

### Consulta solicitada à Sra. Camila Gonçalves Marques.

As empresas abaixo mencionadas foram constituídas com o aparente propósito de desenvolver as seguintes atividades:

- **Rental Coins** operações de compra, venda, custódia e intermediação dos criptoativos.
- **Interag Consultoria** desenvolvimento de franquias: licencia seus produtos e desenvolve o Marketplace das demais empresas.
- **Compralo Administradora de Cartões e Compralo Intermediações**, meios de pagamentos e carteira digital que possibilitariam pagar, receber, converter, rentabilizar, gerar boletos etc.. Os criptoativos geridos deveriam permitir utilização com as demais empresas.
- **Intertradec** corretora de criptoativos,
- **Intergalaxy** desenvolvimento dos softwares utilizados.

A RENTAL COINS teve a falência decretada, ocasião em que nomeado este escritório para o exercício da função de pessoa jurídica Administradora Judicial (AJ). No exercício de suas atividades, o AJ manejou incidente de desconsideração de personalidade jurídica distribuído em apenso à Falência, ocasião em que incluídas as demais empresas retro mencionadas, entre outras.

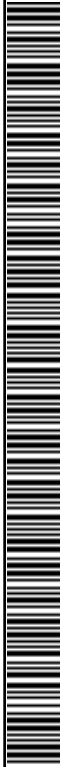
Iniciadas as atividades próprias da Falência, este escritório passou a identificar as duas principais relações jurídicas encetadas pelas falidas e, dentre elas, descortinou-se o seguinte:

#### **a) Locações de criptoativos típicos**

Tratam-se de operações por intermédio das quais o cliente era possuidor de um criptoativo reconhecido (*Bitcoin, Ethereum*, p. ex.), transferiu este criptoativo por intermédio de uma corretora (*Binance*, p. ex.) em favor da FALIDA e firmou um contrato em que a contraprestação da FALIDA seria o pagamento de uma quantia mensal pela **locação** do ativo.

#### **b) Locações de criptoativos BRCP e BRMV**

Tratam-se de operações aparentemente iguais às anteriores. Porém, o cliente não é possuidor do criptoativo em sua carteira privada.



Nestas operações o **CLIENTE** promovia o depósito de recursos financeiros (*reais*) em favor da FALIDA e a própria FALIDA deveria adquirir o criptoativo e, por conseguinte, remunerar os **clientes** a partir de locações dos criptoativos adquiridos. Estes criptoativos adquiridos pela própria FALIDA receberam as designações BRCP e BRMV.

Com efeito, aparentemente os **CLIENTES** não possuíam uma carteira (*wallet*) por intermédio da qual pudessem negociar diretamente estes criptoativos. O único meio de negociá-los era por intermédio da própria plataforma virtual criada pelas FALIDAS.

Feitas estas observações, **consulta**:

***1. Quais os critérios tecnológicos para que um determinado criptoativo seja assim reconhecido?***

*Como descrito no parecer técnico, a rede bitcoin e a rede ethereum são redes “sem permissão”, portanto qualquer pessoa pode desenvolver tokens e aplicativos sem a necessidade de prova de identidade, valor ou funcionalidade do desenvolvimento. O que caracteriza um criptoativo é o padrão de código, por exemplo na rede Ethereum esse padrão é chamado ERC-20<sup>1</sup>, escrito na linguagem de programação chamada Solidity<sup>2</sup>, linguagem desenvolvida especificamente para possibilitar a criação de contratos inteligentes que interajam com a EVM (Ethereum Virtual Machine)<sup>3</sup>.*

*O nome técnico de um criptoativo é “token fungível”, ele segue um padrão de código que caracteriza-o como um token em que cada unidade tem as mesmas características/valor, de forma que ele possa ser um token intercambiável e somável entre si, por exemplo: 1 BRCP + 1 BRCP = 2 BRCP ou 1 BRCP = 1 BRCP. Essa característica do token, assemelha-se ao padrão que utilizamos como moeda (ex. REAL), o que tornou a utilização desse padrão de código popular para a criação das chamadas criptomoedas.*

*Um token ERC-20 deve apresentar as seguintes funções:*

- *Transferir tokens de uma conta para outra*
- *Checar balanço do token na conta*
- *Checar o total de tokens disponíveis na rede*

<sup>1</sup> Fonte: <https://ethereum.org/pt/developers/docs/standards/tokens/erc-20/>, acessado 28/06/2023 às 17:10.

<sup>2</sup> Fonte: <https://docs.soliditylang.org/en/v0.8.20/>, acessado 28/06/2023 às 17:38. O código do token ERC-20 pode ser acessado no endereço eletrônico: <https://etherscan.io/address/0x73484a262730d1d422610729e828346f9b2ff480#code>

<sup>3</sup> Descrito no parecer técnico em detalhes.



- *Aprovar uma determinada quantidade de tokens que um terceiro pode “gastar” em nome de uma conta terceira*

*Se um contrato inteligente<sup>4</sup> apresenta essas funções descritas em sua linha de código ele é caracterizado tecnicamente como um token ERC-20 (“Criptoativo”).*

*Desse modo, para que seja caracterizado um “criptoativo” ele precisa corresponder a um padrão de código que o reconheça como intercambiável e somável com outros que tenham semelhante padrão de código.*

## ***2. BRCP e BRMV foram inscritos em Blockchain? A inscrição é regular? Em que valor? É possível identificar seu criador?***

*Sim, ambos os tokens estão escritos na rede blockchain Ethereum mainnet<sup>5</sup>. Ambos os tokens seguem o padrão técnico que os caracteriza como tokens ERC-20, sua inscrição pode ser considerada regular, quando de sua criação eles não possuíam qualquer valor atrelado. A criação dos tokens na plataforma Ethereum é “sem vínculo”, conforme se especifica abaixo:*

### ***Token ERC-20 BRCP***

*A hash criptográfica da transação de criação do contrato é:*  
*0xed7a02d3e7c2dd80b62431d523b92690d10091d6a7e658e17eaecf5ef7b539a6*

*Informações referente a transação de criação podem ser visualizadas no endereço eletrônico:*  
*<https://etherscan.io/tx/0xed7a02d3e7c2dd80b62431d523b92690d10091d6a7e658e17eaecf5ef7b539a6>*

*O token ERC-20 BRCP tem a hash endereço de contrato:*  
*0x73484A262730d1d422610729e828346F9B2ff480, esse endereço é único, representa a identidade do token na blockchain Ethereum.*

*Todas as interações com o token BRCP ocorrem através deste endereço, devido ao carácter público de visualização das transações na rede blockchain do Ethereum, o histórico de*

<sup>4</sup> Descrito em detalhes no relatório técnico

<sup>5</sup> Rede funcional da blockchain Ethereum, devido à complexidade de desenvolvimento de aplicações em blockchain existem redes de teste (testnet), onde é possível simular a funcionalidade antes de lançar na rede principal. Uma vez que a aplicação é lançada na rede principal, seu código é imutável, ou seja, não pode ser alterado ou corrigido em caso de falhas de design.



