# Blockchaining IoT

by

Anthony Darden

Varun Dass

Karis Kim

Poitier Pognon

Kennesaw State University

Author Note

Correspondence concerning this article should be addressed to Anthony Darden, Department of CCSE, Kennesaw State University, Marietta, GA 30060. Contact: adarde11@students.kennesaw.edu

# Abstract (Anthony)

Internet of Things (IoT) is a network of smart devices that connect via the internet. The proliferation of IoT devices exhibits a trend toward constant connectivity and interdependency. Consumers are attracted to these devices for reasons such as convenience, efficiency, monitoring, and even fitness. As IoT networks expand, so do the capabilities of connected devices. However, IoT networks suffer from security, and to a lesser extent, connectivity issues. Specifically, security as it relates to data validity during network transport. The focus of this paper is to perform a survey on the use of blockchain technology in IoT networks. An explanation of blockchain technology is presented to justify why it is a good fit for IoT networks. Next, blockchain network architecture is examined to depict how decentralized networks improve IoT network security. Lastly, smart contracts are discussed as a method of data validation in IoT block-chained networks.

*Keywords*: IoT, blockchain, security

## Table of Contents

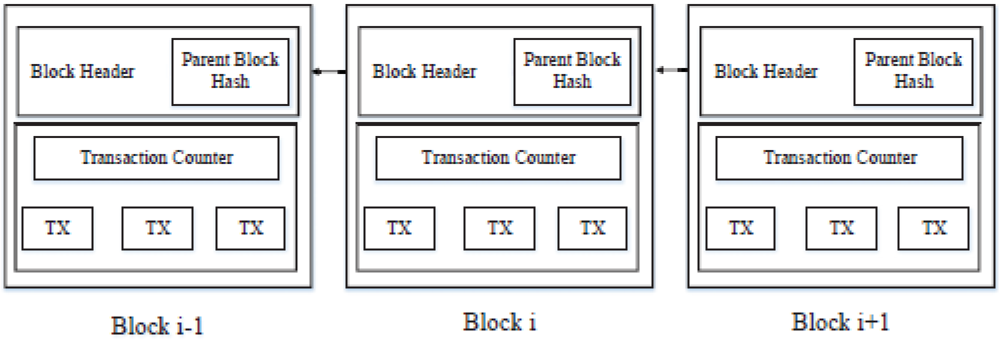
## Blockchaining IoT (Anthony)

IoT devices such smart phones, computers, refrigerators and other internet connected devices enables collection of data variety and volume. Data collection and access are a highly debated topic; however there remains a bigger issue: security. The recent data breaches at Target, Bank of America and other large corporations exploit network vulnerabilities via unsecured devices, prompting need for better security mechanisms. With IoT's rapid growth, device security is integral to overall network security. However, according to Banafa (2017), "functionality becomes the main focus and security takes a back seat" when it comes to IoT. Since security is not a priority in IoT devices, it makes it easier for "cyber criminals to probe for security vulnerabilities and then install malicious malware to control devices" (Department of Justice, 2017). IoT's security issues are only exasperated by network growth, which "will defy the very structure of current communication models and the underlying technologies" (Banafa, 2017). Current network structure, a centralized, client/server architecture, is insufficient for IoT, with connected devices numbering in the billions. The ever-rising number of connected smart devices creates a bottleneck on centralized networks, increasing resource expenditure (Banafa, 2017). Future IoT networks will require an alternate network structure capable of handling growth. Blockchain is a form of decentralized digital ledger technology proposed to enhance IoT security (McGrath, 2018). This network scheme is mostly used in cryptocurrency, but has gained traction in other industries including finance, health, and real estate (McGrath, 2017). Implementation of blockchain technology on IoT networks not only improves network security, but also aids in transaction validity.

## What is Blockchain? (Karis)

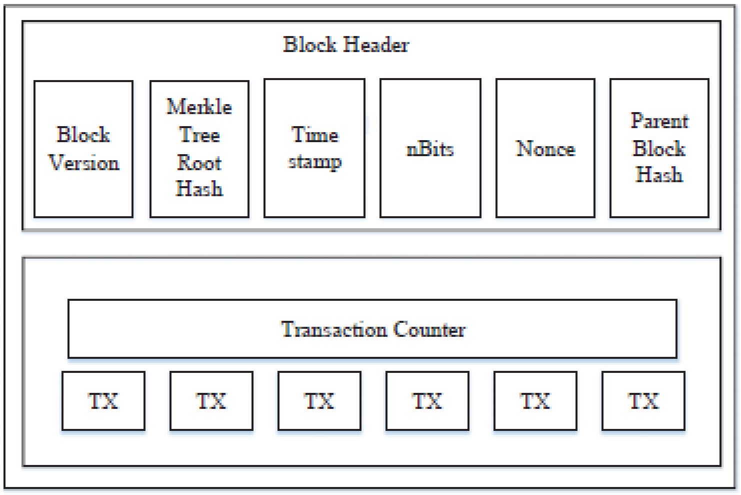
Blockchain is series of logical blocks in which each block carries a list of transaction records like those found in a traditional public ledger (Zheng et al., 2017). Each block is composed of a header and a block body and contains multiple transactions. The very first block is called the genesis block. All subsequent blocks contain a hash of the previous block in the header. The previous block is called the parent block. The parent block hash points the current block to the previous block and links or “chains” the blocks together, giving the name “blockchain” to this architecture. In addition to the parent block hash, the header also contains the block version, the hash of transactions in the block, the timestamp, nBits, and Nonce (Makhdoom et al., 2018; Zheng et al., 2017). The block body contains a transaction counter and the transactions.  The size of a block determines the count and size of the transactions that can be contained in the block.

