Atlântica - Instituto Universitário, Portugal

Tecnologias de Informação de Suporte às Criptomoedas

Cryptocurrencies Support Systems

2021

Editores:
António Aguiar, Atlântica - Instituto Universitário
João Zambujal-Oliveira, Universidade da Madeira

Publicado em Portugal por
Atlântica - Instituto Universitário
Fábrica da Pólvora,
2730-036 Barcarena, Portugal
Tel:+351 215 859 460
Email:informa@uatlantica.pt
Website: https://www.uatlantica.pt/

Para acesso eletrónico a esta publicação, aceder a: https://repositorio-cientifico.uatlantica.pt.

Tecnologias de Informação de Suporte a Criptomoedas / António Aguiar & João Zambujal-Oliveira, Editores

Inclui referências bibliográficas e índice.

Resumo: "O objetivo desta publicação é reunir algumas das ideias, conceitos e sistemas que permitem o desenvolvimento e utilização das principais criptomoedas. Cada capítulo concentra-se numa determinada criptomoeda, mostrando alguns tópicos históricos, modo de funcionamento e pontos fortes e fracos dessa criptomoeda", fornecido pelos editores.

ISBN 978-972-97787-5-9 (ebook) 1. Dogecoin – DOGE - XDG. 2. Bitcoin. 3. Litecoin. 4. Repeated Games. 5. PancakeSwap - CAKE. 5. Shiba Inu. 6. Ripple - XRP. 7.Cardano ADA.

Published in Portugal by
Atlântica - Instituto Universitário
Fábrica da Pólvora,
2730-036 Barcarena, Portugal
Tel:+351 215 859 460
Email:informa@uatlantica.pt
Website: https://www.uatlantica.pt/

For electronic access to this publication, please access: https://repositorio-cientifico.uatlantica.pt.

Cryptocurrencies Support Systems, / António Aguiar & João Zambujal-Oliveira, Editors.

Includes bibliographical references and index.

Summary: "The purpose of this publication is to bring together some of the ideas, concepts and systems that allow the development and use of the main cryptocurrencies. Each chapter focus in one cryptocurrency, showing some historical topics, how it works and the strengths and weaknesses of the cryptocurrency. "– Provided by editors.

ISBN 978-972-97787-5-9 (ebook) 1. Dogecoin – DOGE - XDG. 2. Bitcoin. 3. Litecoin. 4. Repeated Games. 5. PancakeSwap - CAKE. 5. Shiba Inu. 6. Ripple - XRP. 7.Cardano ADA.

Índice

Capítulo 1

Dogecoin – DOGE - XDG

Bernardo, Gonçalo

Resumo

Nos últimos anos temos visto um grande crescimento no interesse nas criptomoedas. A Dogecoin apesar de ter começado como uma brincadeira é um verdadeiro fenómeno no ecossistema criptográfico, e que rapidamente se apercebeu que iria ter sucesso. O uso do "meme" de um cão de raça Shiba Inu de cor amarela, foi uma das armas de dar uma imagem à mesma. A Dogecoin é a 6ª criptomoeda mais valiosa neste momento, estando com valores de crescimento neste ano bastante significativos. Mas à medida que a Dogecoin se torna mais popular, alguns aspetos técnicos ultrapassados começam a ficar mais evidenciados.

Palavras-Chave: Bitcoin, Blockchain, Criptocurrency, DOGE, Dogecoin, XDG.

Abstract

In recent years we have seen a huge growth in interest in cryptocurrencies. Dogecoin, despite having started as a joke, is a true phenomenon in the crypto ecosystem, and it quickly realised it would be successful. The use of the meme of a yellow Shiba Inu dog was one of the weapons used to give it an image for a greater credibility. Dogecoin is the 6th most valuable cryptocurrency at the moment, being with growth figures, quite significant. But as Dogecoin becomes more popular, some outdated technicalities are becoming more apparent.

Keywords: Bitcoin, Blockchain, Criptocurrency, DOGE, Dogecoin, XDG.

DOGECOIN – DOGE - XDG

I. INTRODUÇÃO

Esta criptomoeda (*Dogecoin*) tem uma especial curiosidade pelo seu fenómeno de surgir como uma "moeda de brincadeira" e com um *meme* de um cachorro amarelo de raça *Shiba Inu*, que a tornou numa das criptomoedas mais acarinhada pelos investidores. A *Dogecoin* é uma criptomoeda "*peer-to-peer*" de código aberto, criada em Dezembro de 2013, e teve um enorme crescimento nos anos seguintes.

Mas porque é que existe a necessidade do aparecimento destas "moedas"? Temos visto um enorme interesse nas criptomoedas, no *Blockchain*, na criptografia, a popularidade da *Bitcoin* e de grandes referências mundiais, como o exemplo do CEO da Tesla *Elon Musk*, a investirem neste mercado.

Ao contrário dos sistemas bancários tradicionais, a grande maioria destas criptomoedas usam um sistema descentralizado, isto é, são moedas digitais globais que não usam nem pessoas, nem governos nem nações para a sua gestão e manipulação.

A tecnologia *Blockchain*, como sistema aberto permitiu que outros *developers* e investidores tivessem conhecimento de cada passo dentro do circuito, passando uma imagem de transparência e confiança para todos os que se interessam nestas novas "moedas digitais".

Estas criptomoedas, que podemos de apelidar de *tokens*, porque não são mais do que *tokens* eletrónicos que permitem transferir fundos de um ponto A para um ponto B em qualquer parte do mundo, em qualquer horário, sem ter de confiar o mesmo a uma terceira parte.

II. HISTÓRIA DA DOGECOIN

A *Dogecoin* foi criada em Dezembro de 2013 por *Billy Markus*, ex-engenheiro de software da IBM e também *Jackson Palmer*, um gestor de produtos da ADOBE. A *Dogecoin* é uma criptomoeda, ou seja, um *token* eletrónico "*peer-to-peer*" descentralizado, isto é, sem estar dependente de terceiros (denominam-se terceiros, as entidades bancárias ou governos). Apesar de ser mais uma criptomoeda, igual a tantas outras, a sua criação foi diferente. A mesma foi inspirada pelo "*meme*" *DOGE,* que começou a circular em 2009, com a sua imagem acompanhada de variadas legendas em *Comic Sans* (fonte digital da *Microsoft*).

A piada do *DOGE* foi o início do que estava para acontecer, a origem da *Dogecoin*, a criptomoeda que valorizou mais de 8000% em 2021. Apesar de tudo, os valores das criptomoedas, têm uma grande volatilidade, subindo e descendo de acordo com os níveis de interesse pelas mesmas. Estes níveis de interesse são muito influenciados por menções das mesmas nas redes sociais e na internet.

