




TAL TECH

 blockchain.taltech.ee

BLOCKCHAIN TECHNOLOGY FOR SECURE IOT

Alex Norta (Assoc.Prof.PhD.MSc.)
Department of Software Science/ Institute of Information Technology
Tallinn University of Technology

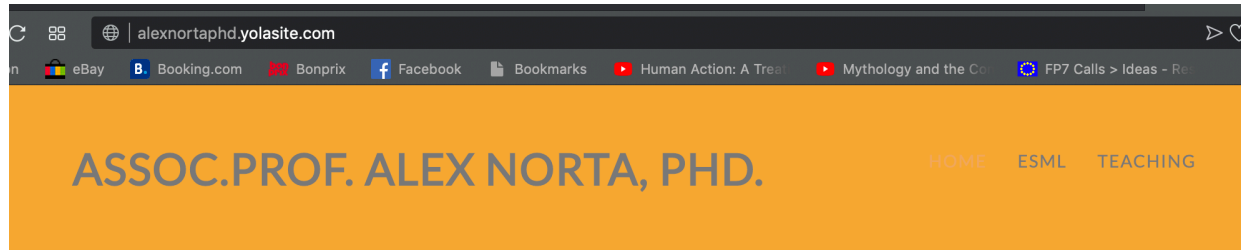
24.08.2020

AGENDA

- My quick introduction
- Understanding IoT, blockchain and security
- The relationship between IoT, data, blockchain and security
- Application cases
- Open issues, limitations and future work
- Conclusions

MY QUICK INTRODUCTION

<https://www.researchgate.net/lab/Blockchain-Technology-Group-Alex-Norta>



alexnortaphd.yolasite.com

ASSOC.PROF. ALEX NORTA, PHD.