*transações pode ser consultado em tempo real no endereço eletrônico:*  
<https://etherscan.io/address/0x73484a262730d1d422610729e828346f9b2ff480>

*O BRCP foi criado na data 17/08/2020, o hash da carteira pública do seu criador é:*  
*0xAdaB4aEE8FD4A86f8f8a169EE67d976B8E251f72*

*As transações feitas pela carteira do seu criador podem ser consultadas em tempo real no endereço eletrônico:*

<https://etherscan.io/address/0xadab4aee8fd4a86f8f8a169ee67d976b8e251f72>

*Conforme descrito anteriormente o caráter de “sem permissão” da rede blockchain Ethereum, não exige cadastro pessoal para criação do endereço da carteira criptográfica<sup>6</sup>, é anônimo e qualquer pessoa pode ter mais de um endereço, no entanto, para utilização da carteira criptográfica é necessário a utilização de um passcode e a carteira deve estar registrada no computador utilizado (Private Key), o que confere à carteira características de uso privado, já que uma vez tendo a gerência da carteira, tem-se o acesso aos fundos nela contidos e poderes sobre todas as transações futuras.*

*O código do token, uma vez na blockchain é impossível de ser alterado. O caráter inovador dos criptoativos é essencialmente a criação de um código que quando lançado na blockchain não pode ser alterado, e toda a sua funcionalidade está predeterminada no código de forma transparente e auditável, como um contrato, essa tecnologia visa a eliminação da ação de terceiro para medição da sua funcionalidade. Na teoria o código deve ser livre de qualquer interferência humana, no entanto, como não há um órgão fiscalizador, fica na responsabilidade do usuário avaliar a confiabilidade dos criptoativos ao qual ele utiliza.*

---

<sup>6</sup> Informações detalhadas no relatório técnico



```
26 contract BrcpToken {
27     string public name = 'BRCP';
28     string public symbol = 'BRCP';
29     uint8 public decimals = 18;
30     uint256 public totalSupply = 250000000;
31
32     mapping (address => uint256) public balanceOf;
33     mapping (address => mapping (address => uint256)) public allowance;
34
35     event Transfer(address indexed from, address indexed to, uint256 value);
36
37     event Burn(address indexed from, uint256 value);
38
39     function BrcpToken(
40         uint256 initialSupply,
41         string tokenName,
42         string tokenSymbol
43     ) public {
44         totalSupply = initialSupply * 10 ** uint256(decimals);
45         balanceOf[msg.sender] = totalSupply;
46         name = tokenName;
47         symbol = tokenSymbol;
48     }
49 }
```

Parte do código do token BRCP<sup>7</sup>

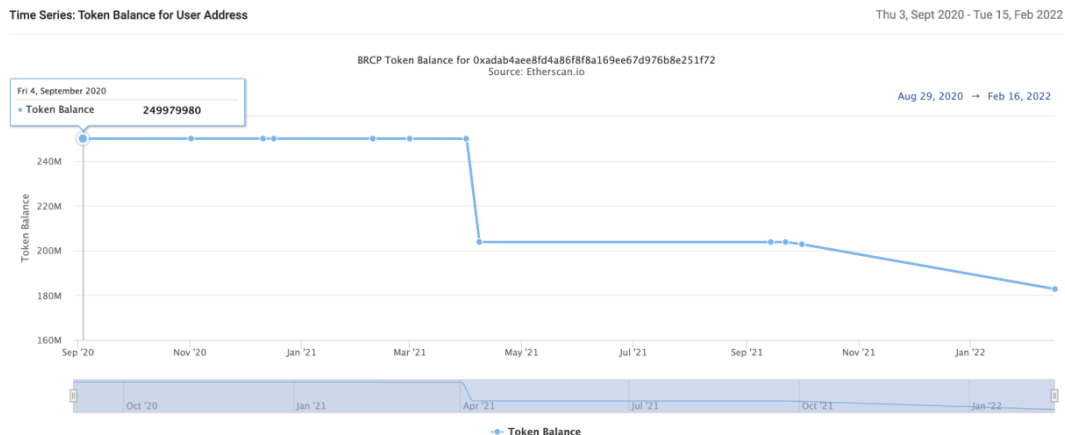
No código do token BRCP foi especificado:

- Linha 27 o nome do token: BRCP
- Linha 28: o símbolo<sup>8</sup>: BRCP
- Linha 30: Total de unidades do token BRCP 250.000.000, sendo esse valor imutável, não há como emitir mais tokens BRCP.
- Linha 39 a 48: Definida a primeira função do contrato inteligente. Na linha 45 a função define que o balanço total de tokens BRCP criados neste contrato será enviado/propriedade do criador do contrato (msg.sender, indica a carteira de quem está executando a função, no caso a criação do contrato), o que podemos confirmar checando o saldo de tokens BRCP na carteira do criador na data especificada.

<sup>7</sup> fonte: <https://etherscan.io/address/0x73484a262730d1d422610729e828346f9b2ff480#code>, acessado 28/06/2023 às 19:05.

<sup>8</sup> Abreviação do nome do token, por exemplo: Bitcoin é o nome, BTC o símbolo.





### Balanco Token BRCP carteira do criador do Token BRCP<sup>9</sup>

Podemos observar no endereço do contrato do BRCP <https://etherscan.io/address/0x73484a262730d1d422610729e828346f9b2ff480><sup>10</sup> que não há nenhum valor de mercado no token, o token não tem valor unitário. Como também não existe nenhum ativo em colateral trancado no contrato<sup>11</sup>.

ERC-20	Market	Other Info
<b>Overview</b> MAX TOTAL SUPPLY 250,000,000 BRCP HOLDERS 18 TOTAL TRANSFERS 1,160	<b>Market</b> FULLY DILUTED MARKET CAP \$0.00 CIRCULATING SUPPLY MARKET CAP -	<b>Other Info</b> TOKEN CONTRACT (WITH 18 DECIMALS) <a href="https://etherscan.io/address/0x73484a262730d1d422610729e828346f9b2ff480">0x73484a262730d1d422610729e828346f9b2ff480</a>

### Token ERC-20 BRMV

A hash criptográfica da transação de criação do contrato é:  
0x93411e830bd4eb8d3af72345d10dbd186fccf4d2d527e03761bcd4b888e00e58

<sup>9</sup>fonte:

<https://etherscan.io/token/0x73484a262730d1d422610729e828346f9b2ff480?a=0xadab4aee8fd4a86f8f8a169ee67d976b8e251f72#tokenAnalytics>, acessado 28/06/2023 às 19:40.

<sup>10</sup> Acessado 28/06/2023 às 19:52

<sup>11</sup> Exemplo de ativos com colateral bloqueados no contrato inteligente detalhados no relatório técnico.