Figure 1. Chain of blocks in a blockchain.



*Reprinted from Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Retrieved November 21, 2018, from https://ieeexplore.ieee.org/document/8029379*

*Figure 2. Structure of one block.*



*Reprinted from Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Retrieved November 21, 2018, from https://ieeexplore.ieee.org/document/8029379*

## Key Characteristics of Blockchain (Karis)

Blockchains can be categorized mainly into: 1) public blockchains, 2) private blockchain, or 3) hybrid or consortium blockchains (Makhdoom et al., 2018; Zheng et al., 2017). Characteristics that are key to understanding any blockchain architecture are: decentralization (Makhdoom et al., 2018; Zheng et al., 2017), persistency/immutability (Reyna et al., 2018; Panarello et al., 2018; Zheng et al., 2017), and auditability (Makhdoom et al.; 2018, Reyna et al., 2018; Panarello et al., 2018; Zheng et al., 2017).

### Decentralization

Blockchain can be considered a “decentralized database that is managed by distributed computers on a peer-to-peer (P2P) network”, in which each peer holds a copy of the ledger (Rouse, n.d.).  Instead of relying on a single, central point of authority or storage, blocks of data are stored on multiple systems distributed throughout the world forming a blockchain. This decentralization is enabled by consensus mechanisms used to preserve data integrity in a blockchain's distributed network. In contrast, for example, traditional financial transactions rely on a trusted third party like a central bank to authenticate, authorize, and/or store a transaction, which can create bottleneck delays and be vulnerable to corruption at the central server (Zheng et al., 2017). In blockchain, this centralized third-party reliance is removed with consensus algorithms. In simple terms, consensus means that peers in the blockchain node must agree on the transactions and thereby verify the integrity of the data, since there is no central trusted agency. Types of consensus algorithms include PoW (Proof of Work), PoS (Proof of Stake), PBFT (Practical Byzantine Fault Tolerance) and DPoS (Delegated Proof of Stake), among others (Reyna et al., 2018). Each transaction must be approved through governing consensus mechanisms by the node, in order for the transaction to be recorded onto a blockchain.

**Immutability**

Persistency or immutability refers to the fact that data cannot be maliciously manipulated, corrupted or deleted once a transaction has met consensus protocols and been recorded on the blockchain (Panarello et al., 2018; Zheng et al., 2017). Many sources use the analogy of sending out an email to thousands of recipients worldwide; once the email is sent, it cannot be un-sent. More specifically, the reason why a transaction written on a block would be virtually impossible to delete or edit is because each block holds a hash of the parent block, and this chain is repeatedly copied. If data in one block is edited, the change will result in a different block hash, requiring the subsequent block to be revised, which will propagate yet another block hash that requires the process to be continued until the end of the chain. However, while this theoretical edit is being made block by block, new blocks will be generated into the chain simultaneously, and so the edits will require an exponential amount of computing power possible only in theory. Immutability of blockchains is considered to be the highest achieved level of security that is so attractive to industry applications like financial transactions. However, Zheng et al. and multiple other sources warn that immutability is not as strong in private or consortium blockchains than in public blockchains (2017).

### Auditability

Auditability in blockchain architecture is possible because every block can be traced back to the genesis block through the parent block hash and timestamp. Each user on the blockchain maintains an identical copy of the ledger, and the distributed ledger in a P2P network maintains a public history of transactions (Bible et al., 2017). The transaction history is open to anyone and near real-time, providing transparency and auditability (Bible et al., 2017).

