Blockchain characteristics and consensus in modern business processes

Wattana Viriyasitavat[a,*], Danupol Hoonsopon[b]

[a] Business Information Technology Division, Department of Statistics, Faculty of Commerce and Accountancy, Chulalongkorn University, Pathumwan, Bangkok 10330, Thailand
[b] Department of Marketing, Faculty of Commerce and Accountancy, Chulalongkorn University, Pathumwan, Bangkok 10330, Thailand

ABSTRACT

Blockchain technology has attracted a great deal of attentions as an effective way to innovate business processes. It has to be integrated with other Business Process Management system (BPM) components to implement specified functionalities related to the applications. The current efforts in integrating this technology into BPM are at a very early stage. To apply Blockchain into business processes efficiently, Blockchain and business process characteristics must be identified. Inconsistency of confirmation settlement that heavily relies on the implementation of consensus protocol poses a major challenge in business process operations, especially ones that are time-critical. In addition, validators, nodes responsible for performing consensus operations in a Blockchain system, can introduce bias and as a result are not trustable. This paper first defines Blockchain and also investigates the characteristics of Blockchain and business processes. Then, we suggest an architecture of business processes in Blockchain era to overcome the problems of time inconsistency and consensus bias. The architecture provides persistency, validity, auditability, and disintermediary that Blockchain offers. The architecture also provides flexibility by allowing business partner to select nodes in performing consensus; thus bias is mitigated.

1. Introduction

Over the past decades, consensus mechanisms have been extensively studied in a classical distributed system. After the success of Bitcoin [1], the first cryptocurrency appeared in early 2009, Blockchain technology has attracted attentions from academia and industry sectors [2]. Currently, the rise of Blockcahin applications spans across diverse range far beyond crytocurrencies, including insurance [3], medicine [4–6], economics [7–9], Internet of things [10–12], supply chain, software engineering [13–15], etc. The core element of any Blockchain application is its consensus protocol for reaching consensus of information sharing, replicating state, and broadcasting transactions, among participants. This has made the consensus mechanisms received revived attentions in recent years [16,59]. There exists multiple implementations of consensus in decentralized settings, and some are still in their proposals.

The key properties of integrity, resilience, and transparency of Blockchain make it an attractive option to enterprises to revolutionize their business processes. With the growth and integration of modern technologies including Business Process Management (BPM), Service Workflow, Internet of Things (IoT), Cloud Computing, Service-oriented Architecture (SoA), and Cyber-Physical Systems (CPSs) in Industry 4.0, centralized BPM tools face their limits in meeting the conflicting requirements and trade-off of scalability, security, openness, trust, and

cost [18,19]. To survive in a competitive market, implementing flexible business processes in opened environments is unavoidable, as to promote collaboration, knowledge sharing, and collective decision [20,40,60,64]. The advancement of the technologies provides a wide range of opportunities for automating, sharing information, and transforming businesses [21], especially when IoT devices are becoming prevalent [65]. From this perspective, the newly developed Blockchain technology can be integrated as an essential ingredient for business processes to alleviate the issues of security, distribution, openness, cost-effectiveness, and most importantly trust. With the application of modern technologies, the innovative business process termed business process 4.0 strives for the ultimate goals of interoperation, automation, trust, and transparency.

There are rapidly growing researches on theories and applications on Blockchain and consensus mechanisms. Prior works relevant to this area try to solve the fundamental agreement problem mainly exercised in Asynchronous Byzantine-related consensus exhibited in distributed systems [16,22], which can explain as a system with *n* asynchronous processes that still ensure agreement on a single value despite having some faulty nodes. This field has been extensively studied in the distributed systems community for closed systems since the 1970s. At present, there is a slight shift on the landscape of how consensus is exercised.

* Corresponding author.
E-mail address: hardgolf@gmail.com (W. Viriyasitavat).

1. Now it relies heavily on a message-passing model where not all nodes are required to find a solution, but once proposed, it will be broadcasted to other nodes that can easily verify the correctness.
2. System configurations can vary regarding the degree of centralization and openness. Private and permissioned Blockchains tend to be more centralized than public Blockchains, while information access is more opened in public Blockchain.
3. Other economic and psychology parameters are incorporated such as in PoS-based consensus.
4. Unlike closed systems usually exhibited in traditional distributed systems, Blockchain systems are more opened and lead to a plethora of new designs of consensus algorithms [23].

To study the effect of Blockchain and its consensus in modern business processes, we conduct a survey on consensus mechanisms exercised in distributed Blockchain applications in the field of business process 4.0 and then presents an architecture for consensus by incorporating the 2nd generation of Blockchain, *smart contract,* to be more flexible and better support user requirements. Thus, the paper makes the following contributions:

1. We provide definitions and characteristics of Blockchains with respect to consensus mechanisms.
2. We identify the relations of Blockchain and business process characteristics.
3. We propose an architecture and guidelines for making consensus to be more flexible and reliable that better reacts to user requirements in the field of business process interoperation.

We believe that our architecture and guidelines will attract and encourage many researchers to implement effective consensus in solving time inconsistency and bias. In addition, the paper will serve as a good reference for and raise awareness of Blockchain researchers and practitioners to understand the relationship in adopting Blockchain the technology and consensuses in the context of business processes.

The remainder of this paper is organized as follows. Section 2 provides the definitions of Blockchain technology and consensus mechanisms. Section 3 identifies the classification of Blockchain systems and explains the characteristics and relations of Blockchain and business processes. Section 4 introduces our architecture for applying Blockchain technology to business processes. Lastly, Section 5 concludes the paper.

