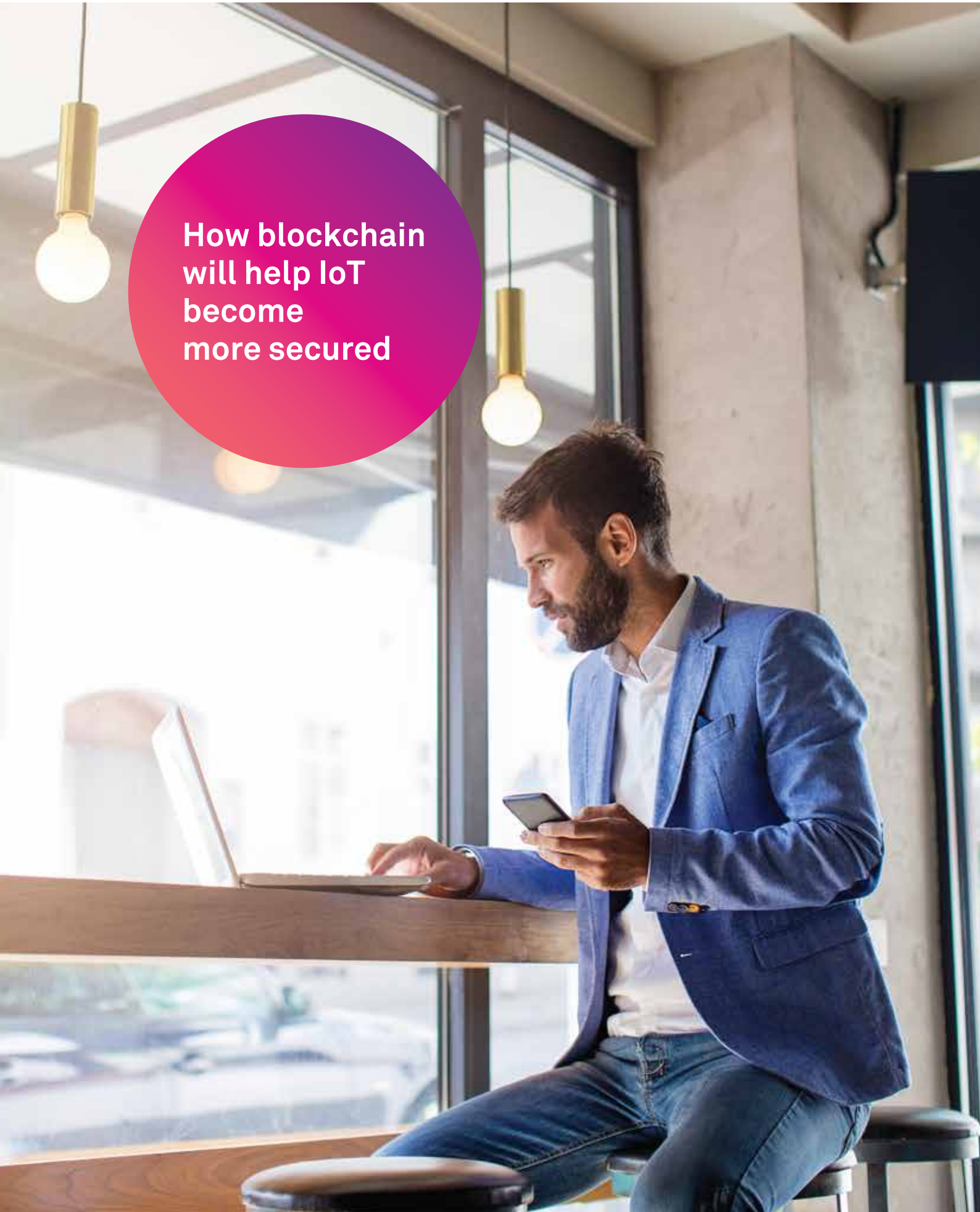

# How blockchain will help IoT become more secured

In today's age of rapid technological transformation, IoT is playing a pivotal role in bringing together all the devices and things in the world and connecting them to the internet. All the transactional information associated with IoT is the driving force behind the success of IoT. Since information is the key to IoT, its security holds high significance. Any breach of information or data stealing not only leads to malfunctioning of devices associated with IoT but can further pose a threat to life or assets. Hence the need for securing IoT, by ensuring proper security of data and information.

