

Criptomoedas

Aldryn V. Costa¹, Leonardo A. Murça², Pedro G. Cruz³, Mateus F. Souza⁴

¹Departamento de Informática – Instituto Federal de Minas Gerais - Sabará
Caixa Postal 34.590-390 – Sabará – MG – Brasil

aldryncosta@yahoo.com, leonardoamurca@gmail.com,

mateusfilipe557@gmail.com, pedrogabrielcruz00@gmail.com.

Resumo. *As criptomoedas, desde o início da década de 2010, tem entrado numa ascensão constante no mercado financeiro e tecnológico. Porém, principalmente no Brasil, essa nova forma de economia ainda é muito desconhecida pelos cidadãos leigos no assunto. Tendo em vista este cenário, neste artigo iremos elucidar diversos tópicos sobre essa nova tecnologia como: o surgimento da primeira criptomoeda, como elas são valorizadas no mercado de ações, como funciona uma Blockchain, Mineração de moedas em grupo e individual, carteiras virtuais, dentre outros tópicos importantes.*

1. História

1.1. História do Dinheiro

Ninguém pensava em compra e venda no início dos tempos, tudo se baseava com o objetivo de trocar (escambo) algo que tenha em abundância em algo que tenha em escassez.

Com o passar do tempo foi surgindo à necessidade de uma moeda, para impor um valor de referência para os produtos. Inicialmente foram produzidas moedas de ouro e prata no séc. VII a.C. para tentar sanar algumas das necessidades da época.

Não existe ao certo uma linha do tempo para contar a história do dinheiro, pois foram surgindo novas moedas com as necessidades de cada região do mundo. É claro que as revoluções e os avanços na tecnologia influenciaram drasticamente o modo como se vê a economia hoje em dia. Tornando as transações de dinheiro cada vez mais seguras, justas e globalizadas em meio à sociedade atual. E agora chegou a vez das criptomoedas para acabar com as taxas bancárias.

1.2. Surgimento das Criptomoedas

A palavra criptomoeda vem de Cryptocurrency que existia apenas na teoria pelos defensores da criptografia. Com o objetivo de aplicar os princípios computacionais e matemáticos de ponta em alternativas para as primeiras moedas digitais, a fim de resolver algumas limitações políticas.

Em meados dos anos 1980 um criptógrafo americano chamado David Chaum, inventou um algoritmo de cegueira exclusiva, tornando-se a base para a criptografia moderna. Esse algoritmo permitiu a troca de dados de maneira segura e inalterável entre partes, assim criou-se a base para as transações de moedas digitais.

Chaum tentou comercializar o conceito de dinheiro cego, criando o DigCash gerando unidades monetárias de acordo com esse algoritmo cego. As moedas foram extintas por ordem do banco central da Holanda.

A partir de Chaum, o investimento em transações financeiras eletrônicas foi gigantesco, fazendo com que os pagamentos virtuais se tornassem cada vez mais seguros como o Paypal. Foram feitas várias tentativas de introduzir uma moeda no mercado digital, essas moedas foram de alguma forma extintas principalmente por influências políticas.

Até então só efetuávamos pagamentos com dinheiro. Com a chegada dos cartões de crédito, para efetuar uma compra, era necessário uma série de validações (bancos, operadoras de cartão e outros intermediários) para garantir que o pagamento foi feito com sucesso. Essas validações geram um custo embutido na compra realizada, tornando o produto ou serviço mais caro do que deveria ser.

Quando chegou em outubro de 2008, um pseudônimo Satoshi Nakamoto, publicou na internet como tornar essas validações de graça. A blockchain que valida as transações sem precisar de mediadores, tornando aquele pagamento válido. Assim, Satoshi também colocou em sua publicação a primeira criptomoeda (Bitcoin), dando espaço para que outras criptomoedas surgissem.

No ano de 2009 a moeda Bitcoin estava acessível ao público valendo pouquíssimos centavos de dólar. E em 22/05/2010 foi feita a primeira compra com Bitcoin, o famoso caso de duas pizzas que foram compradas por 10 mil Bitcoins (40 dólares na época) por um programador chamado Laszlo Hanyec, assim foi marcada a primeira transação monetária do Bitcoin. Desde então, algumas empresas e pessoas começaram a aceitar o Bitcoin como forma de pagamento. Claro que no início era uma coisa rara de achar, alguém que aceitasse o Bitcoin como forma de pagamento, mas a partir desse fato, o número de transações foi só aumentando e valorizando a moeda digital.

1.3. As Principais Criptomoedas no Mercado

Com a popularização da Bitcoin, originaram-se diversas outras moedas no mercado, cada uma com sua particularidade. Segue a lista com as 5 principais criptomoedas no mercado atualmente (excluindo a Bitcoin):

1. Ethereum



Figura 1. Ethereum.

Considerada a segunda moeda de maior valor entre as moedas digitais, a Ether usa a plataforma Ethereum de código aberto para efetuar transações. Ficando

atrás apenas da Bitcoin.

2. Cardano



Figura 2. Cardano.

Foi criada em 2015, é uma ramificação da Ethereum mais dinâmica e econômica. Valorizou bastante em 2017 e também conhecida como Ethereum dp Japão, devido a sua grande popularidade no Japão.

3. Litecoin



Figura 3. Litecoin.

É uma moeda de fácil acesso, pois não é necessário ter um grande poder de processamento para obtê-la. Foi criada em 2011, e atualmente uma das 10 mais valiosas do mercado.

4. Stellar



Figura 4. Stellar.

Também está entre as mais valiosas, devido a possibilidade de efetuar transações em qualquer tipo de moeda em sua plataforma. Não é necessário minerar e possui total liberdade em suas transações.

5. NEM



Figura 5. NEM.

Utilizando um algoritmo diferente do Bitcoin, a moeda NEM é mais fácil de ser minerada e de fácil comércio. Por isso se tornou uma das 10 mais valiosas, podendo ser mineirada por qualquer computador. Apresentando uma maneira mais ecológica para as criptomoedas.

2. Blockchain

2.1. Definição

Blockchain é um tipo de base de dados distribuída que armazena um registo de transações permanente e à prova de violação. Sua principal abstração para o mundo real, como o próprio nome sugere, é a materialização de uma cadeia de blocos que forma um bloco maior. Sua principal aplicação, mas não única, é nas moedas virtuais por exemplo. Ainda confuso? Veremos a seguir quais conceitos estão por trás desse tipo de definição.

2.2. Arquitetura Distribuída (P2P ou Peer-to-Peer)

Para entendermos melhor como funciona um sistema de Blockchain, primeiro precisamos entender como é organizado uma arquitetura P2P.

P2P é um arquitetura de rede em que cada computador (agora chamado de node ou nó), através de seu respectivo provedor de internet, se conecta à outros computadores integrantes da rede, de forma que a transmissão de pacotes é feita diretamente de node para node.

Através desse tipo de organização distribuído, é possível manter um sistema em funcionamento mesmo que algum dos nodes saia do ar.

