Internet of Things (IoT) in Blockchains and Smart Contracts

Sruthi Maria Abraham
PG Student
Department of Computer Science & Engineering
Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, Kerala, India

Abstract—Blockchains allow us to have distributed peer-to-peer network where untrusted members can interact each other without a trusted intermediary in a verifiable manner. In this paper, motivated by recent explosion around blockchain, examines whether they make good fit for IoT sector. Also reviews how this mechanism works and also look into smart contracts-scripts that reside on the blockchain that allow for the automation of multi-step processes. For blockchain-IoT combination: 1) facilitates the sharing of services and resources leading to the creation of a marketplace of services between devices and 2) allows us to automate in a cryptographically verifiable manner several existing, time-consuming workflows. This paper also point out certain issues that should be considered before the deployment of a blockchain network in an IoT setting: from transactional privacy to the expected value of the digitized assets traded on the network. The blockchain-IoT combination is powerful and can cause significant transformations across several industries, paving the way for new business models and novel, distributed applications.

Key words: Blockchains, Internet of Things (IoT), Smart Contracts

I. INTRODUCTION

BLOCKCHAINS enables the creation of smart contracts, with terms and conditions both sides can specify and that assure trust in the enforceability of the contract and identity of the counterparty. Blockchains have recently attracted the interest of stakeholders across a wide span of industries: from finance and healthcare to utilities real estate and the government sector. The reason for this explosion of interest: With a blockchain in place, applications that could previously run only through a trusted intermediary, can now operate in a decentralized fashion, without the need for a central authority, and achieve the same functionality with the same amount of certainty. This was simply not possible before.

Also say that the blockchain enables trustless networks, because the parties can transact even though they do not trust each other. The absence of a trusted intermediary means faster reconciliation between transacting parties. The heavy use of cryptography, a key characteristic of blockchain networks, brings authoritativeness behind all the interactions in the network. Smart contracts -self-executing scripts that reside on the blockchain-integrate these concepts and allow for proper, distributed, heavily automated workflows. This should make blockchains enticing to researchers and developers working in the Internet of Things (IoT) domain.

Of course the transition to a decentralized network may not always make sense. On top of that, even if such a transitions desirable, the application’s requirements may be such that a blockchain-based network cannot fulfil them. Blockchains and smart contracts bring a slew of advantages to the table, but as they also come with a bag of disadvantages.

The goal of this work is to provide a detailed description of how blockchains and smart contracts work, to identify the pros and cons that their introduction brings to a system, and highlight the ways the blockchains and IoT can be used together. This will allow them to identify potentially new use cases for their IoT work, and also make educated decisions when integrating a blockchain in their project.

The paper is structured as follows. Explains what a blockchain is, it’s working and how smart contracts allow us to radically redefine how interactions between transacting parties on a network can be set up and automated. End the section with a taxonomy for blockchains. Examines into how IoT and blockchains can be used together, and highlight existing IoT-on-the-blockchain applications. Also note down the issues that the IoT developer/researcher would need to keep in mind when deploying a blockchain-based solution for their and ends with conclusions.

II. LITERATURE SURVEY

A. Double Spending

Double-spending is a result of successfully spending some money more than once. Bitcoin protects against double spending by verifying each transaction added to the blockchain to ensure that the inputs for the transaction had not previously already been spent. Other electronic systems prevent double-spending by having a master authoritative source that follows business rules for authorizing each transaction. Bitcoin uses a decentralized system, where a consensus among nodes following the same protocol is substituted for a central authority. Bitcoin has some exposure to fraudulent double-spending when a transaction is first made, with less risk as a transaction gains confirmations. Blockchain was introduced with Bitcoin to solve the double-spending problem.

1) Risk Management

There are third-party services to assist traders and merchants to help manage the risk or to insure against losses.

2) Attack Vectors

Includes Race attack, Finney attack, Vector76 attack, Brute force attack, >50% attack.

III. PROPOSED SYSTEM

A. Blockchains

A blockchain is a distributed data structure that is replicated and shared among the members of a network. It was introduced with Bitcoin to solve the double-spending problem. Each block is identified by its cryptographic hash. Each block references the hash of the block that came before it. This establishes a link between the blocks, thus creating a chain of blocks, or blockchain. Each block in the chain...
carries a list of transactions and a hash to the previous block. The exception to this is the first block of the chain (not pictured), called genesis, which is common to all clients in a blockchain network and has no parent as shown in Fig. 1. Any node with access to this ordered, back-linked list of blocks can read it and figure out what is the world state of the data that is being exchanged on the network.

