Aula 002 - Tecnologia Blockchain

Fundamentos, Conceitos, Características. Arquitetura, Benefícios e Limitações.

Prof. Rogério Aparecido Gonçalves[1]
rogerioag@utfpr.edu.br

[1]Universidade Tecnológica Federal do Paraná (UTFPR)
Departamento de Computação (DACOM)
Campo Mourão - Paraná - Brasil

Programa de Pós Graduação em Ciência da Computação
Mestrado em Ciência da Computação
PPGCC17 - Tópicos em Redes de Computadores e Cibersegurança

Agenda i

Introdução

Objetivos

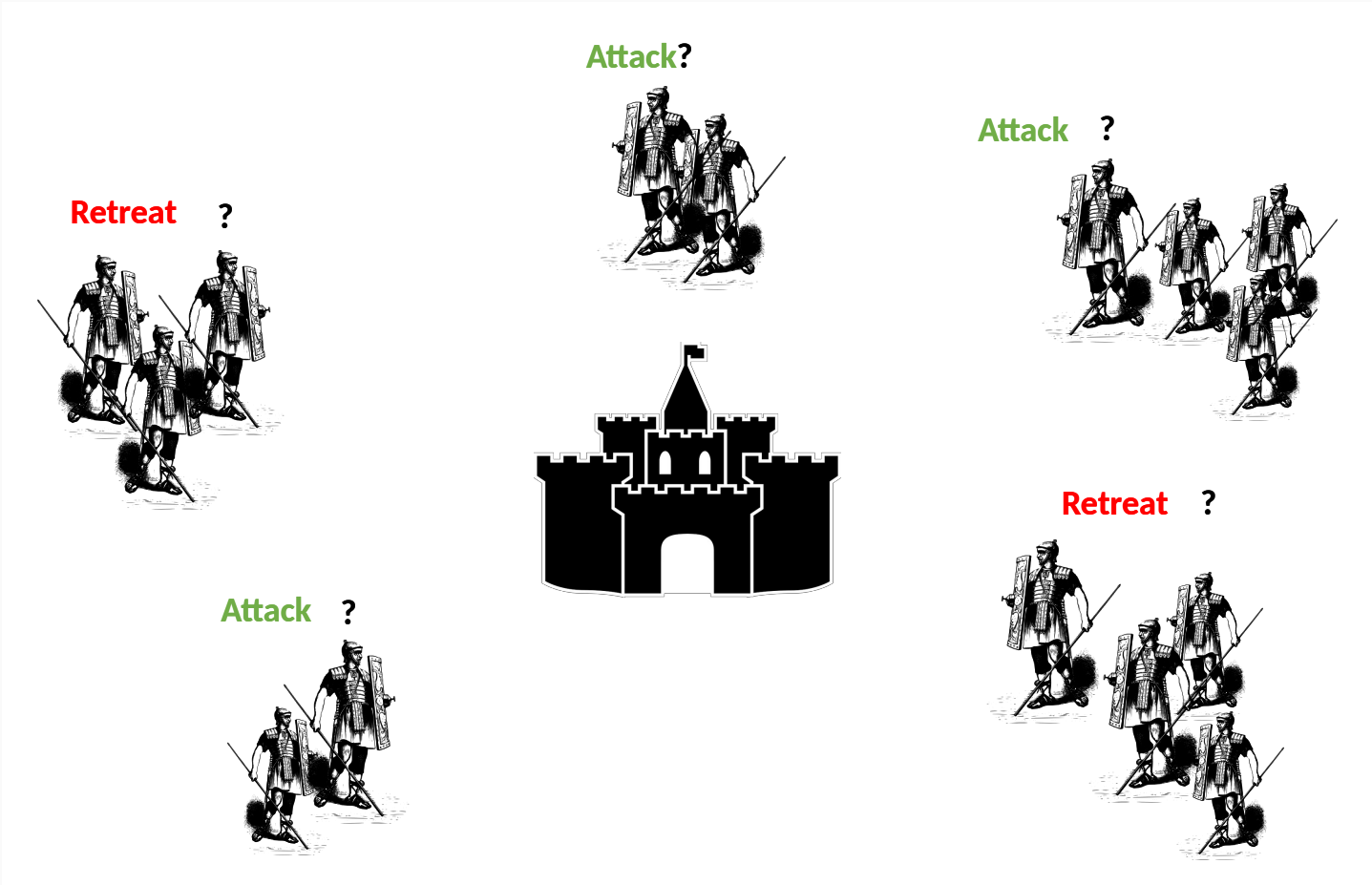
- Descrever os fundamentos de Sistemas Distribuídos
- Definição da Tecnologia Blockchain
- Entender como a Tecnologia Blockchain foi desenvolvida
- Detalhar os elementos de uma Blockchain
- Identificar os benefícios e limitações da Tecnologia Blockchain.

