

Blockchain como meio de comunicação para recursos, agentes e dispositivos para IoT. Formalização da comunicação e formas de interação, bem como a prova de características e propriedades

Aluno: Luiz Carlos da Silva Leão

Professor: Alexandre Sztajnberg

Universidade Estadual do Rio de Janeiro – UERJ

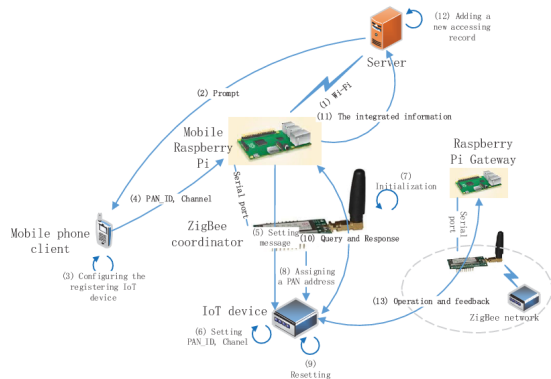
Seminário da disciplina Tópicos Especiais: Contexto e IoT

Rio de Janeiro, 27 de Junho de 2022

- 1 Introdução**
- 2 Motivação**
- 3 Pressupostos**
- 4 Blockchain como meio de comunicação**
- 5 Formalização da comunicação e formas de interação**
- 6 Prova de características e propriedades**
- 7 Uma Aplicação Prática**
- 8 Considerações Finais**

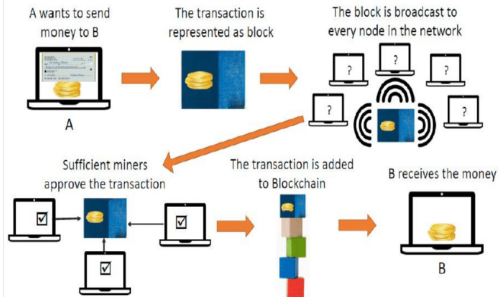
Introdução

- O que é IoT?
- Como se dá a comunicação entre dispositivos IoT?
- O que são recursos, agentes e dispositivos para IoT?



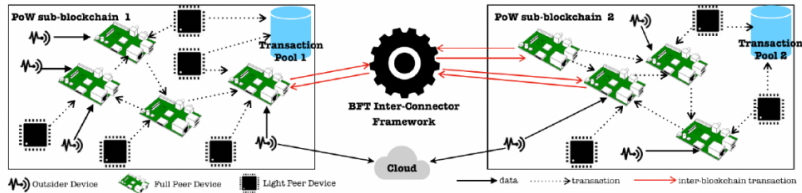
[1]

How Blockchain works?



[2]

- O que é uma Blockchain?
- Como a Blockchain funciona?
- Blockchain como meio de comunicação



[3]

- Quais os riscos na comunicação entre dispositivos IoT?
- O que a Blockchain resolve e porque é útil para comunicação entre dispositivos?
- Os requisitos de IoT estarão atendidos com a Blockchain?



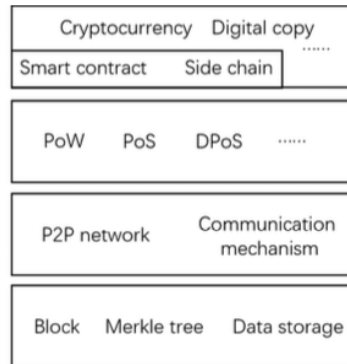
[4]

Application layer

Consensus layer

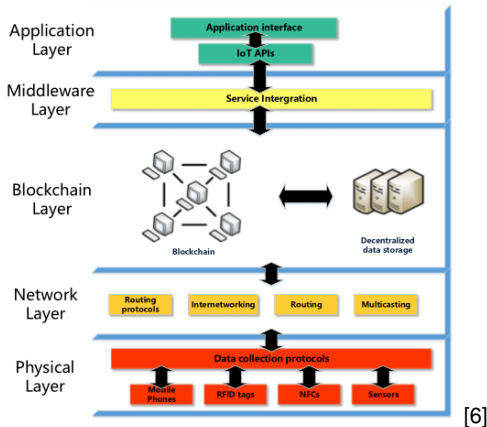
Network layer

Data layer



[5]