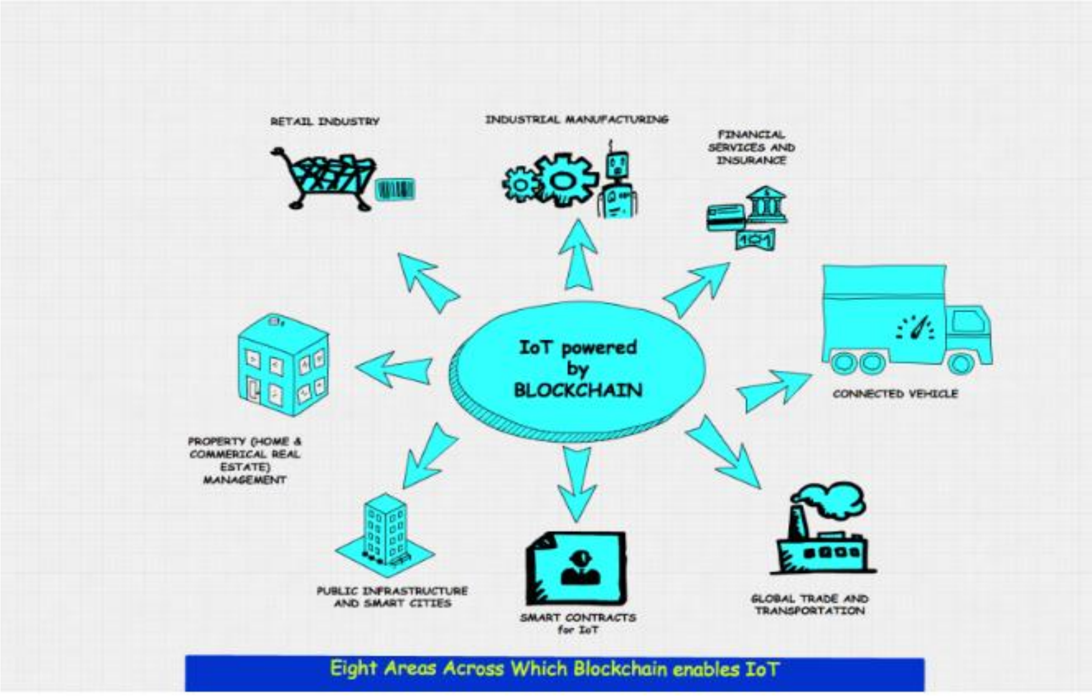
## Advantages of Blockchain for IoT (Karis)

IoT applications generate large volumes of data and require extensive connectivity as well as computational power. Centralized architectures face difficulties and shortcomings in supporting such environments. Blockchain offers the alternative with its decentralized and distributed ledger system (Kumar & Mallick, 2018). Also, security is a major requirement of IoT; for example, healthcare devices that precipitate private medical data demand security and privacy (Makhdoom et al., 2018) and smart home alarm devices that hold the potential risk of burglary from hacking (Panarello et al., 2018). Blockchain's perceived security benefits with immutability of transactions, data integrity/authentication, and auditability appears to be a promising solution to the IoT security issue. Blockchain can meet the IoT demands of self-regulated self-managed system, high throughput, and scalability, as well as security and privacy issues with persistency, transparency and reliability (Makhdoom et al., 2018; Panarello et al., 2018).

## Network Architecture (Poitiers)

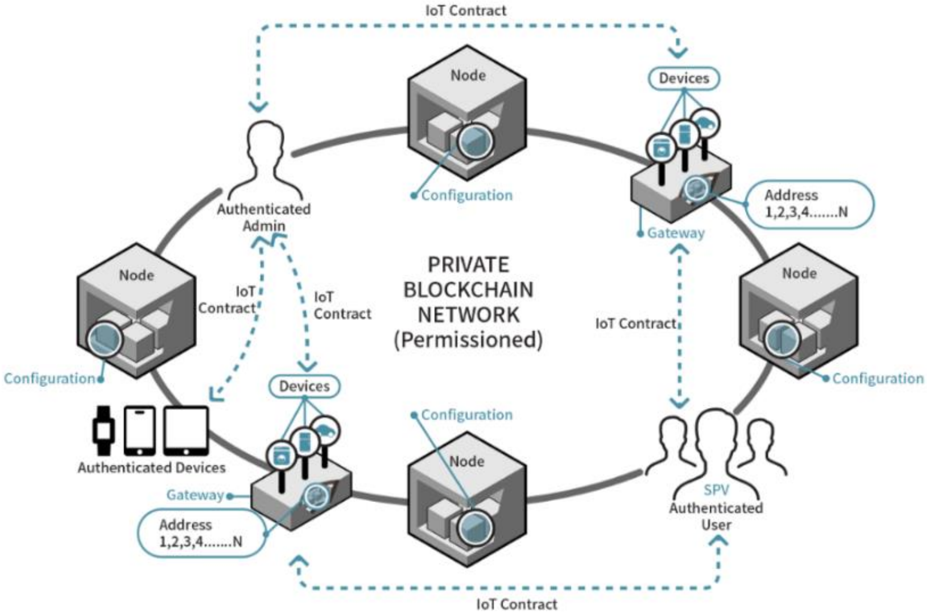
In a few years, billions of devices will come online and increase amount of data exchanged on the internet massively. For that reason, an IT infrastructure capable of dealing with massive secure data, secure communication transaction and peer to peer device exchange is necessary. The issue can be categorized in three dimensions: cloud based IoT system, security risks, and enabling ultimate dynamic resources allocation between machines. IoT systems often depend on a synchronize architecture where information is sent from device to the proper cloud network where the data is processed and sent back to the other IoT device to coordinate them. Coordination is important in centralized systems, which occurs peer to peer, reducing system failure and centralizing security and vulnerability. In order to coordinate, devices must have the capability to make decisions locally, process data locally and be able to share resources locally between devices on demand. These coordination requirements are a huge security issue when it comes to IoT. Blockchain is promising for IoT security because it provides assurance that all data are put into the well-defined database. Blockchain uses a peer to peer communication model allowing for "process[ing] the hundreds of billions of transactions between devices will significantly reduce the costs associated with installing and maintaining large centralized data centers and will distribute computation and storage needs across the billions of devices that form IoT networks" (Banafa, 2017b). Furthermore, blockchain distributes computation and storage needs across nodes, forming a global IoT (Banafa, 2017b). This architecture prevents network shutdown in the event of a node failure. Using blockchain as an IoT solution could "enable secure, trustless messages between devices in an IoT network" (Banafa, 2017b). For example, a door lock that is connected to a smart contract on the blockchain that controls when and who can open the lock. In this model the blockchain will treat messages exchanged between devices like financial transactions in a bitcoin network, DAV network.