2. The definition of Blockchain and consensus properties

2.1. Definitions

Across most current researches, how Blockchain is defined is informal, mostly described specifically to the context of use and using some marketing words in terms of properties Blockchain offers or how security can be attained. These include, for example, a public ledger for recording transactions maintained by many nodes without central authority through a distributed cryptographic protocol [16]; a decentralized database with the ability to operate in a decentralized setting without relying on trusted intermediaries [17]; a decentralized, replicated, immutable and tamper-evident log, allowing anyone to read data and verify the correctness [16]; a type of distributed ledger (data structure) containing information about transactions or events, which is replicated and shared among the participants in the network [2]. Most of them include terms immutability, auditability, transparency, distributed database or ledger, and no trusted intermediary.

Oxford dictionary defines Blockchain as *"A system in which a record of transactions made in bitcoin or another cryptocurrency are maintained across several computers that are linked in a peer-to-peer network".* However, the scope is limited within cryptocurrency in which the technology can be further employed in a diverse range of applications

[24]. In this paper, we extend the Blockchain definition to address a broader context as *"A technology that enables immutability, and integrity of data in which a record of transactions made in a system are maintained across several distributed nodes that are linked in a peer-to-peer network".* Some properties can be inferred in the definition. For example, transparency can be enhanced according to the degree of information disclosed to the public outside the system. This allows the system to be auditable. Resilience is another property benefited from distributed setting. The degree of resilience depends on the number of participating nodes. The system correctness relies heavily on the assumption that the majority of nodes are benign. Since the data can be trusted, central intermediaries are no longer required.

Apart from cryptography including cryptographic hash and digital signature, the key success of Blockchain relies on consensus mechanisms that determine overall performance and scalability of a system. Consensus is described as the agreement among a group of nodes onto the truth about their data. However, the common Blockchain consensus has not yet been defined. Oxford dictionary defines the term consensus as *"A general agreement".* Therefore, in this paper, we use the definition of Blockchain consensus as *"The agreement of common value among a group of nodes in Blockchain systems".*

2.2. Consensus properties

The research on consensus has extensively been studied in distributed systems to be resilient to node failures, partitioning of the network, message delays, messages out-of-order or missing, and compromised messages. In the context of Blockchain, consensus mechanisms need to deal with selfish, faulty, or malicious nodes and ensure that all nodes in the network agree upon a consistent global state. Any Blockchain consensus tries to address three key properties based upon which its applicability and efficacy can be determined [25].

1. *Safety: Safety* property guarantees that something bad will never happen. It corresponds to *validity* and *agreement* properties in the traditional consensuses appeared in distributed systems. Validity is defined as if some correct processes propose the same value v, then any correct process that decides, decides v. *Agreement* ensures that no two correct processes decide differently. Generally, a consensus mechanism is safe if at least one honest node produces a valid output then all other nodes produce or receive the same output. The results are valid and identical to all nodes, referring as consistency of the share state [26].
2. *Liveness: Liveness* guarantees that something good will happen eventually. This is also known as *termination* in the traditional consensus in distributed systems stating that every correct process eventually decides on a value. A consensus mechanism ensures *liveness* if all benign nodes participating in a consensus eventually produce a value and all correct requests will be eventually processed. There is no bound on the time it takes to decide on a value, such that this property does not require every node to have an identical state at a given point of time.
3. *Fault Tolerance*: A consensus mechanism provides fault tolerance if it is resilient (operate correctly) from failures of some nodes participating in a consensus at any point. As long as faulty nodes are limited, the correct consensus is still being reached. The failure of nodes exhibits in two categories. Fail-stop or crash-failure deals with nodes that stop to process temporarily or permanently in emitting or receiving messages, or participating in the consensus protocol. Byzantine failures on the other hand deal with malicious nodes that are specially crafted to defeat properties of a consensus protocol. The second category was well identified and characterized by Leslie Lamport as the Byzantine General's Problem [28].

While all the three properties are important, Fischer Lynch Paterson (FLP) [29] impossibility result has proven that any deterministic

asynchronous consensus system can have at most two of the three properties. Any distributed consensus system in asynchronous environments must sacrifice one of the three properties depending on its requirements and assumptions in implementing its consensus. Since fault tolerance is considered the most important, most Blockchain applications tend to sacrifice either safety or liveness [26]. For example, Paxos [30], Raft [31], view-stamped replication [32] employ consensus algorithms that favor fault tolerance and safety over liveness, which means that everyone will agree on what the ledger is at a point of time. Ripple/Stellar [33,38], Bitcoin [1], Ethereum [34], and many cryptocurrencies choose fault tolerance and liveness over safety. This emphasizes ledger closes and availability over that everyone actually has the same ledger [35].

3. Blockchain and business process characteristics

The purpose of this section is to identify general characteristics and the relations between Blockchain and business processes. The relations and analysis of these two will be discussed along the way in the following subsections.

3.1. Blockchain characteristics

There are multiple factors that characterize Blockchain systems. In what follows, we identify important characteristics in the aspects of deployments, implementation, and properties.

(1) *Private, Public, and Permissioned Blockchain:* The distinction among these types of Blockchains is the scheme of ledger sharing and who is allowed to participate in a system [36]. In private Blockchain, ledgers are shared in and validated by a predefined group of nodes. The system requires initiation or validation to nodes that want to be part of the system. Authorized nodes are responsible for maintaining consensus. Private Blockchain is suitable for closed systems, where all nodes are fully trusted. The owner has highest authority to control access to authorized nodes.

