WHITE PAPER

IoT and Blockchain

Securing data pertaining to IoT devices is becoming important. With traditional client-server architectures being vulnerable to cyber-attacks, Blockchain distributed ledger technology can be used to store records of transactions between devices in a secure manner. By providing the ability to verify the origin of a physical device, Blockchain can curtail fraud and encourage the customer to enter into genuine, trusted transactions.

Blockchain platforms are either private or public or private. Ethereum™ is a popular public Blockchain platform with tools that can be used to build Blockchain applications for IoT. Blockchain as a Service (BaaS) is also now available from leading cloud services vendors such as AWS® and Microsoft® Azure®.

THINXTREAM®

Introduction

As Internet of Things (IoT) deployments increase across industries worldwide, securing data pertaining to IoT devices is becoming important. Traditional client-server architectures are vulnerable to cyber-attacks due to their single point of security intelligence on the server. A decentralized and distributed alternative provides a verifiable, secure and permanent method of recording data generated by these smart devices. Businesses that relied on expensive, complex data security systems can now rely on open source and vendor-neutral technologies like Blockchain.

Blockchain is a distributed ledger technology that secures the transaction between two end-users without the need for intermediaries. While it has been used extensively to store cryptocurrency transactions, it can also be used to store records of transactions (financial and non-financial) between devices in a secure manner.

In this white paper, we examine the challenges faced by the industry concerning IoT data security, how it can be solved with Blockchain and some use-cases of Blockchain in IoT.

IoT Security Challenges

In 2016, distributed denial of service (DDoS) attacks on as many as 100,000 IoT devices exposed the inadequacy of IoT security. Distributed client-server designs that use a central authority to manage IoT devices, along with all the data generated across an IoT network offered a single point of security failure. Architectural limitations prevented IoT devices from making security decisions without the support of the central authority, leading to a single point of decision-making that is prone to security failure. This calls for a distributed and decentralized security architecture that is resilient to failure.

While traditionally transactions have been maintained and validated with the help of intermediaries, this is an expensive proposition for the massive scale of operations in IoT. This calls for a scalable technology solution, which can algorithmically validate the transaction and automatically determine fraudulent sources at zero or minimal cost.

When data is held by a single business entity, there are chances that it can be manipulated and falsified. It is quite important to maintain the integrity of the data so that any modifications of the original data can be algorithmically and independently derived, agnostic to who owns the data.

As IoT deployments involve devices and software from multiple vendors, it is often impractical to agree on a single solution or a vendor for implementing IoT security. Such implementations will lead to silos, duplication and maintenance chaos. This calls for a standardized, vendor-neutral, democratized (no single owner) approach that can be easily integrated into IoT devices and software.

Last, but not the least, to reap the benefit of a truly-connected and self-reliant IoT system, we need to empower IoT devices/applications to execute commercial transactions on behalf of humans. The system should handle responsibility issues when IoT devices/applications take actions based on an operation that is automatically executed by a chain of linked applications from different entities in the ecosystem.

Blockchain Benefits

Blockchain is a decentralized design that creates a secure, democratized platform independent of all involved entities. Blockchain removes the single point of decision-making and hence a single point of security failure by enabling networks to protect themselves by allowing participating nodes to form group consensus about what is normal and abnormal, and quarantining any nodes that behave unusually.

Use of encryption and distributed storage would result in data being trusted by the concerned entities. Machines will autonomously and securely record details of transactions that take place between IoT devices, with no human intervention. These records will be immutable once recorded.

Data here is automatically replicated in multiple nodes and access to it can be controlled. It can be a private permission-based Blockchain as well as publicly accessible. All data stored is signed and each device is accountable for its actions.

There is no single entity exclusively holding the records since data is replicated in multiple nodes owned by multiple entities. No one entity can modify or delete the data. All participating nodes have an identity secured by a public key. This ensures protected communication and builds trust in the overall network.

Most of the data associated with IoT is personal and this has to be shared with external applications to derive value from it. Unfortunately, this increases opportunities for hackers to attack. Blockchains provide an additional level of security as they are built on top of robust encryption standards available today.

In the IoT environment, we need to empower devices to make transactions on behalf of humans. Blockchains allow the creation of agreements called 'smart contracts', which get executed when specific conditions in the contract are triggered. These conditions could indicate delivery of a service and on the execution of a contract, one system could make a payment to the other securely without any human intervention.

