Blockchain and Smart Contract Solutions for Internet of Things Systems: A Systematic Review

***Abstract*—Internet of Things systems pose various technical problems, especially in the area of device management and security. Blockchain (BC) and Smart Contract (SC) systems have been integrated into IoT systems as solutions for the problems that they pose.**

In this paper, we present a systematic literature review on the integration of Blockchain and Smart Contract into IoT systems. We approach this topic from three perspectives: (i) the problems posed by IoT systems that call for BC and SC solutions, (ii) the specific way that BC and SC systems have been integrated into IoT systems, and (iii) optimisations done on BC and SC systems so that they can work with the constrained computing resources in IoT systems. Our review covers 90 research works. From these works, we identify real problems of IoT systems that have been addressed by BC and SC in these works. We also identify how BC and SC have been integrated into these IoT systems, as well as optimisation on individual components and architecture of a whole BC system so that it can work with IoT systems.

While prediction and ideas on how BC can be integrated and solve IoT problems have been discussed a lot in different mediums, from research writing to technical magazines; this paper is different in the sense that it derives these knowledge directly from the real works that have been conducted instead of prediction and anticipation. Comparing to some existing reviews on the topic, our review covers more perspectives, more articles, and also conduct in a more systematic way.

For IoT system engineers, this paper provides a catalogue of problems in IoT systems that have been addressed by BC and SC solutions. It also shows how the integration of BC and SC into IoT system has been conducted, and present some optimisation that has been conducted to enable such integration. For IoT researchers, this paper provides an overview of the landscape of IoT problems that have been addressed by BC technologies. Such overview helps to identify areas in IoT that would benefit from additional BC integration. For BC researchers, this paper provides an overview of how BC has been adapted and applied to IoT problems. Such an overview helps them to identify potential improvement so that BC can serve IoT systems better.

***Keywords*-Internet of Things, Blockchain, Smart Contract, Systematic Literature Review**

I. Introduction

Blockchain (BC) is a core component behind the emergence of cryptocurrency. This terminology can denote a distributed, potentially public, ledger which stores all transactions in a cryptographically-chained blocks [1], or the protocol that enables the distributed ledger. BC allows distributed peer-to-peer network among non-trusting members, in which they can interact with each other in a verifiable manner without relying on a trusted intermediary [2]. Due to these features, blockchain has been applied to logistics, smart cities [3], smart homes [4], vehicular networks [5], and more fields. In a tactical environment, blockchain allows distributed information sharing, immutable and auditable information, and consensus of information.

A. What is this work?

Review of Blockchain and Smart Contract solutions to problems of IoT systems. It includes:

- Collection and classification of problems posed by IoT systems
- Collection and classification of solutions based on BC and SC technology to solve those problems
- Collection and classification of optimisation done to fit BC and SC systems into limited resources of IoT systems.

Results of this review can be used as a play book to apply BC and SC in systems with similar problems as IoT

B. Why do this work?

IoT systems are important, with impacts in many areas in life

- Health care
- Home automation
- Infrastructure management
- City management
- Agriculture
- Business and supply chain

Problems posed by IoT systems are relevant in other types systems:

- Centralised storage of data
- Integrity of data at rest and in-transmission
- Integrity of low-power hardware nodes
- Data ownership
- Data and control distribution (to the edge)

Potentially relevant types of systems: tactical systems that involve low-power wireless nodes and operate on unreliable, untrustworthy networks. Examples:

- TEXAS
- Security operation systems, if we consider endpoint- and intrusion-detection systems as sensors

Research on Blockchain and SC solutions for IoT exploded. In the past several years. [First paper year? Current number? Growth per month? Per year?]

A systematic collection and classification of BC-SC solutions for IoT can be used as a play book for not just IoT but relevant systems.

For BC-SC researchers, this review helps:

- Identify problems in IoT systems that have not been addressed
- Identify gaps in the existing BC-SC research
- Help to align research on BC-SC for IoT

For IoT researcher, this review helps:

- Bring BC-SC solutions to solve problems of IoT systems.
- Learn about the possibilities enabled by BC-SC systems

For practitioners (IoT system designers and developers):

- Provide information on how BC-SC have been applied to solve similar problems to their systems. It provides a starting point for further analysis and applications.