No caso da *Dogecoin*, esses influenciadores foram os responsáveis pelo crescimento acelerado da valorização. Depois da criação da criptomoeda em 2013, a "piada" relacionada ao *meme* perdeu força e os valores da moeda começaram a ficar mais estáveis. Em 2019, no entanto, o entusiasmo em relação à XDG voltou a subir,

inicialmente em fóruns do *Reddit* (plataforma de fóruns online com mais de 67 milhões de visitantes por mês), que depois começou a ser a porta para as contas de *Twitter.*

Um dos maiores impulsionadores foi *Elon Musk*, CEO da Tesla, ele que é apelidado pelo "oráculo do *hype*", onde tudo o que ele toca ou menciona, ganha relevância. Bastou um *tweet* de *Elon Musk* em Dezembro de 2020 para dar mais um empurrão à *Dogecoin:*

> *"... One Word: DOGE ..."*
>
> *Elon Musk, CEO da Tesla*

Com este *tweet* o valor da *Dogecoin* subir mais de 20%. Em Abril, *Musk* fez mais um *tweet* com grande impacto:

> "*... Doge Barking at the Moon ...*"
>
> *Elon Musk, CEO da Tesla*

Da mesma maneira que estes influenciadores com os seus *tweets* ajudam, outros desses *tweets*, são uma completa desgraça. Em Maio, no programa "*Saturday Night Live*" da NBC, a Mãe de *Elon* fez um comentário sobre o Dia da Mãe:

> "*... - I'm excited for my Mother's Day gift, Maye Musk said.*
> *- I just hope it's not dogecoin!*
> *- It is,Elon Musk said. It sure is. …*"
>
> *May e Elon Musk*

Este comentário fez com que os investidores vendessem a *Dogecoin*, com quebras de 40% no valor negocial da criptomoeda.

Existem outros influenciadores bem conhecidos, como *Snoop Dogg, Gene Simmons, Kevin Jonas* que já fizeram *tweets* a mencionar a *Dogecoin*.

III. FUNCIONAMENTO DA DOGECOIN

A *Dogecoin* é uma criptomoeda, que possui um código-fonte aberto, isto é, qualquer pessoa pode aceder ao mesmo, dando assim confiança e credibilidade ao código que está por baixo da mesma. É descentralizada como muitas das outras criptomoedas, e com um funcionamento "*peer-to-peer*", sem envolver nenhum servidor ou 3 entidade como entidades bancárias ou governos.

A grande diferença desta criptomoeda, é a sua criação menos convencional. A *Dogecoin* não possui nenhum documento oficial sobre a sua criação, como por exemplo a *Bitcoin* com o *White Paper* de *Satoshi Nakamoto*.

A DOGE funciona com o protocolo *Proof of Work (PoW)* tal e qual como a *BitCoin*. Isto significa que a inserção de novos *tokens* (XDG) no circuito acontece por meio de mineração, processo no qual os operadores de rede validam as transações que ocorrem dentro do *Blockchain,* sendo recompensados por essa tarefa, com unidades do mesmo *token*.

Este algoritmo (*PoW*) é um tipo de infraestrutura que começa a entrar em desatualização ou ineficácia, pois exige a resolução de equações matemáticas extremamente complexas. Estas equações são tão complicadas que o hardware necessário para as processar consome muita energia.

Então porque é que as moedas criptográficas como XDG e BTC ainda utilizam este algoritmo? É praticamente impossível alterar o núcleo de uma infraestrutura de rede de uma cadeia de bloqueios já existente. A única forma de se afastar deste algoritmo (*PoW*) é construir uma nova moeda criptográfica a partir do zero.

O maior problema do XDG é o facto da mesma não ser uma moeda deflacionária como a BTC, e por isso é suscetível à inflação tal como as moedas tradicionais (Dólar e Euro). A taxa de inflação da XDG não é tão má como a taxa de inflação da moeda tradicional, pois a sua oferta ainda é ilimitada - novas moedas XDG serão produzidas ao longo do tempo, indefinidamente. A completa falta de inflação é uma das principais razões que tornaram a BTC tão popular, e a fazem dela uma tremenda reserva de valor.

Por não ter um limite de moedas, e já com mais de 100 biliões de XDG já em circulação, esta criptomoeda não vão conseguir aumentar muito o seu preço ao longo dos anos, como acontece com outras.

Apesar da sua criação ser tão diferente a mesma já possui um valor capitalizado de mais de 6 biliões de euros.

IV. EXCHANGE DOGE

Uma "*cripto exhange*" centralizada funciona basicamente da mesma forma que as plataformas clássicas de troca de ativos.
Hoje em dia, a DOGE encontra-se disponível numa ampla variedade de corretoras e empresas e /ou aplicações de *exchanges*:

- ETORO
- COINSMART
- BITPANDA
- BINANCE
- COINBASE
- EXMO
- REVOLUT
- GEMINI
- KUCOIN
- BITPAY

A primeira aquisição de produto com a *Dogecoin*, foi um hambúrguer da cadeia de *fast-food Burger King* pela aplicação BiTPay.

Uma das mais recentes notícias do uso da criptomoeda XDG para pagamento de serviços ou produtos, foi a equipa de basquetebol *Mavericks* da NBA (Liga profissional Basquetebol Americano) que passou a permitir a aquisição de bilhetes para os seus jogos bem como a aquisição de artigos das suas lojas.

"… The Mavericks have decided to accept Dogecoin as payment for Mavs tickets and merchandise for one very important, earth shattering reason, because we can! Because we can, we have chosen to do so. …"

Dallas Mavericks owner, Mark Cuban

V. XDG vs BTC

A descrição da criptomoeda *Dogecoin* não é muito diferente da sua irmã – a *Bitcoin*. Em ambas é usado um algoritmo *hash* do tipo *scrypt* de chaves totalmente públicas. A situação é semelhante no código-fonte. São quase idênticas, com pequenas diferenças. Os desenvolvedores da XDG fizeram pequenas mudanças e modernizaram-na. A principal e mais essencial característica é o curto período de mineração.