Currently, to ensure the trustworthiness of IoT data, all the information is collected at a unique location, which means a single point of security intelligence, hence, a single point of failure. This is highly risky. A decentralized approach to IoT networking has the capability to remove the single point of failure of decision-making by enabling IoT device networks to develop an effective defense mechanism by which these devices can be allowed to form consensus for identifying what is normal within a given network, and thereby isolating any nodes over blockchain that behave in an unusual manner. Secondly, blockchain has the capability to form trust in IoT data by enabling digital security primitives: availability, auditability, accountability, integrity and confidentiality.

## Blockchain ensures better security of IoT

Blockchain as a distributed ledger for various IoT transactions can have data that is digitally signed and any changes made therein can be traced back, which is auditable. Numerous IoT devices over a network can be connected and spread over distributed fabric where all the IoT transactions like registration, sharing of resources, authentication, authorization, alert etc., can be written in ledger and remain unaltered. Any change in the transaction can be easily tracked. This ensures security.
A permissioned blockchain allows consensus & permissioned membership services.
Decentralized ledger allows data to be stored & spread everywhere. It is transparent and accessible to users.

As an example: Blockchain like Hyperledger Fabric functions as a distributed transaction ledger for various IoT transactions as depicted in the below diagram.

The Hyperledger Fabric functions as a distributed transaction Ledger for various IoT transactions

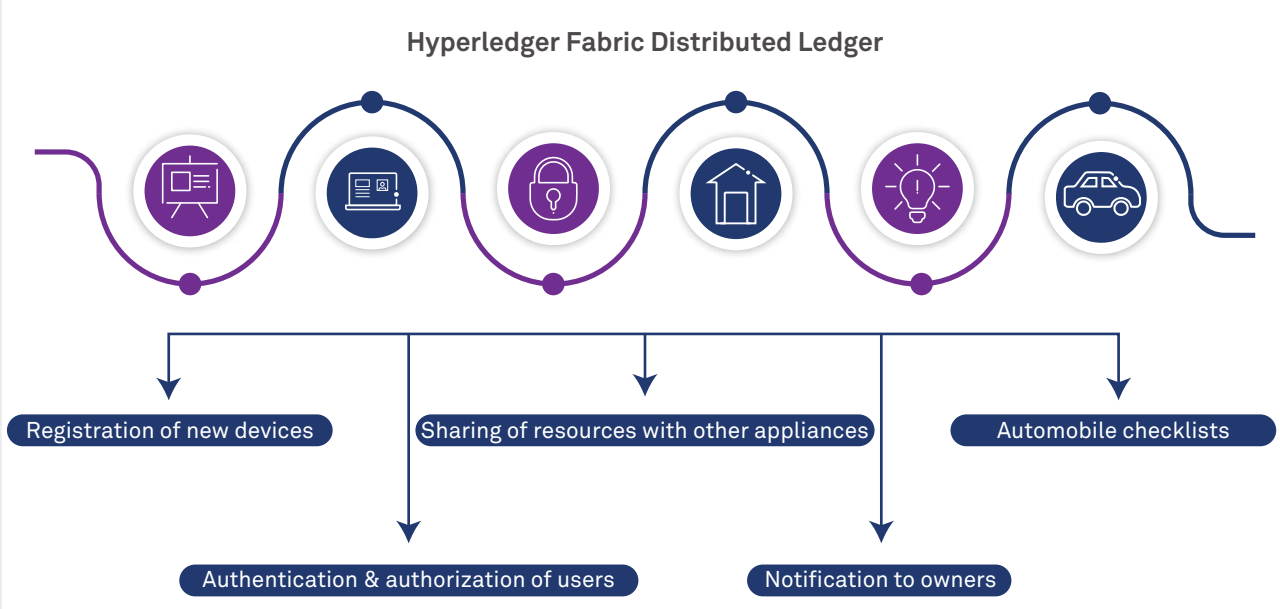


Figure 1: Hyperledger Fabric as a Distributed Ledger

**Blockchain and IoT together have a disruptive potential of decentralization, removal of 3rd party validation, non-repudiation of transactions and anonymity of identity.**

This decentralized security model will be easy and far less expensive in terms of scaling, maintaining and managing. Most importantly, it will not have a single point of failure. With the exponential increase in devices, it becomes quite difficult to identify, authenticate and secure devices. With the introduction of blockchain, authentication and identification of devices will be secured over distributed database technology. Each IoT node can be registered and authenticated in the blockchain and will have a unique ID and address. Thus, it will help in unique identification of the device. If any device wants to connect with another device, it will use its unique blockchain ID and its local blockchain wallet to raise a request. The wallet will create a unique digitally signed request using a key and send it to the target device, which in turn will use blockchain services to validate the signature using the public key of the sender. This is how machine to machine authentication can happen without the need for any centralized support system.