Blockchain Programming

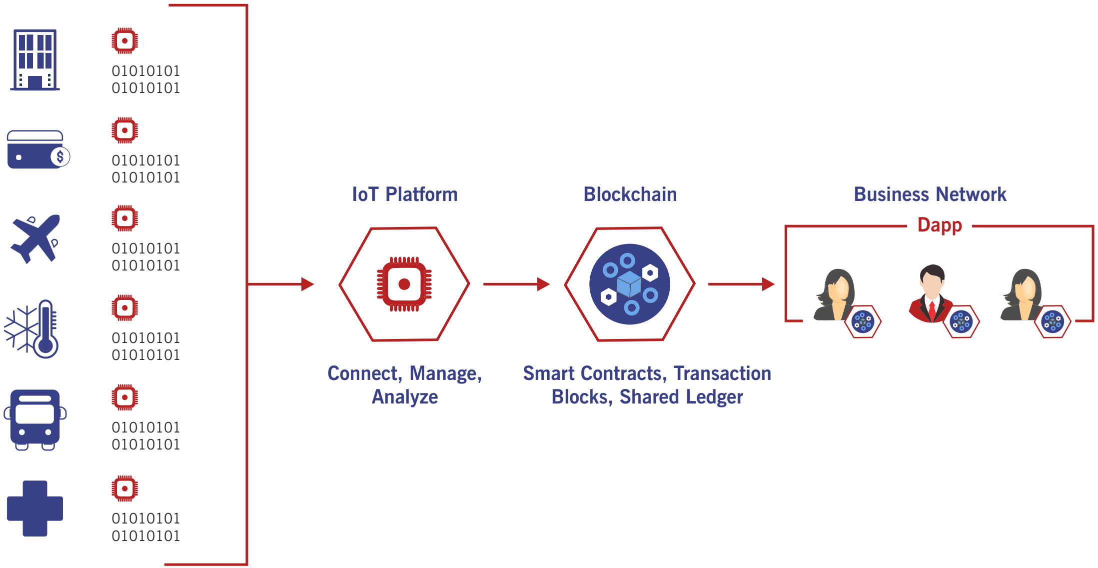

Figure 1. Decentralized Blockchain based IoT Application

Programming Terminologies

- Dapp is a decentralized application that runs on a decentralized peer-to-peer network owned by multiple entities in a trustless protocol setup. It is not controlled by any single entity on the network. BitTorrent®, Popcorn Time, Bitmessage, Tor®, are all decentralized applications that run on a peer-to-peer network, but not on a Blockchain. A smart contract connects decentralized apps to Blockchain. Traditional Web apps and decentralized Blockchain apps differ as indicated below when it comes to software development:

  - Traditional Web apps: Front End → API → Database
  - Dapp enabled Web apps: Front End → Smart Contract → Blockchain

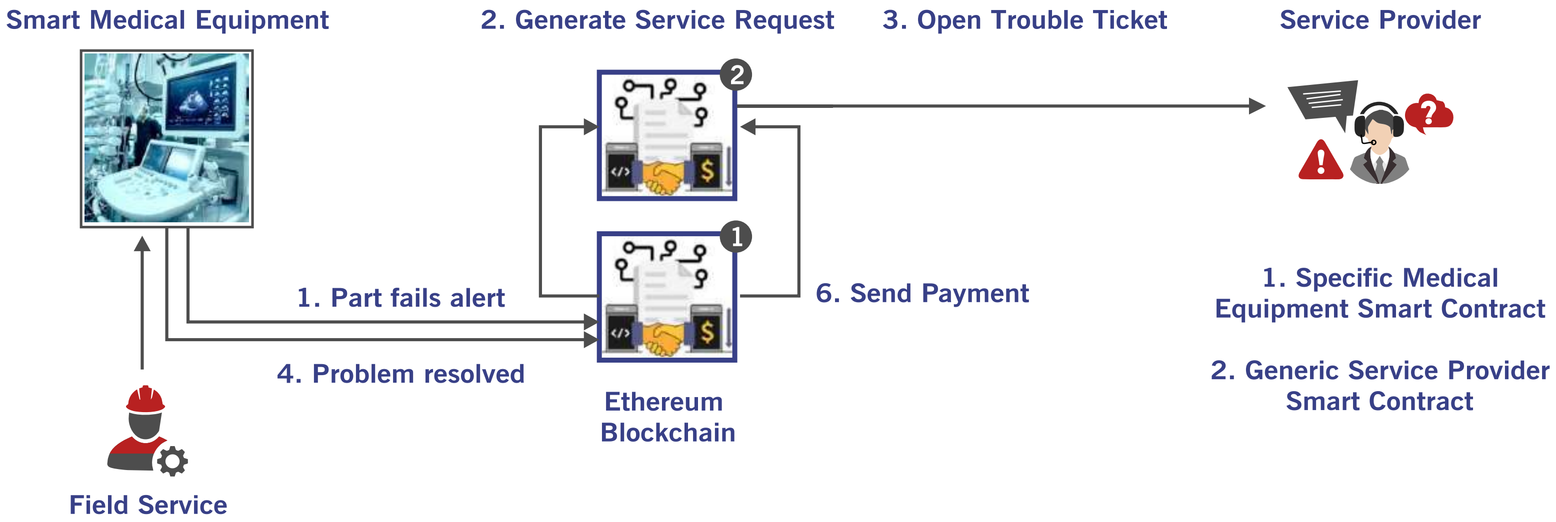

Figure 2. Smart Contract and Field Service

- Smart Contract is a software program on the distributed ledger, allowing an immutable, verifiable and secure record of all contracts and transactions. The typical lifecycle of a Smart Contract includes:

  - It records the terms of a contract between two direct entities on a Blockchain shared between all participants and validated by validators. Regulators and auditors keep a tab on the system through read-only access to Blockchain.
  - It connects with the external world to collect trigger points – e.g., account balance, stock prices, etc.
  - It waits for external triggers to evaluate pre-defined conditions. When the conditions are met, this contract self-executes. Transactions are recorded on Blockchain.
  - It provides data for compliance and reporting when needed.

Platforms & Development Tools

Blockchain platforms are either private or public.

Private platforms are for limited and defined number of users. They are more useful in industrial and niche sectors where a limited number of entities take part.

In public platforms, all users and applications share the entire ledger. There are currently three main public Blockchain platforms: Bitcoin, Hyperledger™ and Ethereum. Most applications are built on these.

We will restrict our discussion in this section to only Ethereum.

Ethereum provides developers with a foundation, which allows them to write a smart contract and decentralized applications. This enables developers to create their own custom rules for ownership, transaction formats, and state transition functions. Smart Contracts are written in either Solidity™, Serpent, or LLL. The Ethereum development ecosystem typically comprises the following tools and technologies:

- A virtual machine that stores Blockchains and executes Smart Contracts.
- A Web-based IDE 'Remix' aimed at Solidity. This allows developers to check out code from GitHub and Swarm, compile, deploy and run Smart Contracts on customized environments like a JVM or Web3.JS.
- A test network/node like the popular Ganache™ CLI that offers a personal Blockchain on which developers can deploy Smart Contracts, develop applications, and run tests. (A test network/node is required as Blockchain is immutable by design and every Smart Contract update has to be deployed as a new instance.) Ganache is available for Windows®, Mac®, and Linux® flavors as both, a desktop application as well as a command-line tool. Using Ganache, you can see the status of accounts, debug using logs and configure mining.
- A CLI based Ethereum development tool such as Truffle. It enables smart contract compilation, linking, automated contract testing, deployment and binary management.

- As the code in Blockchain typically deals with money, analyzing code for security and storage is of paramount importance. Solium™ is a solidity code linter that works like an interpreter, continuously checking code for style and security issues.
- Browsers enable users to see the state of accounts, receipts, and transactions. Mist is one of the popular browsers that offers the ability to create wallets, and deploy smart contracts, send and receive transactions, and store ether. MetaMask™ is another tool which turns Google Chrome™ into an Ethereum browser. It fetches data from the Blockchain and enables users to securely send or receive signed transactions.
- Decentralized Finance (DeFi), a significant ecosystem within the Ethereum economy, offers an alternative worldwide financial system with cryptocurrencies that hold a stable value ("stablecoins"), for any realistic payment use-case.
- In recent advancements, as enterprises look to deploy the Blockchain technology, popular cloud platform vendors have launched Blockchain as a Service (BaaS) offerings that allow customers to leverage cloud-based solutions to build, host and use their own Blockchain apps, smart contracts, and functions on the Blockchain.

Blockchain as a Service (BAAS)

Blockchain as a Service (BaaS) is a cloud-based Blockchain service offering that enables you to develop, use and host your Blockchain apps, functions and smart contracts on the cloud, while the service provider manages to keep the infrastructure operational and agile.

By utilizing BaaS, enterprises benefit from improved transparency and accountability, data security and trust minimization without having to develop their own Blockchain ecosystem or invest in expensive in-house computing resources. It holds the promise of accelerating Blockchain adoption.

BaaS capabilities include:

- Identity -based consensus mechanism instead of proof–of-work or proof-of-stake,
- Block monitoring and explorer tools, and
- Permissioned Blockchains

Some BaaS providers include Azure, AWS, IBM®, EDF, Alibaba, Oracle®, and Corda™.

Amazon Managed Blockchain

Amazon® Managed Blockchain provide a fast and easy way to create and deploy secure Blockchain networks using popular open source frameworks. They enable you to focus on building your Blockchain applications instead of setting up your Blockchain network.

AWS Blockchain Templates deploy the Blockchain framework chosen by you as containers directly on an Amazon EC2® instance running Docker®, or on an Amazon Elastic Container Service (ECS) cluster.

AWS supports Ethereum and Hyperledger Fabric. Every framework offers distributed consensus algorithms, smart contract functionality and access control features. In addition, AWS Blockchain Templates includes components to manage, monitor, and browse your Blockchains.