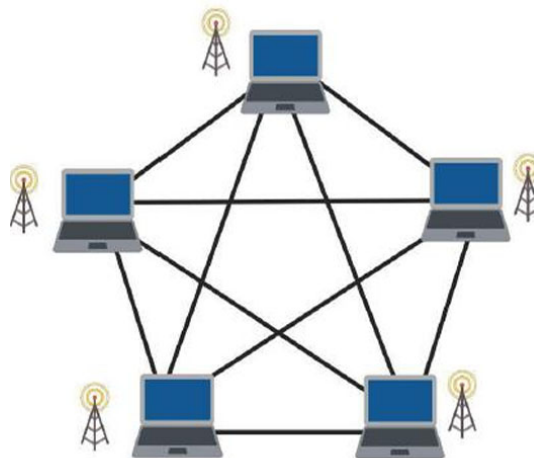


Figura 6. computadores arquitetados em P2P.

Dessa forma, conseguimos compreender a definição citada acima, pois com essa arquitetura temos um sistema *descentralizado* e *totalmente à prova de violação*. Assim, diferente dos sistemas centralizados, onde se têm um servidor central suscetível à ataques, a blockchain é muito mais segura pois não está sujeita às vontades de uma determinada pessoa ou empresa.

2.3. Funcionamento da Blockchain

Tendo conhecimento de como uma Blockchain é mantida no ar, entenderemos como é realizado os processo dentro desse sistema distribuído. Usaremos como exemplo principal, o sistema que vigora a Bitcoin.

2.3.1. Hashes

Para compreendermos os processos dentro do sistema da Bitcoin primeiro precisamos entender o que é uma hash.

Uma função hash é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo. Os valores retornados por essa função é chamada de *hash*. No contexto de uma Blockchain, uma hash é considerada a impressão digital de um determinado bloco dentro dessa cadeia de blocos, ou seja, ela é única e indecifrável.

Exemplo:

Entrada: Eu amo João Monlevade!

Hash de Saída(md5): 46556648688d3b501fbdaa8f2ee6107f

Veja agora que quando retiramos apenas um caractere, no caso uma exclamação "!", toda a hash será modificada e mesmo assim terá o mesmo comprimento (length).

Entrada: Eu amo João Monlevade

Hash de Saída(md5): 6fad71c6545c3da54834b54d4f681fa5

Essa tecnologia permite o controle de todo o sistema, uma vez que, se algum bloco for modificado, toda a hash será modificada e o sistema não aceitará essa modificação já que todo bloco depende dos outros blocos para ser único. Veremos a seguir como são organizados esse blocos.

2.3.2. Blocos

Um bloco é parecido com o funcionamento de uma hash, porém, as entradas são subdivididas em número do bloco, nonce e conteúdo.

Bloco de Cristiane

Bloco: # 1

Nonce: 89452

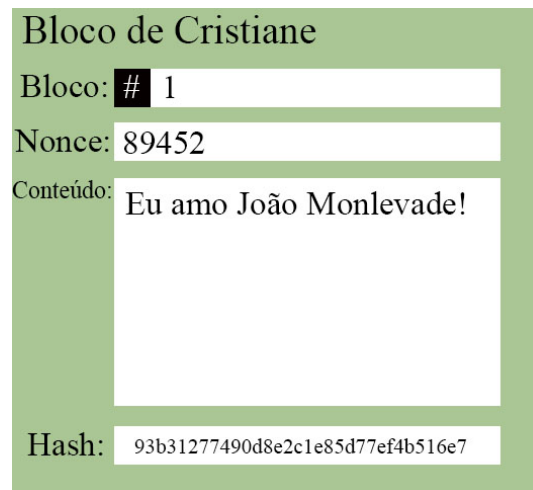
Conteúdo:

Hash: 00001277490d8e2c1e85d77ef4b516e7

Figura 7. Bloco da Cristiane (Signed).

Observe na Figura 7 que o campo *Bloco* indica o número do bloco dentro da Blockchain, o campo *Nonce* será explicado mais adiante nesse artigo, o *Conteúdo* é semelhante à entrada de uma hash comum e o campo *Hash* indica a hash gerada.

Perceba que a hash gerada acima inicia com 0000. Esses zeros iniciais são chamados de *leading zeros* e indica que esse bloco é válido (*signed*). Além dessa indicação, esses zeros é quem define a dificuldade variável no processo de mineração de criptomoedas que veremos na seção seguinte.



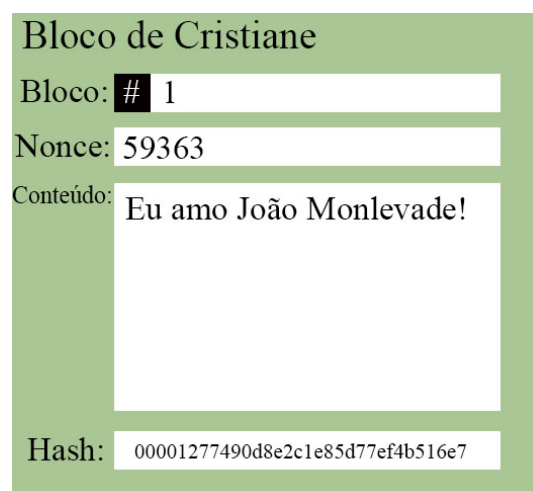
The image shows a form titled "Bloco de Cristiane" with a light green background. It contains four input fields: "Bloco:" with a black square icon and the value "1"; "Nonce:" with the value "89452"; "Conteúdo:" with the text "Eu amo João Monlevade!"; and "Hash:" with the value "93b31277490d8e2c1e85d77ef4b516e7".

Bloco de Cristiane	
Bloco:	# 1
Nonce:	89452
Conteúdo:	Eu amo João Monlevade!
Hash:	93b31277490d8e2c1e85d77ef4b516e7

Figura 8. Bloco da Cristiane (Not Signed).

Veja agora que o conteúdo do bloco mudou e, consequentemente a hash gerada também alterou. Como essa hash não é iniciada com os zeros como do bloco anterior, esse bloco se torna inválido (*not signed*).

É nessa parte que entra a importância do *nonce*. Alterando o *nonce*, a *hash* irá alterar também. A ideia de modificar o *nonce* é de basicamente de validar um bloco, ou seja, torná-lo *signed*. Esse processo de encontrar o *nonce* compatível com a hash do bloco é a espinha dorsal do processo de mineração das criptomoedas.



The image shows a form titled "Bloco de Cristiane" with a light green background. It contains four input fields: "Bloco:" with a black square icon and the value "1"; "Nonce:" with the value "59363"; "Conteúdo:" with the text "Eu amo João Monlevade!"; and "Hash:" with the value "00001277490d8e2c1e85d77ef4b516e7".

Bloco de Cristiane	
Bloco:	# 1
Nonce:	59363
Conteúdo:	Eu amo João Monlevade!
Hash:	00001277490d8e2c1e85d77ef4b516e7

Figura 9. Bloco da Cristiane minerado (Signed).

O *nonce* acima mudou para 59363 e assim a hash começou com os 4 zeros novamente. O bloco então se tornou válido! (*signed*). Logo, se entendemos o conceito de um bloco, uma Blockchain é uma cadeia de blocos interligados.

2.3.3. A Blockchain

Como citado no tópico anterior, a Blockchain nada mais é que todos esses blocos interligados por uma corrente.

A diferença desses blocos ligados em cadeia é o fato de cada bloco, além de possuir as suas próprias informações, ele possui a informação da hash do bloco anterior.



Figura 10. Exemplo de Blockchain.