Computação Distribuída

Computação Distribuída i

- Um Sistema Distribuído é um paradigma da Computação onde dois ou mais nós trabalham em conjunto e maneira coordenada para alcançar um objetivo comum.
- Um Sistema Distribuído é modelado de maneira que os usuários finais veem ele como uma única plataforma lógica.
- Exemplos: *Clusters* e *clouds*.

Problema dos Generais Bizantinos i



- Atacar ou recuar? O **Consenso** é necessário para vencer.

Problema dos Generais Bizantinos ii

- Em 1982, um experimento foi proposto por Lamport e outros em um artigo (Lamport, Shostak, and Pease 1982), **The Byzantine Generals Problem**.
- Como analogia a sistemas distribuídos, os generais podem ser considerado os **nós**, os traidores como **nós bizantinos** (maliciosos), e o mensageiro pode ser pensado como um canal de comunicação entre os generais.
- O problema foi resolvido em 1999 por Castro e Liskov, apresentaram o algoritmo *Practical Byzantine Fault Tolerance (PBFT)* (Castro and Liskov 1999), onde o consenso é alcançado depois de um certo número de mensagens serem recebidas contendo o mesmo conteúdo assinado.

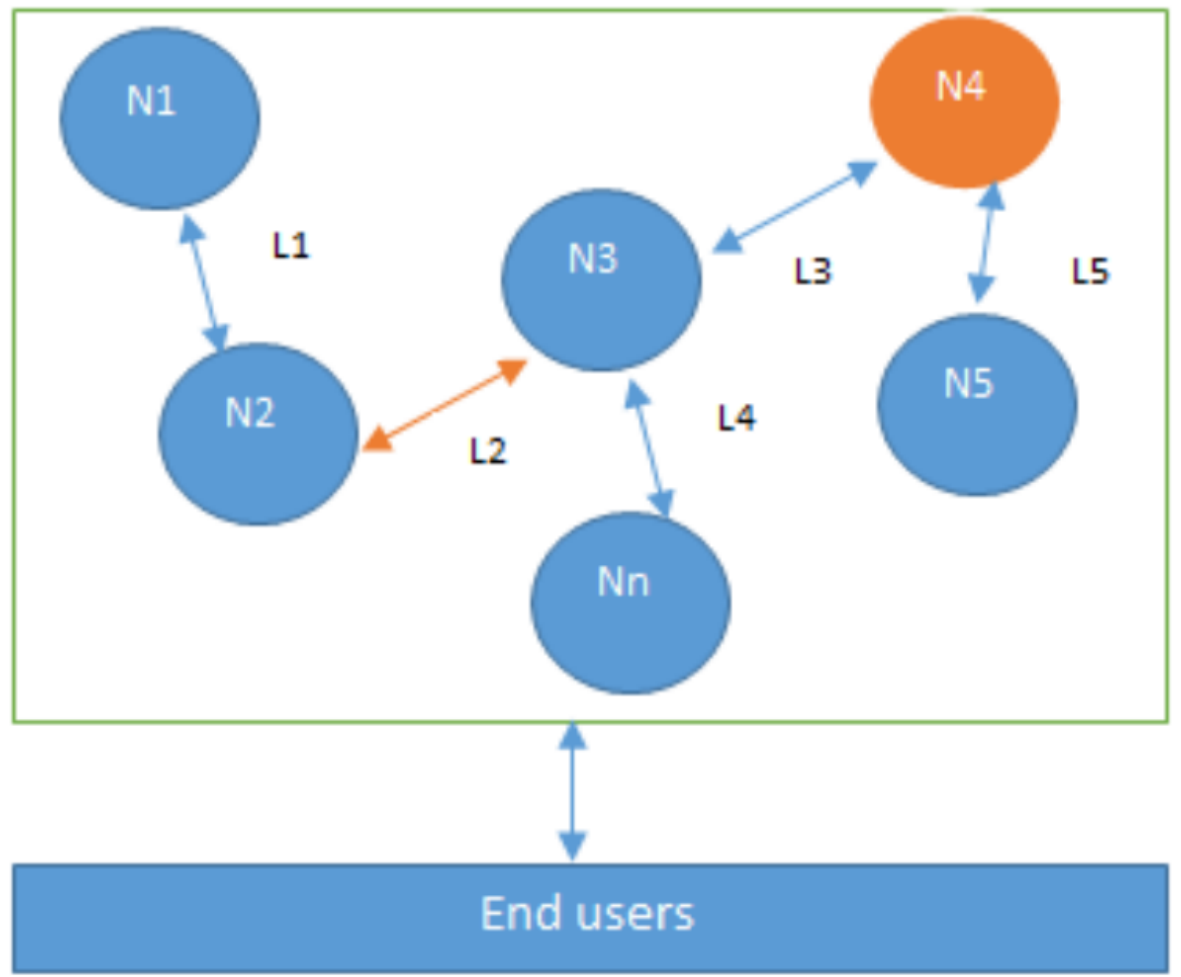
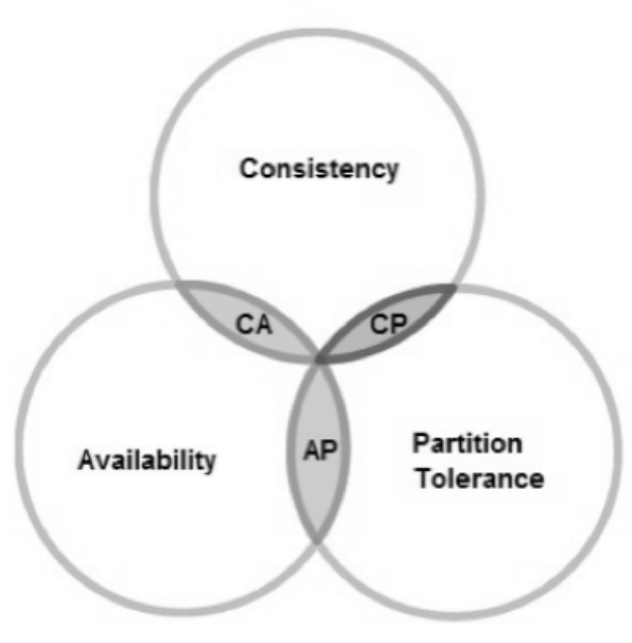