Figure 3. IoT Connected to Blockchain


RETAIL INDUSTRY
INDUSTRIAL MANUFACTURING
FINANCIAL SERVICES AND INSURANCE
IoT powered by BLOCKCHAIN
PROPERTY (HOME & COMMERICAL REAL ESTATE) MANAGEMENT
CONNECTED VEHICLE
PUBLIC INFRASTRUCTURE AND SMART CITIES
SMART CONTRACTS for IoT
GLOBAL TRADE AND TRANSPORTATION
Eight Areas Across Which Blockchain enables IoT

*Reprinted from Chemitiganti, V. (2017, February 15). What Blockchain Can Do for IoT - DZone IoT. Retrieved November 28, 2018, from https://dzone.com/articles/what-blockchain-can-do-for-the-internet-of-things*

Figure 4. Network Architecture

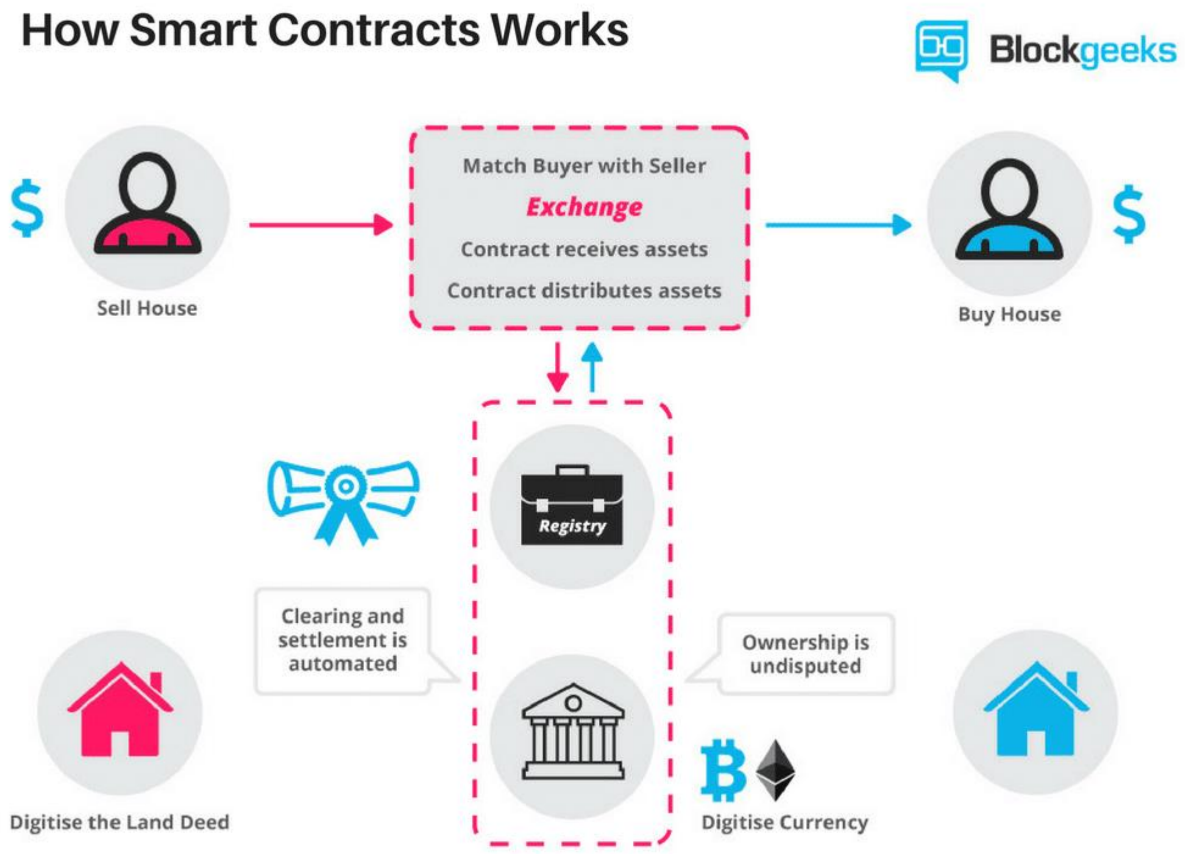


*Reprinted from Ecurrencyhodler. (2017, November 21). The Solution to IoT is Blockchain Security. – Hacker Noon. Retrieved November 28, 2018, from https://hackernoon.com/the-solution-to-iot-is-blockchain-security-3e52a8dd812f*

## Smart Contracts (Varun)

One of blockchain's unique features is that it is a decentralized network. These networks exist between all parties allowing P2P communication, eliminating the need to pay “the middleman” and saving time by reducing conflict between parties.