*Informações referente a transação de criação podem ser visualizadas no endereço eletrônico:*  
<https://etherscan.io/tx/0x93411e830bd4eb8d3af72345d10dbd186fccf4d2d527e03761bcd4b888e00e58>

*O token ERC-20 BRMV tem a hash endereço de contrato: 0x501e8726d06Cdef66f3e0cb67f54924CcA1cC894, esse endereço é único, representa a identidade do token na blockchain Ethereum.*

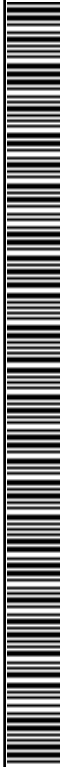
*Todas as interações com o token BRMV ocorrem através deste endereço, devido ao carácter de visualização público das transações na rede blockchain do Ethereum, o histórico de transações pode ser consultado em tempo real no endereço eletrônico:*  
<https://etherscan.io/address/0x501e8726d06cdef66f3e0cb67f54924cca1cc894>

*BRMV foi criado na data 08/06/2020, o hash da carteira pública do seu criador é:*  
`0xfDe57B2137824eF09fB141Ed0E16c88595EB0Dd5`

*As transações feitas pela carteira do seu criador podem ser consultadas em tempo real no endereço eletrônico:*  
<https://etherscan.io/address/0xfde57b2137824ef09fb141ed0e16c88595eb0dd5>

*O código do token BRMV ERC-20 pode ser acessado no endereço eletrônico:*  
<https://etherscan.io/token/0x501e8726d06cdef66f3e0cb67f54924cca1cc894#code>

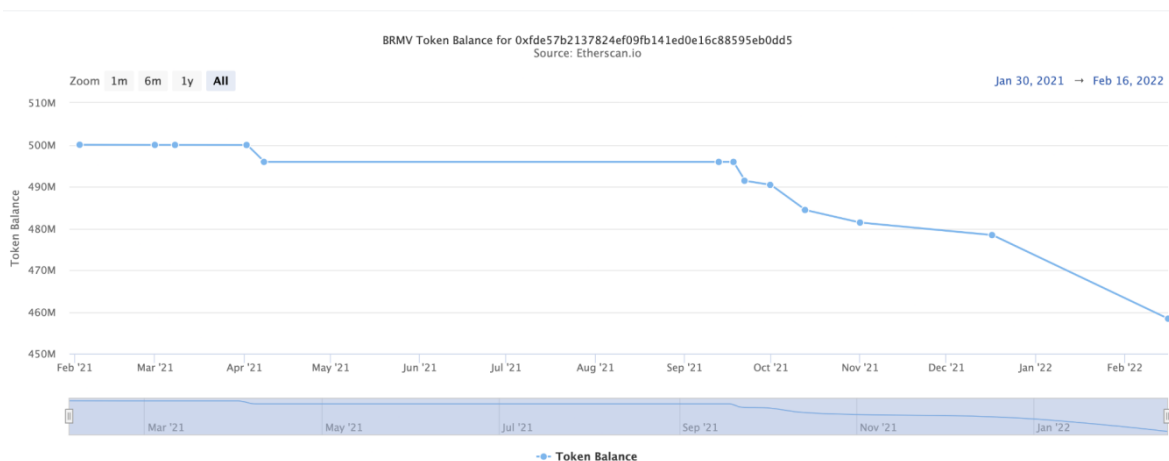
```
26 contract Brmv {
27     string public name = 'BRMV';
28     string public symbol = 'BRMV';
29     uint8 public decimals = 18;
30     uint256 public totalSupply = 500000000;
31
32     mapping (address => uint256) public balanceOf;
33     mapping (address => mapping (address => uint256)) public allowance;
34
35     event Transfer(address indexed from, address indexed to, uint256 value);
36
37     event Burn(address indexed from, uint256 value);
38
39     function Brmv(
40         uint256 initialSupply,
41         string tokenName,
42         string tokenSymbol
43     ) public {
44         totalSupply = initialSupply * 10 ** uint256(decimals);
45         balanceOf[msg.sender] = totalSupply;
46         name = tokenName;
47         symbol = tokenSymbol;
48     }
49 }
```



fonte: <https://etherscan.io/token/0x501e8726d06cdef66f3e0cb67f54924cca1cc894#code><sup>12</sup>.

No código do token BRMV foi especificado:

- Linha 27 o nome do token: BRMV
- Linha 28: o símbolo: BRMV
- Linha 30: Total de unidades do token BRMV 500000000 sendo esse valor imutável, não há como emitir mais tokens BRMV.
- Linha 39 a 48: Definida a primeira função do contrato inteligente. Na linha 45 a função define que o balanço total de tokens BRMV criados neste contrato será enviado/propriedade do criador do contrato (msg.sender, indica a carteira de quem está executando a função, no caso a criação do contrato), o que podemos confirmar checando o saldo de tokens BRMV na carteira do criador na data especificada.



fonte:

<https://etherscan.io/token/0x501e8726d06cdef66f3e0cb67f54924cca1cc894?a=0xfde57b2137824ef09fb141ed0e16c88595eb0dd5#tokenAnalytics><sup>13</sup>.

Balanço Token BRMV carteira do criador do Token BRMV<sup>14</sup>

Podemos observar no endereço do contrato do BRMV <https://etherscan.io/address/0x501e8726d06cdef66f3e0cb67f54924cca1cc894> que não há

<sup>12</sup> Acessado 28/06/2023 às 20:50.

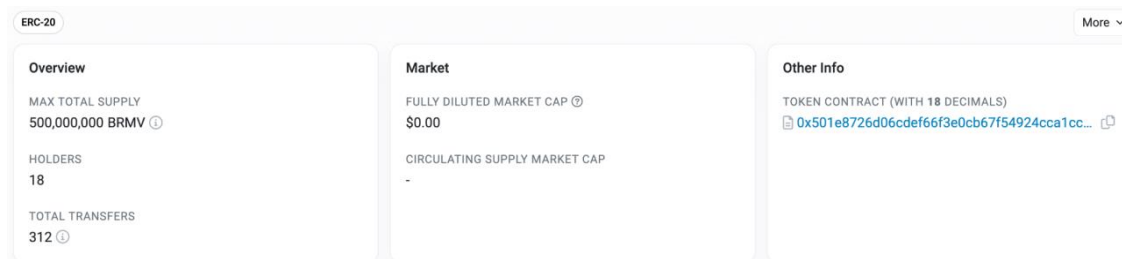
<sup>13</sup> Acessado: 28/06/2023 às 20:52.

<sup>14</sup>

Fonte:  
<https://etherscan.io/token/0x501e8726d06cdef66f3e0cb67f54924cca1cc894?a=0xfde57b2137824ef09fb141ed0e16c88595eb0dd5#tokenAnalytics>, acessado: 28/06/2023 às 20:52.



*nenhum valor de mercado no token, o token não tem valor unitário. Como também não existe nenhum ativo em colateral trancado no contrato<sup>15</sup>.*



ERC-20	More	
<b>Overview</b> MAX TOTAL SUPPLY 500,000,000 BRMV ⓘ  HOLDERS 18  TOTAL TRANSFERS 312 ⓘ	<b>Market</b> FULLY DILUTED MARKET CAP ⓘ \$0.00  CIRCULATING SUPPLY MARKET CAP -	<b>Other Info</b> TOKEN CONTRACT (WITH 18 DECIMALS) 0x501e8726d06cdef66f3e0cb67f54924cca1cc... ⓘ

fonte: <https://etherscan.io/token/0x501e8726d06cdef66f3e0cb67f54924cca1cc894><sup>16</sup>.