Figura 1: N4 é um nó Bizantino, L2 está quebrado ou é um link de rede lento

Teorema CAP i

- Ele afirma que um Sistema Distribuído pode não ter todas as três propriedades desejadas simultaneamente. Sendo elas:
  - Consistency
  - Availability
  - Partition tolerance

Teorema CAP ii



CA - os dados estão consistentes em todos os nós, e todos os nós estão *online*.

CP - os dados estão consistentes em todos os nós, e mantém *partition tolerance* (prevenindo dessincronizações), torna-se indisponível quando um nó fica inativo.

AP - os nós permanecem *online* mesmo que não possam se comunicar entre si.

Ressincronizarão os dados assim que a partição for resolvida, mas não há garantia de que todos os nós terão os mesmos dados (durante ou após a partição).

Tipos de falhas em Sistemas Distribuídos

- *Fail-stop faults (crash faults)*
  - Onde os componentes falham ou param de operar
  - Mais simples de lidar
- *Byzantine faults*
  - As quais os componentes são potencialmente não confiáveis ou maliciosos
  - Difícil de lidar

Conceitos e Fundamentos de Blockchain

Definição de Blockchain i

Definição de Layman

Blockchain is an ever-growing, secure, shared recordkeeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update.

Definição Técnica

Blockchain is a peer-to-peer distributed ledger that is cryptographically-secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.

Definição de Blockchain ii

- *Peer-to-peer*
- *Distributed Ledger*
- *Criptograficamente Seguro*
- *Append only (Permitido anexar novos blocos)*
- *Atualizável via consenso dos pares.*

Como a Tecnologia Blockchain foi desenvolvida i

1950s – Hash functions

1970s – Merkle trees - hashes in a tree structure

1970s continued – Research in distributed systems, consensus, state machine replication

1980s – Hash chains for secure logins

1990s – *e-Cash for e-payments*

1991 – Secure timestamping of digital documents.

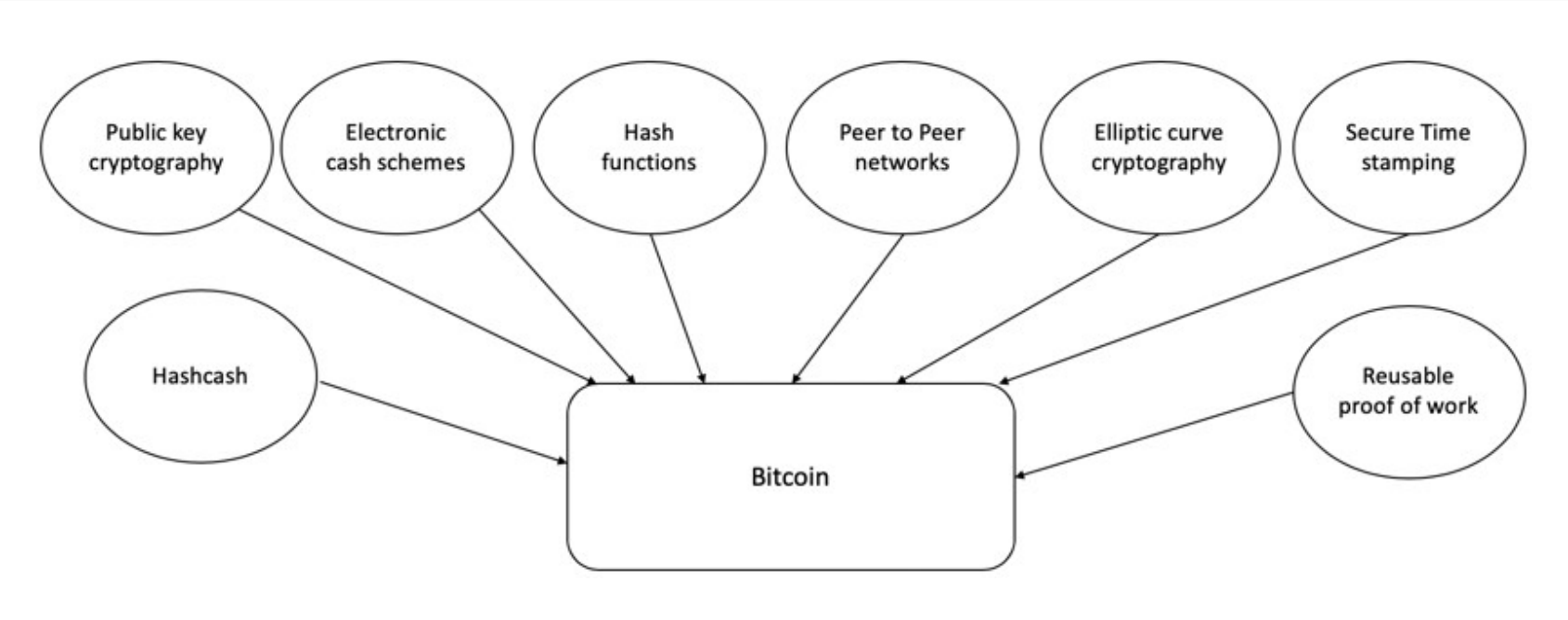
1992 – Hashcash idea to combat junk emails