In 1994, cryptographer Nick Szabo discovered that distributed ledgers can be used for self-executing contracts, which are now referred to as "Smart Contracts" or "Digital Contracts" (Siddiqui, 2018)  These types of contracts can be converted into machine code and stored on the system which is controlled and monitored by the network of other computers running the blockchain. This results in ledger feedback are like the sending and receiving of money, products, and services (Kuster, 2017).



*Reprinted from Nguyen, G., Rosic, A., Westerhof, P., Urling, M., Andonov, S., & Mihaylov, M. (n.d.). What Are Smart Contracts? A Beginner's Guide to Smart Contracts. Retrieved from https://blockgeeks.com/guides/smart-contracts/*

Smart contracts can facilitate a transfer of money, shares and other assets in a way which is not only conflict-free but also fast and reliable, without requiring an intermediary (Siddiqui, 2018). The smart contract process can be understood by comparing it to a vending machine transaction. In most cases, one would consult a notary and pay them for their services while you wait to get your official documents. However, with smart contracts, customer transactions are inserted into the ledger (vending machine), along with customer driver's license number and escrow account, identifying every transaction uniquely. Furthermore, smart contracts also come with rules and regulations, penalties, and agreement governing the agreement, just like a traditional ledger transaction. Smart contracts can be used for various situations like financial derivatives, credit enforcement, crowdfunding agreements, legal processes, insurance premiums (Siddiqui, 2018).

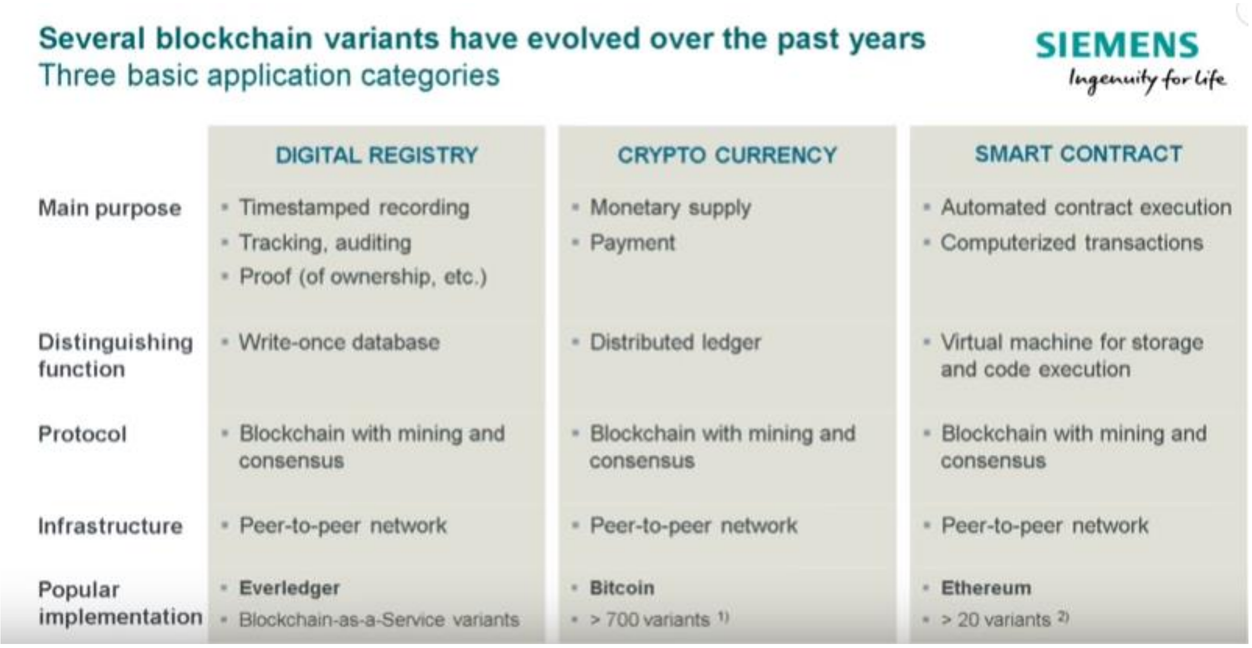
Smart contracts provide us with the following features:

- Secured and Safe
- Speed
- Accuracy
- Trust
- Autonomy
- Backup

## Database Application (Poitiers)

The database security that blockchain provides is unparalleled. Blockchain itself is a secure, distributed database specializing recording transactions or digital interactions (Banafa, 2017b). Distributed databases, created from millions of networked computers, record and authenticate exchanges of value. With blockchain, value of any kind can be exchanged directly via peer to peer without a centralized authority to record and validate the transaction. This decentralized approach could eliminate single points of failure, bottlenecks and make data and transactions more secure. For example, one block can contain transaction (data), hash of the data and data about the previous block. Verification of every transaction in each node, origin and destination, allows for the application of different security measures at the database level. Even if one block is hacked, it will take time to decrypt all other blocks. Application of smart contracts only allow database writes, preventing data changes. This prevention is the guarantee of blockchain mining and consensus algorithms. If the transaction state of a block changes in the network, it triggers the execution of a script that compares the data inside that block to the others (Gazdecki, 2018). If no matches are found, the block is automatically shut down. In order to evaluate the applicability of blockchain to databases, 3 security factors must be considered: low security guarantees as consequence of distributed consensus, susceptible to traditional IT security weaknesses, and attacks on physical world to digital world interface.