The decentralized and trusted ledger concept and capabilities of blockchain are necessary to enable and facilitate various regulatory compliances and requirements for industrial IoT applications.

**How IoT is more secure with blockchain w.r.t the current IoT solution?**

| | Current Solution of IoT | Blockchain-based IoT Security |
|---|---|---|
| 1 | **Security -** Data chunks are not encrypted and easy to read and access. | Data chunks are encrypted in blockchain, integrity protected, digitally authorized and authenticated. |
| 2 | **Trust -** Risk of leaking of owner key or password. | Even in case where the owner's key is leaked, blocks cannot be modified due to blockchain immutability (except for block in the current break). |
| 3 | **Upgrade & Update -** Lack of guarantee that the software embedded in each device (e.g., firmware, scripts) is always up-to-date and satisfies regulations and security requirements of the network. | The integration of IoT systems with blockchain technologies (like smart contracts) can help to improve the security of IoT systems by automatically-updating IoT device firmware to remedy vulnerable breaches. |

### IoT powered by Blockchain ensures better scalability, performance & trustworthiness

Blockchain technology will not only help in tracking millions of connected devices, but at the same time also enable these devices to process transactions and coordinate among each other with better scalability and performance. This decentralized approach would invariably create a more resilient ecosystem for devices to run on. Use of blockchain will truly help execute financial transactions, without the need for a centralized party or intermediaries. This type of autonomy is possible because the nodes in the blockchain will authenticate the transaction without relying on a centralized authority.

The IoT is vulnerable to a wide variety of network attacks that undermine its confidentiality, integrity, authentication and availability. Blockchain already implements several mechanisms including data security, data integrity, authentication, public/private encryption, hashing, consensus and fault-tolerance whose effectiveness in terms of security have been widely investigated and verified w.r.t many networking scenarios. The combination of blockchain and IoT has disruptive potential in terms of helping IoT's expansion in our society by providing multiple advantages including decentralization, absence of third-party validation, non-repudiation of transactions and anonymity of identity.

To sum up, blockchain can serve as a tool to both log data in a form highly resistant to tampering, and to fight the introduction of malicious IoT devices into networks and this can complement IoT systems with the improved privacy and security. The most common IoT applications nowadays over blockchain can be witnessed in the areas of smart energy, smart environments, robotics, transportation, and supply chain.

According to a recent report published by Gartner, there will be 20.4 billion connected IoT devices, almost three per person, in 2020. While the upcoming 5G also promises to provide unprecedented speed and scale to IoT operations, it brings along a new generation of security threats. Moreover, traditional security models optimized for 4G/LTE cannot fit neatly to address 5G-enabled IoT, especially in areas like edge-focused processing, the vast distribution of decentralized, small-cell networks. Under such a scenario, blockchain technology will thus emerge as the most effective next-generation technology since it is appropriately suited to respond to both the challenges and opportunities of a 5G-enabled IoT. However, we need to address the various issues (e.g. slow performance, scale) faced by blockchain technology before integrating it with IoT, as 5G rollout will encompass an explosion in transactions between these devices.

Scalability, security and decentralization are prerequisites to any blockchain-based IoT network, and deficiencies in any of these three areas could be catastrophic for users and would undermine the purpose of using such a protocol. Hence, IoT networks will have more limited use until there is some alternate design to achieve high throughput over blockchain without sacrificing security or decentralization.

## References:

https://bit.ly/2n6ltNc

**Gautam Sarkar**
Vice President, Global IT Practice &
Solutions Head, Communications BU,
Wipro Ltd.

Gautam is a business & technology leader with 25+ years of telco experience in handling Business, Presales, Large Digital Transformation Program Delivery, Domain Consultancy, E2E Solution Architecting, Practice Development, Product Engineering and Innovation. He played a vital role in setting up Wipro's India and ME Telecom Business, Telco Shared Service Centre, multiple E2E green field Telco IT rollouts and leading IT outsourcing large engagement. In his current role, he is leading Global IT Practice, Technology Solutions and Innovations. As a passionate technologist, he has been creating platforms, solutions and frameworks for adoption of new technologies and enabling digital experience.

**Subrat Saurabh**
Principal Consultant, Blockchain &
Telco Domain Expert, Communication BU,
Wipro Ltd.

Subrat has more than 12 years of experience in Technology Solutions, domain consultancy and B/OSS large delivery transformation. He has been instrumental in developing Blockchain-led platforms and solutions for telcos.

**Wipro Limited**
Doddakannelli, Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
**wipro.com**

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**

IND/B&T/OCT2019-MAR2020