1994 – S/KEY application for Unix login.

1997/2002 – *Hashcash*

2008/2009 – Bitcoin (the first blockchain)

Como a Tecnologia Blockchain foi desenvolvida ii



Interesse no termo “blockchain”

- Interesse ao longo do tempo (Fonte: Google Trends):

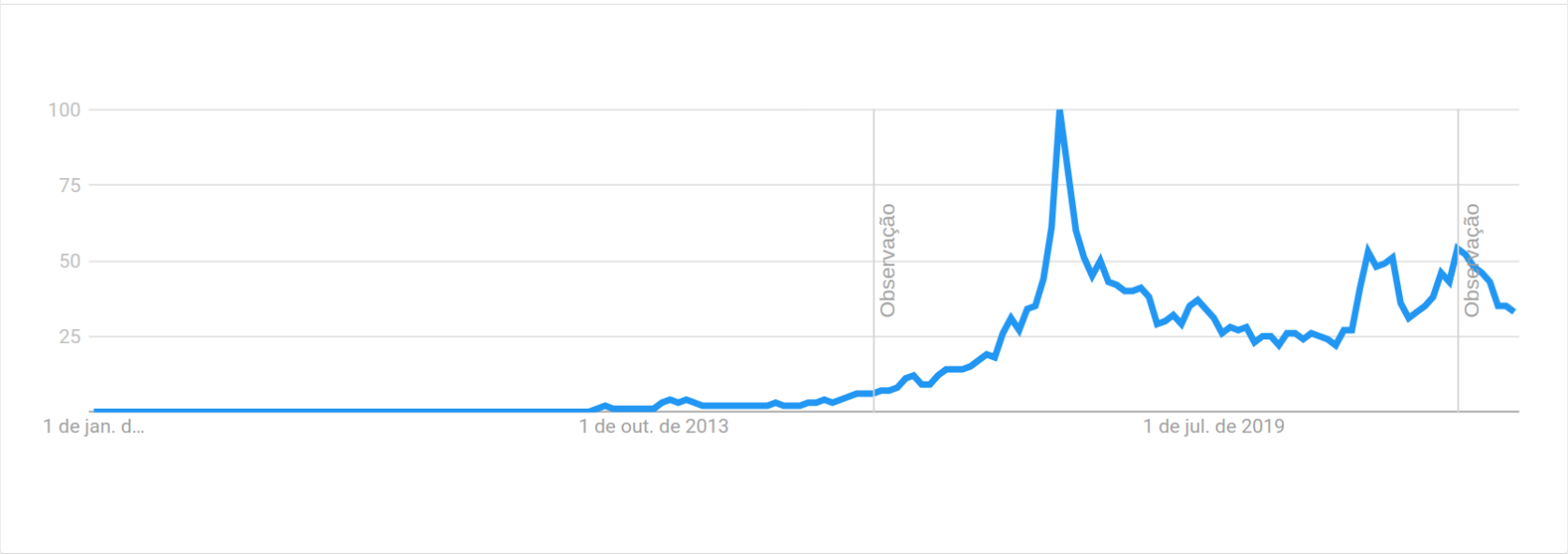
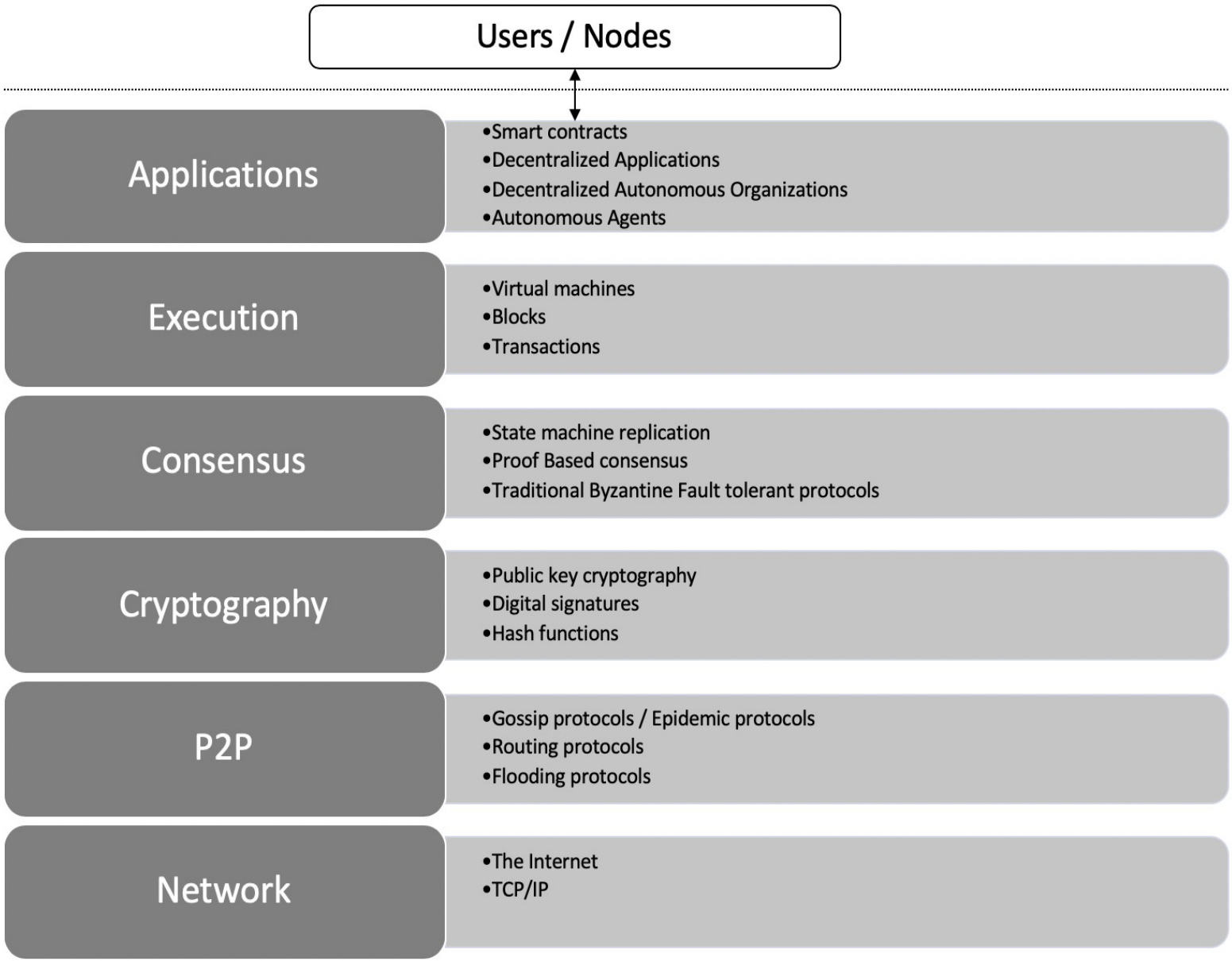


Figura 2: Pesquisas sobre o termo “blockchain”

