Communications and Networks*. Elsevier Ltd, (August 2019). doi: 10.1016/j.dcan.2019.12.001.

Dávid-Barrett, E. and Fazekas, M. (2020) 'Anti-corruption in aid-funded procurement: Is corruption reduced or merely displaced?', *World Development*, 132. doi: 10.1016/j.worlddev.2020.105000.

Ghimire, S. *et al.* (2016) 'IoT based situational awareness framework for real-time project management', *International Journal of Computer Integrated Manufacturing*, pp. 1–10. doi: 10.1080/0951192X.2015.1130242.

Grilo, A. *et al.* (2017) 'Relationship between investors and European startup ecosystems builders', in *2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. IEEE, pp. 538–550. doi: 10.1109/ICE.2017.8279932.

Guo, R. *et al.* (2018) 'Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems', *IEEE Access*, 3536(c). doi: 10.1109/ACCESS.2018.2801266.

Jardim-Goncalves, R. *et al.* (2013) 'Reference framework for enhanced interoperable collaborative networks in industrial organisations', *International Journal of Computer Integrated Manufacturing*, 26(1–2), pp. 166–182. doi: 10.1080/0951192X.2012.687130.

Khan, K. M., Arshad, J. and Khan, M. M. (2020) 'Investigating performance constraints for blockchain based secure e-voting system', *Future Generation Computer Systems*. Elsevier B.V., 105, pp. 13–26. doi: 10.1016/j.future.2019.11.005.

Lu, N. *et al.* (2020) 'A secure and scalable data integrity auditing scheme based on hyperledger fabric', *Computers and Security*. Elsevier Ltd, 92, p. 101741. doi: 10.1016/j.cose.2020.101741.

Mehrbod, A. *et al.* (2015) 'Matching heterogeneous e-catalogues in B2B marketplaces using vector space model', *International Journal of Computer Integrated Manufacturing*, pp. 1–13. doi: 10.1080/0951192X.2015.1107915.

Mehrbod, A. *et al.* (2017) 'Gamification in supported geocaching tours', in *2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. IEEE, pp. 1419–1423. doi: 10.1109/ICE.2017.8280049.

Meng, W. *et al.* (2018) 'When Intrusion Detection Meets Blockchain Technology: A Review', *IEEE Access*, 3536(c), pp. 1–10. doi: 10.1109/ACCESS.2018.2799854.

Mirabelli, G. and Solina, V. (2020) 'Blockchain and agricultural supply chains traceability: Research trends and future challenges', *Procedia Manufacturing*. Elsevier B.V., 42(2019), pp. 414–421. doi: 10.1016/j.promfg.2020.02.054.

Nakamoto, S. (2008) 'Bitcoin: A Peer-to-Peer Electronic Cash System', *Www.Bitcoin.Org*, p. 9. doi: 10.1007/s10838-008-9062-0.

Nodehi, T. *et al.* (2015) 'ICIF: an inter-cloud interoperability framework for computing resource cloud providers in factories of the future', *International Journal of Computer Integrated Manufacturing*, pp. 1–11. doi: 10.1080/0951192X.2015.1067921.

Nodehi, T. *et al.* (2018) 'Review paper on use cases of blockchain', in *ICE/IEEE ITM: 25rd INTERNATIONAL CONFERENCE ON ENGINEERING, TECHNOLOGY AND INNOVATION*. Stuttgart.

Putz, B., Menges, F. and Pernul, G. (2019) 'A secure and auditable logging infrastructure based on a permissioned blockchain', *Computers and Security*. Elsevier Ltd, 87, p. 101602. doi: 10.1016/j.cose.2019.101602.

Sousa, J., Bessani, A. and Vukolic, M. (2018) 'A byzantine Fault-Tolerant ordering service for the hyperledger fabric blockchain platform', in *Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018*, pp. 51–58. doi: 10.1109/DSN.2018.00018.

Zhang, S. and Lee, J. H. (2019) 'Analysis of the main consensus protocols of blockchain', *ICT Express*. Elsevier B.V., 6(2), pp. 93–97. doi: 10.1016/j.icte.2019.08.001.

Zheng, Z. *et al.* (2020) 'An overview on smart contracts: Challenges, advances and platforms', *Future Generation Computer Systems*. Elsevier B.V., 105, pp. 475–491. doi: 10.1016/j.future.2019.12.019.

Zutshi, A., Mota, D., *et al.* (2018) 'A game theory approach to online lead generation for oligopoly markets', *Computers & Industrial Engineering*, 121, pp. 131–138. doi: 10.1016/j.cie.2018.04.045.

Zutshi, A., Grilo, A., *et al.* (2018) 'Simulation and forecasting of digital pricing models for an e-procurement platform using an agent-based simulation model', *Journal of Simulation*, 12(3), pp. 211–224. doi: 10.1057/s41273-016-0045-6.

Zutshi, A. and Grilo, A. (2019) 'The Emergence of Digital Platforms: A Conceptual Platform Architecture and impact on Industrial Engineering', *Computers & Industrial Engineering*, 136, pp. 546–555. doi: https://doi.org/10.1016/j.cie.2019.07.027.

Biographies

Tahereh Nodehi has a Ph.D. degree from Department of Electrical and Computer Engineering, Nova University of Lisbon with a background on Cloud Computing. She is currently a Post-Doc researcher at the Department of Industrial Engineering, at the Nova University of Lisbon. Her main research interests are "Blockchain Technology and Applications", "Digital Platform Strategy for Business", and "Innovation and Entrepreneurship".

Aneesh Zutshi is working as Invited Assistant Professor at the Department of Industrial Engineering and Management at Universidade Nova de Lisboa. His Ph.D. was on Digital Business Models. His research work is focussed on the emergence of Digital Platforms and Blockchain Technology, and their role in disrupting traditional forms of Businesses. He has led numerous projects on Digital Entrepreneurship for the European Commission. He has also been engaged in research in Entrepreneurship, a key member of the responsible for the building up of the Entrepreneurial Ecosystem at NOVA School of Science and Technology.

Antonio Grilo has a Civil Engineering degree by IST, Portugal, a MSc and PhD from the University of Salford, UK. He is an Academic, Researcher and Consultant with a passion for the application in real-life projects of the state of art of innovative management and technology concepts. He has been doing this for over 15 years, in Large and SME companies, public organizations, in Portugal and across Europe. He is currently head of the Department of Mechanical and Industrial Engineering, director at UNIDEMI - Research and Development Unit for Mechanical and Industrial Engineering. Also, he is heading the MADAN Parque University Incubator.