HOME ESML TEACHING



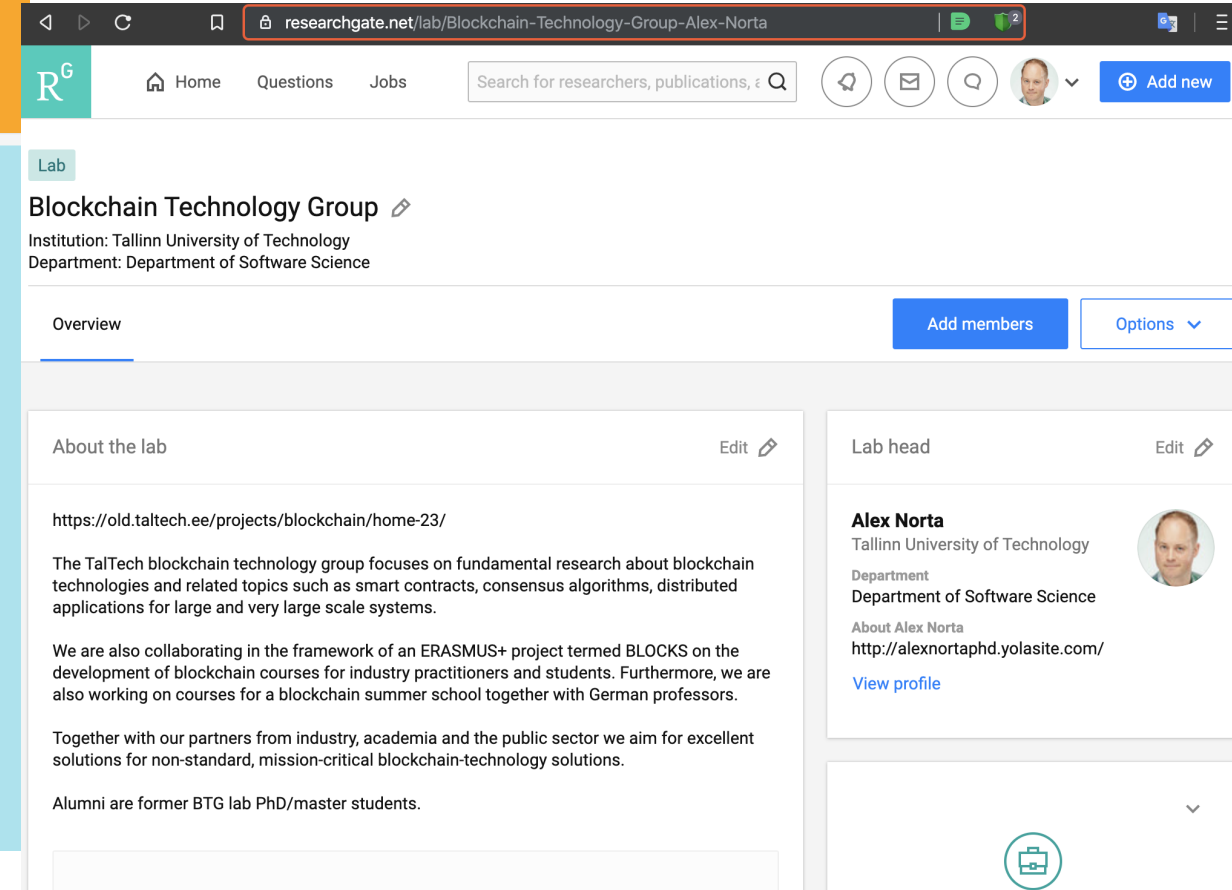
DEPARTMENT OF INFORMATICS,
TALLINN UNIVERSITY OF TECHNOLOGY,
ESTONIA

[LinkedIn](#), [CV and Academic Profile](#), [Facebook](#)

Twitter: [@alexbafana](#), Skype: alexbafana, Mobile: +37256294420, Email:
alexander.norta@ttu.ee, alex.norta.phd@ieee.org

OLDER LINKS:

[University Helsinki](#), [ResearchGate](#), [GoogleScholar](#)



researchgate.net/lab/Blockchain-Technology-Group-Alex-Norta

Home Questions Jobs Search for researchers, publications, € Add new

Lab

Blockchain Technology Group

Institution: Tallinn University of Technology
Department: Department of Software Science

Overview Add members Options

About the lab Edit

<https://old.taltech.ee/projects/blockchain/home-23/>

The TalTech blockchain technology group focuses on fundamental research about blockchain technologies and related topics such as smart contracts, consensus algorithms, distributed applications for large and very large scale systems.

We are also collaborating in the framework of an ERASMUS+ project termed BLOCKS on the development of blockchain courses for industry practitioners and students. Furthermore, we are also working on courses for a blockchain summer school together with German professors.

Together with our partners from industry, academia and the public sector we aim for excellent solutions for non-standard, mission-critical blockchain-technology solutions.

Alumni are former BTG lab PhD/master students.

Lab head Edit

Alex Norta
Tallinn University of Technology
Department
Department of Software Science
About Alex Norta
<http://alexnortaphd.yolasite.com/>
[View profile](#)

UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY

UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY: IOT

- IoT build a bridge between the digital and physical worlds
 - without human intervention
- IoT functionality
 - (smart) sensor-laden devices
 - autonomously exchange data across the internet
 - receiving and transmitting the data to different devices
 - allows more than one device to be connected with each other
 - create real-time linkages
- Creation of business opportunities and opening of new markets
 - now 55 billion IoT devices by 2025 up from about 9 billion in 2017
 - nearly \$US15 trillion in aggregate IoT investment between 2017 and 2025
 - potential to improve our lives, e.g., monitoring health patients, energy-use optimization, etc.

UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY: IOT

- Significant problems of IoT
 - billions of transactions per device (latency)
 - lacking standards
 - low computing power and data storage
 - network connectivity
- Security- and privacy problems, examples:
 - Amazon's Alexa [spying on conversations](#)
 - hackable heart pacemaker
 - hacked security cameras
 - hacked baby monitor
 - two-thirds of consumers think [IoT devices are 'creepy'](#)

UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY: IOT

- Currently a centralized model for IoT systems
 - connects only to identified and verified devices through cloud services that have high data storage capabilities
 - high maintenance cost
 - extra infrastructure added with best IoT solutions
 - if a number of IoT devices is interconnected at a time
 - number of communication will increase
 - economic scalability engineering issues
 - If these issues go beyond a limit, disruption of cloud services occur leading to security issues
- Solution lies in a decentralized network!

UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY: BLOCKCHAIN

- Blockchain built to underpin and authenticate cryptocurrency transactions
- Accepted by many businesses, researchers, and customers for its underlying framework in crypto assets
 - popularity of Blockchain to increase up to 20 billion \$ by 2024
 - 15% of banks will soon adopt Blockchain to overcome security issues
 - [EU blockchain initiatives](#)
- Blockchain is a 'cryptographically secured, immutable distributed ledger technology.'
 - encryption and cryptography are the very essences of blockchain technology
 - strong public/private-key cryptograph
 - strong cryptographic hash

UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY: BLOCKCHAIN

- Whitepaper of Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

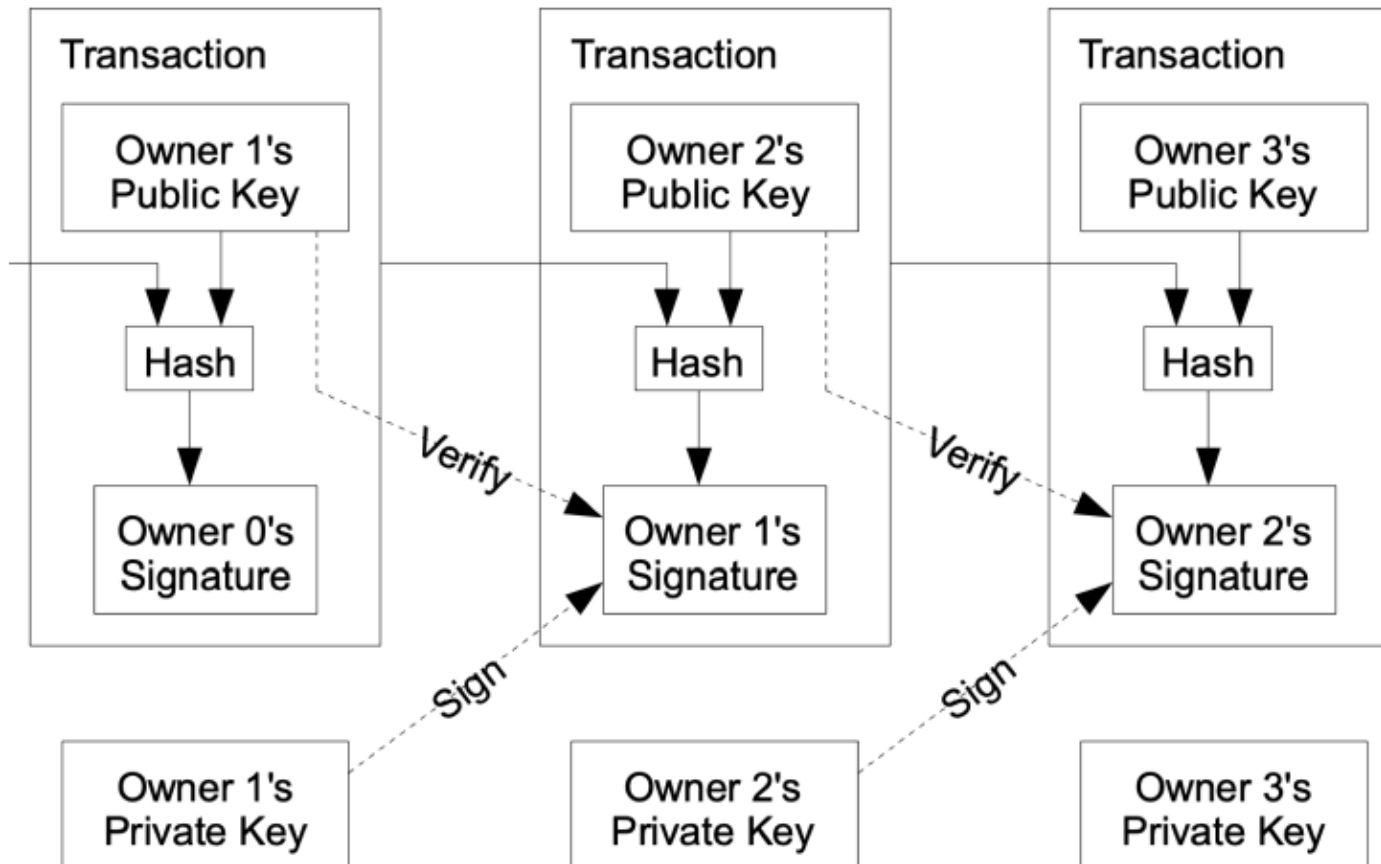
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org



Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY: BLOCKCHAIN

- Whitepaper of Satoshi Nakamoto



UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY: BLOCKCHAIN

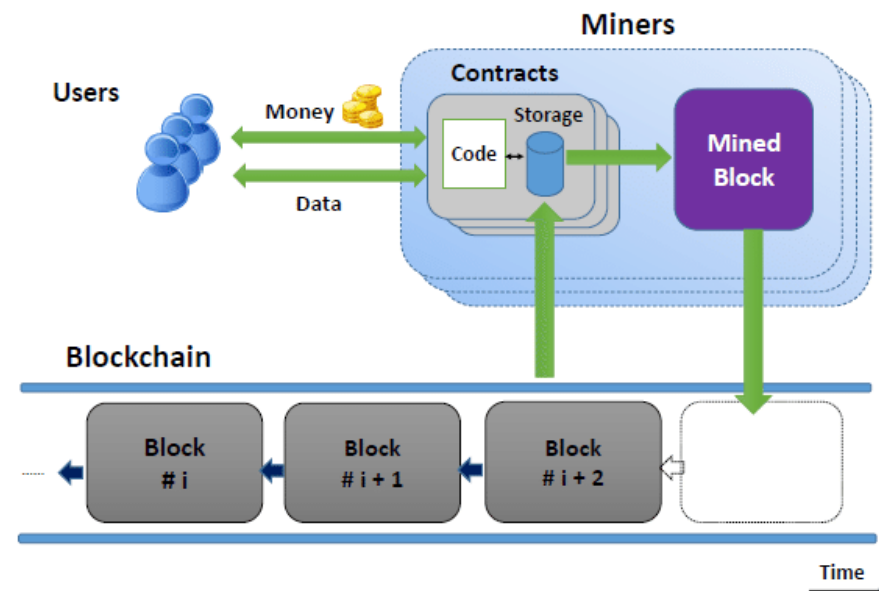
- Decentralized approach
 - does not require the third-party presence
 - blocks are the key concept of the technology
 - small sets of occurred transactions
 - each new block stores reference of the previous transaction by including a SHA-256 hash of the previous transaction
 - creates a `chain` of blocks
 - blocks are computationally difficult to create
 - generation requires mining (time/resource consuming)
 - to tamper one block: tamper previous block, follow the chain
 - tamper resistant

UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY: BLOCKCHAIN

- Nodes in the blockchain verify themselves at every entry
 - creates a genuine entry
 - information once entered in blocks cannot be changed
 - cryptographic algorithms for validation:
 - [proof of work](#), [proof of stake](#)
- Adding a transaction
 - everyone in the network validates through an algorithm
 - takes a lot of processing time to create even a single block
 - information is linked as chains with reference to previously added data in blocks
 - approved transactions are gathered into a block
 - blocks are distributed to each node in the network
 - new block and successive blocks are validated with a single fingerprint corresponding to the previous block

UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY: BLOCKCHAIN

- Participating nodes can see the blocks
 - can not see the actual content of the transaction
 - protected by private keys
- Each block contains the cryptographic hash of previous block timestamp and transaction data
- Blockchain records all the entries in different blocks across the chain
- Replicates copies of the ledger across a network of independent nodes
 - blockchain is carrying the useful information needed by more than one source
 - data is scattered all along the chain
- Smart contracts
 - Turing-complete language in protocol layer on blockchain
 - potentially solves issues of scalability, reliability, privacy, security, trust, authentication



UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY: BLOCKCHAIN

- [Ethereum](#) as first smart-contract system

A Next-Generation Smart Contract and Decentralized Application Platform

glitter Docs chat

An introductory paper to Ethereum, introduced before launch, which is maintained.

Satoshi Nakamoto's development of Bitcoin in 2009 has often been hailed as a radical development in money and currency, being the first example of a digital asset which simultaneously has no backing or [intrinsic value](#) and no centralized issuer or controller. However, another - arguably more important - part of the Bitcoin experiment is the underlying blockchain technology as a tool of distributed consensus, and attention is rapidly starting to shift to this other aspect of Bitcoin. Commonly cited alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments ([colored coins](#)), the ownership of an underlying physical device ([smart property](#)), non-fungible assets such as domain names ([Namecoin](#)), as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules ([smart contracts](#)) or even blockchain-based [decentralized autonomous organizations](#) (DAOs). What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