Visão Arquitetural do Blockchain



Estrutura Genérica de um Blockchain i

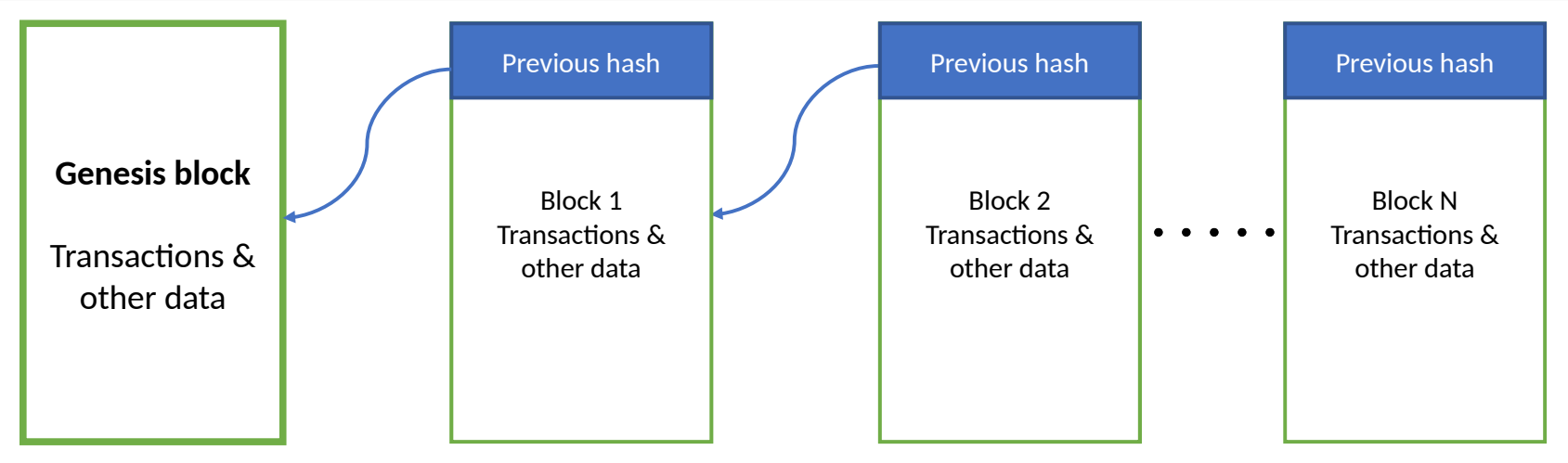


Figura 3: Estrutura Genérica de um Blockchain

Elementos Genéricos de um Blockchain i

- Endereços
- Contas
- Transações
- Blocos
- Redes *Peer-to-peer*
- Scripting ou Linguagens de Programação
- Virtual machines
- Máquinas de Estado
- Nós (nodes)
- Contratos Inteligentes *(Smart contracts)*