Sendo todos os blocos interdependentes, podemos concluir que um sistema de *Blockchain* é extremamente segura, pois não dá margens para alterações em transações.

3. Mineração

3.1. Definição

Quando o assunto é mineração de criptomoedas, muitos usuários, principalmente aqueles não que não estão inseridos na área do computação, têm suas dúvidas de como funciona a obtenção de suas moedas por esse meio. Além disso, mesmo aqueles que possuem conhecimento prévio sobre o processo de mineração, ainda assim não sabem como calcular a rentabilidade ao minerar as diversas criptomoedas no mercado. Veremos a seguir como funciona todo esse sistema de mineração e como ponderar os ganhos desse processo chamado de *mining*.

3.2. O Problema Matemático

Como vimos anteriormente, os registros das transações de uma determinada criptomoeda são armazenados em blocos e o conjunto desses blocos formam uma blockchain. Vimos também que cada bloco é único e criptografado. A solução do problema matemático citado acima é basicamente encontrar a chave que criptografa os blocos e também fazem o registro de suas transações. Essa chave é chamada de *hash* e este processo não é feito de forma linear. A tarefa de encontrar o hash é feito através da resolução desses problemas matemáticos que validam as transações, isso é feito de forma simultânea por todos os mineradores a cada novo bloco. Sempre que o hash correto é encontrado, o minerador recebe uma recompensa pelo trabalho e o resultado é postado na rede. A partir daí, todos os mineradores passam a trabalhar na resolução do hash do próximo bloco. A capacidade total de processamento dos usuários envolvidos nessa tarefa é denominada hash rate. De maneira geral, minerar criptomoedas é fornecer poder computacional para a manutenção dos sistemas de moedas digitais.

3.3. Hardwares para Mineração

Entendido o funcionamento do processo de mineração, como podemos minerar na prática e qual hardware ideal para realizar esse *mining*?

Seu computador possui basicamente duas fontes de processamento: a CPU (Unidade Central de Processamento, em outras palavras, o processador principal da sua máquina) e a GPU (Unidade Gráfica de processamento, as famigeradas placas de vídeo). Ambos podem ser utilizados para a mineração, mas o uso da GPU costuma ser mais comum, já que costuma ser pouco requerida em atividades que não envolvem jogos, vídeos ou modelagem 3D ? ficando exclusivamente disponível para uso na mineração.

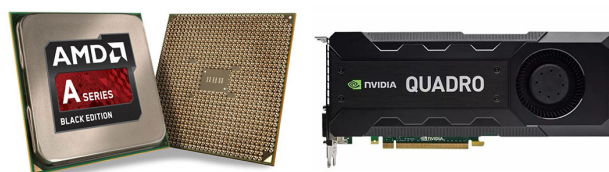


Figura 11. CPU AMD A8-7600 e GPU Pny Nvidia Quadro K5200.

Existem também hardwares vendidos especificamente para serem utilizados na mineração. Eles combinam, de forma eficiente, alta durabilidade, grande capacidade de procedimento e reduzido consumo de energia, mas são caros e não devem ser adquiridos sem planejamento prévio.



Figura 12. Rig montada para mineração.

É comum entre as pessoas que trabalham com esse tipo de equipamento usarem termos diferentes do nosso cotidiano. Como por exemplo o termo *rig*. Esse termo é muito utilizado nessa comunidade para se referir a máquinas projetadas e montadas especialmente para a mineração. Caso queira adquirir máquinas específicas para tais processos, saiba que irá encontrar esse termo frequentemente.

3.4. Tipos de Mineração

Para cada um dos equipamentos citados acima, existem dois tipos principais de se minerar uma determinada criptomoeda: sozinho ou em grupo.

3.4.1. Mineração Individual

Na mineração individual, cada usuário deve encontrar, por si só, a hash do bloco lançado na rede, competindo com todos os demais, incluindo aqueles que estão trabalhando em grupo. Caso obtenha sucesso, receberá sua recompensa de forma integral, mas em caso contrário, não receberá nada.

Devido à esse fato, a mineração solo torna-se inviável, uma vez que o poder de processamento de apenas uma máquina dificilmente irá conseguir competir com o resto da rede.

A *Figura 13* ilustra como acontece esse sistema de recompensa pela mineração. Perceba que o computador com maior poder de processamento consegue a maior parte das recompensas, enquanto o que possui o hardware mais fraco não ganha recompensa alguma.

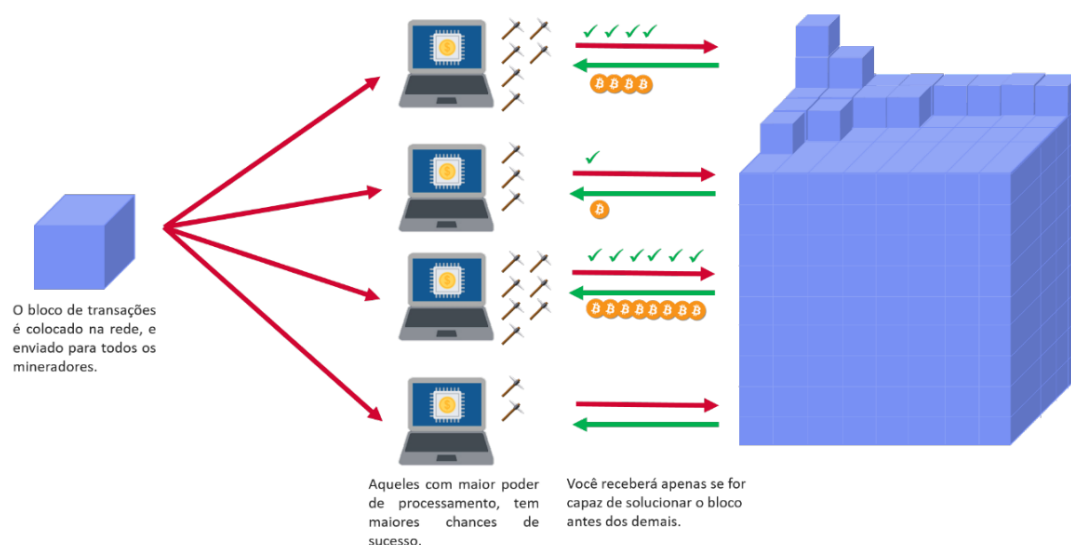


Figura 13. Mineração individual.

3.4.2. Mineração em Grupo(ou Pool)

Já na mineração em grupo, também chamada de pool, vários mineradores combinam seus poderes de processamento visando um objetivo em comum. No caso, encontrar a hash do bloco em questão.

Se vários participam da tarefa, consequentemente a eficiência do trabalho será bem maior. Desse modo, as chances de encontrarem o hash do bloco atual será bem maior. Caso obtenham sucesso na empreitada, a recompensa integral será destinada à pool vencedora, e assim, essa recompensa será dividida proporcionalmente dentro do próprio grupo. Ou seja, se um integrante disponibilizou um maior poder de mineração, maior quantidade de moedas ele receberá da sua pool.

Mas será que realmente vale a pena minerar em grupo? Bom, considerando que da forma individual o usuário receberia a recompensa de maneira integral, porém de forma esporádica e não compensaria seus gastos com energia. Contudo, a mineração em grupo aumenta a probabilidade do minerador receber suas recompensas de maneira mais constante, especialmente para com moedas com mais dificuldade. Porém, na prática, essas pools infelizmente concentram o poder para o proprietário do pool de mineração, pois ele define a recompensa para cada usuário colaborador dentro de sua pool.