*Ambos os tokens BRMV e BRCP apresentam a mesma estrutura na codificação, declaração das variáveis e funções no mesmo número de linha. O que é um forte indicativo que não houve um processo de desenvolvimento ou melhoramento do código do token, os tokens são a cópia um do outro, mudando apenas: nome, símbolo e total fornecido.*

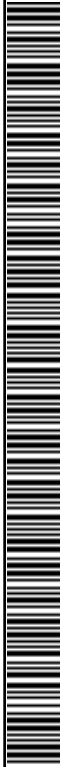
### **3. Houve a entrega de algum recurso financeiro (Reais ou moeda estrangeira) a alguma instituição quando da criação do BRCP e BRMV?**

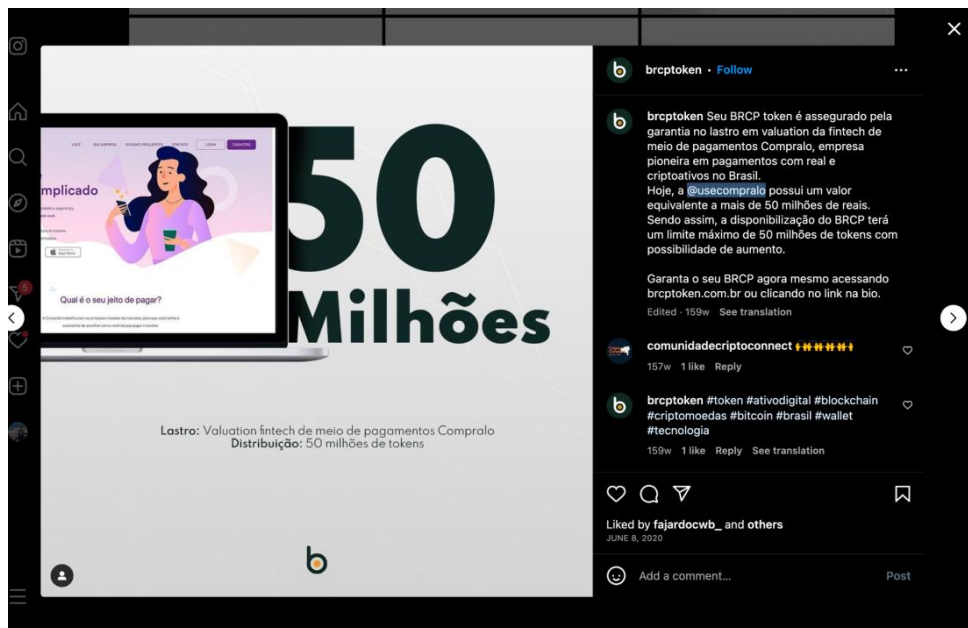
*Não há nenhum dado disponível na rede da blockchain Ethereum que comprove qualquer lastro das moedas BRCP, BRMV.*

*No contrato inteligente desse token não existe nenhuma função que garanta lastro de valor real para esses tokens, o contrato inteligente desses tokens criou um número determinado de tokens, conforme mostrado anteriormente, onde o dono majoritário dos tokens é o próprio criador do token.*

<sup>15</sup> Exemplo de ativos com colateral bloqueados no contrato inteligente detalhados no relatório técnico.

<sup>16</sup> Acessado em 28/06/2023 às 21:11.





fonte: <https://www.instagram.com/p/CBLvjI3JtUR>, acessado 01/07/2023 às 17:30.

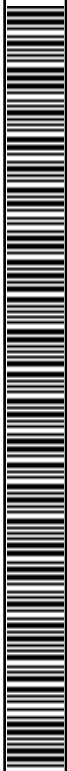
*Segundo a rede social brcptoken, o BRCP é um token digital que tem o mesmo valor monetário que o real, no caso o token seria uma stablecoin, assim chamado os criptoativos que tem valor lastreado em moedas reais. Segundo a rede social do BRCP, o lastro do BRCP é assegurado por um valuation de uma fintech de meio de pagamentos chamada Compralo, no entanto, na criação do contrato inteligente não existe nenhuma conexão entre o valor da empresa "dado como lastro" e os tokens, o valuation de uma fintech não é garantia de que o dinheiro de fato exista, e portanto não é garantia de lastro para emissão de token que deveria representar o valor do Real. Não existe nenhum órgão de regulamentação de criptos, logo, não existe uma regulamentação sobre os tokens emitidos e sobre a existência de lastro para emissão dos tokens.*

*Hipoteticamente, se os tokens BRCP/BRMV fossem criptoativos com lastro no Real, ao criar os 250000000 BRCP tokens, deveria haver "trancado" no contrato inteligente ou em alguma instituição que garantisse de fato o valor atrelado ao token, o que acontece com a stablecoin chamada Tether<sup>17</sup>.*

*O valor do token é exclusivamente especulativo, criado a partir de procura e demanda.*

#### **4. Os clientes da Falida têm chave de acesso ou qualquer outro instrumento que lhes permita mobilizar o BRCP e o BRMV junto ao Blockchain?**

<sup>17</sup> <https://tether.to/en/how-it-works>. Acessado em 12/07/2023 às 15:15.



*Improvável, conforme dados apresentados anteriormente, os tokens BRMV e BRCP estão alocados majoritariamente na carteira dos seus respectivos criadores. Para que os clientes tivessem acesso à chave que permitiria a mobilização dos referidos tokens eles deveriam tê-los recebido em carteiras próprias, contudo, dos contratos firmados entre falida e clientes, analisados por amostragem, não há indicativo de chave de acesso aos efetivos tokens.*

*Durante o tempo de atividade houve transferência para outros endereços de carteiras, no entanto, apenas 18 endereços tem hoje posse dos tokens BRCP e BRMV.*

### **Carteiras com posse do Token BRMV e/ou BRCP em julho de 2023:**

Endereço Carteira	Tokens BRMV em posse [%]	Tokens BRCP em posse [%]	Obs:
0xfDe57B2137824eF09fB141Ed0E16c88595EB0Dd5	91.667	-	criador do token BRMV
0xAdaB4aEE8FD4A86f8f8a169EE67d976B8E251f72	-	73.1160	criador token BRCP
0x4cfc8E2869E7Ce079C28E4f1bD7100b3177a8860	4.0199	7.9979	
0xDf5f77F007aE1829AC06ea35E411282ABf895175	2.0819	-	
0x7F5E249eA2DE2C4f22e0aD339E754065C57eE033	2.0819	0.3600	
0x0430D7B7455be2e24ee3aD50b44Dfb55B907dea4	0.9232	0.7817	
0x263937B5a28F3fFB7AEd0FC7294307A2D69e543F	0.5100	-	
0xC8f841D8d02541A569CD2dd874DE5F5F8D911e9f	-	0.04	
0xebC4e377bFD91E115a20a892b7c338a57961ecf9	0.4568	0.0250	
0x35e29aF2c2f717175C4e47CdDe0f78D37c0FAAd29	0.3001	-	
0x536fB25D7cAa449dc1e7824ADA267e309B2A5710	0.0181	0.0070	