II. Research Method

A. Systematic Literature Review method

Guided by research questions

Systematic search for articles

1) Systematic selection of articles: Based on inclusion / exclusion criteria

Cross-validation

2) Systematic extraction of data from articles: Based on predefined extraction templates

Templates are generated based on the information need, defined by the research questions

Synthesis into new insights

Report the findings

B. Research questions

1) RQ1: What problems of IoT systems do BC-SC works address?: **What is the overall objective?**

Add new functionality?

Improve a certain quality attribute?

What is the technical problem that this work addresses to reach the objective?

Relations between technical problem and objective tend to be many to many.

2) RQ2: How have BC-SC been used to solve problems of IoT systems?: **How do BC-SC fit into IoT systems?**

Which functional component of IoT systems do they replace or add?

How are BC-SC deployed within computing infrastructure of IoT?

Cloud, fog, or edge?

What kind of BC-SC node on what kind of hardware?

How do BC-SC designed and implemented?

Functional decomposition?

Ledger and smart contract?

Access right?

Implementation tech?

3) RQ3: How have BC-SC been optimised to work in IoT systems?: What are the perceived problems of using BC-SC in IoT?

How do these problems addressed?

C. Selection (reported in the paper)

What query? Why?

What source? Why?

What criteria? Why?

1) Statistics of the selected papers: Visualisation of the data

Where to get the papers?

D. Extraction

1) For RQ1: **Improvement objective**

New functionality

Improve quality attributes (Use ISO/IEC 25010 software quality taxonomy)

Technical problem

2) For RQ2: **For 2.1**

Affected IoT components

Deployment Perspective

Types of nodes

Miner

Full node

Light weight node

Web client

Deployment location

Cloud

Fog

Edge

For 2.2

Functional Decomposition Perspective

Key generation mechanism (create wallet)

Key-pair for whom?

Which algorithm?

Key management mechanism

Wallet (managing private key)

Association service (mapping key to entity)

Transaction dissemination mechanism

Code Execution Mechanisms

Bitcoin script

Ethereum Virtual Machine

Block generation mechanism

Block dissemination mechanism

Consensus protocol

Transaction validation rule

Block validation rule

Block creation rule

Proof-of-*

Ledger and Smart Contract Perspective

Ledger Structure

Blockchain

Tangle

Shared state

UTXO

Account state

On-ledger data

On-ledger contract

Off-ledger data

Access Perspective

Read right

Transaction generation right
Block generation right
Code execution right
Anonymous participant
Implementation Perspective
What technology or library?
3) For RQ3: BC-SC problems
BC-SC optimisations

E. Synthesis

1) Iterative and incremental: Batches of 15
Update model after each batch
Based on new data
Based on previous model
Random check with a paper in previous batches for consistency
Random cross-validation by co-investigators

III. Background

A. IoT System

1) What is ...: **IoT system?**
Generate insights and actions from data and events sent by devices.
Devices
Tag
Sensor
Actuator
Resources
Services
Virtual Entity
Value proposition of IoT?
Collecting real world data
Analysing real world data
Acting on real world data
What are different parts of them (i.e., logical architecture)? (in the paper)
Deployment architecture of IoT system? (in the paper)

B. Blockchain

1) What is blockchain?: Cryptographically secured
Transactional singleton machine
Move to the next state by transactions
All users share a same machine (singleton)
With shared state
State of the singleton machine is available for everyone
How does it work?
What are different parts of it?
What is so good about it?

C. Smart Contract

What is smart contract?
How does it work?
What is so good about it?

IV. Findings (TBA)

A. RQ1

Improvement Objective
Technical problem

B. RQ2

1) 2.1: Affected IoT component
Deployment within IoT infrastructure
2) 2.2: Functional decomposition
Consensus protocol
Ledger and Smart Contract
Access Control
Implementation
RQ3

V. Discussions (TBA)

References

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, pp. 557–564.

[2] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[3] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of things, blockchain and shared economy applications," in *Procedia Computer Science*, vol. 58, pp. 461–466.

[4] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, pp. 618–623.

[5] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-vn: A distributed blockchain based vehicular network architecture in smart city," *Journal of Information Processing Systems*, vol. 13, no. 1, pp. 184–195, 2017.