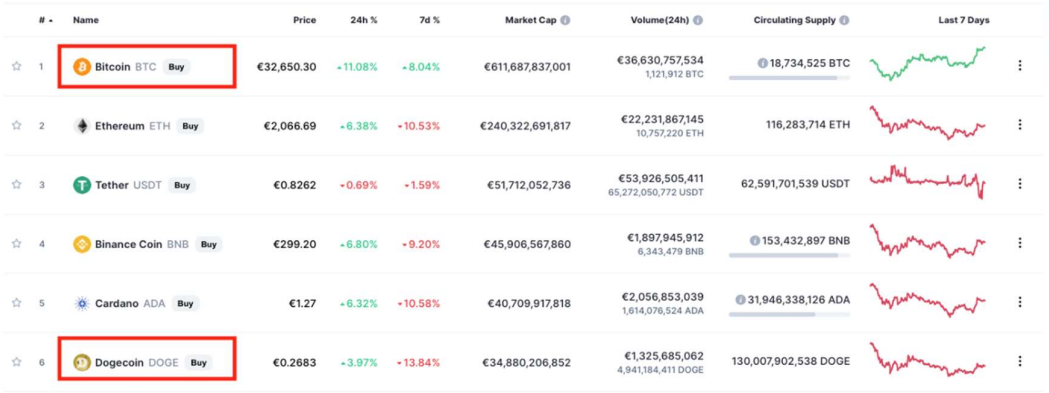
A BTC é a maior e a mais conhecida moeda no mundo das criptomoedas, teve a sua criação em 2009 e revolucionou o uso *Blockchain*, a XDG teve a sua criação em 2013, e rapidamente ganhou muitos seguidores pelo modo como a mesma foi criada. Para conseguirmos perceber a evolução do preço, precisamos de perceber alguns aspetos acerca destas criptomoedas:

1. A XDG é usada apenas para caridade e outras tarefas legais, por usa vez a BTC é vista muitas vezes como meio de transferência de dinheiro;
2. A XDG não tem um limite de emissão – pode ser minerada indefinidamente;
3. O baixo preço da XDG é um dos seus pontos fortes;
4. A comissão de transferência é de apenas 1 XDG;
5. Mecanismos de proteção complexos, pois são alvo de constantes tentativas de *Hacking.*

Em Maio de 2021, a Tesla interrompeu os pagamentos em *Bitcoin* por motivos ambientais, fazendo cair o preço da moeda e o mercado de cripto em geral, e por sua vez, voltou a mencionar a XDG como ecologicamente mais correta que a BTC.

Gráfico 1 – Valor criptomoeda. Fonte: krptomat.io em 14/06/2021

A grande diferença do valor de cada unidade da XDG em relação ao valor da BTC.



#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC Buy	€32,650.30	11.08%	8.04%	€611,687,837,001	€36,630,757,534 1,121,912 BTC	18,734,525 BTC	
2	Ethereum ETH Buy	€2,066.69	6.38%	10.53%	€240,322,691,817	€22,231,867,145 10,757,220 ETH	116,283,714 ETH	
3	Tether USDT Buy	€0.8262	0.69%	1.59%	€51,712,052,736	€53,926,505,411 65,272,050,772 USDT	62,591,701,539 USDT	
4	Binance Coin BNB Buy	€299.20	6.80%	9.20%	€45,906,567,860	€1,897,945,912 6,343,479 BNB	153,432,897 BNB	
5	Cardano ADA Buy	€1.27	6.32%	10.58%	€40,709,917,818	€2,056,853,039 1,614,076,524 ADA	31,946,338,126 ADA	
6	Dogecoin DOGE Buy	€0.2683	3.97%	13.84%	€34,880,206,852	€1,325,685,062 4,941,184,411 DOGE	130,007,902,538 DOGE	

Gráfico 2 – Principais criptomoedas, com preço, taxas de variação e volume. Fonte: CoinMarketcap.com em 14/06/2021

Como podemos avaliar a XDG situa-se como a 6ª criptomoeda mais valiosa neste mercado. A BTC continua como a principal, mas com um preço muito elevado. O preço da XDG é muito baixo, permitindo que quem queira entrar neste universo, possa optar por esta criptomoeda por ter um valor tão baixo.

Gráfico 3 – Evolução último ano da Dogecoin. Fonte: Kriptomat.io em 14/06/2021

A XDG teve um aumento bastante significativo neste ano de 2021, conforme se pode verificar, mas a BTC também tem tido um crescimento, não tão acentuado, mas também bastante considerável no ano de 2021. Relembrar que a escala de valor nestes gráficos é diferente entre as criptomoedas, mas demonstra o crescente interesse no uso destas "moedas digitais".

VI. CONCLUSÃO

Assim podemos concluir que as criptomoedas vieram para ficar e para serem tidas em consideração nos próximos tempos. Muitas alterações estão para vir, e neste momento existem mais de 5000 criptomoedas no mercado. Ainda vão existir alterações a nível do *BlockChain*, no modo de valorização de cada criptomoeda, ou do tipo de controlo de movimento de dinheiro, e sem dúvida cada vez mais serviços, produtos e bens a serem adquiridos com estas "moedas digitais".

Neste estudo e análise, podemos confirmar que a XDG é muito similar às restantes criptomoedas do mercado, e que a volatilidade do valor da mesma está dependente muitas vezes de terceiros, com vários interesses por trás das mesmas. A sua dependência de "*tweets*" e fóruns como o *Reddit,* criam uma instabilidade no seu valor. A intervenção de *Elon Musk* mostra isso mesmo, e como um simples comentário pode afetar a sua estabilidade.

Os problemas com a inflação e com o *PoW* (algoritmo da Prova de Trabalho) são apenas dois dos problemas mais significativos com a criptomoeda XDG.

A *Dogecoin* é uma moeda criptográfica de 2013. Mas já não estamos em 2013 e por isso o que temos vindo a constatar, é o surgimento de novas soluções para as criptomoedas, como por exemplo as *DeFi*. As *DeFi* ou finanças centralizadas, são a recriação dos serviços financeiros bancários sem centralização e intermediários tradicionais.

> "... O objetivo do *DeFi* é reconstruir o sistema bancário para todo o mundo desta forma aberta e sem permissão. ..."
>
> *Alex Pack, CEO* da *Dragonfly Capital*

Ao aparecimento da *Dogecoin Cash* entre outras, vem dar ainda mais força e estas novas soluções. A DOG como é conhecida a *Dogecoin Cash,* foi pensada e concebida para resolver os problemas da XDG, como a utilização do algoritmo *PoW* e a inflação, bem como a redução do uso de energia e ainda proporcionar um rendimento passivo.