A arquitetura de aplicações para blockchain-IoT é composta de 5 camadas: Física, Rede, Blockchain, Middleware e Aplicação

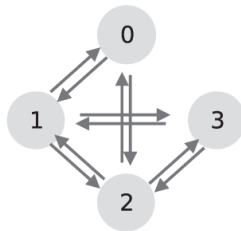


Motivação

```
// total number of nodes  
const int N = 4;
```

```
SCPQuorumSlice qs[N] =  
    {{0, {0, 1, 2, N}},  
     {0, {0, 1, 2, 3}},  
     {0, {0, 1, 2, 3}},  
     {0, {N, 1, 2, 3}}};
```

(a) Textual representation



(b) Figure

- O que é a formalização?
- Quais são as formas de interação?

[7]

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

- Qual a prova de características e de propriedades o whitepaper do Bitcoin [8] apresenta?

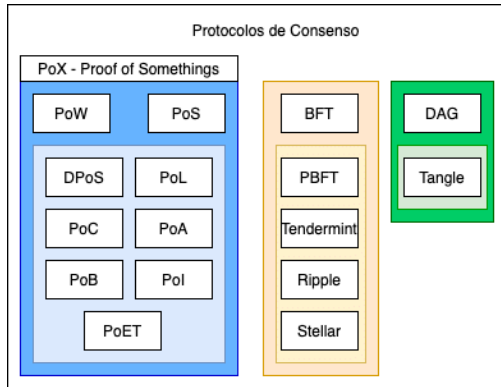
$$\lambda = z \frac{q}{p}$$

- Seria possível haver esse tipo de demonstração para uma rede Blockchain de dispositivos IoT?

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \leq z \\ 1 & \text{if } k > z \end{cases}$$

$$1 - \sum_{k=0}^z \frac{\lambda^k e^{-\lambda}}{k!} (1 - (q/p)^{(z-k)})$$

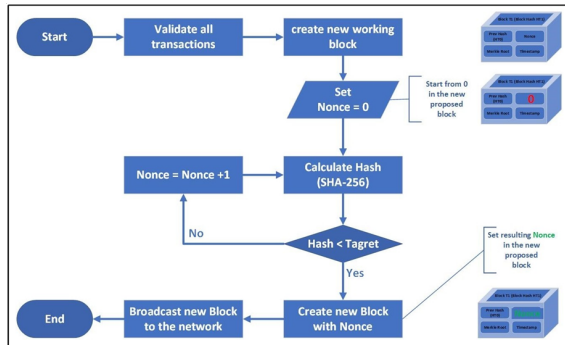
Pressupostos



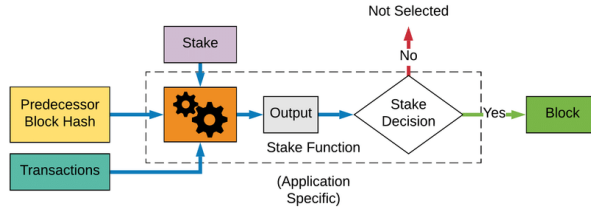
[9]

- O consenso é um problema fundamental em computação distribuída
- Permite com que um conjunto de participantes (ou nós) numa rede chegue a um acordo sobre um conjunto de transações, ou sobre um determinado estado do sistema
- O consenso, portanto, mantém o estado consistente das réplicas e a disponibilidade do sistema

- Cada nó da rede precisa resolver um desafio computacional (um quebra-cabeça criptográfico) para poder propor à rede um bloco de transações
- O nó que resolver o quebra-cabeça matemático obterá uma recompensa na forma de criptomoeda
- Após a formação do bloco, o nó irá encaminhá-lo à rede, e todos os nós irão agregá-lo a uma "blockchain"