Public Blockchains like Bitcoin, Ethereum, etc. on the other hand allow anyone to access and maintain the distributed ledger with permissions to validate the integrity of the ledger by running consensus mechanism. A public Blockchain network is completely opened and distributed; anyone can freely join, participate, and leave the system. Therefore, this system operates under unknown and untrusted nodes.

Permissioned Blockchains are hybrid between private and public Blockchains by incorporating many parties and the main nodes are initially and strictly selected. Permissioned Blockchain is suitable for semi-closed systems consisting of a few enterprises, often organized in the form of a consortium. The degree of data openness varies, usually involving access controls, defined by the consortium, to control access in both participants and information inside Blockchains. Even though the system is not fully opened, the benefits of decentralization can be partially gained. For example, the system has some degree of false tolerance in the event of some nodes acting maliciously. Hyperledger Fabric [37], Ripple [33] and Stellar [38] are examples of permissioned Blockchain implementations.

Although they are different in setting, all types of Blockchain share the following similarities regarding the benefits that Blockchain technology provides. (1) They operate on Peer-to-Peer (P2P) network that provides some degree of decentralization, (2) multiple nodes maintain the integrity of the ledger through consensus mechanisms, and (3) data are stored in Blockchain which provides immutability, even when some nodes are faulty or malicious [39]. We summarize the works in [17,27,41–43] with the comparison of the three Blockchain types given in Table 1. The following evaluation metrics are used: Cost per transaction, Performance, Trust of the system, Scalability, and Maintenance. This broad view captured by the table assists in visualizing capabilities of each type of Blockchain. The metrics are associated with three main factors of #1 the number of nodes, #2 how nodes are selected, and #3 the selection of consensus mechanisms. #1, #2, and #3 are referenced in Table 1.

(2) *Centralization and Decentralization:* In traditional centralized database systems, transactions are inherently trusted or endorsed through central trusted intermediaries that guarantee validity. This incurs additional cost and the performance becomes a big issue when using central servers. Blockchain technology is a promising solution to the distributed transaction management problems [41], being conducted among peers in P2P network. Public Blockchains exhibit in a fully decentralized setting, allowing trust of the transactions to be established among previous unknown or untrusted nodes. Private Blockchains work in a closed and trusted environment and employ access control techniques to achieve the same stance. The degree of decentralization is characterized by the node selection under the control of an owner. This setting is similar to traditional distributed database system. Like private Blockchains, Permissioned Blockchains operate in a trusted environment but have the higher degree of decentralization. Nodes are granted the membership status based on consortium policies. All nodes maintain Blockchain information, where no single entity has the full control of the system. All types of Blockchains share common benefits of decentralization in different degrees, which diminish the single point of failure and data integrity.

(3) *Persistency:* Transactions recorded in a Blockchain ledger is considered persistent as they spread across the network, where each node maintains and controls its records. As long as the majority of nodes are benign, persistency is persistently retained. Several properties are derived from this characteristic including transparency, and immutability (temper resistance). This transparency and immutability mean that Blockchains are auditable [25].

(4) *Validity:* Unlike some distributed systems, Blockchains do not require executions from each node. Transactions, or blocks, broadcasted in a Blockchain system would be validated by other nodes. So any falsification could be detected easily. This system consists of three major roles: (1) proposers who propose a value, (2) acceptors who validate and decide which value to be taken, and (2) learners who accept on the chose value [16].

(5) *Anonymity and Identity:* Anonymity is the main characteristic of public Blockchains. Identity in this system can be untied to a user real-world identity. One user can obtain multiple identities to avoid identity exposure [44]. There is no need for any central entity to maintain private information. As a result, according to the transaction information, the real-world identity cannot be obtained, preserving a certain amount of privacy. On the other hand, identity is usually required in the systems that are operated and governed by known entities in the settings like private and permissioned Blockchains.

(6) *Auditability.* Record timestamp and persistent information allow ones to easily verify and trace previous records through nodes in a Blockchain network. The degree of auditability depends on types of Blockchain systems and their implementations. Private Blockchains are the least auditable as nodes are administrated by one entity, permissioned Blockchains come second in which some agreements, such as encrypted data, may prevent information to be fully auditable, and public Blockchains are the highest as nodes are truly decentralized.

(7) *Closeness and Openness:* Opened Blockchains rely on public nodes to maintain records of transactions. Therefore, anyone can publish a transaction and join the system by following a set of rules and information inside this Blockchain is public. Permissioned Blockchains are considered semi-opened as nodes are pre-specified or validated before joining. They lie between public and private

Table 1
Evaluations of Public, Private, and Permissioned Blockchain Systems.

Type	Cost per Transaction #1, #3	Performance #1, #3		Trust of the Systems #1, #2, #3	Scalability #1, #3	Maintenance #1, #2	Openness #2
		Throughput	Latency				
Public	High	Low	High	High	High	Low	High
Private	Low	High	Low	Low	Low	Medium	Medium
Permissioned	Medium	Medium	Medium	Medium	Medium	High	Low

*The evaluation is assumed all systems operate in the same scale.
**The performance is inversely proportional to scalability [27].

Blockchains. Information inside this Blockchain is controlled by the policies of the consortium, which can regulate the information to be fully opened, partially opened, or closed. Like permissioned Blockchains, private Blockchains control how nodes are selected and the degree of data openness based on policies. However, they rely on a single entity or owner.

3.2. Business process characteristics

This section summarizes business process characteristics presented in [48] as follows.