REFERÊNCIAS

[1] *Bitcoin*: A moeda na era digital—Fernando Ulrich—Google Livros. (sem data). Obtido 14 de Junho de 2021, de https://books.google.pt/books/about/Bitcoin_A_moeda_na_era_digital.html?id=s-lDDwAAQBAJ&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=false

[2] *Bitcoin? Etherium? Dogecoin? Your guide to the crypto coins that matter—CNN*. (sem data). Obtido 14 de Junho de 2021, de https://edition.cnn.com/2021/04/22/investing/cryptocurrency-guide-top-five-bitcoin-ethereum/index.html

[3] *Chohan, U. W.* (2017). *A History of Dogecoin. SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3091219

[4] *Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCa*p. (sem data). Obtido 14 de Junho de 2021, de https://coinmarketcap.com/

[5] *Differences between bitcoin and dogecoin: Experts.* (sem data). Obtido 14 de Junho de 2021, de https://www.cnbc.com/2021/05/07/differences-between-bitcoin-and-dogecoin-experts.html

[6] *Dogecoin*. (sem data). Obtido 14 de Junho de 2021, de https://dogecoin.com/

[7] *Dogecoin tumbles after Elon Musk jokes about it on SNL - CNN*. (sem data). Obtido 14 de Junho de 2021, de https://edition.cnn.com/2021/05/09/investing/dogecoin-elon-musk-snl/index.html

[8] *Kriptomat*. (sem data). Obtido 14 de Junho de 2021, de https://kriptomat.io/pt/

[9] O que são Criptomoedas e como investir com segurança? (sem data). *InfoMoney*. Obtido 14 de Junho de 2021, de https://www.infomoney.com.br/guias/criptomoedas/

[10] *The Dogecoin Survival Guide, 2nd Edition—Imgur*. (sem data). Obtido 14 de Junho de 2021, de https://imgur.com/a/Sgyox#47KDghm

Capítulo 2

Bitcoin

Sezaltino, Gabriel

Resumo

Atualmente o conceito de dinheiro mudou, novas tecnologias apareceram, como as moedas digitais, o bitcoin foi a primeira criptomoeda criada e contribuiu de maneira revolucionaria na criação e desevolvimento de outras moedas virtuais, como a ethereum por exemplo. Mesmo com o alto nível de concorrencia o bitcoin permanece no topo e desenvolve-se com novos serviços cada vez estando mais presente no mercado financeiro e aumentando seu nível de negociação.

Palavras-Chave: Criptomoeda, bitcoin, ethereum.

Abstract

Bitcoin was the first cryptocurrency created and has contributed in a revolutionary way to the creation and development of other virtual currencies, such as ethereum, for example. Even with the high level of competition, bitcoin remains at the top and develops new services, becoming more and more present in the financial market and increasing its level of trading.

Keywords: Cryptocurrency, bitcoin, ethereum.

Bitcoin

Introdução

No princípio, antes da criação das criptomoedas todos tinham uma determinada ideia sobre o dinheiro, sendo ele algo físico, porém com a determinação de Satoshi Nakamoto grupo ou pessoa de aniquilar a banca, gerou a criação da primera criptomoeda mostrando assim uma nova forma de representação financeira, vendas são efetuadas com moedas virtuais que estão cada vez mais em alta no mercado, uma delas é a Bitcoin.

Este trabalho abordará a cerca da maior criptomoeda e a primeira ja criada, chamada Bitcoin, sendo ela de suma importancia para o desenvolvimento das mesmas. Mesmo com muitas quedas no mercado a Bitcoin sempre foi uma das maiores moedas do mundo e sempre esteve no topo, no ano de 2020, sendo este o período pandemico teve uma taxa de crescimento extremamente acentuada, mostrando novamente sua força.

Será tratado questões sobre o funcionamento da criptomoeda Bitcoin evidenciando suas tecnologias e retratando as mesmas no mercado financeiro mostrando a impotancia de sua evolução e como isso impactou no restante das criptomoedas.

O que é Bitcoin

O bitcoin é uma moeda digital peer-to-peer, uma arquitetura de rede de computadores em que cada ponto ou nó da rede atua como cliente e servidor, de forma que serviços e dados possam ser compartilhados sem um servidor central. Essa criptomoeda é considerada única por ser o primeiro sistema de pagamento global descentralizado.

História

A apresentação ao mundo da bitcoin foi realizada em 31 de outubro de 2008, sendo este o ano do auge da crise financeira, foi apresentada por uma pessoa com pseudônimo Satoshi Nakamoto, em 3 de janeiro de 2009 o primeiro bloco de Bitcoin foi extraído, conhecido como “bloco de gênese” e a primeira transação de teste ocorreu uma semana depois.

Existem precursores para o bitcoin: Adam Back's Hashcash, inventado em 1997, e subsequentemente Wei Dai's B-money, Nick Szabo's bit gold, e Hal Finney's Reusable Proof of Work.

O próprio white paper bitcoin cita Hashcash e b-money, bem como vários outros papéis que cobrem vários campos de investigação.

"*In the early days, the first transactions with Bitcoin were 'negotiated' on internet forums with people bartering for goods and services in exchange for bitcoin*," disse Garrette Furo, sócia da Wilshire Phoenix, uma empresa de gestão de investimentos com sede em Nova York. "*The value of bitcoin was originally arbitrary.*

Como funciona

- **Transações**

As transacções são verificadas, e o duplo gasto é evitado, através da utilização inteligente da criptografia de chave pública. Tal mecanismo requer que para cada utilizador sejam atribuídas duas "chaves", uma privada, que é mantida em segredo, como uma senha, e uma pública, que pode ser partilhada com todos**.**

A transacção, e portanto uma transferência de propriedade das bitcoins, é registada, carimbada no tempo, e exposta num "bloco" da cadeia de bloqueio (a grande base de dados, ou ledger da rede Bitcoin). A criptografia de chave pública assegura que todos os computadores da rede têm um registo constantemente actualizado e verificado de todas as transacções dentro da rede Bitcoin, o que impede duplicação de despesas e fraude de qualquer tipo .