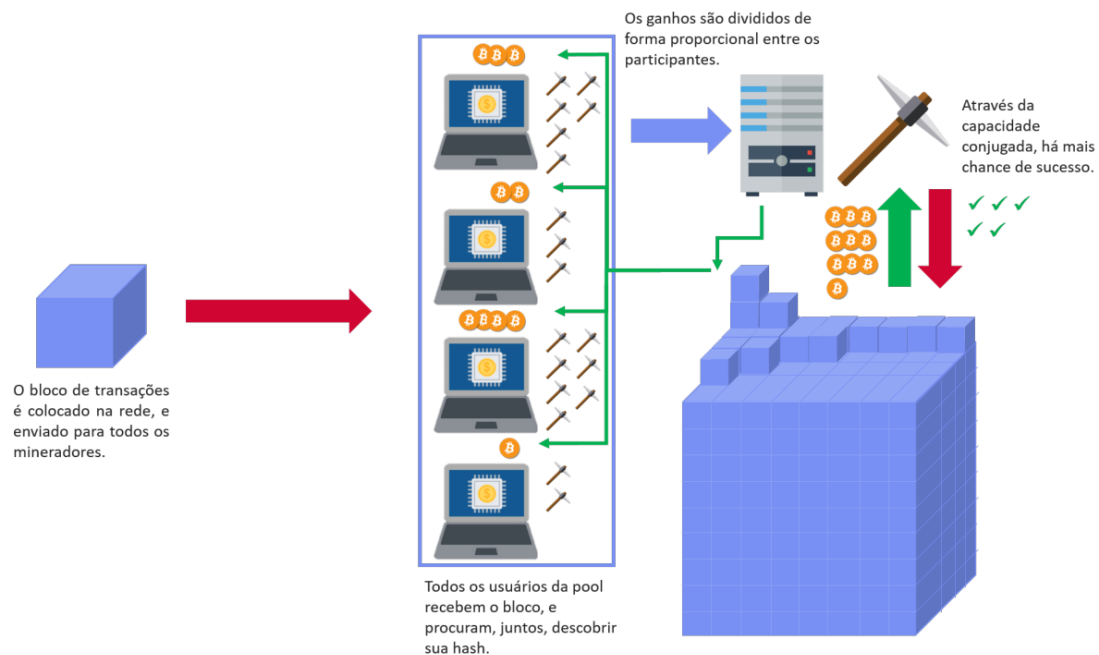


Figura 14. Mineração em pool.

Tendo em vista o conhecimento do funcionamento das pools acima, segue abaixo a relação das maiores pools de mineração do mundo. Ela tem como base as informações do gráfico da Blockchain sobre distribuição da taxa de hash (Acesso em 22/06/2018 às 23h e 49min):

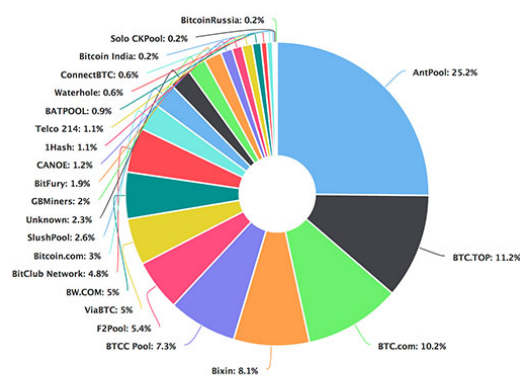


Figura 15. Maiores pools de mineração.

3.5. Algoritmos de Criptografia

Independente do tipo de mineração que irá utilizar, será necessário a utilização de um software para realizar determinada tarefa. Existem softwares para mineração específicos para CPUs e GPUs, e nesse último caso, eles ainda podem variar de acordo com o fabricante da placa de vídeo.

Além disso, eles ainda podem variar de acordo com o algoritmo de criptografia da moeda em questão. Os 3 algoritmos de criptografia mais usados nas criptomoedas atualmente são: SHA-256, Scrypt e X11.

1. SHA-256(Secure Hash Algorithm-256)

É utilizado nas moedas Bitcoin, Bitcoin Cash e Bytecoin. Essa função de hash pertence ao grupo de funções SHA 2. Uma função de hash, basicamente converte de maneira unidirecional strings de qualquer tamanho em strings de tamanho único. É comum esse tipo de função ser utilizada para checar integridade de arquivos. O grau de complexidade desse algoritmo supera 800.000 TH/s (800 mil Tera Hashes por segundo).

2. Scrypt

É utilizado nas moedas Litecoin, Dogecoin e Gridcoin. Em paralelo com a SHA-256, essa função diminui drasticamente (mais precisamente em 2,5 minutos) o tempo de chegada de blocos na Blockchain. Porém, por ser mais rápida, mais fácil de minerar e mais simples, ela é considerada menos segura que a SHA-256, tornando-se mais suscetível à ser quebrada. O grau de complexidade desse algoritmo chega à 300 kH/s (300 kilo Hashes por segundo).

3. X11

É utilizado nas moedas Paccoin, Nicehash-X11 e MonetaryUnit(MUE). Assim como o SHA-256, é um algoritmo de prova de trabalho(PoW). Foi utilizado em 2014 no Darkcoin (conhecida atualmente como Dash). O algoritmo X11 usa várias rodadas de 11 hashes diferentes (blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo), tornando-se assim um dos mais seguros e sofisticados hashes criptográficos em uso por modernas criptomoedas.

3.6. Mineradores

Tendo conhecimento das maneiras de se minerar (individual ou em pool), o hardware a se utilizar (CPU ou GPU) e os algoritmos de criptografia das moedas, veremos a seguir alguns softwares utilizados para realizar tal processo.

1. CGminer

Esse software é o mais popular minerador para GPUs. É open-source, escrito na linguagem C e multiplataforma (Linux, Windows e OS X). O que o faz tão popular é o fato de ser baseado em um minerador muito famoso e conceituado chamado Cppminer.

```
cgminer version 2.7.5 - Started: [2012-09-25 15:06:23]
(1s):718.7 (avg):701.2 Mh/s | Q:12 A:0 R:0 HW:0 E:0% U:0.0/n
TQ: 0 ST: 5 SS: 0 DM: 0 NB: 1 LW: 2 GF: 0 RF: 0 MH: 0.0
Connected to http://ntred.com:8337 with LP as user
Block: 000004b8032437c4278899d9f2cf6f35... Started: [15:06:23]

[P]ool management [G]PU management [S]ettings [D]isplay options [Q]uit
GPU 0: 63.0C 1833RPM | 380.3/388.4Mh/s | A:0 R:0 HW:0 U:0.00/n I: 8
GPU 1: 62.5C 1959RPM | 323.5/328.8Mh/s | A:0 R:0 HW:0 U:0.00/n I: 5

[2012-09-25 15:06:23] Started cgminer 2.7.5
[2012-09-25 15:06:23] Probing for an alive pool
[2012-09-25 15:06:23] Long-polling activated for http://ntred.com:8337/LP
[2012-09-25 15:06:23] Pool 0 http://ntred.com:8337 alive
[2012-09-25 15:06:23] Pool 1 http://pool.ABCPool.co:8332 alive
```

Figura 16. CGminer.