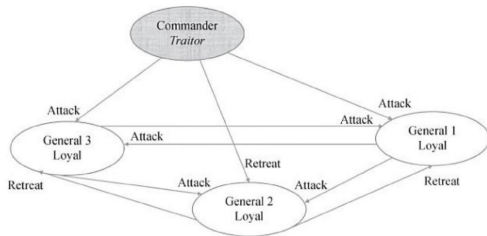


[10]



[11]

- Surge a partir das desvantagens do PoW: segurança (ataques de duplo gasto possíveis), alto consumo energético e desperdício de recursos (no processo de competição/mineração) ou baixa vazão - throughput (poucas quantidades de transações acordadas no tempo)
- o PoS baseia-se na hipótese de que os usuários com a posse de mais moedas (ou recursos computacionais - "stake") são mais propensos a garantir a confiabilidade do sistema e têm menos probabilidade de se comportar como nós maliciosos



[12]

- Se houver $3m + 1$ generais, só poderá haver tolerância a m traidores [13]
- A blockchain Neo usa uma estrutura de consenso chamada de Delegated Byzantine Fault Tolerance (dBFT) [14]

Blockchain	Mecanismo de consenso	Data de lançamento
Bitcoin	PoW	Jan 2009
Litecoin	PoW	Out 2011
NEO	BFT	Fev 2014
Ethereum	PoW / PoS	Jul 2015
Tangle	DAG	Abr 2018

[6]


Blockchain como meio de comunicação

IoT-Blockchain applications.


Application	Classification	Platform
LO3 Energy [87]	Energy microgrid	Ethereum
ADEPT [80]	Smart contracts involving IoT devices	Ethereum
Slock.it [85]	Renting/Selling/Sharing smart objects	Ethereum
Aigang [88]	Insurance network for IoT assets	Ethereum
MyBit [89]	Investment in IoT devices	Ethereum
AeroToken	Sharing airspace market for drone navigation	Ethereum
Chain of things [146]	Identity, security and interoperability	Ethereum
Chronicle [111]	Identity, data provenance and automation	Multiplatform
Modum [84]	Data integrity for the supply chain	Multiplatform
Riddle and Code [147]	Sharing and machine economy	Multiplatform
Blockchain of things [82]	Secure connectivity between IoT devices	Multiplatform

[15]


Blockchain IOT	Mecanismo de consenso	Data de lançamento
IoT Chain	PBFT / DAG	Fev 2014
IoTeX	RoIDPoS	Mai 2017
IOTA	DAG	Abr 2018
HDAC	ePoW	Dez 2018

Google Acadêmico 

Artigos Aproximadamente 4,560 resultados (0,04 s)

Google Acadêmico 

Artigos Aproximadamente 245 resultados (0,04 s)

Google Acadêmico 

Artigos Aproximadamente 154 resultados (0,03 s)



IoTChain Proj... IoTChai...

A high-security lite IOT OS driven by blockchain



7 repositories



0 members



HdacTech

HdacTech



Repositories 14



57 followers



IoTeX Network iotexpr...

A Decentralized Network for Internet of Trusted Things



Decentralized



109 repositories



7 members



IOTA iotalledger

Verified

IOTA is a distributed ledger based on the Tangle. It allows for feeless value transfers and data integrity proofs.



Berlin, Germany



217 repositories



19 members

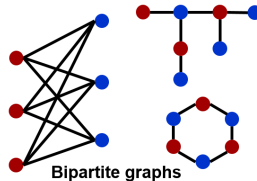
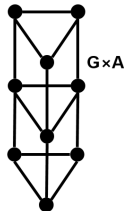
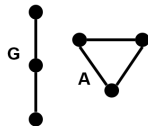
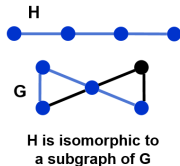
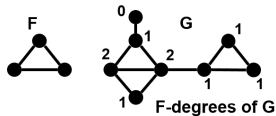
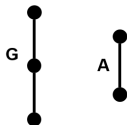
Formalização da comunicação e formas de interação