(1) *Transient and Persistent:* Business workflow is said to be transient, or ad hoc, if it operates in a short time basis. In a common use case, the workflow instance terminates when its goals are accomplished. This characteristic exhibits in the situation where services are abundant and can be acquired when needed. It frequently interacts with previously unknown and usually distributed, autonomous, and heterogeneous services in a short period. Persistent workflow on the other hand repeats processes for the same objectives serveral times. This characteristic can be seen dating back to the old-fashioned business process like in traditional ERP systems such as payroll and automobile. Persistent characteristic can also be found in modern ERP where the changes of business workflows are not many, but the services executing workflow tasks may be selected dynamically.

(2) *Dynamic and Static:* A static, or dynamic, workflow is characterized by the change frequency. During workflow enactment, a static workflow has no change, or a few changes, while a dynamic workflow is dealing with constant changes throughout its lifetime [35]. In this context, the changes involve the change in sequences of tasks and branches inside a workflow structure, or the change of services that deliver functionalities for specific tasks. In opened environments, the latter brings about an important challenge in the aspect of service selection, composition, and replacement [45] as (1) services often reside in different distributed domains where changes of the services are uncertain, (2) services may provide similar functionalities with different QoS attributes, and (3) changes can introduce the instability of performance and security.

(3) *Workflow Formation and Enactment:* A workflow process can be divided in two stages. The first stage is workflow formation that establishes structure during planning and designing phrases. This includes activities such as process definitions, workflow structure (sequences of tasks and branches), service selection and composition, process controls, and analysis models [46]. The enactment stage occurs during workflow executions. The enactment activities generally include process scheduling, service interaction, monitoring, and real-time service evaluation and replacement. In opened environments, workflow enactment usually encounters dynamicity and uncertainties.

(4) *Centralized and Decentralized Management:* Centralized workflow management relies on a single centralized entity responsible for managing services, coordinating workflow tasks, and enforcing central policies throughout the workflow processes [47]. In the era

of cross-organizational business process where services are available and behave autonomously at distributed sites, centralized management is not effective. Localizing workflow management becomes an attractive solution by permitting each service, or a group of services in the form of consortium, ability to isolate from global policies' enforcement. However, coalitions of these services may introduce interoperability problems and trustworthiness of service vendors.

3.3. The relation of Blockchain and business process characteristics

This section discusses how Blockchain and its characteristics can improve business processes by identifying their relations to business process characteristics described in the previous section. There are many aspects in which Blockchain benefits can be realized in business processes.

(1) *Transient and persistent:* In either case, business process workflows require services to deliver functionalities to its internal tasks. There are two aspects of Blockchain technology to improve business processes that tend to rely on distributed and autonomous services. (1) Trust of services can be improved when implemented with Blockchain in which persistency, validity, and auditability can be inherently gained. Identity is necessary in the process of service selection. (2) Specialized Blockchain systems can be used to maintain QoS attributes of services and provides accesses to QoS information for service selection purpose. Permissioned Blockchain is a suitable choice where a group of entities are responsible for maintaining QoS ledgers. The QoS information can be opened or closed depending on consortium policies. Private Blockchains are questionable about trust, while public Blockchains face an obstacle regarding time inconsistency for confirmation settlement (also known as transaction finality).

(2) *Dynamic and static:* In opened environments, changes are common for businesses to optimize their processes to achieve better efficiency and cost effectiveness. Modern business processes become more dynamic and changes are very difficult to solved when multiple organizations are involved. The dynamicity in the aspect of services has been addressed by trust and QoS that Blockchain provides. However, changes in internal processes can introduce another trust issue, when changes from one organization may have cascade effect on another. Cross-organizational business processes must be opened by manifesting its business logics across involved parties. To obtain Blockchain benefits for process executions, smart contract can be employed where a business process can be encoded into smart contract transactions [66]. The business logic is closed to public but open for involved parties. Permissioned Blockchain fit in this context where the degree of decentralization varies depending on the number of involved parties. However, certain degree of persistency, validity, and auditability can be achieved.

(3) *Workflow formation and enactment:* Workflow formation is the stage when business workflow is constructed with process definitions. Enactment stage involved with process executions at runtime.

When many organizations are involves, Blockchain technology serves two purposes. (1) It is the repository for business process descriptions that guarantee the correctness of workflow structure and flow controls. This operation is simple, as we need only a special type of transaction to record static descriptions. And (2) after a business process workflow is instantiated as an instance, process executions will be generated and encoded into smart contracts [66,67], which guarantee operation validity as specified in the workflow descriptions. Since smart contract code is deployed and truthfully executed by external actors to change the state of a Blockchain ledger, abstracting business process descriptions and instances, which are stored as transactions, will directly gain Blockchain benefits. Specifically, a process workflow comprising tasks executed by multiple services can be coordinated by smart contracts operating on a Blockchain infrastructure. It also enables users to track the state of process instances from a global viewpoint.

(4) *Centralized and decentralized management:* As business processes become more distributed, centralized workflow management is facing major challenges in meeting the conflicting requirements of scalability, security, openness, and cost. Interoperation and integration of cross-organizational business processes rely on distributed, autonomous, and also heterogeneous services for task executions. However, one security issue of decentralized management is the trustiness of services, in which Blockchain technology becomes a vital role to establish trust as already mentioned. In either aspect, centralized management perhaps is able to gain Blockchain benefits by using private Blockchain configuration, while the configuration of decentralized management is more opened for either permissioned or public Blockchain.

In summary, cross-organizational business processes frequently involve several enterprises that form as a consortium. Permissioned Blockchain is a suitable choice for this setting. Since it is Blockchain-implemented, the benefits including persistency, validity, and auditability can be gained at some level depending on organizations (nodes) involved in a Blockchain network. The degree of closeness and openness varies as being mandated by consortium policies and other factors such as local law and regulations. Identity must be clear for authentication and authorization among involved organizations.