Como um Blockchain funciona i

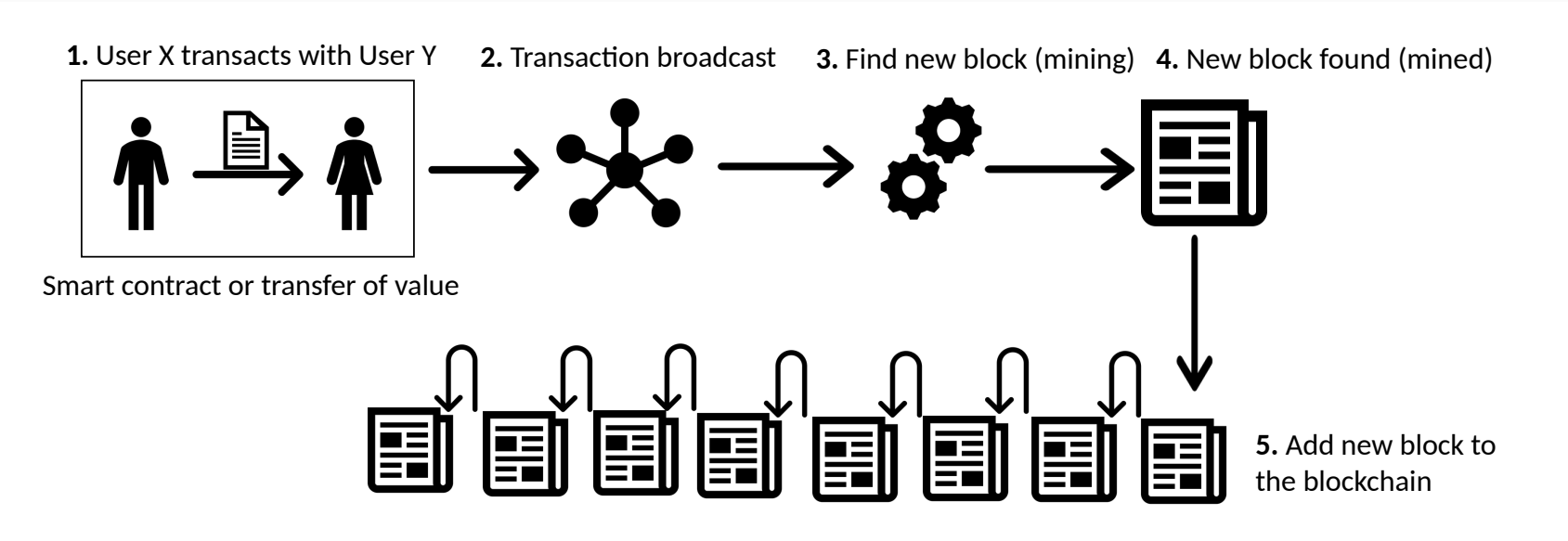


Figura 4: Funcionamento de um Blockchain

Estrutura Genérica de um bloco i

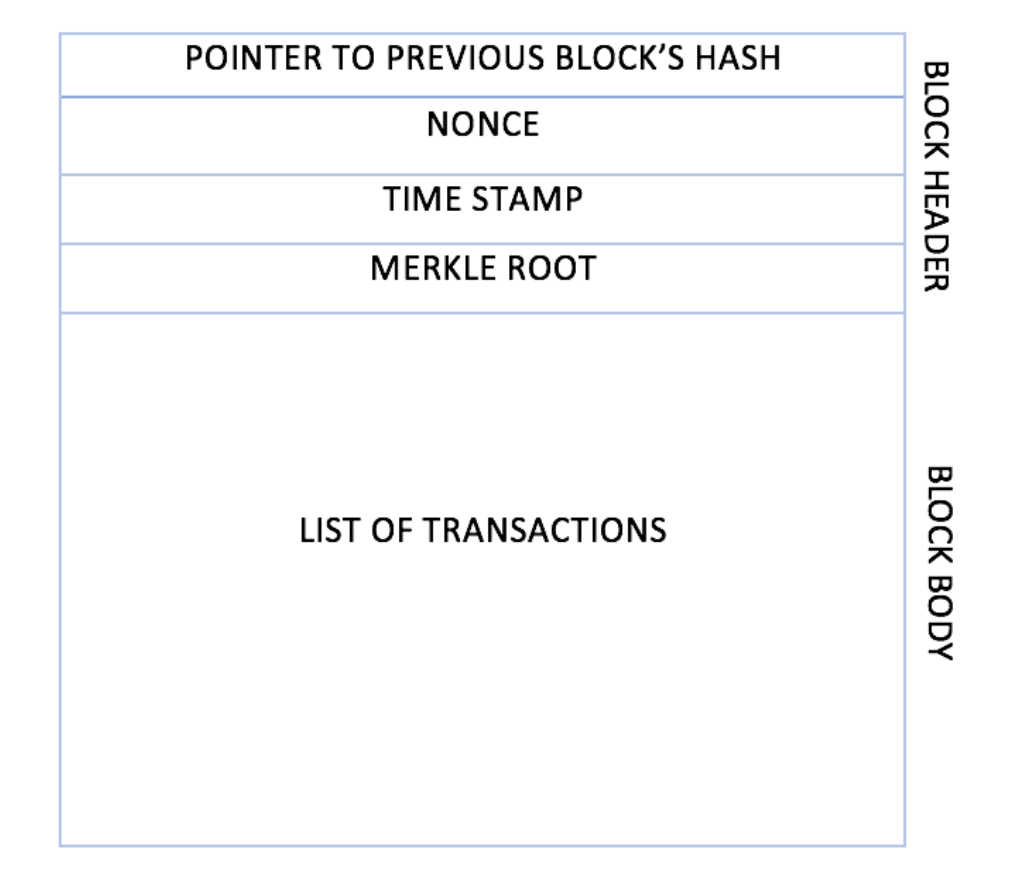


Figura 5: Estrutura de um Bloco

Benefícios e Limitações de um Blockchain

Benefícios

Descentralização

Transparência

Confiança

Imutabilidade

Alta disponibilidade

Altamente Seguro

Simplificação de paradigmas atuais

Transações rápidas

Cost saving

Limitações

Escalabilidade

Adaptabilidade

Regulação

Tecnologia Relativamente Imatura

Privacidade

Características Principais i

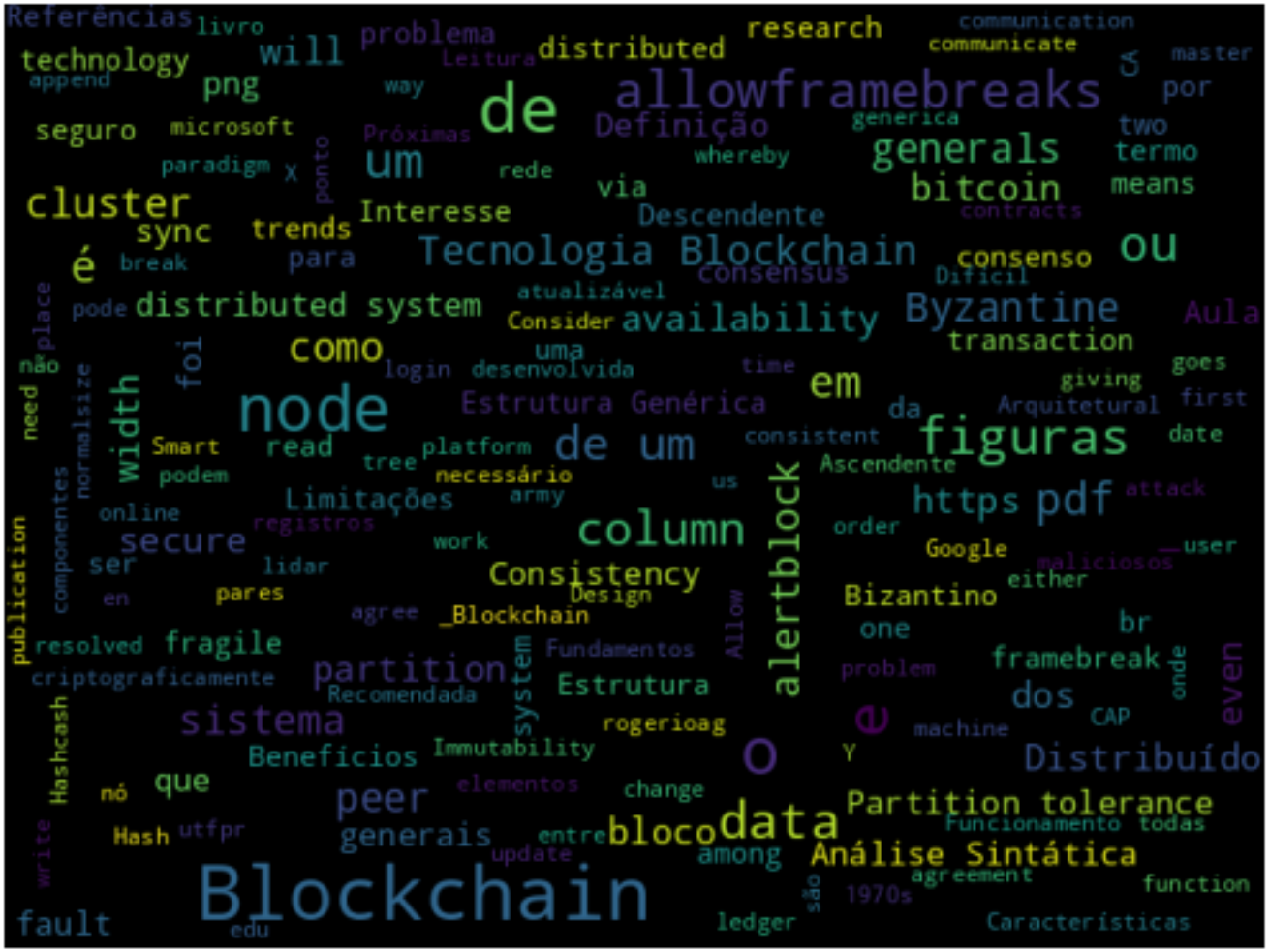
- Consenso Distribuído
- Verificação de Transações
- Plataforma para *smart contracts*
- Transferência de valores entre pares
- Generação de criptomoedas
- Provedor de Segurança
- Imutabilidade
- Unicidade ou singularidade (Uniqueness)

Atividade

Leitura

Bitcoin paper: https://bitcoin.org/bitcoin.pdf

Word Cloud


Referências
livro
problema
research
communication
communicate
technology
will
distributed
Leitura