A node can generally act as an entry point for different blockchain users into the network, but for simplicity, we assume that each user transacts on the network via their own node. These nodes form a peer-to-peer network where:

1) Users interact with the blockchain via a pair of private/public keys.
2) The neighboring peers make sure this incoming transaction is valid before relaying it any further; invalid transactions are discarded.
3) The transactions that have been collected and validated by the network using the process above during an agreed-upon time interval, are ordered and packaged into a time stamped candidate block. This is a process called mining.
4) The nodes verify that the suggested block:
   - Contains valid transactions, and
   - References via hash the correct previous block on the chain.

When each node in the network follows the steps listed above, the shared blockchain it operates on becomes an authenticated and time-stamped record of the network's activity.

The nodes do not have to trust any other entity, giving rise to the term trustless environment; instead, trust is achieved as an emergent property from the interactions of different participants in the system.

Assume that Alice knows Bob's public key. She signs a transaction that modifies her row, decreasing the value of X by 2, and creates a new row, whose "owner" is set to Bob's public key, and whose "asset type" and "value" fields are set to "X" and "2" respectively. Alice transferred 2 units of X to Bob by creating a new row with that information and assigning it to him; see Fig. 2. Bob's new balance of asset "X" can be calculated by aggregating all the rows in the database that correspond to his public keys, and whose "asset type" is set to "X". Same goes for Alice.

A transaction then basically deletes a set of rows (UTXO) and creates a set of new rows (UTXO) in the database. These existing, not-yet-deleted rows are called unspent transaction outputs (UTXO) in Bitcoin. The UTXO that a transaction consumes are called transaction inputs; the UTXO that a transaction creates are called transaction outputs.

C. Smart Contracts

Smart contract is a computerized transaction protocol that executes the terms of a contract as in Fig. 3. Smart contracts are contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system. The potential benefits of smart contracts include low contracting, enforcement, and compliance costs; consequently it becomes economically viable to form contracts over numerous low-value transactions. The potential risks include a reliance on the computing system that executes the contract. At this stage, the risks and benefits are largely theoretical because the technology of smart contracts is still in its infancy, and some time away from widespread deployment. Smart contracts operate as autonomous actors, whose behavior is completely predictable.

Characteristics of smart contracts are the following:

1) The contract has its own state and can take custody over assets on the blockchain.
2) The contract allows us to express business logic in code.
3) A smart contract is triggered by messages/transactions sent to its address.
4) A smart contract is deterministic; the same input will always produce the same output.
5) Since all the interactions with a contract occur via signed messages on the blockchain, all the network participants get a cryptographically verifiable trace of the contract's operations.

Smart contracts also give rise to the concept of "decentralized autonomous organizations" (DAOs), entities on the blockchain whose behaviour may be modified, if a certain process that is encoded in the contract.
D. Blockchain Taxonomy

There are several ways to categorize a blockchain network. A blockchain gives us the following benefits:

1) A robust, truly distributed peer-to-peer system that is tolerant of node failures.
2) A network that can identify conflicts and forks and resolve them automatically so as to converge to a single, globally accepted view of events.
3) Transparency, verifiability, auditability on the network's activity.
4) A method for tagging different pieces of information as belonging to different participants, and enforcing this form of data ownership without a central authority.
5) A system that allows non-trusting participants to interact with each other in a predictable, certain manner.

E. Blockchains and IoT

All the IoT devices of a manufacturer operate on the same blockchain network. The manufacturer deploys a smart contract that allows them to store the hash of the latest firmware update on the network. The devices either ship with the smart contract's address baked into their blockchain client.

![Image](45x350 to 550x510)

**Fig. 4:** Asset tracking example using smart contracts and IoT.

Or they find out about it via a discovery service. They can then query the contract, find out about the new firmware, and request it by its hash via distributed peer-to-peer file system. The first requests for this file will be served by the manufacturer's own node (also taking part into the network), but after the binary has propagated to enough nodes, the manufacturer's node can stop serving it. Assuming the devices are configured so as to share the binary they got, a device that joins the network long after the manufacturer has stopped participating in it, can still retrieve the sought-after firmware update and be assured that it is the right file. This all happens automatically, without any user interaction. Compare and contrast with the centralized scenario where the device polls the manufacturer's server for an update and gets a 404 error.