4. Architecture for Blockchain consensus in business processes

There exist multiple consensus protocols in asynchronous environment like the Internet. The selection of a consensus depends on assumptions and requirements of a system to be implemented. In the context of business processes, what we have to concern about selecting a consensus is the time used for transactions to be confirmed, known as transaction finality. However, FLP impossibility suggests that only two from three properties can be achieved in a distributed and asynchronous setting. This becomes problematic when a business process needs to interact with multiple Blockchain-implemented services.

For example, Bitcoin Proof-of-Work (PoW) and other Proof-of-X (PoX) are probabilistic protocols that guarantee liveness and fault tolerance but not safety, meaning that nodes might end up having different views of Blockchain ledger (forks) because of latency in propagation [17]. Therefore, Bitcoin would not guarantee finality; instead, a transaction will be confirmed after six blocks deep as suggested in [68], which takes about sixty minutes. Proof-of-Stake (PoS) is another popular consensus by which participants vote on new blocks weighted by their amount of currency held in the Blockchain. The leader is randomly elected to perform Block inclusion. This could cause a problem, as validators have to stake their tokens, which implies that they have to possess tokens in the system. Practical Byzantine False Tolerance (PBFT) by Castro and Liskov [23] is another class of consensus that runs on a system with a partially synchronous setting. It offers both liveness and safety and also provides some degree of false tolerance where at

most $\left\lceil \frac{n-1}{3} \right\rceil$ out of total n exhibit Byzantine false. However, scalability is a major concern, which polynomially increases, $O(n^2)$, to the number of nodes.

There are pros and cons on different classes of consensus, which will be impractical for business process operations. What we concern in the context of business process is time and trust of the nodes who perform consensus processes. Time in this context is the amount of time between the moment of a transaction being produced and the moment when it is confirmed. Trust of the nodes is relatively a new issue to be addressed. In a very distributed setting mostly in public Blockchains, if majority of nodes are benign, the consensus is inherently trusted. However, permissioned Blockchain involves limited nodes to perform consensus. Trusting these nodes is unavoidable and perhaps risky. Existing protocols do not allow users to express their requirements regarding which nodes are authorized, or preferred, to execute for their consensus. This will be problematic if a Blockchain system contains a group of collusive nodes to produce bias results.

We argue that because business processes can be encoded into smart contracts, the executions of the contracts should be performed and also reach its consensus by a group of nodes agreed by users (business partners). Business processes usually involve multiple organizations and Blockchain systems should allow them to select nodes for performing consensus. The idea is achievable by using Blockchain smart contracts.

Fig 1 illustrates a system architecture. PBFT is chosen as it guarantees safety, liveness, and some degree of fault tolerance. PoW is impractical since the confirmation settlement is too long and unreliable. The scalability problem of PBFT is solved since the system allows business partners to agree on the nodes, which are subset of the node universe in a Blockchain system. In addition, the confirmation settlement is the matter of milliseconds [23,49]. This is practical for business process operations especially the time-critical ones.

The architecture is divided into two layers: (1) the business process layer managed by business management technologies including, business management system, service selection and composition, service workflow specification languages [50–53,61–63], and compliance checking [54–58] for real-time monitoring, and (2) the Blockchain of Business Processes layer where business processes are encoded into smart contracts. The nodes variable in this smart contract indicates nodes to perform consensus. Any *function()* with keyword *consensus* will notify a Blockchain system about nodes and the system should be implemented to restrict that only authorized nodes can perform consensus. *emit* and *event* keywords are responsible for logging Blockchain internal consensus operations such as recording a leader from the nodes in each round as part of PBFT algorithm. Other nodes outside the ones responsible for consensus will receive a block with validated transaction from the consensus nodes. They will perform validation and chain a new block into their main chain if everything is correct.

Our intention at this stage is to present an approach in solving problems regarding time inconsistency and bias that may occur in current consensus mechanisms. The architecture is present and the focal point is on the Blockchain of Business Processes that encodes business processes into Blockchain smart contracts. In the future, we plan to implement a prototype to realize our architecture and also develop metrics for evaluations.