Table 1: Application Categories



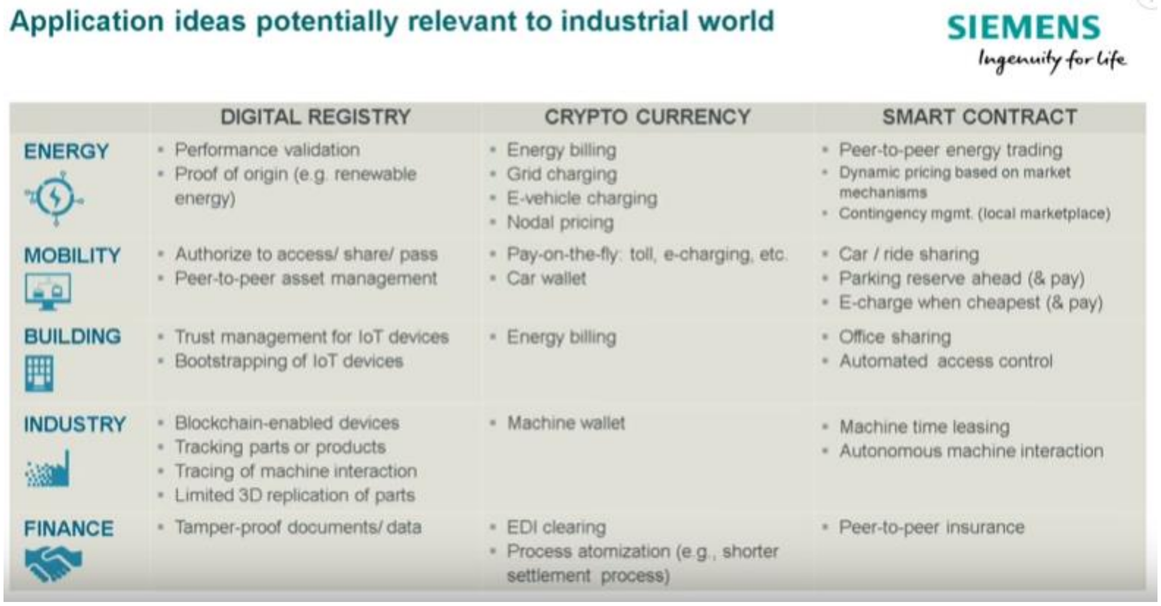
**Several blockchain variants have evolved over the past years**
Three basic application categories

SIEMENS
Ingenuity for life

| | DIGITAL REGISTRY | CRYPTO CURRENCY | SMART CONTRACT |
|---|---|---|---|
| Main purpose | ▪ Timestamped recording<br>▪ Tracking, auditing<br>▪ Proof (of ownership, etc.) | ▪ Monetary supply<br>▪ Payment | ▪ Automated contract execution<br>▪ Computerized transactions |
| Distinguishing function | ▪ Write-once database | ▪ Distributed ledger | ▪ Virtual machine for storage and code execution |
| Protocol | ▪ Blockchain with mining and consensus | ▪ Blockchain with mining and consensus | ▪ Blockchain with mining and consensus |
| Infrastructure | ▪ Peer-to-peer network | ▪ Peer-to-peer network | ▪ Peer-to-peer network |
| Popular implementation | ▪ **Everledger**<br>▪ Blockchain-as-a-Service variants | ▪ **Bitcoin**<br>▪ > 700 variants [1)] | ▪ **Ethereum**<br>▪ > 20 variants [2)] |

*Reprinted from Blocher, U. (2017, April 27). Blockchain: Application Scenarios and Security [Video file]. Retrieved from https://www.youtube.com/watch?v=tS70z3VqT4Y*

Table 2: Application Industries



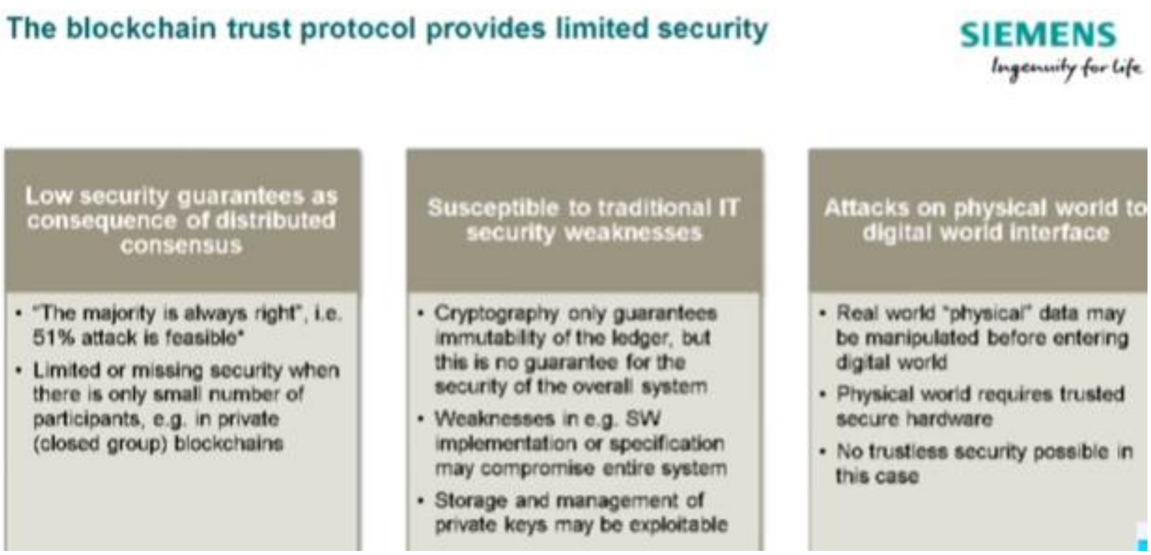
**Application ideas potentially relevant to industrial world**