0xF71AfE21Cd32959113Fc47aE2EF886B43A9413d5	0.0049	0.0120	
0x72E5263FF33D2494692D7F94A758aA9F82062F73	0.0040	0.0082	
0x069dd930fB03904025674Efe490a56f4AaACD55D	0.0031	0.0004	
0x8bF3AB18c29a3405C167Ea026c53a265c9b49081	0.0002	-	
0x530767A2F99e0ce12b66ECB863fC2b3C9A17Cb84	-	0.0021	
0x62d7DdA6EB14f3B569Ac6dBea69eDCD46b4C0E9C	0.0001	17.6474	
0x9E5FFFfe236cF7E18C67008771ECde53778Dd57a	-	0.0014	
0x3580680d55936E687AF650D6Cd29D10383F0230C	-	0.0008	
0x3305a55A75218B245d3f86B7F8f0b58275300A72	0.000001		
0xb7C092f67fc91B226699ce8092aaa27f6575C68a	0.00000		
0x030eE1B4d8f7cFABc69DAa23ad83D9C69ca4E576	0.000	0.000	carteiras com 10 Tokens
0x70a36f1e932ba52Fcb92F0ABaCfdd6dB95d2BABE	0.000		carteiras com 10 Tokens
0x55754cf7B9eBD7ab923Bb2DDa26e9335052c582F	-	0.00001	carteiras com 10 Tokens
0x6ec42d754383182afC57D20A64abDaf1E580d30d	-	0.0000	carteiras com 10 Tokens
0xAB0a0C619dd355a5D342265b908b8eC0e3714B98	-	0.0000	carteiras com 10 Tokens

**5. É possível consultar atualmente a existência de BRCPs e BRMVs? Em caso positivo, possuem algum valor financeiro?**

*Sim, é possível consultar através dos links mencionados nas questões anteriores. Os dados da blockchain ethereum são públicos, os tokens existem na rede Ethereum, mas não apresentam nenhum valor real monetário, conforme recortes apresentados na resposta à questão 02.*



*O token BRMV e o BRCP estão listados em uma exchange chamada FinexBox<sup>18</sup>, existe um par de troca BRMV/USDT e BRCP/USDT, o valor do token é especulativo, baseado em oferta e demanda.*

**BRMV Markets**  Display Unconverted Data

Affiliate disclosures

#	Exchange	Pair	Price	Spread	+2% Depth	-2% Depth	24h Volume	Volume %	Last Updated	Trust Score
1	 FinexBox	BRMV/USDT	\$0.100012	0.01%	\$6	\$2	\$122	100.00%	Recently	<span style="color: yellow;">●</span>

fonte: <https://www.coingecko.com/en/coins/brmv-token>, acessado 02/07/2023 as 14:20.

**BRCP Markets**  Display Unconverted Data

Affiliate disclosures

#	Exchange	Pair	Price	Spread	+2% Depth	-2% Depth	24h Volume	Volume %	Last Updated	Trust Score
1	 FinexBox	BRCP/USDT	\$0.01999918	0.01%	\$1	\$1	\$74.54	100.00%	Recently	<span style="color: red;">●</span>

fonte: <https://www.coingecko.com/en/coins/brcp-token>, acessado 04/07/2023 as 22:00.

**6. Teça as considerações adicionais que reputar convenientes de maneira a elucidar se as criptomoedas BRCPs e BRMVs podem de fato ser reconhecidas como um ativo acessível e individualizável dos clientes da Falida.**

*Ao analisar os dados disponíveis na blockchain ethereum dos tokens BRCP e BRMV o que se observa é que ambos os tokens desde a sua criação, lançamento no blockchain, não apresentem utilidade e valor financeiro, por mais que sigam o padrão de código ERC-20 do ethereum blockchain, o código não apresenta nenhuma medida de segurança essencial<sup>19</sup> e largamente discutidas pela comunidade para proteção do token contra-ataques externos. Devido ao caráter imutável do blockchain é fundamental a proteção do código contra-ataques, pois uma vez que o código é lançado no blockchain sem essas medidas, a vulnerabilidade não pode ser corrigida e todos os donos do token podem sofrer consequências severas de um ataque, como a perda de tokens.*

*Tokens que apresentam quaisquer vulnerabilidades em sua segurança mostram a falta de comprometimento com o desenvolvimento do código e com a complexidade da programação em blockchain, e não deveriam ser ofertados publicamente, pois em seu core já representam um alto risco ao usuário final.*

<sup>18</sup> <https://www.finexbox.com/Home/Orders/market/pair/BRMV-USDT.html>. Acessado em 12/07/2023 às 15:26.

<sup>19</sup> <https://docs.openzeppelin.com/contracts/4.x/>. Acessado em 12/07/2023 às 15:30.



**Compiler specific version warnings:**

The compiled contract might be susceptible to DirtyByteArrayToStorage (low-severity), ABIDecodeTwoDimensionalArrayMemory (very low-severity), KeccakCaching (medium-severity), EmptyByteArrayCopy (medium-severity), DynamicArrayCleanup (medium-severity), ImplicitConstructorCallCheck (very low-severity), TupleAssignmentMultiStackSlotComponents (very low-severity), MemoryArrayCreationOverflow (low-severity), privateCanBeOverridden (low-severity), SignedArrayStorageCopy (low/medium-severity), ABIEncoderV2StorageArrayWithMultiSlotElement (low-severity), DynamicConstructorArgumentsClippedABIV2 (very low-severity), UninitializedFunctionPointerInConstructor\_0.4.x (very low-severity), IncorrectEventSignatureInLibraries\_0.4.x (very low-severity), ExpExponentCleanup (medium/high-severity), NestedArrayFunctionCallDecoder (medium-severity), ZeroFunctionSelector (very low-severity) Solidity Compiler Bugs.

Erros apontadas pelo compilador solidity ao compilar o código do token BRCP fonte: <https://etherscan.io/token/0x73484a262730d1d422610729e828346f9b2ff480#code>, acessado 04/07/2023 as 22:35.

Outra bandeira vermelha nos tokens BRCP e BRMV é o fato do dono majoritário dos tokens ser o próprio criador do contrato, levanta a suspeita de um golpe chamado **“pump and dump”**. Nesses casos cria-se uma atmosfera de prosperidade em torno do sucesso do token, através de marketing digital, mídias e outros. Nessa atmosfera de prosperidade do token, cria-se um fenômeno popularmente conhecido como **Fear of Missing Out (FOMO)**, e pelo medo de perder a oportunidade de comprar a próxima criptomoeda que vai torná-las milionárias (como aconteceu com o ETH e BTC), começa uma alta procura pelos tokens em exchanges que têm os tokens listados, e como o dono majoritário dos tokens é o próprio criador, existem poucos tokens disponíveis para compra o que faz por um breve momento o valor do token subir de forma puramente especulativa, pois existe grande procura para compra e pouca demanda de venda.

Quando o valor do token atinge um patamar X, que é um valor financeiro considerável, o dono majoritário dos tokens vende um volume gigantesco de tokens e faz com que o valor do token despenque e todas as pessoas que compraram o token no momento do pump, são deixadas com um token que não tem nenhum valor pois agora o mercado tem muito mais token disponível do que demanda por ele.

Isso pode ser visto nos gráficos do valor do par de token BRMV/USDT e do par de tokens BRCP/USDT.