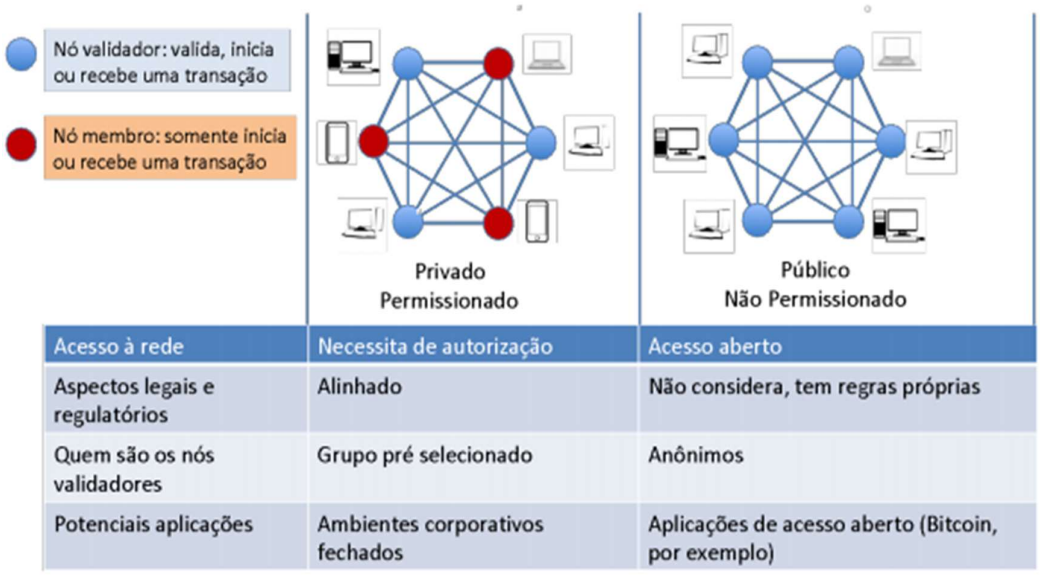
Sendo assim quando um cliente ‘A’ deseja fazer uma transação para um cliente ‘B’ a mesma cria uma mensagem, chamada de “transação”, contendo a chave pública do cliente ‘B’, que assina com sua chave privada. Tendo em conta a chave pública do cliente ‘A’, qualquer um por meio do blockchain pode verificar se a transação foi de fato assinada com sua chave privada, sendo assim, ocorre uma troca autêntica em que o cliente ‘B’ é o novo proprietário dos fundos.

- **Blockchain**

É uma plataforma tecnológica utilizada para o funcionamento de criptomoedas como o Bitcoin por exemplo que é a primeira e mais conhecida aplicação da Blockchain.

Este sistema funciona de forma distribuida em uma base de dados em logaritmo, sendo gerido e mantido de forma compartilhada e descentralizada na qual os que participam são responsaveis por manter a mesma.

Esta tecnologia foi feita tendo como referencia quatro principais arquitecturas: segurança nas operações, descentralização de armazenamento, integridade de dados e regularidade nas transações.



Acesso à rede	Necessita de autorização	Acesso aberto
Aspectos legais e regulatórios	Alinhado	Não considera, tem regras próprias
Quem são os nós validadores	Grupo pré selecionado	Anônimos
Potenciais aplicações	Ambientes corporativos fechados	Aplicações de acesso aberto (Bitcoin, por exemplo)

Figura 1 – Tipos de redes

As redes em cadeia de blocos estão actualmente divididas em dois grandes grupos: As redes públicas ou sem autorização e as redes privadas ou com autorização. A figura 1 mostra algumas características de tais redes.

- **Servidor Timestamp**

Este tipo de sevidor gera um "*hash*", ou seja transforma dados de tamanhos variaveis para dados de tamanho fixo de um bloco de itens e o pública amplamente, da mesma forma que um post Usenet ou um jornal.Além disso o timestamp também prova que os dados devem

ter existido para poder entrar no “hash”.Cada um dos timestamp contém o anterior em seu “*hash*”, formando assim uma cadeia, com os timestamp complementar reforçando assim os que vieram antes do mesmo.

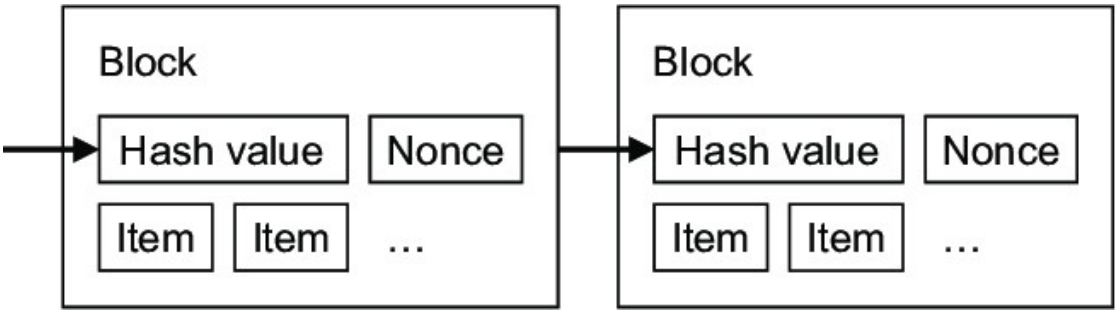


Figura 2 – Timestamp

Modelos de Privacidade

No modelo bancário tradicional há uma limitação ao acesso perante as partes envolvidas e aos terceiros confiáveis atingindo assim um certo nível de privacidade.

Sendo assim a necessidade de anunciar todas as transações se opõe a este modelo, porém a segurança e privacidade ainda pode ser mantida quebrando o fluxo de informação, criando chaves públicas anônimas.

Tendo em conta esse novo modelo imposto pelas criptomoedas sabe-se que o público tem a informação de qual transição ocorre mas não há detalhes que ligam a transação a outro indivíduo.

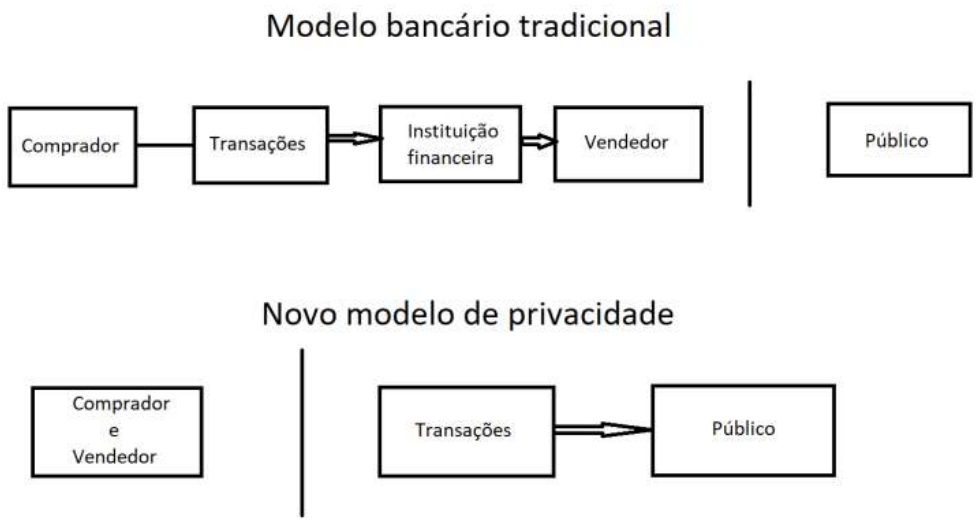


Figura 3- modelo de privacidade

A Bitcoin no Mercado

A Bitcoin teve sua primeira aparição no mercado em 2009 aonde não teve nenhum valor monetário, apenas fãs trocando a moeda em fóruns como um teste.