SIEMENS
Ingenuity for life

| | DIGITAL REGISTRY | CRYPTO CURRENCY | SMART CONTRACT |
|---|---|---|---|
| ENERGY | ▪ Performance validation<br>▪ Proof of origin (e.g. renewable energy) | ▪ Energy billing<br>▪ Grid charging<br>▪ E-vehicle charging<br>▪ Nodal pricing | ▪ Peer-to-peer energy trading<br>▪ Dynamic pricing based on market mechanisms<br>▪ Contingency mgmt. (local marketplace) |
| MOBILITY | ▪ Authorize to access/ share/ pass<br>▪ Peer-to-peer asset management | ▪ Pay-on-the-fly: toll, e-charging, etc.<br>▪ Car wallet | ▪ Car / ride sharing<br>▪ Parking reserve ahead (& pay)<br>▪ E-charge when cheapest (& pay) |
| BUILDING | ▪ Trust management for IoT devices<br>▪ Bootstrapping of IoT devices | ▪ Energy billing | ▪ Office sharing<br>▪ Automated access control |
| INDUSTRY | ▪ Blockchain-enabled devices<br>▪ Tracking parts or products<br>▪ Tracing of machine interaction<br>▪ Limited 3D replication of parts | ▪ Machine wallet | ▪ Machine time leasing<br>▪ Autonomous machine interaction |
| FINANCE | ▪ Tamper-proof documents/ data | ▪ EDI clearing<br>▪ Process atomization (e.g., shorter settlement process) | ▪ Peer-to-peer insurance |

*Reprinted from Blocher, U. (2017, April 27). Blockchain: Application Scenarios and Security [Video file]. Retrieved from https://www.youtube.com/watch?v=tS70z3VqT4Y*

Table 3: Security Aspects



**The blockchain trust protocol provides limited security**

SIEMENS
Ingenuity for life

| Low security guarantees as consequence of distributed consensus | Susceptible to traditional IT security weaknesses | Attacks on physical world to digital world interface |
|---|---|---|
| • "The majority is always right", i.e. 51% attack is feasible"<br>• Limited or missing security when there is only small number of participants, e.g. in private (closed group) blockchains | • Cryptography only guarantees immutability of the ledger, but this is no guarantee for the security of the overall system<br>• Weaknesses in e.g. SW implementation or specification may compromise entire system<br>• Storage and management of private keys may be exploitable | • Real world "physical" data may be manipulated before entering digital world<br>• Physical world requires trusted secure hardware<br>• No trustless security possible in this case |

*Reprinted from Blocher, U. (2017, April 27). Blockchain: Application Scenarios and Security [Video file]. Retrieved from https://www.youtube.com/watch?v=tS70z3VqT4Y*

## Disadvantages of Blockchain for IoT (Varun)

Data found on most IoT networks cannot be considered trustworthy until it is reviewed and passed through a single security "gate" which controls and monitors the flow. Just like Mirai incidents, a barrage of specifically configured bots can focus on attacking a single point via DDoS (Distributed Denial of service) attacks. Once the attacker has successfully passed through the security gate undetected, the attacker can access all available resources on the IoT network. Hence, all connected IoT devices are compromised.

Currently, a bitcoin-based blockchain can manage 7 transactions per second, whereas Ethereum based blockchain handles 25 transactions in one second. Speeds like these are extremely slow if blockchain were ever implemented on IoT network, where hundreds of connected devices are transacting simultaneously. An exact number of transactions per second is not known to prove that blockchain is fast enough for IoT integration; however, the faster blockchain becomes, the more chances of adopting it with IoT increases.

Generally, IoT devices are built with connectivity in mind, not computation. This results in IoT devices that lag in average processing power when compared to other smart devices. IoT networks are not designed to handle computational algorithms. This is another major concern over adopting Blockchain on IoT devices.

Organizations which are currently seeking to deploy blockchain based applications do not have necessary technical knowledge and skills to design, develop and deploy a blockchain based systems in house, without getting support from outside. Vendors of blockchain applications create a blockchain system ready to use out of the box and sell it to such organizations. The value of such applications is based on the vendor's credibility. Blockchain as a service market is still in its initial phase, a business should wisely select a blockchain vendor that can appropriately sculpt the application to cover all risks associated with the blockchain implementation on IoT.