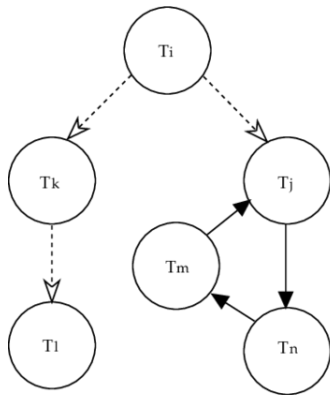


THE BACKBONE OF IOT IS HERE

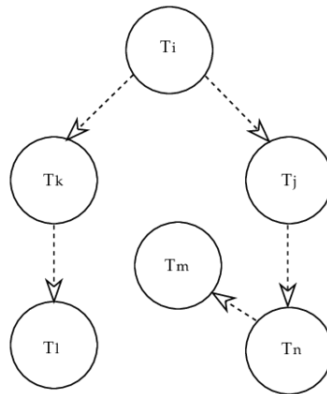
Scalable, Decentralized, Modular, No Fees

[16]



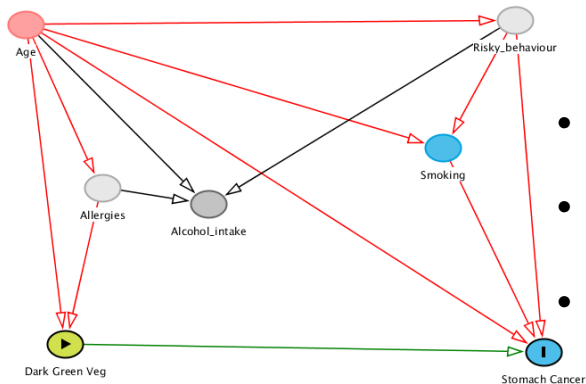


(a) Wait-for graph with a cycle



(b) Wait-for graph with no cycles

[17]

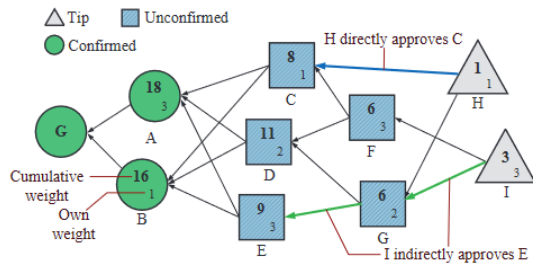
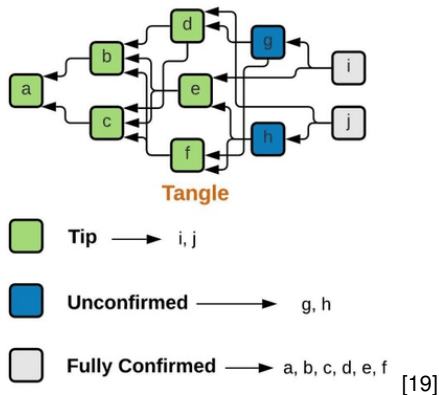


- DAG é um grafo que é direcionado e sem ciclos conectando às outras arestas
- Isso significa que é impossível percorrer todo o grafo começando em uma borda
- As bordas do grafo direcionado só seguem um caminho

[18]

DAGitty: a browser-based environment for creating, editing, and analyzing DAGs

Iota Tangle Visualization

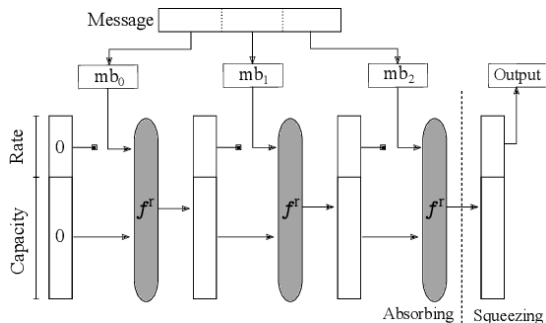


[20]



Prova de características e propriedades

- Curl-P (às vezes chamado de Curl) é uma função de hash criptográfica projetada especificamente para uso em IOTA
- Ele tem sido usado para vários propósitos no IOTA, incluindo a criação de endereços de transação, criação de hashes de mensagens, Proof-of-Work (PoW) e assinaturas baseadas em hash
- Heilman et al [22] demonstrou vulnerabilidades no Curl-P