Em 22 de maio de 2010 o "*user*" Laszlo Hayneck fez a primeira transação, comprou duas pizzas em Jacksonville, Flórida, por 10,000 BTC.

Em fevereiro de 2011, o preço do Bitcoin ultrapassou o limite de US $ 1. "No início, à medida que crescia, seu preço era inferior a US $ 2", disse Marszalek. "Em junho de 2011, ele borbulhou pela primeira vez, subindo para cerca de US $ 31 e caindo para a faixa de um dígito." Quase dois anos depois, em abril de 2013, o Bitcoin atingiu US $ 200. No final de novembro do mesmo ano, seu valor ultrapassava US $ 1.000. Em seguida, aumentou dez vezes em novembro de 2017, chegando a US $ 10.000. Earle disse que o preço mais alto do Bitcoin era de aproximadamente US $ 19.650 em meados de dezembro de 2017 e apontou que o preço máximo varia de troca para troca. "Então, ele cairá significativamente nos próximos anos." Furo afirmou que a bolha de 2017 a 2018 foi causada principalmente pelo

impacto no mercado da emissão inicial de moeda ou ICO. Alguns veteranos do setor comparam a bolha do Bitcoin aos impactos da Internet no final do século XX.

“De seu vizinho ao mais rico administrador de fundos de hedge, todo mundo está falando sobre Bitcoin ou alguns altcoins, novas redes ou protocolos”, disse Furo. "O boom da ICO trouxe bilhões de dólares para o espaço criptográfico. Os investidores viram uma queda acentuada no valor dos tokens nos primeiros meses de 2018, devido à incerteza, fraude e falta de confiança, bem como outros fatores psicológicos e técnicos pessoal que fez os preços despencarem. " Depois que o valor do Bitcoin caiu, o que você pode chamar de "mercado maduro" surgiu em torno das criptomoedas. "A Fidelity entrou no espaço de custódia (e) o National Bank está autorizado a manter ativos digitais", disse Furo. Hoje, a Square oferece transações de Bitcoin em todos os 50 estados.

“Por causa desses desenvolvimentos, o mercado de Bitcoin se tornou relativamente maduro”, disse Furo. "Existem trocas inteligentes e eficientes, e os principais participantes no nível institucional estão tomando as medidas necessárias para criar um mercado sustentável e viável para o comércio e investimento de Bitcoin e outras criptomoedas." Marszalek disse que a pandemia global em 2020 também é uma bênção para as moedas digitais, cujo preço atual ultrapassa US $ 10.000.

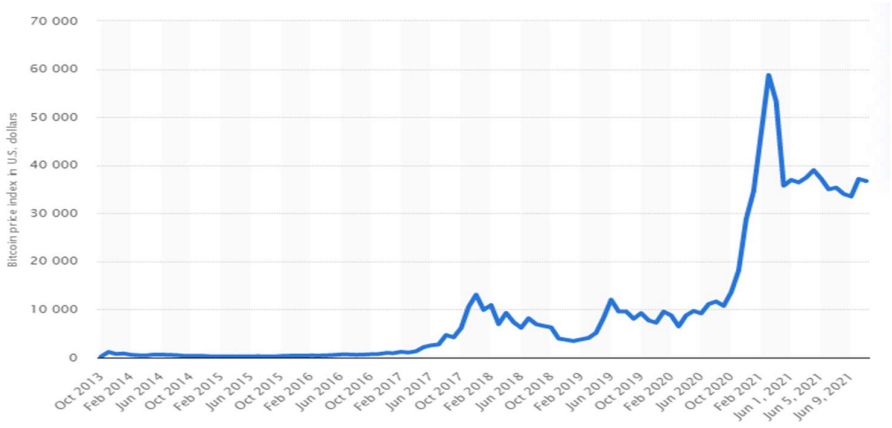


Figura 4 - gráfico de preços

Conclusão

Tendo em conta todos os tópicos abordados sobre a criptomoeda Bitcoin concluisse que a mesma foi a primeira a ser criada e teve grandes desenvolvimentos abrindo assim o mercado para outras moedas digitais.

Em termos de tecnologia, a Bitcoin utiliza um blockchain, servidores timestamp para realizar suas transações, factor muito importante visto que essa área visa sempre a segurança e mantém a mesma com suas tecnologias de chaves, possibilitando os clientes fazerem transações sem que as informações sejam partilhadas, porém a realização da transação seja divulgada para o público, essa transação entra em uma cadeia de blocos aonde o público a realiza, sendo assim o cliente possuirá uma chave privada (com as informações detalhadas) e uma chave pública (divulgada para o público) possibilitando assim ter uma sofisticação nas transações.

No mercado a moeda virtual sempre permaneceu no topo, mesmo com algumas quedas nunca ouve alguma outra criptomoeda que superou a Bitcoin, sendo ela a maior do mundo.

Referências

A História do Bitcoin | Plus500. (sem data). Obtido 17 de Junho de 2021, de https://www.plus500.com/Instruments/BTCUSD/The-History-of-Bitcoin~3

Bit2Me, A. (2019, Janeiro 31). *O que é o Bloco de Gênesis? De Bitcoin | Academia Bit2Me*. Bit2Me Academy. https://academy.bit2me.com/pt/o-que-%C3%A9-o-bloco-de-g%C3%AAnese/

Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCap. (sem data). Obtido 17 de Junho de 2021, de https://coinmarketcap.com/

Nakamoto, S. (sem data). *Bitcoin: A Peer-to-Peer Electronic Cash System*. 9.