Blockchain is famous for its extremely high-security levels, but a blockchain based system is only as secure as it's access point. In a public blockchain based system, anyone has the access to the private key of a specific user. Malicious users can use private keys to "sign" transactions on the public ledger and can easily validate unauthorized transactions. This is because blockchain does not currently support 2 factor authentication.

## Conclusion (Anthony)

IoT network growth and expansion results from the need for constant connectivity. Rapid and rabid technological advances ask consumers to sacrifice data (privacy) for convenience. On the surface, this sacrifice seems harmless, but recent breaches have shown otherwise. IoT devices, and by association, IoT networks pose a bigger threat than just data leakage. As networks expand, management becomes harder, increasing risk and vulnerabilities. Furthermore, user ignorance adds to network vulnerability, creating “weak” points. Blockchain is an alternative network proposed to handle IoT growth. Although this type of network increases transaction security via smart contracts, it is not yet ready for IoT. The blockchain process of validating transactions would slow down IoT networks due to computational overhead. Also, the blockchain feature of decentralization is lost because ledgers expand as a result of smart contract growth, which will eventually require a management scheme. While blockchain is a feasible solution to the inevitability of IoT growth, the technology must mature before widespread application and acceptance.

# References

Banafa, A. (2017a, March 14). Three Major Challenges Facing IoT. Retrieved November 27, 2018, from https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot.html

Banafa, A. (2017b, August 17). How to Secure the Internet of Things (IoT) with Blockchain. Retrieved November 27, 2018, from https://datafloq.com/read/securing-internet-of-things-iot-with-blockchain/2228

Bible, W., Rapael, J., Riviello, M., Taylor, P., & Valiente, I. O. (2017). *Blockchain Technology and Its Potential Impact on the audit and Assurance Profession*[White paper]. Toronto: Deloitte Development LLC. Retrieved November 21, 2018 from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf

Blocher, U. (2017, April 27). Blockchain: Application Scenarios and Security [Video file]. Retrieved from https://www.youtube.com/watch?v=tS70z3VqT4Y

Chemitiganti, V. (2017, February 15). What Blockchain Can Do for IoT - DZone IoT. Retrieved November 28, 2018, from https://dzone.com/articles/what-blockchain-can-do-for-the-internet-of-things

Ecurrencyhodler. (2017, November 21). The Solution to IoT is Blockchain Security. – Hacker Noon. Retrieved November 28, 2018, from https://hackernoon.com/the-solution-to-iot-is-blockchain-security-3e52a8dd812f

Gazdecki, A. (2018, October 12). How Secure Is Blockchain Technology? Retrieved November 27, 2018, from https://www.forbes.com/sites/forbestechcouncil/2018/10/12/how-secure-is-blockchain-technology/#b48710a72f03

Kumar, N., & Mallick, P. (2018). Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science,132*, 1815-1823. Retrieved November 21, 2018, from www.elsevier.com/locate/procedia.

Kuster, F. (2017, July 14). What Are Smart Contracts in Blockchain Technology? Retrieved December 2, 2018, from https://captainaltcoin.com/blockchain-smart-contracts/

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2018). Blockchain's adoption in IoT: The challenges and a way forward. *Journal of Network and Computer Applications,125*, 251-279. Retrieved November 21, 2018, from http://www.elsevier.com/locate/jnca

McGrath, S. (2018, September 25). Using Blockchain Technology to Secure the Internet of Things (IoT). Retrieved November 27, 2018, from https://www.datasciencecentral.com/profiles/blogs/using-blockchain-technology-to-secure-the-internet-of-things-iot

Nguyen, G., Rosic, A., Westerhof, P., Urling, M., Andonov, S., & Mihaylov, M. (n.d.). What Are Smart Contracts? A Beginner's Guide to Smart Contracts. Retrieved from https://blockgeeks.com/guides/smart-contracts/

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT Integration: A Systematic Survey. *Sensors,18*(8), 2575. doi:10.3390/s18082575

Reyna, A., Martin, C., Chen, J., Soler, E., & Diaz, M. (2018). On blockchain & its integration with IoT: Challenges and opportunities. *Future Generation Computer Systems,88,* 173-190. Retrieved November 21, 2018, from http://www.elsevier.com/locate/fgcs

Rouse, M. (n.d.). What is consensus algorithm? - Definition from WhatIs.com. Retrieved November 21, 2018, from https://whatis.techtarget.com/definition/consensus-algorithm

Siddiqui, I. (2018, April 27). What is Smart Contract? – Coinmonks – Medium. Retrieved December 2, 2018, from https://medium.com/coinmonks/what-are-smart-contract-and-whats-so-smart-about-them-a-beginners-guide-4228999305b

United States, Department of Jusice, Computer Crime & Intellectual Property Section. (2017, July 12). *Securing Your "Internet of Things" Device*. Retrieved November 27, 2018, from https://www.justice.gov/criminal-ccips/page/file/984001/download

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Retrieved November 21, 2018, from https://ieeexplore.ieee.org/document/8029379