master
append
png
way
de
allowframebreaks
por
seguro
microsoft
Próximas
Definição
generica
two
paradigm
ponto
um
rede
whereby
generals
termo
cluster
via
bitcoin
means
sync
Interesse
Descendente
contracts
trends
é
break
para
Tecnologia Blockchain
consenso
ou
consensus
Difícil
pode
distributed system
atualizável
Consider
availability
Byzantine
Aula
como
uma
transaction
não
login
desenvolvida
time
em
giving
goes
width
foi
Estrutura Genérica
da
Arquitetural
first
node
need
Smart
read
de um
consistent
figuras
date
podem
platform
Ascendente
tree
necessário
us
Limitações
army
https
pdf
attack
online
secure
column
order
registros
work
Google
user
ser
lidar
Consistency
maliciosos
pares
Design
Bizantino
either
en
agree
_Blockchain
one
br
resolved
fragile
Fundamentos
framebreak
criptograficamente
partition
Estrutura
problem
dos
even
Recomendada
sistema
rogerioag
machine
CAP
Hashcash
Beneficios
Immutability
Y
Distribuído
que
nó
peer
elementos
change
Partition tolerance
Hash
utfpr
generais
entre
bloco
data
Funcionamento
todas
update
among
Análise Sintática
Blockchain
agreement
function
fault
edu
ledger
1970s
Características

Leitura Recomendada

Leitura Recomendada

Capítulo 1: Blockchain 101

Livro: IMRAN BASHIR. Mastering Blockchain : Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition.

Próximas Aulas

Próximas Aulas: Tecnologia Blockchain

- Arquitetura, Benefícios e Limitações.

Referências

Referências i

Castro, Miguel, and Barbara Liskov. 1999. “Practical Byzantine Fault Tolerance.” In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, OSDI ’99, USA: USENIX Association, 173–86.

Imran, Bashir. 2018. *Mastering Blockchain : Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition.* Packt Publishing. https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=1789486&lang=pt-br&site=eds-live&scope=site.

Lamport, Leslie, Robert Shostak, and Marshall Pease. 1982. “The Byzantine Generals Problem.” *ACM Transactions on Programming Languages and Systems*: 382–401. https://www.microsoft.com/en-us/research/publication/byzantine-generals-problem/.