[22]

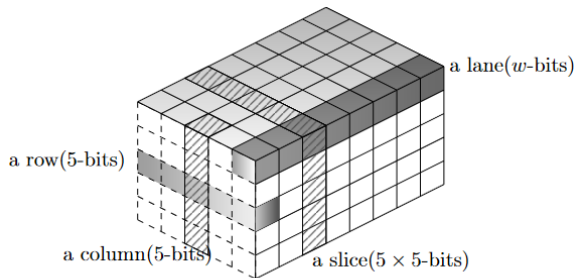
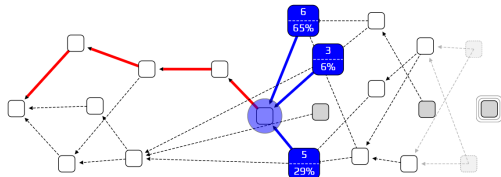


Fig. 2. A state in KECCAK

[23]

- SHA-3 (Secure Hash Algorithm version 3) é um algoritmo para geração de códigos hash. Foi lançado em 2015 para substituir os antecessores SHA-1 e SHA-2
- Em 2 de Novembro de 2007 o NIST anunciou uma competição pública para definir um novo algoritmo de hash tendo em vista substituir os algoritmos SHA-1 e SHA-2, em 2012
- Em 2 de outubro de 2012, o algoritmo Keccak, foi declarado vencedor da competição [24]

Como a IOTA atinge o consenso: Markov Chain Random Walk



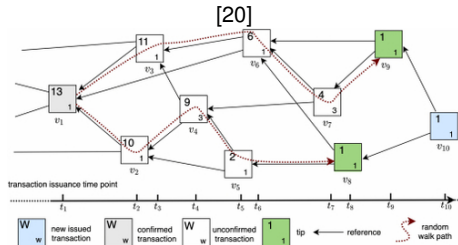
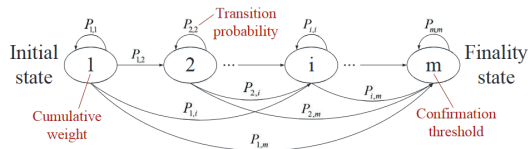
[25]

$$P_{T_0 T_1} = \frac{e^{-0.1(6-2)}}{e^{-0.1(6-2)} + e^{-0.1(6-3)} + e^{-0.1(6-1)}} = 0.33$$

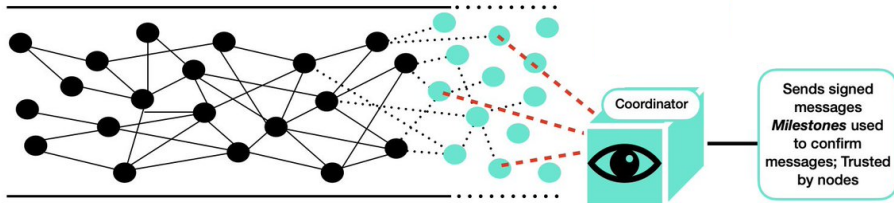
$$P_{T_0 T_2} = \frac{e^{-0.1(6-3)}}{e^{-0.1(6-2)} + e^{-0.1(6-3)} + e^{-0.1(6-1)}} = 0.37$$

$$P_{T_0 T_3} = \frac{e^{-0.1(6-1)}}{e^{-0.1(6-2)} + e^{-0.1(6-3)} + e^{-0.1(6-1)}} = 0.30$$

[26]



[27]



[28]

- O Tangle requer um “Coordenador” que é um item que valida as transações
- Portanto, o IOTA ainda não possui uma arquitetura verdadeiramente descentralizada
- A fundação IOTA considera que esta centralização é necessária enquanto se espera por um número suficiente de nós para poder remover este coordenador
- A fundação está empenhada em retirar o coordenador o mais rápido possível, mas disse que ainda não é possível estimar quando serão cumpridas as condições para esta paralisação.