The History of Bitcoin | Investing | US News. (sem data). US News & World Report. Obtido 17 de Junho de 2021, de https://money.usnews.com/investing/articles/the-history-of-bitcoin

Times, D. B. completa S. o L. S. o T. J. F. é um escritor experiente em uma ampla variedade de tópicos de notícias de negócios e seu trabalho foi apresentado na I. e no T. N. Y., & Frankenfield, entre outros S. mais sobre nossas políticas editoriais J. (sem data). *Bitcoin Definition*. Investopedia. Obtido 17 de Junho de 2021, de https://www.investopedia.com/terms/b/bitcoin.asp

Sobrenome, P. M. (Ano). *Título do Livro.* Nome da Cidade: Nome da Editora

Capítulo 3

Litecoin

Bule, Gustavo

Resumo

A Litecoin é uma criptomoeda e uma das principais concorrentes da *Bitcoin*. Algumas das suas vantagens incluem uma oferta fixa e um baixo custo de transação. Litecoin (LTC) é uma das primeiras "Altcoins", versão alternativa da *Bitcoin*, que ganhou destaque e permaneceu popular desde então. Foi projetada para ser mais barata de usar e mais rápida de confirmar nas transações, importante tanto para particulares, como para comerciantes, para que a criptomoeda se torne amplamente aceite.

Keywords: LTC, Cryptocurrency, Altcoins, Bitcoin, Transactions, Scrypt, Miner.

Abstract

Litecoin is a cryptocurrency and one of the major competitors to bitcoin. Some advantages include that it has a fixed supply and low transaction cost. Litecoin (LTC) is one of the earliest "Altcoins," or alternative versions of Bitcoin, that rose to prominence and has remained popular ever since. It was designed to be cheaper to use and faster to confirm in transactions, important for both customers and merchants if Crypto is to become widely accepted as a currency.

Keywords: LTC, Cryptocurrency, Altcoins, Bitcoin, Transactions, Scrypt, Miner.

Litecoin

Fundada em 2011, 2 anos apos a moeda Bitcoin, por um ex-engenheiro da Google chamado Charlie Lee, a Litecoin é uma das mais antigas alternativas à bitcoin.

Com uma velocidade de transação de 2.5 minutos a Litecoin é transacionada a 4 vezes velocidade da moeda Bitcoin.

A Litecoin possui um limite máximo de 84 milhões de moedas, um valor 4 vezes superior ao da moeda Bitcoin que apenas tem 21, sendo por esta razão muitas vezes denominada de a "prata" para o "ouro" da Bitcoin.

Como surgiu a moeda?

Lançada em 2011 por Charlie Lee, a moeda Litecoin surgiu come uma resposta direta as limitações da Bitcoin, com o objetivo principal de ser utilizada em transações mais pequenas e de ser uma moeda mais eficiente para utilização no dia a dia.

Com um processo de "Mining" (isto é resolver funções "hash" para obter blocos de moedas) diferente da moeda Bitcoin, a moeda Litecoin de início pretendia tornar o processo mais justo para mineiros que não utilizavam a máquinas baseadas na tecnologia ASIC, mas com a evolução destas máquinas ao longo do tempo o processo tem se tornado cada vez mais dominado por máquinas baseadas em ASIC.

Qual o propósito desta moeda

Como as outras cripto moedas, o propósito principal de uma cripto moeda é criar uma moeda virtual através da qual tanto indivíduos como instituições podem realizar compras de produtos e efetuar transações entre contas, tudo isto sem depender de uma entidade centralizada como um banco.

Outro propósito desta moeda é ser uma moeda de rápida transação para utilização no dia a dia.

Como funciona

A moeda Litecoin ao contrário das moedas convencionais não é emitida por um governo regulado por um banco central que emite uma moeda, a Litecoin possui uma quantidade máxima limitada (84 milhões) e a cada 2.5 minutos é então gerado um novo bloco pela Litecoin Network, este bloco é então verificado por um software de "Mining" e tornado visível para qualquer participante (normalmente denominado "Miner") o poder verificar (este processo é denominado blockchain).

Existe um incentivo para "minar" Litecoin sendo que o primeiro "Miner" a verificar um bloco recebe Litecoins, este valor, no entanto vai sendo reduzido ao longo do tempo por metade até a moeda número 84 000 000 ser minada.

A quantidade de Litecoins atribuídas por bloco foi reduzida por metade em agosto de 2019 de 25 para 12.5 e espera-se que volte a reduzir em agosto de 2023 de 12.5 para 6.25.

Quais as tecnologias utilizadas

A moeda Litecoin utiliza o algoritmo "scrypt", este algoritmo do tipo "proof of work", requer que os membros de uma rede resolvam puzzles matemáticos de maneira a prevenir que utilizadores manipulem o sistema para benefício próprio.

Este sistema é utilizado por outras cripto moedas como tais como a Dogecoin, no entanto quando utilizado em escala este sistema requer grandes quantidades de energia e este valor continua a aumentar a medida que mais utilizadores se juntam a rede.

Em que difere a Litecoin das outras cripto moedas

Velocidade, a Litecoin demora 2:30 minutos a completar uma transação.

Grande quantidade de moedas, a Litecoin tem 4 vezes o número de moedas que a Bitcoin.

Longevidade, o facto de ser uma das primeiras "Altcoins" e ainda circular em mercado.

Evolução em comparação ao euro

(dados obtidos do site livecoinwatch.com no dia 17 de junho)

Em que Exchange se pode transacionar

Top 5 LTC/EUR

Litecoin Markets Spot Perpetual Futures — Pair EUR

#	Source	Pairs	Price	+2% Depth	-2% Depth	Volume	Volume %	Confidence	Liquidity	Updated
1	Kraken	LTC/EUR	€137.92	€690,306.40	€632,314.98	€2,468,367	0.15%	High	520	Recently
2	Coinbase Exchange	LTC/EUR	€138.01	€332,446.17	€481,686.24	€2,438,012	0.14%	High	328	Recently
3	Binance	LTC/EUR	€137.90	€131,161.76	€174,700.60	€2,262,950	0.13%	High	700	Recently
4	Bitstamp	LTC/EUR	€138.02	€240,525.89	€486,529.35	€1,783,919	0.11%	High	276	Recently
5	EXMO	LTC/EUR	€138.13	€5,480.50	€8,607.62	€162,368	0.01%	High	91	Recently

Top 5 global

Litecoin Markets Spot Perpetual Futures — Pair All

#	Source	Pairs	Price	+2% Depth	-2% Depth	Volume	Volume %	Confidence	Liquidity	Updated
1	Binance	LTC/USDT	€137.90	€678,496.00	€1,667,911.45	€74,527,195	4.42%	High	628	Recently
2	Huobi Global	LTC/USDT	€137.87	€605,266.78	€1,798,443.26	€41,087,464	2.44%	High	605	Recently
3	Bithumb	LTC/KRW	€143.58	€130,740.24	€367,421.75	€34,844,377	2.07%	High	260	Recently
4	Coinbase Exchange	LTC/USD	€137.86	€1,382,413.13	€1,425,493.40	€26,004,502	1.54%	High	538	Recently
5	Gate.io	LTC/USDT	€137.87	-	€628,389.62	€13,073,048	0.78%	High	405	Recently

(dados obtidos do site coinmarketcap.com no dia 17 de junho)

Video - Charlie Lee's Litecoin presentation at BTC Miami Conference

Conclusão

Após investigar e pesquisar informações sobre a moeda virtual Litecoin, foi possível observar a diversidade, volatilidade e funcionalidade das moedas virtuais e perceber o papel da Litecoin no mar das cripto moedas.