5. Conclusion

Blockchain technology has revealed its great potential to innovate business processes. The properties of persistency, validity, auditability, and disintermediary that Blockchain offers can greatly improve modern business processes to achieve digitalization, automation and transparency. However, efforts spent for integrating Blockchain into business processes is still at infancy. This paper takes an initial step to define Blockchain and investigates the characteristics of Blockchains with
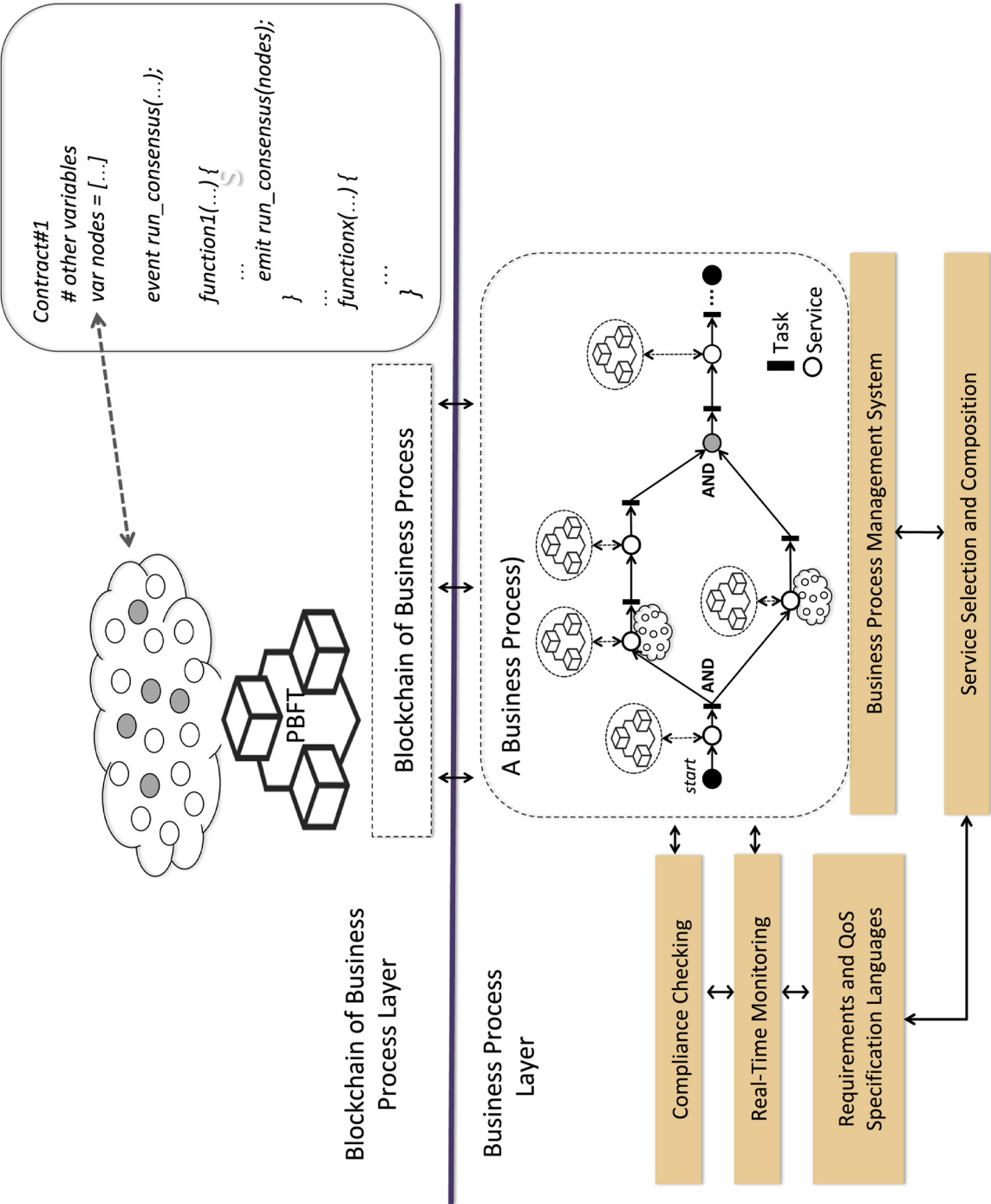
```
Contract#1
# other variables
var nodes = [...]

event run_consensus(...);

function1(...) {
    ...
    emit run_consensus(nodes);
}
...
functionx(...) {
    ...
}
```

PBFT

Blockchain of Business Process

A Business Process)

start

AND

AND

■ Task
○ Service

Business Process Management System

Service Selection and Composition

Compliance Checking

Real-Time Monitoring

Requirements and QoS Specification Languages

Blockchain of Business Process Layer

Business Process Layer

Fig. 1. A system architecture for consensus based on selected nodes.

respect to business processes. Then, based on the characteristics, we propose an architecture consisting of key technologies and guidelines to the innovation of business processes in Blockchain era. The core elements of our architecture is the use of PBFT with smart contracts to overcome the problem of time inconsistency regarding confirmation settlement and also the bias that may arise about nodes responsible for performing consensus. This makes the consensus more flexible and reliable, which better reacts to user requirements in the area of business process interoperation.

References

[1] N. Satoshi, Bitcoin: A peer-to-peer electronic cash system, Available: https://bitcoin.org/bitcoin.pdf, Accessed on 23rd of January 2018.

[2] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of Blockchain, Future Gener. Comput. Syst. (2017) 1–13.

[3] Z. Hess, Y. Malahov, J. Pettersson, Æternity blockchain: the trustless, decentralized and purely functional oracle machine, White Paper (2017) Available https://aeternity.com/aeternity-blockchain-whitepaper.pdf Accessed on 23rd of January 2018.

[4] A. Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, A Case Study for Blockchain in Healthcare: Medrec Prototype for Electronic Health Records and Medical Research Data, 2016, 2016 White paperAvailable https://www.media.mit.edu/publications/medrecwhitepaper/ Accessed on 23rd of January 2018.

[5] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: using blockchain for medical data access and permission management, International Conference on Open and Big Data, OBD, 2016, pp. 25–30.

[6] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, J. Med. Syst. (2016) 218, https://doi.org/10.1007/s10916-016-0574-6.

[7] S. Huckle, R. Bhattacharya, M. White, N. Beloff, Internet of things, blockchain and shared economy applications, Proc. Comput. Sci 98 (2016) 461–466.

[8] P. Bylica, Ł. Gleń, P. Janiuk, A. Skrzypczak, A. Zawłocki, A probabilistic nano-payment scheme for golem, Available, 2015. http://golemproject.net/doc/GolemNanopayments.pdf.

[9] P. Hurich, The virtual is real: an argument for characterizing bitcoins as private property, in: Banking & Finance Law Review 31 Carswell Publishing, 2016.

[10] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for Iot security and privacy: the case study of a smart home, in: IEEE Percom Workshop on Security Privacy and Trust in the Internet of Thing, 2017.