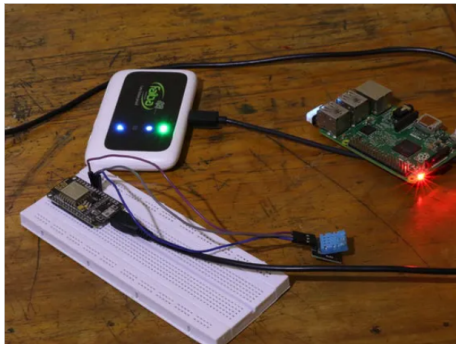


[29]

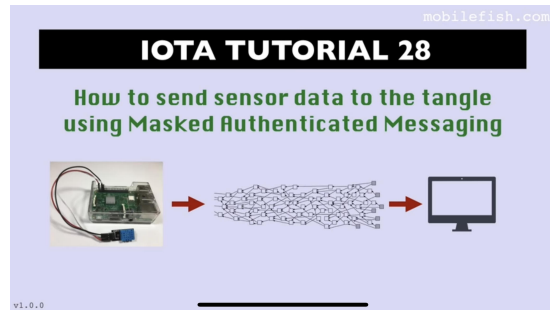


[30]

Uma Aplicação Prática

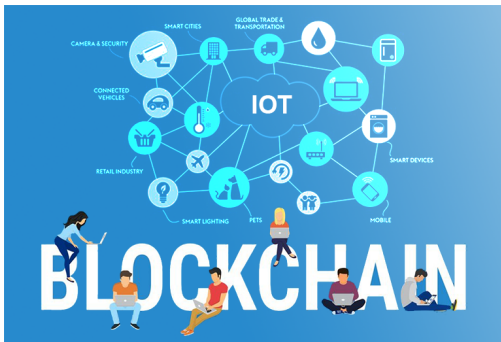


[31]




[32]

Considerações Finais



[33]

- Ainda há poucas Blockchains focadas em dispositivos IoT
- Nem mesmo a Tangle da IOTA (a mais citada) ainda não conseguiu resolver de forma absoluta o problema (ainda é centralizada e possui questionamentos quanto à segurança da sua criptografia)
- Isso abre oportunidades para pesquisas de um Blockchain para dispositivos IoT que apresente as características fundamentais e formas de interação e que formalize e prove características e propriedades tais como a descentralização, a criptografia e o mecanismo de consenso

 Ming Tao, Xiaoyu Hong, Chao Qu, Jie Zhang, and Wenhong Wei.

Fast access for zigbee-enabled iot devices using raspberry pi.

2018 Chinese Control And Decision Conference (CCDC), pages 4281–4285, 2018.

 Dr. Ashok Chopra.

Blockchain technology in food industry ecosystem.

IOP Conference Series: Materials Science and Engineering, 872:012005, 06 2020.

 Emanuele Ragnoli.

A blockchain architecture for the internet of things.

[https:](https://www.ibm.com/blogs/research/2018/10/blockchain-internet-of-things/m)


[//www.ibm.com/blogs/research/2018/10/blockchain-internet-of-things/m](https://www.ibm.com/blogs/research/2018/10/blockchain-internet-of-things/m).

Acessado: 2022-06-01.

 Alexandre Sztajnberg, Roberto Macedo, and Matheus Stutzel.


Protocolos de Aplicação para a Internet das Coisas: conceitos e aspectos práticos, pages 99–148.

Sociedade Brasileira de Computação, 07 2018.

 Mingli Wu, Xiaoqin Cai, Song Guo, Minyi Guo, and Chunming Rong.

A comprehensive survey of blockchain: From theory to iot applications and beyond.

IEEE Internet of Things Journal, PP:1–1, 06 2019.

 Laphou Lao, Zecheng Li, Songlin Hou, Bin Xiao, Songtao Guo, and Yuanyuan Yang.

A survey of iot applications in blockchain systems: Architecture, consensus, and traffic modeling.

ACM Computing Surveys (CSUR), 53:1–32, 02 2020.

