



Blockchain & Criptomoedas 101

Matheus Degiovani

Desenvolvedor independente – Decred

matheusd.com

Meu trabalho na Decred

- Criptomoeda baseada em blockchain
- Proof of Work (PoW) e Proof of Stake (PoS)
- Autofinanciada (10% da recompensa de bloco)
- Autogerida (Entidade Autônoma Descentralizada)
- Totalmente Software Livre
- Totalmente Remoto
- Time Global

Go(lang)

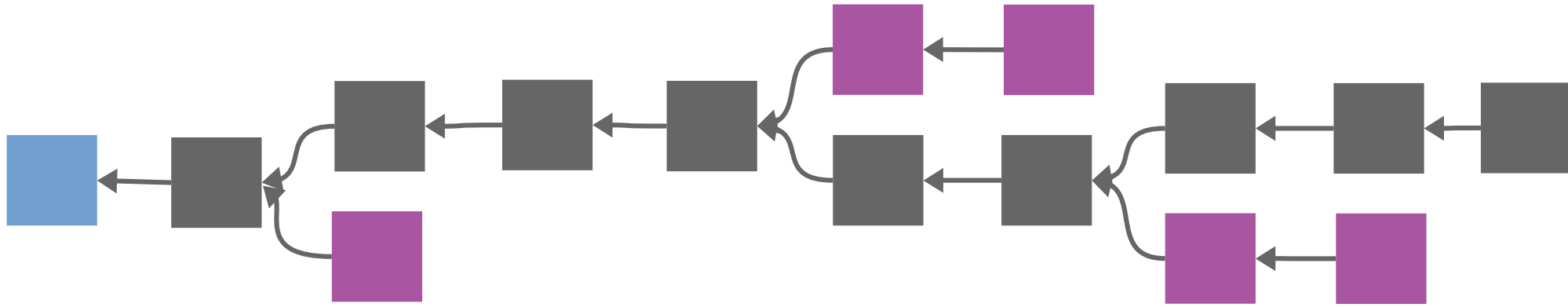
- Rob Pike & Ken Thompson (Unix), Robert Griesemer
- @ Google, 2007

```
type Bloco struct {  
    BlocoAnterior *Bloco  
    Nonce          uint64  
    Dados          []byte  
}
```

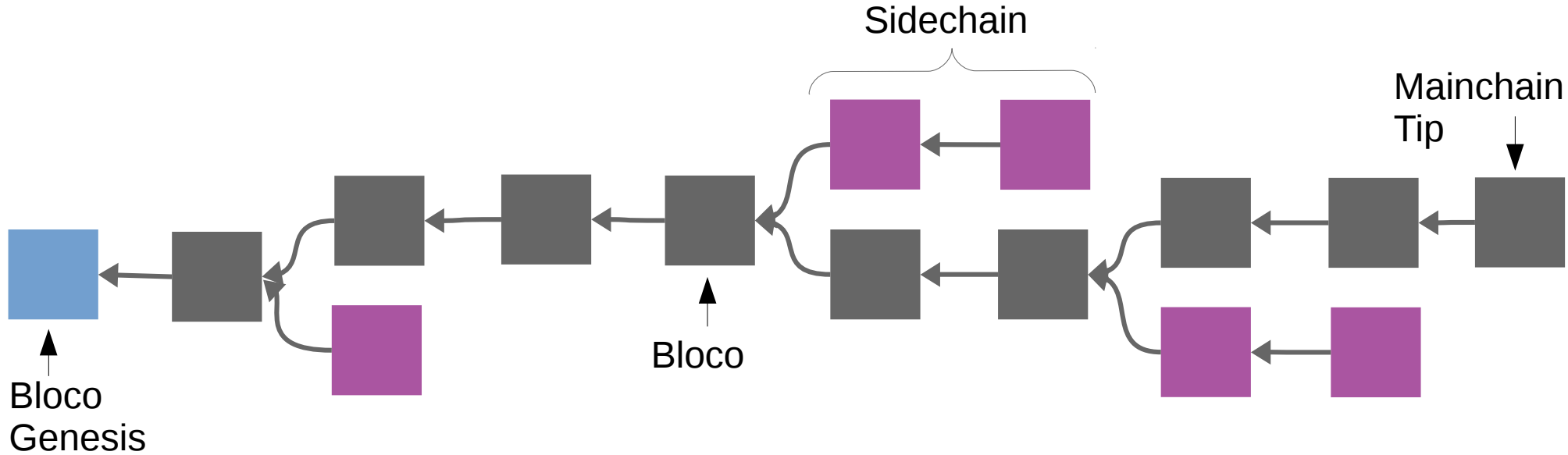
```
func (b *Bloco) Hash() []byte {  
    h := sha256.Sum256(b.Serializar())  
    return h[:]  
}
```

```
func (b *Bloco) Serializar() []byte {  
  
    // Init do buffer p/ serializar blocoAnterior+nonce+dados  
    buffer := make([]byte, 32+8+len(b.Dados))  
  
    // BlocoAnterior do genesis é nil; testar antes de copiar  
    if b.BlocoAnterior != nil {  
        copy(buffer, b.BlocoAnterior.Hash())  
    }  
  
    // Copiar nonce (8 bytes) e buffer de dados (variável)  
    binary.LittleEndian.PutUint64(buffer[32:], b.Nonce)  
    copy(buffer[32+8:], b.Dados)  
  
    return buffer  
}
```