The usefulness of blockchains in an IoT setting does not stop there. Consider the typical supply chain example that is used to highlight the value of a blockchain: a container that leaves the manufacturer's site (point A), gets transported via railway to the neighbouring port (point B), then gets shipped to the destination port (point C), gets transported again to the distributor's facilities (point D), until it finally reaches the retailer's site (point E). This process involves several stakeholders and checks along the way, all of them depicted in Figure 4 (a).

![Image](524x28 to 556x42)

Each stakeholder usually maintains their own database to keep track of the asset, which they update based on inputs from the other parties along the chain. A blockchain network though that is set up to track this asset would mean that there is now one shared database to keep track of, where updates come with cryptographic verifiability, get propagated along the network automatically, and create an auditable trail of information.

In Fig 4 (b), focus on the B-C stage. The carrier of the container performs a handshake with the dock at the destination port (C) to confirm that the container is delivered to the expected location. Once that handshake is completed, it posts to a smart contract to sign the delivery. The destination port follows along to confirm reception. If the node at C does not post to the contract within an acceptable timeframe, the shipping carrier will know and can initiate an investigation on the spot. When the shipping carrier reaches the destination port, they send a signed message allowing everyone on the chain to know that the container is now at point C. Since the transaction is signed, it acts a cryptographically verifiable receipt of the shipping company's claim that the container has reached the destination port. The receiver at the port posts the same smart contract to confirm that it is in possession of the container.

F. Deployment Considerations

Here, identify several issues that may come up when IoT makers experiment further with blockchains, and have their IoT devices participate in a blockchain network.

In a blockchain, each node performs the same task leaving no room for parallel task execution, i.e. we do not have sharding. This situation is even more pronounced in blockchains that do smart contracts because of the concurrency issues. Work towards shardability is being done for at least one major blockchain platform, though aworking and tested implementation is still ways off.

Maintaining privacy on the blockchain is a complicated issue. A participant does not need to know everybody else's key; they just need the key of their transacting counterparty. However, all the transactions in a blockchain happen in the open. By analyzing this data, an interested party can identify patterns and create connections between addresses, and in the end make informed inferences about the actual identities behind them. In the case of private blockchains, it is advisable to not use the same blockchain for all transactions if another participant may get a competitive advantage by tracking your device's activity.

Another issue to consider when in a blockchain network is deciding on the miner set.it can prevent a new, valid transaction from being added to the blockchain, effectively censoring it. The nodes of the mining set need to be selected wisely so that the chances of collusion between them are minimized. In a private network, legal contracts should be signed so that collusions are penalized appropriately.

Legal enforceability of smart contracts is limited. A way to increase the chances of legal enforceability is to include a reference to the actual real-world contract in the smart contract, and vice versa. This is a process called “dual integration” and it works as follows:
1) Deploy the smart contract, record its address on the blockchain, and include that address in the real contract.

2) Hash the corresponding real-world contract, record its hash digest, store the real contract in a safe space (can be centralized, or decentralized).

3) Send a transaction to the smart contract that includes the real contract’s hash in its metadata; the contract then stores that piece of information in its own, internal database.

Tangential to this is the issue of the expected value of tokenized assets. Blockchains are used to trade these tokens because they are associated with some value.

Complete Autonomy is a Double-Edged Sword.

A blockchain network may also need the following mechanisms to complement its functionality:

- A DNS service that holds pointers to resources.
- Secure communication and file exchange.

IV. CONCLUSION

The combination of blockchains and IoT can be pretty powerful. Blockchains give us resilient, truly distributed peer-to-peer systems and the ability to interact with peers in a trustless, auditable manner. Smart contracts allow us to automate complex multi-step processes. The devices in the IoT ecosystem are the points of contact with the physical world. When all of them are combined we get to automate time-consuming workflows in new and unique ways, achieving cryptographic verifiability, as well as significant cost and time savings in the process.

ACKNOWLEDGEMENT

The author would like to thank everyone who supported to do this study and also thankful to Mount Zion College of Engineering and KTU for giving a platform to do this work.

REFERENCES