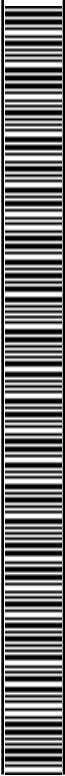
## BRMV Price Chart (BRMV)

Last updated 01:40AM UTC. Currency in USD.

☆ [Add To Watchlist](#)



fonte: <https://www.coingecko.com/en/coins/brmv-token>, acessado 04/07/2023 as 22:57.



## BRCP Price Chart (BRCP)

Last updated 09:47PM UTC. Currency in USD.

☆ Add To Watchlist



fonte: <https://www.coingecko.com/en/coins/brcp-token>, acessado 06/07/2023 as 19:02.

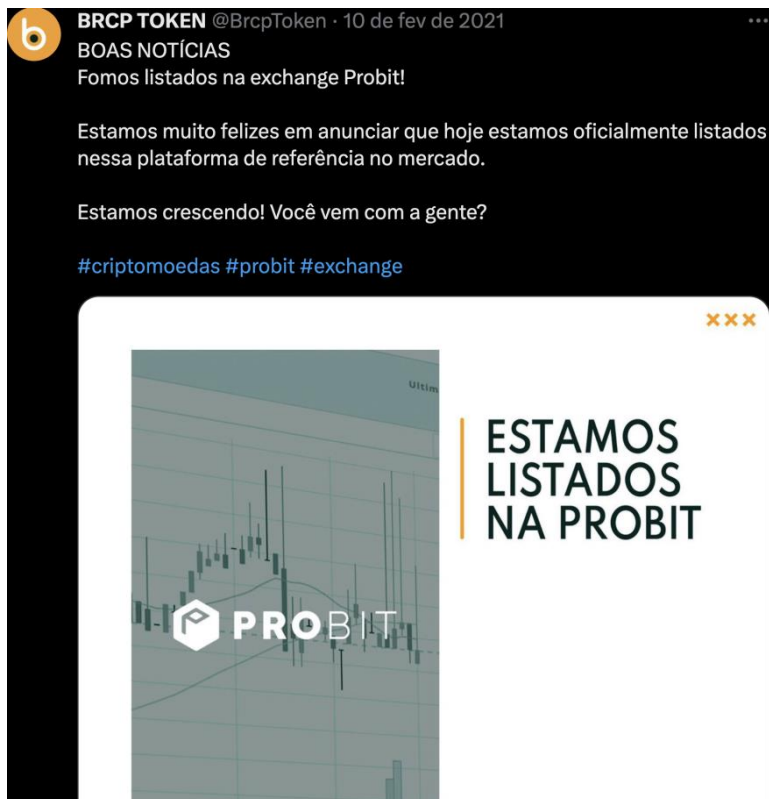
*Ambos os gráficos apresentam características de aumento repentino no "valor" do token e em um espaço curto de tempo a queda para um valor muito inferior ao máximo. Essas características são um indicativo do golpe "pump and dump".*

*Outra bandeira vermelha, é o fato de o token ser ofertado aos clientes como uma moeda "estável" que é lastreada pelo valor do Real, portanto, não é esperado de uma stablecoin variação tão grande em seu valor, contudo, a variação do preço dos tokens mostrada no gráfico é superior a 50%, outro indicativo de risco de fraude.*





Segundo a rede social das empresas falidas, o token **BRCP** foi listado na exchange **Probit**<sup>20</sup> na data 10 de fevereiro de 2021 e na exchange **Finebox**<sup>21</sup> na data de 30 de agosto de 2021.



fonte: <https://twitter.com/BrcpToken/status/1359622418751438850>, acessado em 06/07/2023 as 19:22.



fonte: <https://twitter.com/BrcpToken/status/1435756206765785093>, acessado em 06/07/2023 as 19:24.

<sup>20</sup> <https://www.probit.com/en-us/>

<sup>21</sup> <https://www.finexbox.com/>





fonte: <https://twitter.com/BrcpToken/status/1427650211321716750>, acessado 06/07/2023 as 19:40.

A exchange Finebox teve as suas atividades suspensas devido a relatos de clientes que tiveram saques e contas bloqueadas, perdendo o acesso aos fundos. A exchange possui baixa pontuação entre os usuários e foi largamente reportada como um Scam (fraudulenta)<sup>22</sup>. O par de troca BRCP/USDT continua listado na exchange finebox<sup>23</sup>.

A exchange Probit<sup>24</sup> continua em funcionamento, apresenta uma reputação regular, apresenta reclamações em relação a problemas com saques e acessos aos fundos pelos usuários, mas continua em funcionamento e com boas avaliações sobre os serviços<sup>25</sup>, ao procurar o par de troca BRMV/USDT ou BRCP/USDT não foi encontrado nenhum par de troca para os tokens na exchange Probit.

### Conclusão técnica final sobre os tokens

Os tokens BRCP e BRMV não parecem representar uma forma segura de investimento, já que não representam um ativo confiável com lastro no Real ou em qualquer outra moeda, os tokens não parecem representar o que foi ofertado aos clientes, pois não apresentam nenhum mecanismo de segurança em seu código, o que os torna uma ativo de alto risco devido a facilidade de serem hackeados. O fato de os tokens terem como dono majoritário o criador do contrato os torna altamente vulneráveis a alterações de valores de forma especulativa havendo indicativos de scams **pump and**

<sup>22</sup> <https://www.cryptowisser.com/exchange/finexbox/>

<sup>23</sup> <https://www.finexbox.com/market/pair/BRCP-USDT.html>

<sup>24</sup> <https://www.probit.com/en-us/>

<sup>25</sup> <https://www.trustpilot.com/review/probit.com>



*dump. Os tokens ofertados não apresentam nenhuma funcionalidade técnica na rede ethereum atrelada a sua existência.*

*Os tokens foram listados em exchanges de procedência duvidosas, por possuírem histórico de fraude para com os usuários, vulnerabilizando os clientes que, ao se registrarem nessas exchanges para adquirir os tokens BRCP e BRMV poderiam se colocar suscetíveis a ter os seus ativos bloqueados.*

*Os tokens BRCP e BRMV não apresentam valor real, qualquer valor atrelado aos tokens visto no passado parece ter sido meramente especulativo, devido a oferta e procura regulada por seu próprio criador. Os tokens não representam tecnicamente um stablecoin e nunca tiveram lastro confirmado no blockchain Ethereum, como foi apresentado aos clientes em redes sociais. Os tokens existem na blockchain, mas atualmente não apresentam nenhum valor monetário atrelado a eles.*

*São as respostas à consulta formulada.*

**Camila Gonçalves Marques**



## Parecer Técnico Token BRCP, Token BRVM

As redes principais de atuação da *Rental coins* foram: o blockchain do Bitcoin e o blockchain do Ethereum, portanto, o foco do parecer técnico será o blockchain Bitcoin e o blockchain Ethereum.

Blockchain é um tipo de base de dados distribuída, onde todas as transações individuais realizadas no blockchain são armazenadas em uma estrutura de bloco, quando o bloco atinge o seu limite máximo de armazenamento, o bloco é "guardado" e um novo bloco é criado. O bloco novo referencia a **hash criptográfica do estado do bloco anterior**, criando uma ligação em cadeia entre os blocos. Essa ligação em cadeia dos blocos através da hash configura a **imutabilidade dos dados da blockchain**, já que qualquer alteração no estado de uma transação em um bloco específico, alteraria o estado do bloco e conseqüentemente sua hash referência.