 Junghun Yoo, Youlim Jung, Donghwan Shin, Minhyo Bae, and Eunkyoung Jee.

Formal modeling and verification of a federated byzantine agreement algorithm for blockchain platforms.

2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), pages 11–21, 2019.



Satoshi Nakamoto.

Bitcoin: A peer-to-peer electronic cash system, 2009.



Jauberth Abijaude, Fabíola Greve, and Péricles Sobreira.

Blockchain e Contratos Inteligentes para Aplicações em IoT, Uma Abordagem Prática, pages 149–197.

Sociedade Brasileira de Computação, 07 2021.



Alibaba Clouder.

Comprehensive review of proof-of-work consensus in blockchain.

[https://www.alibabacloud.com/blog/
comprehensive-review-of-proof-of-work-consensus-in-blockchain_597042](https://www.alibabacloud.com/blog/comprehensive-review-of-proof-of-work-consensus-in-blockchain_597042).

Acessado: 2022-06-06.



Christopher Natoli, Jiangshan Yu, Vincent Gramoli, and Paulo Esteves Veríssimo.

Deconstructing blockchains: A comprehensive survey on consensus, membership and structure.

ArXiv, abs/1908.08316, 2019.



Mike Rogers.

Financing corporate expansion through tokenization.

In The Definitive Guide to Blockchain for Accounting and Business: Understanding the Revolutionary Technology, pages 127–147. Emerald Publishing Limited, September 2020.



Leslie Lamport, Robert E. Shostak, and Marshall C. Pease.

The byzantine generals problem.

ACM Trans. Program. Lang. Syst., 4:382–401, 1982.



Neo.

Practical byzantine fault tolerance (pbft) and delegated byzantine fault tolerance (dbft).

[https:](https://docs.neo.org/v2/tutorials/en-us/7-consensus/3-PBFT_and_DBFT.html)

[//docs.neo.org/v2/tutorials/en-us/7-consensus/3-PBFT_and_DBFT.html](https://docs.neo.org/v2/tutorials/en-us/7-consensus/3-PBFT_and_DBFT.html).

Acessado: 2022-06-17.



Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz.

On blockchain and its integration with iot. challenges and opportunities.

Future Generation Computer Systems, 88:173–190, 2018.



Valerio Vaccaro.

Iota - the backbone of iot is here.

https://miro.medium.com/max/1400/1*IkWDoX1XWc1mM1re2DcLXQ.png.

Acessado: 2022-06-14.



Elisa Bertino, Benjamin Catania, and A. Vinai.

Transaction models and architectures.

08 2000.



Chaochen Wang.

Directed acyclic graphs (dags).

URL: <https://wangcc.me/DAG-CSS/#33>.



Mohd Akhtar, Danish Rizvi, Mohd Ahad, Salil Kanhere, Mohammad Amjad, and Giuseppe Coviello.
Efficient data communication using distributed ledger technology and iota-enabled internet of things for a future machine-to-machine economy.

Sensors, 21:4354, 06 2021.



Bin Cao, Yixin Li, Lei Zhang, Long Zhang, Shahid Mumtaz, Zhenyu Zhou, and Mugen Peng.
When internet of things meets blockchain: Challenges in distributed consensus.

IEEE Network, PP:1, 03 2019.



Simply Explained.

Iota tangle: Simply explained.

URL: https://www.youtube.com/watch?v=CZxH1V_zoug.



Ethan Heilman, Neha Narula, Garrett Tanzer, James Lovejoy, Michael Colavita, Madars Virza, and Tadge Dryja.
Cryptanalysis of curl-p and other attacks on the iota cryptocurrency.

IACR Cryptol. ePrint Arch., 2019:344, 2019.



Rajendra Kumar, Nikhil Mittal, and Shashank Singh.

Cryptanalysis of 2 round keccak-384.

In Debrup Chakraborty and Tetsu Iwata, editors, *Progress in Cryptology – INDOCRYPT 2018*, pages 120–133, Cham, 2018. Springer International Publishing.



Christof Paar and Jan Pelzl.