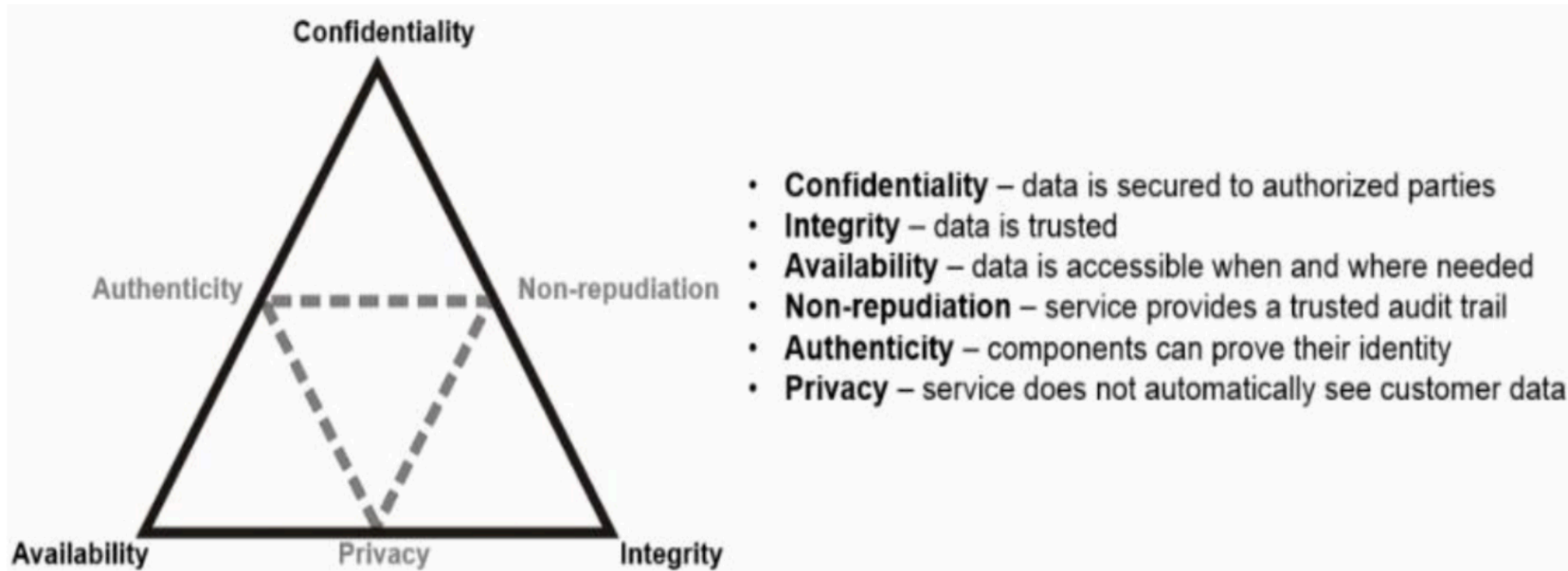
Contents

UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY: BLOCKCHAIN

- Public smart-contract systems
 - allow any person or system to
 - access and view the ledger, propose adding new data blocks to the ledger
 - validate transactions by following established protocols
 - operate without any central authority
 - operate without any central authority
 - parties having little or no knowledge of each other
- Permissioned/private smart-contract systems
 - limit access to the ledger to certain known or trusted parties (verified identities)
 - governance structure and authority to
 - control access to the ledger
 - governance structure and authority to
 - control access to the ledger, apply and enforce rules
 - establish functions and the related code
 - respond to incidents, including cyber threats

UNDERSTANDING IOT, BLOCKCHAIN AND SECURITY: SECURITY

- A small breach in the security system can allow hackers to access a whole lot of information
- If data is stored in one location and is easy for hackers to target



RELATING IOT, DATA, BLOCKCHAIN AND SECURITY

RELATING IOT, DATA, BLOCKCHAIN AND SECURITY: SECURITY & IOT

- IoT security
 - increase of security costs to 20% annually by 2020
 - from 1% in 2015
- IoT bottlenecks and technical deficiencies
 - device autonomy
 - must be integrated in a heterogeneous IoT-system
 - virtual identity
 - creates trust issues and authentication issues
 - point-to-point communication
 - complex to coordinate and can easily be attacked
 - data integrity
 - potentially easy to compromise data