Azure Blockchain Service

Blockchain as a Service on Azure provides a rapid, low-cost, low-risk platform for building and deploying Blockchain applications. It provides several easy-to-deploy, enterprise-ready templates for the most popular ledgers, including Ethereum, Quorum, Hyperledger Fabric, Corda, etc.

Azure Blockchain consists of single-node, multi-node ledgers and tools for development of decentralized applications distributed on a Blockchain.

Azure Blockchain infrastructure allows you to:

- Setup secure environment that exposes protected endpoints. This can be done via Azure Virtual Networks, Azure App Services VNet Integration or Network Security Groups.
- Develop smart contracts using the available development tools, such as Blockstack Core, Ethereum Studio or Truffle.
- Automate deployment of participant components, both virtual machines and Platform-as-a-Service components using Azure Resource Manager and PowerShell scripts.
- Protect access to data and logic, with user-level authentication and authorization, by implementing Azure AD to secure apps and APIs.

In summary, you can build an architecture for enterprise-grade, decentralized Blockchain solution, leveraging Azure enterprise capabilities and worldwide distribution.

Blockchain in IoT

By providing the ability to verify the origin of a physical device, Blockchain can curtail fraud and enable the customer to enter into genuine, trusted transactions.

In the healthcare industry, tags on packaging and Blockchain can assure the quality of medical supplies along the entire supply chain as well as identify counterfeiting. Similarly, personal fitness and diagnostic data collected from wearables can be securely logged in Blockchains.

In the food industry, where products are sensitive to environmental factors like temperature, containers could carry thermometers whose values could be recorded in Blockchains at key locations. This can ensure that the maximum temperature is not breached on the way from producer to consumer.

In the case of the automotive and airline industry, Blockchains could be used to securely log performance and maintenance data. This data can be used for predictive maintenance and product improvements.

Insurance companies can use the data logged by sensors in cars in Blockchains before accidents to ensure fraud-free processing of claims by customers.

In 'chain of custody' applications such as logistics, where shipments move from one entity to another such as shipper to customs, Blockchains can quickly and accurately track a product.

Using smart contracts, smart devices could autonomously execute transactions with no human oversight. A vending machine could solicit bids from distributors and pay for the delivery of new items automatically. Smart appliances and vehicles could diagnose, schedule and pay for their maintenance. Home appliances could optimize their operations by syncing with lower grid prices and reducing the cost of electricity to consumers.

Conclusion

Blockchains are creating a revolution in the digital economy through cryptocurrency. With the increasing adoption of IoT, there is a challenge in securing collected user data and Blockchain is proving to be a good fit. The robustness of Blockchain results in applications like Smart Contracts wherein transactions are automatically carried out by devices when a specific condition is met with no human intervention. This enables innovative non-financial applications like tracking the origin of a good to prevent counterfeiting, recording environment factors of a perishable commodity from producer to consumer to ensure quality, chain of custody applications, feeding data for predictive maintenance, etc. Blockchains help in trust building, cost reduction, accelerated data exchanges and increased security. Popular Blockchain platforms like Ethereum, Hyperledger, and BaaS from cloud services vendors such as AWS and Azure provide the test and development infrastructure and tools to build Blockchain solutions.

As an IoT services provider, Thinxtream has the expertise to assess, architect and implement Blockchain use cases for IoT. We can help implement Blockchain applications for your current offerings and build decentralized apps on top of IoT platforms using available libraries, managed services and tools from Blockchain technology providers. By leveraging the IoT expertise built over a decade, Thinxtream ensures cost-effective, quality and timely delivery of IoT solutions.

References

- Blockchain And The Internet Of Things: 4 Important Benefits Of Combining These Two Mega Trends
- At the Intersection of Blockchain and IoT, Don't Get Run Over
- How Will Blockchain Impact the Internet of Things?
- IoT application for Blockchain
- When IoT met Blockchain
- Best Ethereum Development Tools To Create Dapps

Thinxtream Technologies is a global software company with a portfolio of innovative software platforms, components, solutions, patents, competences and services for Internet of Things (IoT) across several industry verticals and applications, successfully enabling leading customers, including Fortune 500 companies, meet their application, product and business goals.

Interested in learning more? For more information contact:

Thinxtream Technologies Pte. Ltd.
220 Orchard Road #05-01
Midpoint Orchard
SINGAPORE 238852
Phone: +65 66358625
Email: info@thinxtream.com

Thinxtream Technologies, Inc.
10260 SW Greenburg Road
Suite 400 Portland, OR 97223
U.S.A.
Phone: +1 971 230-0729
Email: info@thinxtream.com

www.thinxtream.com

LinkedIn/thinxtream

TT-WP-007-3-1220

THINXTREAM®