Sha-3 and the hash function keccak.

Understanding Cryptography-A Textbook for Students and Practitioners, 2010.



Blog IOTA.

The tangle: an illustrated introduction.

URL: [https:](https://blog.iota.org/the-tangle-an-illustrated-introduction-f359b8b2ec80/)

[//blog.iota.org/the-tangle-an-illustrated-introduction-f359b8b2ec80/](https://blog.iota.org/the-tangle-an-illustrated-introduction-f359b8b2ec80/).



Aminul Islam.

How markov chain is used in iota to select tip.

URL: [https://letsseetech.com/
how-monte-carlo-markov-chain-is-used-in-iota-to-select-tip/](https://letsseetech.com/how-monte-carlo-markov-chain-is-used-in-iota-to-select-tip/).



Caixiang Fan, Sara Ghaemi, Hamzeh Khazaei, Yuxiang Chen, and Petr Musilek.

Performance analysis of the iota dag-based distributed ledger.

ACM Trans. Model. Perform. Eval. Comput. Syst., 6(3), dec 2021.



XX₁133₁221₁1.

Iota coordinator.

URL: <https://www.trendsmap.com/twitter/tweet/1497805681017118721>.



Ben Munster.

Iota suffers costly hack attack and switches its crypto off.

URL: <https://decrypt.co/19282/iota-gets-in-a-spot-of-trouble-and-switches-its-crypto-off>.



IOTA Twitter Account.

Currently, #iota is working with law enforcement and cybersecurity experts to investigate a coordinated attack, resulting in stolen funds. to protect users, we have paused the coordinator and advise users not to open trinity until further notice. updates: <https://status.iota.org>.

URL: <https://twitter.com/iota/status/1227990537799524352>.



Peter Okwara.

Sending temperature and humidity data to the iota tangle.

URL: <https://www.hackster.io/peterokwara/sending-temperature-and-humidity-data-to-the-iota-tangle-91671d>.



Robert Lie.

Sensor dht11 sensor data using raspberry pi 3 to iota tangle using masked authenticated messaging (mam).

URL: [https:](https://www.mobilefish.com/developer/iota/iota_quickguide_raspi_mam.html)

[//www.mobilefish.com/developer/iota/iota_quickguide_raspi_mam.html](https://www.mobilefish.com/developer/iota/iota_quickguide_raspi_mam.html).



Value Coders.

9 ways blockchain iot union help elevate your business value.

URL: [https://www.valuecoders.com/blog/technology-and-apps/](https://www.valuecoders.com/blog/technology-and-apps/9-ways-blockchain-iot-union-help-elevate-your-business-value/)

[9-ways-blockchain-iot-union-help-elevate-your-business-value/](https://www.valuecoders.com/blog/technology-and-apps/9-ways-blockchain-iot-union-help-elevate-your-business-value/).



Hany F. Atlam and Gary B. Wills.

Chapter three - intersections between iot and distributed ledger.

In Shiho Kim, Ganesh Chandra Deka, and Peng Zhang, editors, *Role of Blockchain Technology in IoT Applications*, volume 115 of *Advances in Computers*, pages 73–113. Elsevier, 2019.



Logan Thrasher Collins.

Notes on graph theory.

<https://logancollinsblog.com/2018/05/26/notes-on-graph-theory/>.

Acessado: 2022-06-14.



Robert Lie.

Sensor dht11 sensor data using raspberry pi 3 to iota tangle using masked authenticated messaging (mam).

URL: [https:](https://www.mobilefish.com/developer/iota/iota_quickguide_raspi_mam.html)

[//www.mobilefish.com/developer/iota/iota_quickguide_raspi_mam.html](https://www.mobilefish.com/developer/iota/iota_quickguide_raspi_mam.html).

Blockchain como meio de comunicação para recursos, agentes e dispositivos para IoT. Formalização da comunicação e formas de interação, bem como a prova de características e propriedades

Aluno: **Luiz Carlos da Silva Leão**

Professor: Alexandre Sztajnberg

Universidade Estadual do Rio de Janeiro – UERJ