RELATING IOT, DATA, BLOCKCHAIN AND SECURITY: SECURITY & IOT

- Security threats for IoT
 - unauthorized physical device access
 - software attacks
 - viruses and worms, DoS attacks, man-in-the-middle attack (password)
 - harness unsecure IoT devices to create massive DDoS attack
 - access the data streaming through the IoT network
 - impersonation, device spoofing
- Today, solutions often revolve around identity management & encryption
- IoT data protection needed throughout the device lifecycle
- Blockchain could mitigate providing framework, automated security and attack prevention

RELATING IOT, DATA, BLOCKCHAIN AND SECURITY: SECURITY & BLOCKCHAIN

- Blockchain is a fully decentralized system
- Centralization architecture is a single point of failure
- Secure infrastructure is far from the centralized model
- Every centralized network is potentially insecure
 - user's- and device's identity always has to be private
 - all data must remain
 - fully private
 - confidential
 - have integrity
 - be available
- Blockchains potentially solves these generic issues of centralized architectures

RELATING IOT, DATA, BLOCKCHAIN AND SECURITY: BLOCKCHAIN & IOT

- Blockchain complements IoT
 - creating an internet of trusted things
 - blockchain to trace and authenticate IoT data
 - storing the IoT data in a blockchain
- Every IoT node
 - can be registered on a blockchain with an ID
 - uniquely identify a device in the universal namespace
 - for a device to connect another device use the blockchain id as URL
 - use IoT-device local blockchain wallet to raise an identity request
 - send to the target device
 - target device uses blockchain services to validate the signature using the public key of the sender
- M2M authentication without the need of any centralized arbitrator, or service

RELATING IOT, DATA, BLOCKCHAIN AND SECURITY: BLOCKCHAIN & IOT

- Blockchains promise standardization across different parts of IoT
 - tracking millions of connected devices
 - lifecycle tracking of IoT-devices: list a history of connected equipment
 - coordination between devices
- Decentralized IoT-systems with trust
 - nodes reach a consensus to approve transactions
- Blockchains coordinate the transactional layer of the IoT ecosystem
- Potentially solving the problems in IoT security
 - scalability
 - privacy and confidence

RELATING IOT, DATA, BLOCKCHAIN AND SECURITY: BLOCKCHAIN & IOT

- Blockchains problems for IoT-system use
 - amount of data processed by IoT-systems is enormous
 - latency due to blockchain
 - ledger replication introduces latency
 - acquiring a block may consume extra time
 - not acceptable in a near-time and real-time service situation
 - blockchain is not best suited in a recording of raw data at the source
 - blockchain scalability
 - ledger-size may lead to centralization
 - IoT processing power- and time hurdle, and storage issues
 - perform encryption algorithms for all the objects involved
 - devices may have very different computing capabilities and run heterogeneous systems
 - not all of them will be capable of running the same systems
 - very low storage capacity of most IoT-devices to store many blocks

RELATING IOT, DATA, BLOCKCHAIN AND SECURITY: IOT & DATA & BLOCKCHAIN

- Each CRUD (Create, Read, Update, or Delete) operation on IoT data can be registered as a transaction record in a blockchain block
- Blockchain Identity
 - control access management
 - monitor the information collected by the sensors
 - greater transparency and potential convenience
 - store data in chains of transactions
 - prevents data modification when verified by authentication system
 - disallowing data duplication by any wrong data
 - no third party for data transfer between IoT-devices

RELATING IOT, DATA, BLOCKCHAIN AND SECURITY: IOT & DATA & BLOCKCHAIN

- Blockchains potentially enable a resilient IoT-ecosystem
 - adopting a standardized, point-to-point communication model
 - reduce installation and maintenance costs in Big Data centers
 - reduce storage of IoT-devices
 - preventing errors in nodes due to a collapse, or attack
 - blockchains replicate and restore
 - blockchains record transactions, or digital interactions securely
 - each block registers the operations
 - with a time stamp
 - verifies that they are in the correct sequence
 - without manipulations
 - safe, auditable, transparent, potentially efficient, interruption-resistant
 - No data leaks as in centralized IoT-systems

APPLICATION CASES

APPLICATION CASES: PRODUCT PROVENANCE (LOGISTICS)