2. BFGminer

Esse software é derivado do minerador CGminer citado acima, porém com o foco voltado para processamento utilizando CPUs. Dentre suas funcionalidades estão clocking dinâmico, monitoramento e interface remota.

```
BFGMiner 2.10.5
bfgminer version 2.10.5 - Started: [2013-04-04 18:56:11] - [ 1 day 02:20:49]
5s:3.421 avg:3.378 u:3.389 Gh/s | A:74839 R:170 S:122 HW:670 U:47.3/n
ST: 2 OH: 16515 GH: 5074 LH: 153169 GF: 2 NB: 158 AS: 1 RF: 1 E: 9.02
Connected to multiple pools without LP
Block: ...35ae18b9 #229798 Diff:6.7M Started: [20:50:06] Best share: 81.4k

[P]ool management [G]PU management [S]ettings [D]isplay options [Q]uit
OCL 0: 69.0C 2790RPM | 249.2/249.2/247.4Mh/s | A: 5463 R:11 HW: 0 U: 3.46/n
OCL 1: 67.0C 2357RPM | 239.6/236.7/237.1Mh/s | A: 5235 R:11 HW: 0 U: 3.31/n
OCL 2: 69.5C 3712RPM | 396.5/395.9/398.0Mh/s | A: 8788 R:12 HW: 0 U: 5.56/n
OCL 3: 54.0C 50% | 115.2/115.0/115.1Mh/s | A: 2541 R: 5 HW: 0 U: 1.61/n
BFL 0: 51.7C | 857.6/840.0/822.3Mh/s | A:18159 R:62 HW: 79 U:11.49/n
XBS 0: 42.5C/42.4C | 395.8/398.6/403.7Mh/s | A: 8915 R:18 HW:158 U: 5.64/n
XBS 1: 42.9C/43.3C | 395.8/397.9/405.8Mh/s | A: 8961 R:19 HW:141 U: 5.67/n
XBS 2: 43.6C/43.9C | 362.0/370.4/375.7Mh/s | A: 8296 R:23 HW:116 U: 5.25/n
XBS 3: 43.6C/43.4C | 373.9/374.8/384.1Mh/s | A: 8482 R: 9 HW:176 U: 5.37/n

[2013-04-05 21:16:56] Accepted 247bba24 Diff 7/1 BFL 0 pool 1
[2013-04-05 21:16:57] Accepted de1b694f Diff 1/1 XBS 0 pool 0
[2013-04-05 21:16:58] Accepted 101784de Diff 15/1 OCL 3 pool 0
[2013-04-05 21:16:59] Accepted 0e8fac10 Diff 17/1 XBS 2 pool 0
[2013-04-05 21:17:00] Accepted 9d9384d7 Diff 1/1 OCL 1 pool 1
```

Figura 17. BFGminer.

3. BitMinter

Mesmo não sendo um dos softwares mais populares do mercado, o BitMinter possui um diferencial por ser o minerador que melhor interage com o usuário. Seu principal objetivo, com diz no próprio site do software, é fazer o usuário minerar mais facilmente e maximizar seus ganhos. É multiplataforma, funciona tanto para GPUs e CPUs. Além disso tudo, o diferencial do BitMinter é, por pertencer à uma pool de mineração, o processo de registro e instalação fica bem mais intuitiva para o cliente.

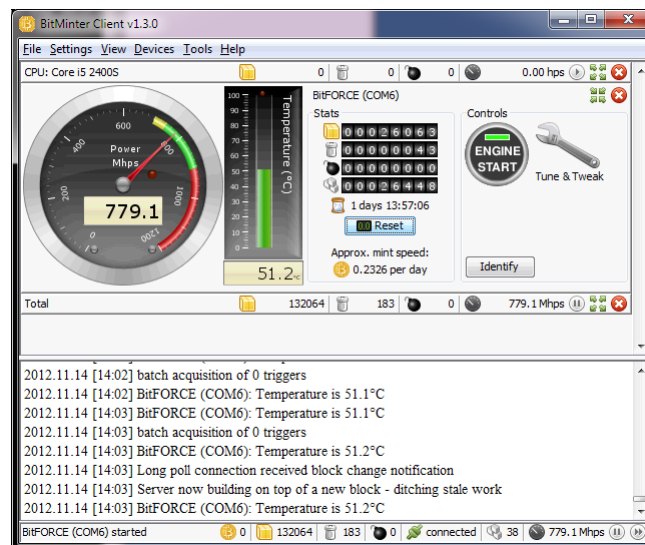


Figura 18. BitMinter.

4. Economia e Monetização

4.1. Bolsa de Valores e Banco Central

Para entender o comportamento econômico e monetário das criptomoedas vamos fazer um paralelo com a Bolsa de Valores e o Banco Central.

A Bolsa de Valores é o local onde ocorre a venda de ações, uma ação é a menor parte do capital social de uma empresa. O objetivo da Bolsa de Valores é proporcionar um local seguro de negociações, assegurando todos os tramites. Hoje a Bolsa é totalmente eletrônica e o sistema realiza as negociações automaticamente.

A principal Bolsa de Valores hoje no Brasil é a B3, união BM&FBOVESPA e da Cetip, por isso há o índice BOVESPA, que é um termômetro da Bolsa de Valores Brasileira. Esse índice é calculado a partir de uma carteira imaginária, nessa carteira há as ações mais negociadas na Bolsa, quando essas ações sobem, a carteira se valoriza e o índice Bovespa aumenta, quando as ações caem, a carteira se desvaloriza e o índice Bovespa cai. Dessa forma o mercado de ações funciona basicamente através da lei da oferta e da procura, quando há muitos compradores as ações se valorizam e seu valor sobe, quando há muitos vendedores as ações se desvalorizam e seu valor cai.

Atualmente o sistema onde ocorrem as transações da Bolsa é chamado Homebroker, ele permite a negociação de ações e outros ativos financeiros por meio da internet. Nele você vai conseguir comprar e vender suas ações, saber quais ações tem em carteira, qual seu saldo financeiro, e acompanhar as ordens de compra e venda que você enviou para a bolsa.

A bolsa é uma instituição centralizada, pois as políticas monetárias utilizadas por ela são reguladas pelo Banco Central.

O Banco Central tem a função de gerir a política econômica, garantir o poder de compra de cada país e do sistema financeiro como um todo. Tem também o objetivo de definir as políticas monetárias (taxa de juros, câmbio e outras) e aquelas que regulamentam o sistema financeiro. O banco faz isso através de um pouco de interferência no

mercado financeiro (bolsa de valores, sociedades corretoras e outras instituições financeiras), vendendo papéis do tesouro, regulando juros e avaliando os riscos econômicos do país.

4.2. Economia

4.2.1. Como as criptomoedas ganham valor?

De acordo com o artigo *"Bitcoin: quanto custa? Compreendendo os principais drivers de um ativo financeiro digital especulativo ao longo de sua breve existência"* publicado por Lucas Regis Slerca, o Bitcoin é movido em grande parte pelas transações de especulação. De acordo com Lucas: *"a partir da falta de uma estrutura como a taxa de juros imposta por bancos centrais e da não existência, por tanto, de uma estrutura a termo da taxa de juros, chegam a conclusão que o Bitcoin está sujeito principalmente à demanda, já que a oferta é fixa."* (2016, p.31).