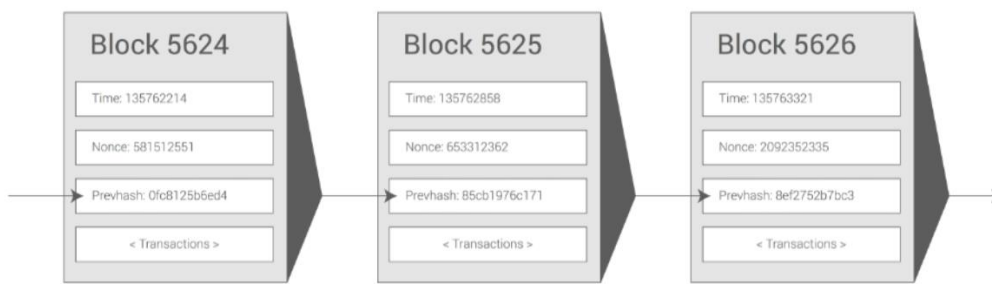


Figura 1: Representação dos blocos, onde cada bloco contém a *timestamp*, *nonce*, a referência (Hash) do bloco anterior, e todas as transações ocorridas naquele bloco [1].

A utilização da tecnologia blockchain data de 1991, onde Stuart Haber, W. Scott Stornetta postularam procedimentos computacionais para "carimbo de data/hora digital (*timestamping*)" de documentos digitais, com o intuito de inviabilizar um usuário retroceder ou antecipar o estado de documentos digitais, com o surgimento da internet e a digitalização de vídeos, imagens e texto esse era um problema crucial para época [2].

É fundamental entender que blockchain é uma tecnologia desenvolvida antes do surgimento do Bitcoin e Ethereum e estas redes utilizam da tecnologia blockchain como base de seu desenvolvimento.

Em 2008, Satoshi Nakamoto<sup>1</sup> descreveu o primeiro blockchain descentralizado no artigo *Bitcoin: A Peer-to-Peer Electronic Cash*. No artigo Nakamoto propôs uma solução ao problema de duplo-gasto (*double-spending*) utilizando uma rede "pessoa-para-pessoa" (peer-to-peer<sup>2</sup>) e melhorou, de forma inovadora, o método para marcar o "carimbo de data/hora

<sup>1</sup> Satoshi Nakamoto foi um pseudônimo utilizado pelo escritor do artigo: *Bitcoin: A Peer-to-Peer Electronic Cash*. 2008, que pode representar uma pessoa ou um grupo de pessoas, até o presente momento não existe registro de quem é criador do Bitcoin.

<sup>2</sup> Peer-to-peer ou P2P é uma arquitetura de redes de computadores onde cada um dos pontos ou Nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.



digital (*time-stamping*)" das transações e dos blocos, tecnologia semelhante ao *Hashcash*<sup>3</sup>, a introdução do hashcash eliminou a necessidade de uma instituição centralizada que garantisse a autenticidade das transações.

O design proposto no artigo foi implementado em 2009, com a criação do blockchain Bitcoin, que serve como *livro razão público* de todas as transações que acontecem na rede, e tem como token nativo a **criptomoeda Bitcoin**. O design do blockchain Bitcoin tem 5 pilares fundamentais: **São redes distribuídas, encriptadas, imutáveis, sem permissão, descentralizadas**<sup>4</sup>, o entendimento desses pilares é fundamental para a compreensão do seu funcionamento.

Em resumo, o Bitcoin surgiu como um sistema de pagamento eletrônico baseado em prova criptográfica em vez de confiança<sup>5</sup>, permitindo que quaisquer duas partes interessadas transacionem diretamente uma com a outra sem a necessidade de um terceiro confiável. Transações cuja reversão é computacionalmente impraticável protegendo os vendedores de fraudes. Ao utilizar uma **rede distribuída "pessoa-para-pessoa" (peer-to-peer)** para gerar prova computacional da ordem cronológica das transações soluciona-se o problema de *duplo-gasto*. O sistema é seguro, desde que os Nós (*nodes*)<sup>6</sup> honestos controlem coletivamente mais potência computacional do que qualquer outro grupo de Nós que ataquem<sup>7</sup> a rede[3].

<sup>3</sup> A Hashcash é um algoritmo de prova-de-trabalho (proof-of-work) utilizado para limitar e-mail spam e ataques DOS (denial-of-service em português negação de serviço) proposto em 1997 por Adam Back. No Bitcoin o Hashcash é a função utilizada na mineração dos blocos.

<sup>4</sup> Características de ambas blockchain analisadas: Bitcoin e Ethereum.

<sup>5</sup> No atual sistema financeiro, os bancos agem como instituições de confiança responsáveis pela mediação entre partes, garantindo que o comprador tem fundo suficiente e que o vendedor irá receber esse fundo, prevenindo o problema de duplo-gasto, o fundo uma vez transferido não pode ser re-usado.

<sup>6</sup> Um nó(nodes) blockchain refere-se a um dispositivo eletrônico (computador) que participa da execução do software de protocolo de uma rede descentralizada. Sua função principal é manter o consenso do registro público, realizado pela validação da transação e monitoramento ao vivo da atividade para garantir a segurança da rede.

<sup>7</sup> Teoricamente, para que ocorra uma alteração de dado de uma transação, 51% dos Nós ativos terão que refazer o trabalho computacional para gerar uma nova hash e no mecanismo de consenso do estado da blockchain mais da metade dos Nós tem que concordar, com base na cópia do estado da transações ocorridas na rede, que a nova hash reflete o verdadeiro estado do blockchain, para assim ser validada como verdadeira. **Mais informações:** Roberts, Jeff John (29 May 2018). "Bitcoin Spinoff Hacked in Rare '51% Attack'". Fortune. Archived from the original on 22 December 2021. Retrieved 27 December 2022.



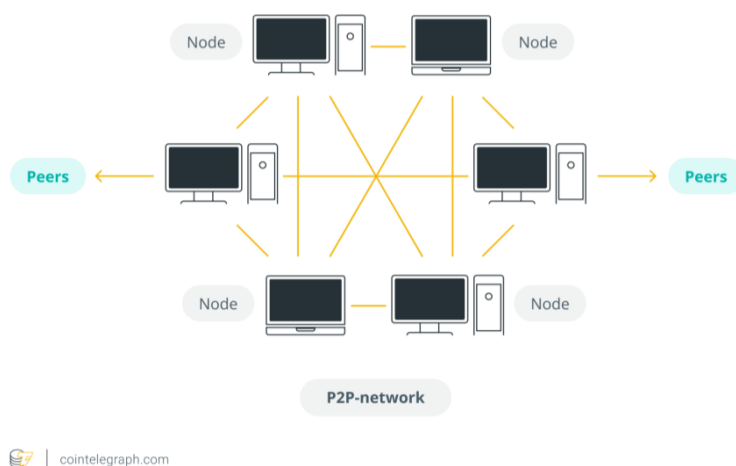


Figura 2: Representação gráfica de uma rede peer-to-peer, todos os nodes(peer), são conectados uns aos outros, não existe um servidor central e qualquer pessoa que tenha um computador potencial computacional suficiente pode ser um nó<sup>8</sup>. Em uma rede peer-to-peer, cada nó age como servidor e cliente, ou seja, pode fazer o download de dados e compartilhar dados com outros Nós, o que garante a eficiência, rapidez e segurança da rede. (fonte: <https://cointelegraph.com/learn/what-are-peer-to-peer-p2p-blockchain-networks-and-how-do-they-work>, acessada 24/06/2023 às 20:04.)