- Blockchains to secure IoT-systems to determine product provenance
 - easily forged products sold to unsuspecting consumers
 - track the integrity of good, e.g., baby formula, wine
 - microchip embedded labels & stored on blockchains
 - product-tracking lifecycle
 - starts from the moment of production
 - throughout the entire supply chain
 - at the point of sale
 - during the final consumer purchase
 - by storing the data in a blockchain
 - product details can not be forged
 - ensures the integrity of the end-product

RANDOM BLOCKCHAIN PRODUCT-PROVENANCE EXAMPLE

- <https://www.zdnet.com/article/ip-australia-and-nrl-trial-blockchain-to-combat-counterfeits/>



IP Australia and NRL trial blockchain to combat counterfeits

Verified trademarks will be marked with a digital "trust badge".

🗨️ in 🇨🇦 🇫🇷 🇧🇮 📧 |  By [Aimee Chanthadavong](#) | August 10, 2020 -- 04:30 GMT (05:30 BST) | Topic: [Innovation](#)



NRL Imagery/Paul Barkley

MORE FROM AIMEE CHANTHADAVONG



Digital Transformation
Modernisation and upping cyber compliance on the agenda for Geoscience Australia



Tech Industry
Qantas focuses on three-year recovery plan as FY20 net profit plunges 91%



Enterprise Software
NSW Health Pathology eliminates 'technical debt' as it tests for COVID-19



Tech Industry
Atlassian touts future of work will be underpinned by flexibility and choice

OTHER BLOCKCHAIN USE-CASES

- Blockchains to secure IoT-systems to determine product provenance
 - easily forged products sold to unsuspecting consumers
 - track the integrity of good, e.g., baby formula, wine
 - microchip embedded labels & stored on blockchains
 - product-tracking lifecycle
 - starts from the moment of production
 - throughout the entire supply chain
 - at the point of sale
 - during the final consumer purchase
 - by storing the data in a blockchain
 - product details can not be forged
 - ensures the integrity of the end-product

APPLICATION CASES: FACILITY MANAGEMENT (COMMERCIAL REAL ESTATE)

- <https://medium.com/coinmonks/blockchain-in-facilities-management-refocusing-on-the-office-experience-7e9efbe9ab29>

Blockchain in Facilities Management: Refocusing on the Office Experience



Aw Kai Shin [Follow](#)

Jan 24, 2019 · 13 min read



Source

Facilities management (FM) for the uninitiated are one of those industries which you never pay heed to unless an issue pops up at your office. The FM industry essentially focuses on providing efficient and effective support services for tenants in a building (commercial real estate for the purposes of this article). Eyes dried out from the air-cond blowing in your face? Complain red-eyed to your FM provider; Office feels like a club? Inform your FM provider of the loose lighting (or not); Spiders running around the

APPLICATION CASES: ENERGY MANAGEMENT

- <https://www.sciencedirect.com/science/article/pii/S1364032118307184>



Download PDF

Share

Export



ELSEVIER

Renewable and Sustainable Energy Reviews

Volume 100, February 2019, Pages 143-174



Blockchain technology in the energy sector: A systematic review of challenges and opportunities

Merlinda Andoni ^a , Valentin Robu ^a , David Flynn ^a , Simone Abram ^b , Dale Geach ^c , David Jenkins ^d , Peter McCallum ^d , Andrew Peacock ^d

Show more

<https://doi.org/10.1016/j.rser.2018.10.014>

Under a Creative Commons [license](#)

Get rights and content

[open access](#)

CONCLUSIONS, LIMITATION, OPEN ISSUES, FUTURE WORK

- IoT-systems with centralized architecture are a single point of failure
- Conceptual security properties exist:
 - confidentiality, integrity, availability + (privacy, authentication, non-repudiation)
- Blockchain-technology for framework securing IoT-system large-data management
- Limitations, open issues and future work
 - the current performance and scalability of IoT are incompatible with blockchain functions
 - new type of blockchain needed for predicted 55 billion connected IoT-devices
 - novel consensus- and validation algorithms needed of IoT peer-to-peer communications
 - IoT platforms are a massive source of raw data
 - need to
 - combine and understand unstructured data
 - extract intelligence, advanced analytics
 - extract actionable intelligence for decision-making



**TAL
TECH**

Thank you very much for your attention!

Q & A?

TALLINN UNIVERSITY OF TECHNOLOGY

blockchain.taltech.ee