[11] Y. Zhang, J. Wen, The IoT electric business model: using blockchain technology for the internet of things, Peer Peer Netw. Appl. (2016) 1–12.

[12] J. Sun, J. Yan, K.Z. Zhang, Blockchain-based sharing services: what blockchain technology can contribute to smart cities, Financ. Innov. (2016), https://doi.org/10.1186/s40854-016-0040-y.

[13] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A.B. Tran, S. Chen, The blockchain as a software connector, in: The 13th Working IEEE/IFIP Conference on Software Architecture, WICSA, 2016.

[14] E. Nordstr.m, Personal Clouds: Concedo (Master's thesis), Lulea University of Technology, 2015.

[15] J.S. Czepluch, N.Z. Lollike, S.O. Malone, The use of block chain technology in different application domains, in: The IT University of Copenhagen, 2015.

[16] M. Correia, G.S. Veronese, N.F. Neves, P. Verissimo, Byzantine consensus in asynchronous message-passing systems: a survey, Int. J. Crit. Comput. Based Syst. 2 (2) (2011) 141–161.

[17] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, G. Danezis, Consensus in the age of Blockchains, Available: Accessed on 23rd of January https://arxiv.org/pdf/1711.03936.pdf, (2018) Accessed on 23rd of January.

[18] Y. Li, Z. Luo, J. Yin, L.D. Xu, Y. Yin, Z. Wu, Enterprise pattern: integrating the business process into a unified enterprise model of modern service company, Enterp. Inf. Syst. 11 (1) (2015), https://doi.org/10.1080/17517575.2015.1053415.

[19] A. Meidan, J.A. Garcia-Garcia, M.J. Escalona, I. Ramos, A survey on business processes management suites, Comput. Stand. Interfaces 51 (2017) 71–86.

[20] H. Ariouat, C. Hanachi, E. Andonoff, F. Benaben, A conceptual framework for social business process management, Procedia Comput. Sci. 112 (2017) 703–712.

[21] F. Rahimi, C. Moller, L. Hvam, Business process management and IT management: the missing integration, Int. J. Inf. Manage. vol. 36, (1) (2016) 142–154.

[22] G. Bracha, S. Toueg, Asynchronous consensus and broadcast protocols, J. ACM (JACM) 32 (4) (Oct. 1985) 824–840.

[23] M. Castro, B. Liskov, Practical Byzantine Fault Tolerance, in the Proceedings of the 3rd Symposium on Operating Systems Design and Implementation, New Orleans, USA, February, 1999.

[24] 19 Industries The Blockchain Will Disrupt [Online], Available: http://futurethinkers.org/industries-blockchain-disrupt/, Accessed on 5th of February 2018.

[25] C. Hammerschmidt, Consensus in Blockchain systems. In Short, Available: https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe, Accessed on 5th of February 2018.

[26] A. Baliga, Understanding Blockchain consensus models, White Paper (2017).

[27] M. Vukolc, The quest for scalable Blockchain fabric: proof-of-work vs. BFT replication, Proc. IFIP WG 11.4 Workshop Open Res. Problems Netw. Secur.

[28] (iNetSec), 2015, pp. 112–125.

[28] L. Lamport, R. Shostak, M. Pease, The Byzantine generals problem, ACM Trans. Prog. Lang. Syst. 4 (3) (1982) 382–401 July.

[39] N. Lynch, M. Fischer, R. Fowler, A simple and efficient Byzantine generals algorithm, In Proceedings of the 2nd Annual IEEE Symposium on Reliability in Distributed Software and Database Systems, IEEE, New York, 1982, pp. 46–52.

[30] Hyperledgers Sawtooth lake aims at a thousand transactions per second. Available: https://www.altoros.com/blog/hyperledgers-sawtooth-lake-aims-at-a-thousand-transactions-per-second/, Accessed on 5th of February 2018.

[31] Lazooz Available: http://lazooz.org, Accessed on 5th of February 2018.

[32] LemonWay, Available: https://www.lemonway.com/en/, Accessed on 5th of February 2018.

[33] Ripple: The world's only enterprise blockchain solution for global payments, Available: https://ripple.com/, Accessed on 5th of February 2018.

[34] Ethereum Blockchain App Platform, Available: https://www.ethereum.org/, Accessed on 5th of February 2018.

[35] Z.M. Qiu, Y.S. Wong, Dynamic workflow change in PDM systems, Comput. Ind. 58 (2007) 453–463 June.

[36] V. Buterin, A next-generation smart contract and decentralized application platform, White Paper (2014).

[37] Hyperledger Architecture, Volume 1, Available: https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf, Accessed on 5th of February 2018.

[38] Stellar, Available: https://www.stellar.org/, Accessed on 5th of February 2018.

[39] P. Jayachandran, The difference between public and private blockchain, Available: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/, Accessed on 5th of February 2018.

[40] L.D. Xu, W. Viriyasitavat, A novel architecture for requirement-oriented participation decision in service workflows, IEEE Trans. Indus. Inf. 10 (2) (May 2014) 1478–1485.

[41] T.T.A. Dinh, J. Wang, G. Chen, R. Liu, B.C. Ooi, K.-L. Tan, BLOCKBENCH: a framework for analyzing private blockchains, Proc. of the ACM International Conf. on Management of Data, 2017, pp. 1085–1100.

[42] J. Garzik, Public versus private Blockchain. Part 1: permissioned Blockchain, White paper, BitFury Group, 2015.

[43] K. Croman, C. Decker, I. Eyal, A.E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gün, On scaling decentralized blockchains, In Proc. 3rd Workshop on Bitcoin and Blockchain Research, 2016.