Os Nós são fundamentais no funcionamento de redes blockchain distribuídas e descentralizadas<sup>9</sup>, são eles que moderam a rede e através de um mecanismo de consenso<sup>10</sup> validam as transações, cada nó detém uma cópia do blockchain (desde do bloco gênese até o último bloco incluso na rede), os Nós também são os responsáveis pela criação de novos blocos na rede, sem Nós, blockchain distribuídas e descentralizadas perdem sua infraestrutura e conseqüentemente sua funcionalidade. Quanto maior o número de Nós<sup>11</sup>, maior a resiliência da rede, aumentando o nível de dificuldade de infiltração por Nós maliciosos.

Resumindo, os Nós são programados algoritmicamente para executar transações com base em um consenso majoritário. Quando os pares de Nós aceitam uma transação, essas são adicionadas ao blockchain, copiadas e distribuídas em toda a rede enquanto as transações reprovadas são eliminadas. Os mecanismos de consenso garantem que todos os

<sup>8</sup>**Pilar de descentralização:** o blockchain não existe como um banco de dados centralizado em uma instituição privada, ele está distribuído em vários computadores espalhados globalmente. Qualquer pessoa pode vir a ser um nó e nós em funcionamento podem a qualquer momento se desconectar da rede. A rede é basicamente composta de pessoas que compartilham do interesse de manter a funcionalidade da rede.

<sup>9</sup>Características de ambas blockchain analisadas: Bitcoin e Ethereum.

<sup>10</sup>Um mecanismo de consenso funciona da seguinte forma: Nós inserem dados de uma transação pendente e, em seguida, reportam o status de aprovada ou reprovada assim que a solicitação é verificada com os registros da rede blockchain dos demais Nós. Por exemplo, se um usuário tentar processar uma transação usando moedas gastas anteriormente (problema duplo-gasto) que já foram contabilizadas, essa solicitação seria negada contra o registro de transações imutáveis presente em cada nó, confirmando pela desaprovação da maioria dos Nós da rede. Os Nós que falham em aderir ao consenso são geralmente banidos da rede.

<sup>11</sup>Segundo bitnodes (fonte: <https://bitnodes.io/>, acessado dia 23/06/2023 às 20:40) existem hoje 17056 Nós em atividade no blockchain Bitcoin, distribuídos globalmente.



Nós permaneçam sincronizados. Novos blocos são processados ao vivo e todas as cópias do registro são atualizadas instantaneamente. Os Nós refletem unanimemente o verdadeiro estado da rede.<sup>12</sup>

O mecanismo de consenso utilizado na rede Bitcoin é a "prova de trabalho (*Proof-of-Work*)", a gênese de todos os mecanismos de consenso, depende de um grande número de nós validadores, que devem completar a prova de trabalho, de uma forma simplificada, consiste em encontrar uma hash<sup>13</sup> do bloco que representa a codificação de todos os dados das transações contidas no bloco, onde essa hash deve começar com um certo número de zeros<sup>14</sup>.

A mineração criptográfica<sup>15</sup> descrita acima, quando resolvida, o Nó responsável pela resolução é recompensado com tokens nativos do blockchain (**Bitcoin**). Isso adiciona um incentivo para que os Nós suportem a rede, e fornece uma forma de distribuir inicialmente moedas para circulação, uma vez que não existe uma autoridade central que as emite [3]. Essa é a única forma de incluir novos Bitcoins em circulação,

O incentivo pode ajudar a encorajar os nós a permanecerem honestos.

**Base de dados distribuída:** Qualquer pessoa que tenha um computador, com poder computacional suficiente, pode ser um validador da rede do blockchain (*Nodes*).

Há 6958 nodes em atividade para o blockchain Ethereum segundo ethernodes, na data de 23/06/2023 <fonte: <https://www.ethernodes.org/>, acessado dia 23/06/2023 às 20:47>. A distribuição de cópias do blockchain para cada um dos nodes dificulta ações maliciosas de alteração do estado a blockchain por um node em particular.

Camila Gonçalves Marques  
Engenheira  
Curitiba, julho de 2023

<sup>12</sup>Fonte: <https://builtin.com/blockchain/consensus-mechanism>, acessado 25/06/2023 às 15:06.

<sup>13</sup> SHA-256: Secure hash algorithm. Hashes criptográficas são funções matemáticas que operam em dados digitais.

<sup>14</sup> A probabilidade de calcular uma Hash que comece com vários zeros é muito baixa, portanto muitas tentativas são feitas até finalmente encontrar a Hash. A dificuldade desse trabalho é ajustada de forma a limitar a taxa de criação de novos blocos. Devido a baixa taxa de sucesso em gerar um novo bloco, é praticamente impossível prever qual computador na rede irá criar o próximo bloco.

<sup>15</sup> Popularmente conhecido como **Minerar Bitcoin**.



# Camila Gonçalves Marques

[camila.gmarques2@gmail.com](mailto:camila.gmarques2@gmail.com), [www.linkedin.com/in/camila-g-marques](http://www.linkedin.com/in/camila-g-marques), +5541999263436

## Experiência

**Ethereum Foundation** - Tradutora voluntária da documentação técnica Protocolo Ethereum

*Sep 2022 - Presente*

**Nethermind** - Internship in Data Blockchain Engineer and Technical Due Diligence Report

*Nov 2022 - Feb 2023*

**Goblockchain** - Solidity Developer

*Nov 2021 - Jul 2022*

## Educação

Universidade Tecnológica Federal do Paraná - Engenharia Mecânica

*Jan 2014 - Jan 2019*

Curitiba, Brazil

Rhenish-Westphalian Technical University - Mechanical Engineer

*Jun 2014 - Jan 2017*

Aachen, Germany

## Linguagens e Frameworks

Blockchain: Solidity, Openzeppelin, HardHat, Remix, Truffle & Web3

Languages: Python, C++, JavaScript, HTML/CSS,

Framework: React.js, Node.js, Ether.js, CadCAD

## Certificações

6 Figures Blockchain Developer

*EatTheBlocks*

*Carga: 20h*

The Complete Python Bootcamp

*Udemy*

*Carga: 22h*

JavaScript Algorithms and Data Structures

*Freecodecamp.org*

*Carga: 30h*

Blockchain Solution Architect Course

*BWBC & Consensus*

*Carga: 15h*

Masterclass: Ethereum Validator Economics

*cadCAD Edu*

*Carga: 3h*

cadCAD Complete Foundations Bootcamp

*cadCAD Edu*

*Carga: 5h*