Não há uma definição única ou majoritária dos perfis dos utilizadores de criptomoedas. Existe uma ampla gama de usuários que possuem diversas e diferentes formas de pensamento que fizeram apostar nessa tecnologia.

Diversas visões tecnológicas, econômicas políticas e até filosóficas existem nesse meio. Devido a isso seguem alguns fatores que proporcionam a valorização das moedas digitais:

- Fator tecnológico: As primeiras adesões às criptomoedas vieram entre aqueles com interesse em novidade tecnológica. A partir da ideia de Satoshi Nakamoto de criar um sistema eletrônico de dinheiro digital P2P, e a superação das dificuldades para se criar dinheiro totalmente digital, juntamente com o envolvimento prático das pessoas possibilitou a valorização material do Bitcoin. A ideia de descentralização e código aberto foi contribuir muito para que a moeda atingisse o alcance que possui hoje.
- Fator Econômico: Um sistema de dinheiro digital não foi ignorado no meio financeiro e de investimento na economia. A ideia de proteção contra as decisões do sistema financeiro hegemônico e centralizado contribuiu para que as criptomoedas caminhassem para o valor atingido hoje.
- Fator Político: Os governos e empresas (principalmente bancos) não irão apenas assistir de fora essa revolução, e certamente irão reagir. Com isso terão que se organizar, estabelecer e conscientizar (bem como juridicamente) em torno das reações vindas da utilização das criptomoedas.
- Fator Filosófico: Temas como liberdade, individualidade, cientificidade, transparência, e outros, surgem e começam a serem debatidos entre as pessoas que se uniram nesse projeto.

4.2.2. Como Comprar e Vender?

Para comprar Bitcoins ou Altcoins (criptomoedas alternativas ao Bitcoin) é necessário ingressar em uma Exchange, que funciona como a Bolsa de Valores, basicamente é um

local onde conectam vendedores e compradores de moedas digitais. Após cadastrado em uma determinada plataforma é necessário ter saldos em reais, que podem ser adicionados através de boleto bancário, cartão de crédito ou transferência bancária.

Na Exchange são emitidas ordens de compras pelos usuários que desejam comprar e ordens de vendas pelos usuários que desejam vender, então esses dados são cruzados ligando um comprador com um vendedor, assim como ocorrem com ações na Bolsa de Valores, sendo assim efetuada a compra/venda.

As maiores exchanges do Brasil são: Mercado Bitcoin, Foxbit, Bitcoin to you e Bitcoin Trade. A figura 1 mostra uma tabela comparativa entre algumas exchanges brasileiras em relação à preços negociados e trades (transações efetuadas).

Devido ao aumento de exchanges brasileiras, e também à grande variedade de preços e volume entre elas, tornou necessário a existência de um indicador de preços que representasse a precificação do Bitcoin em reais com as devidas normalizações, esse índice é o BRXBT, que representa o preço atual de uma unidade de Bitcoin em reais.

Um dos principais pilares do cálculo do Índice BRXBT é que ele se baseia nas informações de negociações (trades) de cada Exchange.

- Frequência: o índice é atualizado em tempo real para representar a situação mais atual.
- Composição: apenas exchanges que operam com o par BTC/BRL, divulgam todos os trades (não apenas um ticker) e aceitam depósitos e retiradas em Reais (R\$) participam do índice.
- Cotação: é considerado apenas o valor do último trade da exchange para compor o índice.
- Peso: o peso da cotação de cada exchange no índice é equivalente à participação daquela exchange no volume total de negócios em Reais nas últimas 24 horas.

Peso = Volume(em R\$) da exchange nas últimas 24 horas.

Fórmula do BRXBT: $\sum(\text{cotacao} \times \text{peso})$

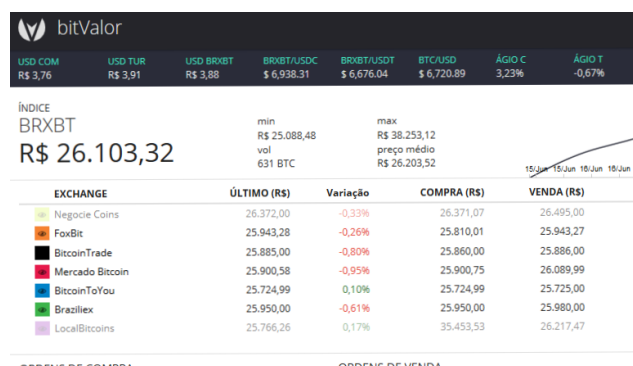


Figura 19. Tabela comparativa Exchanges brasileiras.

Mas não é necessário comprar 1 Bitcoin a R\$26.100,00, pois o Bitcoin possui 8 casas decimais. Portanto pode ser adquirido apenas 0,000000001 BTC.

4.2.3. Limite de Mercado

O limite de mercado de uma criptomoeda, é a quantidade máxima disponível em mercado que a mesma tem para ser negociada / adquirida. Esse limite é pré-estipulado pelo próprio algoritmo. Por exemplo, o Bitcoin possui um limite máximo de criação de 21 milhões de moedas, já o ETH da Ethereum não possui teto máximo para ser produzido.

Estima-se que Bitcoin terá seu teto máximo de produção atingido no ano 2140, e caso isso ocorra não quer dizer que a moeda, a mineração e as transações ocorrerão. Pressupõe-se que as taxas de transação aumentarão, o que fará com que as atividades mineradoras se mantenham dessas taxas.

Esse limite existente para o Bitcoin faz com que seja uma moeda deflacionária, ou seja, devido a sua baixa oferta e grande demanda haverá uma alta significativa em seu valor.

4.2.4. Impacto Social

As criptomoedas trazem uma revolução no mundo dos negócios e das transações comerciais. Os principais impactos das moedas virtuais são:

- Os registros descentralizados e validados pela rede são suficientes, o que dispensa a necessidade de intermediário nas operações. Essa transparência proporcionada pela blockchain reduz o papel de instituições financeiras, como cartórios, bancos e instituições governamentais;
- O controle de dados e informações também deixam de serem centralizados, portanto deixa de pertencer, por exemplo ao Facebook, Google, e outros, para pertencer aos próprios indivíduos. Isso empodera o indivíduo e não a organização que administra os dados unicamente para seu uso e interesse? de acordo com Victor Silveira, especialista em modelagem de negócios e professor da Fundação Dom Cabral.

Enfim, as criptomoedas possuem um potencial muito grande, e com as inovações nessa indústria haverá séries de mudanças, como na forma como os investimentos são realizados, ou na forma que os consumidores decidem pagar seus bens e serviços, o fato é: as criptomoedas, assim como a internet, vieram para mudar o mundo.

5. Carteiras Virtuais

A carteira ou também conhecida como wallet pode ser utilizada como um software de computador, no celular ou em uma interface web(em algum site). As wallets tem como requisito as chaves, privadas e públicas, a chave pública permite a verificação de alguma transação, enquanto a privada lhe dá acesso a sua wallet para que você tenha acesso dentro da blockchain ao seu balanço de moedas. A chave privada pode também ser usada para que possam lhe enviar moedas.