[44] K. Yeow, A. Gani, R.W. Ahmad, J.J.P.C. Rodrigues, K. Ko, Decentralized consensus for edge-centric internet of things: a review, taxonomy, and research issues, IEEE Access vol. 6, (2018) 1513–1524.

[45] S.D. Ramchurn, D. Huynh, N.R. Jennings, Trust in multi-agent systems, Knowl. Eng. Rev. 19 (1) (2004) 1–25.

[46] R.A. Botha, J.H. Eloff, A security interpretation of the workflow reference model, in: R.v. Solms, J.H. Eloff (Eds.), in Proceedings of WG 11.2 and WG 11.1 of IFIP TC11, 2 Sep 1998, pp. 43–50 vol. 2 of Information Security – from Small Systems to Management of Infrastructures, (Vienna, Austria).

[47] N. Kuntze, A. U.Schmidt, Z. Velikova, C. Rudolph, Trust in business processes, in Proc. 9th International Conference for Young Computer Scientists, 2008, pp. 1992–1997 2008. ICYCS 2008., (Hunan, China)IEEE Computer Society.

[48] W. Viriyasitavat, A. Martin, In the relation of workflow and trust characteristics, and requirements in service workflows, in: A. Abd Manaf, A. Zeki, M. Zamani, S. Chuprat, E. El-Qawasmeh (Eds.), ICIEIS 2011, Part I. CCIS, 251 Springer, Heidelberg, 2011, pp. 492–506.

[49] H. Sukhwani, J.M. Martnez, X. Chang, K.S. Trivedi, A. Rindos, Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric), 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), 2017, pp. 253–255 Sept.

[50] W. Viriyasitavat, A framework of trust in service workflows, PhD dissertation, Dept. of Computer Science, University of Oxford, Oxford, 2013.

[51] W. Viriyasitavat, A. Martin, Formal trust specification in service workflows, Proceedings of IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing, 2010, 2010, pp. 703–710.

[52] W. Viriyasitavat, A. Martin, Formalizing trust requirements and specification in service workflow environment, in: Proc. ICEIS (2011) 196–206.

[53] W. Viriyasitavat, L. Xu, A. Martin, SWSpec: the requirement specification language in service workflow environments, in: IEEE Trans. Ind. Inf. 8 (3) (2012) 631–638.

[54] W. Viriyasitavat, A. Martin, An improvement of requirement-based compliance checking algorithm in service workflows, Proc. Int. Conf. Adv. Inf. Technol. (AIT), UACEE, Bangkok, Thailand, 2012, pp. 41–45.

[55] L.D. Xu, W. Viriyasitavat, P. Ruchikachorn, A. Martin, Using propositional logic for requirements verification of service workflow, in IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 639–646, Aug. 2012.

[56] W. Viriyasitavat, L.D. Xu, W. Viriyasitavat, A new approach for compliance checking in service workflows, in: IEEE Trans. Ind. Inf. 10 (2) (2014) 1452–1460.

[57] W. Viriyasitavat, L.D. Xu, W. Viriyasitavat, Compliance checking for requirement-oriented service workflow interoperations, in: IEEE Trans. Ind. Inf. 10 (2) (2014) 1469–1477.

[58] W. Viriyasitavat, Multi-criteria selection for services selection in service workflow, J. Ind. Inf. Integr. 1 (2016) 20–25.

[59] W. Viriyasitavat, L. Xu, Z.M. Bi, A. Sapsomboon, Blockchain-based business process management (BPM) framework for service composition in Industry 4.0, J. Intell. Manuf. (2018), https://doi.org/10.1007/s10845-018-1422-y online published.

[60] W. Viriyasitavat, Modeling delegation in requirements-driven trust framework, 2009 Congress on Services - I, Los Angeles, CA, 2009, pp. 522–529.

[61] W. Viriyasitavat, A. Martin, The reviews and analysis of the state-of-the-art service

workflow specification languages, J. Ind. Inf. Integr. 8 (2017) 1–7.

[62] W. Viriyasitavat, L.D. Xu, Z.M. Bi, A. Sapsomboon, Extension of specification language for soundness and completeness of service workflow, Enterp. Inf. Syst. 12 (5) (2018) 638–657.

[63] W. Viriyasitavat, L.D. Xu, Z.M. Bi, The extension of semantic formalization of service workflow specification language, IEEE Trans. Ind. Inf. (2018), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8294213.

[64] W. Viriyasitavat, A. Martin, A survey of trust in workflows and relevant contexts, IEEE Commun. Surv. Tutorials 14 (3) (2012) 911–940. Third Quarter.

[65] L. Xu, E. Xu, L. Li, Industry 4.0: state of the art and future trends, Int. J. Prod. Res. 56 (8) (2018) 2941–2962, https://doi.org/10.1080/00207543.2018.1444806.

[66] L. García-Bañuelos, A. Ponomarev, M. Dumas, I. Weber, Optimized execution of business processes on Blockchain, in: J. Carmona, G. Engels, A. Kumar (Eds.), Business Process Management. BPM 2017. Lecture Notes in Computer Science, 10445 Springer, Cham, 2017.

[67] O. L´opez-Pintado, L. Garcia-Banuelos, M. Dumas, I. Weber, Caterpillar: a Blockchain-based business process management system, Proceedings of the BPM Demo Track and Dissertation Award (BPM 2017), 2017.

[68] J. Bonneau, How long does it take for a Bitcoin transaction to be confirmed? Available: https://coincenter.org/entry/how-long-does-it-take-for-a-bitcoin-transaction-to-be-confirmed, Accessed on April 9 2018.