Blockchain & Criptomonedas 101




Blockchain & Criptomonedas 101

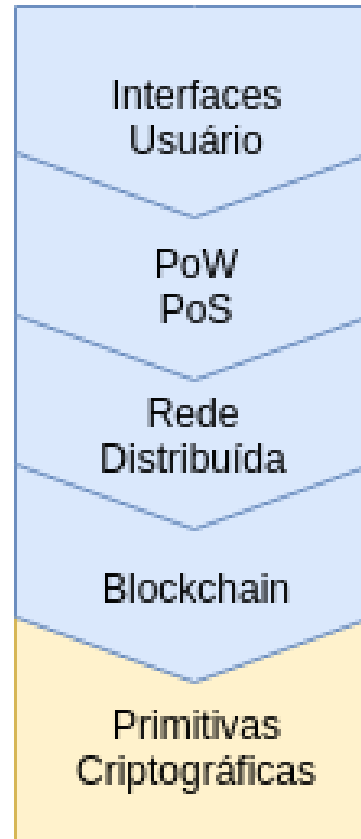



```
type Bloco struct {  
    BlocoAnterior *Bloco  
    Nonce          uint64  
    Dados          []byte  
}
```

Pode ser qualquer coisa



Pilha Tecnológica - Criptomoeda



```
func ProofOfWork(candidato *Bloco) *Bloco {  
    minerado := &Bloco{  
        BlocoAnterior: candidato.BlocoAnterior,  
        Dados:          candidato.Dados,  
        Nonce:           0,  
    }  
  
    // Mineração Simplificada (2 primeiros bytes == 0).  
    for minerado.Hash()[0] != 0 || minerado.Hash()[1] != 0 {  
        minerado.Nonce++  
    }  
  
    return minerado  
}
```

```
$ go run .
```

Bloco 1

```
(00009cf981bf132c3fe05139b5f6c085e2481dc593ee325afca40401709dc26c)
```

```
    Nonce: 19358    Dados: bloco da altura 1; rnd=32c1d999321de9be
```

Bloco 2

```
(00007b28863dd30a54f1980c180ce209b26443eef49c4a0a64840f109867e4f1)
```

```
    Nonce: 31253    Dados: bloco da altura 2; rnd=176ad1241a48f2cf
```

Bloco 3

```
(0000e9182dd70a9517a5bc3ebfc046a6520617cd888d9eddef977cd5930e73cf)
```

```
    Nonce: 85263    Dados: bloco da altura 3; rnd=37c1f9282b79c71c
```

Bloco 4

```
(0000e7d819394534c52ccd1d4a9cdb0f535ecebdb2a4e61a2add9ee7bad1b74d)
```

```
    Nonce: 1229     Dados: bloco da altura 4; rnd=1dd465214e68d843
```

BLOCKCHAIN PROJECT ECOSYSTEM

CURRENCIES

BASE LAYER PROTOCOLS



PAYMENTS

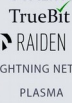


DEVELOPER TOOLS

SMART CONTRACTS



SCALING



ORACLES



SECURITY



LEGAL



INTEROPERABILITY



PRIVACY



DAGs



SOVEREIGNTY

USER-CONTROLLED



GOVERNANCE



VPN



COMMUNICATION



IDENTITY



SECURITY



STABLECOINS



FINTECH

TRADING/DEX



INSURANCE



LENDING



FUNDS/INVESTMENT



VALUE EXCHANGE

CONTENT MONETIZATION



DATA



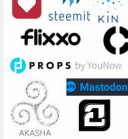
MARKETPLACES



SOCIAL



VIDEO



NON-FUNGIBLE

FILE STORAGE



COMPUTATION



MESH NETWORKING



ENERGY



FUNGIBLE



SHARED DATA

INTERNET OF THINGS



SUPPLY CHAIN/LOGISTICS



ATTRIBUTION



REPUTATION



CONTENT CURATION

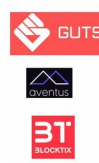


AUTHENTICITY

DATA



TICKETING



REPUTATION



OTHER

PREDICTION MARKETS



VIRTUAL REALITY



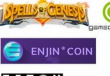
GAMBLING



GAMING/ ESPORTS



MARKETPLACES



CRYPTOCURRENCY



TEAM



compound

@JOSH_NUSSBAUM

Moral da história das blockchains

Estrutura de dados com integridade, não repúdio, imutabilidade

Moral da história das criptomoedas

Política monetária algorítmica ao invés
de por decreto

Moral da história da Ethereum

Gamificação do processamento de dados

Moral da história da Filecoin/IPFS

Gamificação da armazenagem de dados

Moral da história dos Tokens

Gamificação das micro-interações

Moral da história da Decred

Gamificação da governança via PoS

E eu nem falei de...

- Carteiras
- Soluções de Segunda Camada (Second Layer)
- Lightning Network
- Decentralized Exchanges (DEX)
- Decentralized Autonomous Entities (DAEs)
- Stablecoins
- Permissionless
- Relação com IOT
- Relação com fintechs
- Custodial vs não custodial
- Auto financiamento
- ICOs
- Filosofia Cypherpunk
- Política monetária deflacionária vs inflacionária
- Proof of space-time



Blockchain & Criptomoedas 101

Matheus Degiovani

Desenvolvedor independente – Decred

matheusd.com