5.1. Geração das Chaves Privadas

- Não determinista

Cada chave privada é capaz de gerar 1 chave pública que gera 1 endereço.

As wallets mais usadas e conhecidas são não deterministas possuem diversos endereços e várias chaves privadas (0 a infinito) tais chaves ficam armazenadas num arquivo, geralmente um '.dat'.

Uma grande desvantagem deste tipo de wallet é a necessidade de fazer backups para não se perder as moedas, caso haja algum problema se perde tudo.

- Determinista

As chaves privadas, públicas e endereços são gerados a partir de uma única chave privada (mestra), para facilitar, é utilizado uma seed que vai identificar essa chave, seed é uma string de mnemônicos que pode ser memorizada. Essa chave privada mestra pode receber marcadores que esses mesmos irão gerar chaves privadas que gerarão públicas, etc.

Não há necessidade de um arquivo de backup, a seed é simplesmente memorizada, basta inserir a seed em um software próprio e ele identificará as chaves privadas.

- Determinista Hierárquica

Mesma estrutura de seed da determinista, a diferença é a organização hierárquica é possível organizar as chaves privadas, podendo gerar chaves privadas filhas, originando wallets a partir de um grupo ou uma "chave de chaves".

5.2. Forma de Conexão com a Blockchain

- Sincronização Total

A blockchain é baixada para o computador ou seja ela consome a memória secundária da máquina na qual é armazenada. Exemplo: As blockchains da bitcoin possuem 144gb.

Tal blockchain aumenta com o número de transações precisando assim uma atualização sempre que possível, só se torna viável ao utilizar criptomoedas menos famosas a atualização demora muito.

- Acesso pela Nuvem

A blockchain é armazenada numa nuvem e é acessada pela carteira quando preciso, o download só é feito de algumas partes da blockchain mas tais partes são eliminadas depois.

A sincronização passa a ser instantânea, sem a necessidade do download ou da atualização da blockchain, basta acessar as novas informações, caso ela já não atualize automaticamente.

5.3. Armazenamento das Chaves

- Em Poder do Usuário

O modo mais seguro, o usuário terá acesso aos representantes da wallet (chave privada, seed, .dat) e somente ele terá o acesso liberado para tais informações.

A segurança passa depender do usuário, basta não divulgar a sua seed ou seu '.dat' (ou ser invadido) que o processo se manterá seguro.

- Em poder de Terceiros

As chaves privadas ficam armazenadas em uma nuvem que é dominada por outros, você acessa a interface destes terceiros e eles liberam o acesso a sua chave privada, o problema é: eles controlam sua chave e podem a qualquer momento retirar todo o 'dinheiro' da sua wallet.

O método de acesso é como o de uma rede social, sua conta é criada, com email, senha, etc. Com isso você terá o acesso a interface para controlar a sua wallet.

A única vantagem seria se o número de moedas guardadas fosse baixo, pois esse tipo de interface traz uma comodidade e uma certa facilidade com esquemas do tipo padrão de recuperação de conta e dentre outros.

A segurança do servidor conta muito também, pois caso alguém invada o servidor do terceiro, o mesmo tem livre acesso a sua chave privada e consequentemente a sua wallet (O que minimiza os problemas e não requer tanto conhecimento prévio do assunto).

5.4. Conexão com a Internet

- Hot Wallet

Chaves privadas em um servidor que possui conexão com a internet.

Facilidade na utilização das moedas.

Facilidade na apropriação indevida via invasão.

- Cold Storage

Chave privada sem conexão com a internet.

Impossível de ser roubada via ataque cibernético.

A chave pode ser marcada em alguma anotação.

Não é possível enviar suas moedas, é necessário utilizar uma hot wallet para poder usá-la.

5.5. Tipos de Carteiras

5.5.1. Wallet Core

- Não Determinista.
- Sincronização total com a Blockchain.
- Hot Wallet.

É wallet padrão de todas as criptomoedas. Para se instalar essas wallet é preciso baixar toda a blockchain, o que é viável analisarmos moedas mais novas (nevacoin: =5gb), mas ao se analisar uma moeda já consolidada como a bitcoin, passa a ser impossível pelo número alarmante de informações armazenadas na blockchain(=144gb).

Chaves privadas ficam somente em mãos do usuário, só ele possui o arquivo ".dat."

- Pontos Fortes

Todas as moedas tem uma wallet core.

Não é necessário a disponibilização de nenhuma informação.

- Pontos Fracos

Grande demora para sincronização.

Grande necessidade de espaço na memória dependendo da criptomoeda.

Como a sincronização é feita com frequência, ela requer acesso a internet pois é sempre "atualizada".

5.5.2. Wallet Leve

- Determinista
- Sincronização com a Blockchain pela nuvem.
- Hot Wallet

A wallet leve tem sua blockchain armazenada na nuvem, é feita uma consulta à blockchain ou realizado alguns pequenos downloads para que seja possível acessar suas informações. Por ser determinista, ela trabalha com o esquema de seed. Com o uso de uma seed, retira-se a necessidade de um arquivo ".dat" e a necessidade de um backup constante da carteira.

- Pontos Fortes

Por não precisar do download completo da blockchain, a sincronização passa a ser quase que instantânea.

Não é necessária a disponibilização de nenhuma informação pessoal.

Basta memorizar a seed para que possa ser acessada.

- Pontos Fracos

O número de criptomoedas que trabalha com tal wallet ainda é limitado.

Uso de banda da internet para baixar as partes necessárias da blockchain.

5.5.3. Wallet Online

- Variável (Pode ser ou não determinista, depende de quem o armazena).
- Sincronização com a Blockchain pela nuvem.
- Hot Wallet.

A carteira está sob domínio de terceiros, que tem o livre acesso a ela podendo até remover as criptomoedas presentes nela. Todas as informações são armazenadas na nuvem, basta utilizar um "login" e uma senha para obter acesso.

- **Pontos Fortes**
 - Não ocupa espaço na memória
 - Sincronização quase que instantânea.
 - Facilidade ao utilizar.
- **Pontos Fracos**
 - Segurança (Por estar nas mãos de terceiros não é possível saber o que será feito com sua carteira).
 - Falta de privacidade, pois necessita de um email e os terceiros tem informação de todas as suas transações.

5.5.4. Wallet de Papel

- Determinista.
- Não tem Blockchain.
- Cold Storage

Tanto a chave privada quanto o endereço da sua wallet são armazenadas, seja em um bloco de notas ou uma agenda, pois por ser Cold Storage não há necessidade da conexão com a internet. Para que seja feita a manipulação, basta usar a chave privada que se tem em mãos. Caso seja preciso acompanhar como está sua carteira, basta acessar um site utilizando o endereço público.

- **Pontos Fortes**
 - Não existe sincronização com a blockchain (Processo instantâneo).
 - Disponível em todas as criptomoedas atuais.
 - Por ser escrita, não precisa utilizar internet ou espaço de memória.
 - Alta privacidade.
- **Pontos Fracos**
 - A movimentação das criptomoedas presentes nas carteiras se torna mais complexa e consequentemente menos atraente para um usuário "comum".

5.6. Lugares que Aceitam Criptomoedas

5.6.1. Coinmap

O site coinmap mapeia todos os estabelecimentos do mundo que aceitam pelo menos algum tipo de criptomoeda por seus serviços. Observe o mapa abaixo:

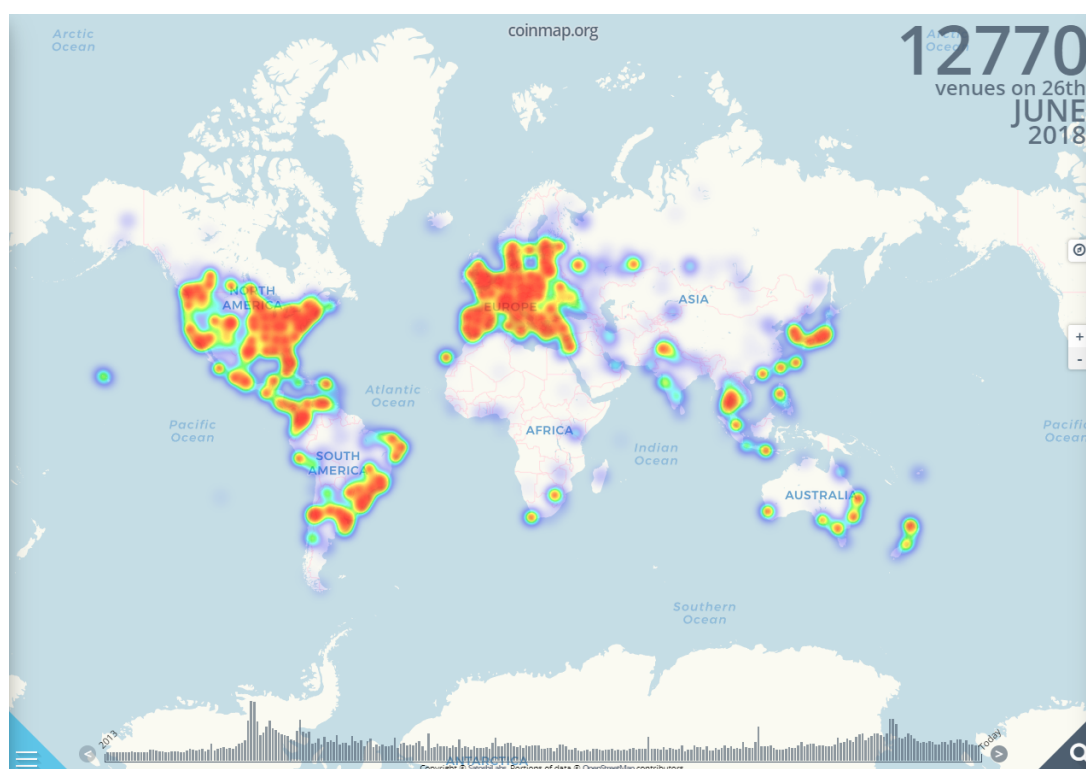


Figura 20. Estabelecimentos que aceitam criptomoedas pelo mundo.

Referências

- Antonioli, Natanael (2016). Manual do Iniciante em Criptomoedas.
- Severeijns, Luc. (2017). What is blockchain? How is it going to affect Business? Supervisionado pelo Prof.Dr. Sandjai Bhulai.
- Portal Buy Bitcoin Worldwide (2017). Pools de Mineração de Bitcoin. <www.buybitcoinworldwide.com/pt-br/minerando/pools>
- Santos, Maria do 99bitcoins (2018). The 6 Best Bitcoin Mining Software. <www.99bitcoins.com/the-6-best-bitcoin-mining-software>
- JuniorS do Confluence (2016). Sobre o Algoritmo de Hashing X11. <www.dashpay.atlassian.net/wiki/spaces/PDDEP/pages/79986844/X11>
- Nunes, Mateus (2018). 3 Melhores programas para mineração de criptomoedas 2018. <www.livecoins.com.br/3-melhores-programas-para-mineracao-de-criptomoedas-2018/>
- JuniorS do Confluence (2018). SHA-256. <www.coin-report.net/en/sha-256/>
- Equipe NB (2017). Mineração com placa de video, ainda vale a pena? <www.nerdbitcoin.com/mineracao-com-placa-de-video-ainda-vale-pena>
- Gomes, Ezequiel (2017). Como as criptomoedas ganham valor? O quê ou quem as valoriza? <www.guiadobitcoin.com.br/como-as-criptomoedas-ganham-valor-o-que-ou-quem-as-valoriza/> Acesso em: 18 de jun. de 2018.

Regis S., Lucas (2016). Bitcoin: Quanto Custa? Compreendendo os Principais Drivers de um Ativo Financeiro Digital Especulativo ao Longo de sua Breve Existência Acesso em: 19 de jun. de 2018.

Portal Confio na Compra (2017). Onde e como comprar Bitcoin (BTC) no Brasil? Acesso em: 18 de jun. de 2018.

Agência Sebrae de Noticias (2017). BITCOIN: CONHEÇA OS IMPACTOS DESSA MOEDA DIGITAL PARA OS PEQUENOS NEGOCIOS <www.revistapegn.globo.com/Negocios/noticia/2017/12/bitcoin-conheca-os-impactos-dessa-moeda-digital-para-os-pequenos-negocios.html> Acesso em: 21 de jun. de 2018.

Portal Insider Pro (2017). Qual o impacto das criptomoedas e da blockchain no mundo? <www.insider.pro/investment/2017-12-13/qual-o-impacto-das-criptomoedas-e-da-blockchain-no-mundo/> Acesso em: 22 de jun. de 2018.

Souza, Samira (2017). Exchanges de Bitcoin: Saiba Como Elas Funcionam <www.investimentosfinanceiros.com.br/exchanges-de-bitcoin-saiba-como-elas-funcionam/> Acesso em: 22 de jun. de 2018.

Guimarães, Eduardo (2017). Glossario: Termos mais usados no trade. <www.criptomoedasfacil.com/glossario-termos-mais-usados-no-trade/> Acesso em: 21 de jun. de 2018.

A CRIPTONARIO (2017). EXAMINANDO A HISTORIA DA CRIPTOMOEDA – COMO EVOLUIU DESDE O INICIO ATE AGORA. <www.criptonario.com.br/examinando-historia-da-criptomoeda/> Acesso em: 18 de jun. de 2018.

COOPERFORTE (2017). A histOria do dinheiro: do escambo as moedas virtuais. <www.economiadiaadia.com.br/a-historia-do-dinheiro-do-escambo-as-moedas-virtuais> Acesso em: 18 de jun. de 2018.

BRAS, Sputnik (2018). Muito além do Bitcoin: conheça 10 criptomoedas que competem no mercado virtuais.

<www.sputniknews.com/economia/2018012010324923-bitcoin-lista-10-criptomoedas-moedas-virtuais> Acesso em: 18 de jun. de 2018.

MENOSSO, Viviane (2017). Tipos de Carteiras Virtuais para Criptomoedas <www.medium.com/blognegociemoins/conhe Acesso em: 19 de jun. de 2018.

RAPHAEL, Cristihan (2017). O que é Seed? Como posso usa-lo para recuperação e segurança da minha Carteira off–line? <www.criptomoedasfacil.com/oque-e-seed-como-posso-usa-lo-para-recuperacao-e-seguranca-da-minha-carteira-off-line/> Acesso em: 19 de jun. de 2018.