Apesar de ser uma moeda derivada da Bitcoin a Litecoin possui diversas funcionalidades que a distinguem e a tornam atrativa a investidores que procuram diversificar os seus investimentos ou até mesmo simplificar transações.

Referencias

7 Reasons Bitcoin Mining is Profitable and Worth It (2021). (n.d.). Retrieved June 17, 2021, from https://www.buybitcoinworldwide.com/mining/profitability/

A Comparison of Litecoin vs. Ethereum: Which is Better? • Benzinga. (2021, May 5). Benzinga. https://www.benzinga.com/money/litecoin-vs-ethereum/

editor, F. B. F. L. C. T. is a technical, Banks, D. C. P. with 25+ Y. of E. at T.-T. I., & Tardi, money-management firms L. about our editorial policies C. (n.d.). *Application-Specific Integrated Circuit (ASIC) Miner Definition*. Investopedia. Retrieved June 17, 2021, from https://www.investopedia.com/terms/a/asic.asp

Litecoin Whitepaper. (2018, May 2). *The Whitepaper Database*. https://www.allcryptowhitepapers.com/litecoin-whitepaper/

topics, F. B. F. L. F. T. J. F. is an experienced writer on a wide range of business news, Investopedia, his work has been featured on, & Frankenfield, T. N. Y. T. among others L. about our editorial policies J. (n.d.). *Proof of Work (PoW)*. Investopedia. Retrieved June 17, 2021, from https://www.investopedia.com/terms/p/proof-work.asp

What is a Litecoin halving? (n.d.). Retrieved June 17, 2021, from https://finance.yahoo.com/news/litecoin-halving-100037031.html

What is litecoin?| CMC Markets. (n.d.). Retrieved June 17, 2021, from https://www.cmcmarkets.com/en/learn-cryptocurrencies/what-is-litecoin

writer, F. B. G. M. is a financial, & McFarlane, co-founder of C. com H. is also the co-author of C. Y. C. M. M. M. S. L. about our editorial policies G. (n.d.). *What Is Litecoin?* Investopedia. Retrieved June 17, 2021, from https://www.investopedia.com/articles/investing/040515/what-litecoin-and-how-does-it-work.asp

Capítulo 4

PancakeSwap - CAKE

Cunha, Ângelo

Resumo

Com a introdução das mais variadas criptomoedas na sociedade tanto como as mais variadas tecnologias como o blockchain, machine learning e deep learning, o mercado online têm vindo sofrendo uma expansão gigantesca. Neste documento exploramos como é que um protocolo, *PancakeSwap*, tem vindo a crescer a proporções gigantescas em pouco menos de um ano. Com *PancakeSwap* vamos visualizar também a variedade demográfica entre a comunidade das criptomoedas que se tem feito sentir nos últimos anos, fazendo com que as criptomoedas não sejam apenas um mais nicho, mas sim um novo mercado para todo o tipo de culturas e pessoas.

Palavras-Chave: criptomoedas, blockchain, PancakeSwap, protocolo, cultura, crescimento

Abstract

With the introduction of various cryptocurrencies in society as well as technologies such as blockchain, machine learning and deep learning, the online market has been undergoing a massive expansion. In this paper we explore how one protocol, PancakeSwap, has grown to gigantic proportions in just under a year. With PancakeSwap we will also visualise the demographic variety among the cryptocurrency community that has taken place in recent years, making cryptocurrencies not just a more niche, but a new market for all kinds of cultures and people.

Keywords: cryptocurrencies, blockchain, PancakeSwap, protocol, culture, growth

PancakeSwap - CAKE

I. INTRODUÇÃO

A “loucura” das criptomoedas não é de facto nova, e já conta com valentes anos de inovação e investimentos bem como o alargamento da quantidade e diferenciação de criptomoedas bem como um grande crescimento do número de utilizadores e benfeitores que se têm vindo a juntar na comunidade.

Durante o último ano, e devido à pandemia, houve um crescimento emergente deste número de utilizadores como também do número de criptomoedas e tecnologias emergentes relacionadas com o “fervor cripto” que se tem vindo sentir. Uma destas moedas, da qual vamos investigar e inspecionar melhor todos os seus segredos, como também estudar a maneira que ela se apresenta perante o publico, é a *PancakeSwap*, tal como ela, existem muitas mais que nasceram no ano anterior como *Uniswap*, *SushiSwap*, entre outras.

Entretanto estas moedas cujo mencionei, incluindo a *PancakeSwap*, trabalham de maneira completamente diferente das criptomoedas normais, assegurando maneiras diferentes de entusiastas entrarem nas criptomoedas de maneira segura, divertida e sem perdendo lucro. Estas moedas também chamadas *Tokens* fazem parte da nova tecnologia em protocolo *DeFi*.

II. *O QUE É O DEFI ?*

O termo "Finanças Descentralizadas", ou “*Decentralized Finance*” em inglês, (DeFi) abrange os serviços financeiros realizados normalmente realizados por organizações bancárias sobre um grande número de leis, processos, protocolos e muitos outras barreiras, cujo dependem sempre de uma autoridade central. Os *DeFi* são, precisamente, serviços financeiros sem essa mesma autoridade central. Os Protocolos *DeFi* usam os elementos tradicionais do sistema financeiro e substitui o tradicional intermediário bancário por um contrato inteligente. Podemos também descrevê-lo como a fusão entre serviços bancários tradicionais com tecnologia Blockchain.

Como o nome indica, *DeFi* para poder funcionar como o devido, deverá estar integrada numa infraestrutura decentralizada, em blockchain, de modo que a sua segurança não seja comprometida nem os seus utilizadores sejam prejudicados. É aqui que as mais variadas criptomoedas entram com as suas plataformas e recursos para o efeito. As mais conhecidas plataformas que oferecem suporte *DeFi* são nada mais que a *Ethereum* ou a *Binance Smart Chain*.

Podemos afirmar que uma grande maioria dos protocolos *DeFi* usam o blockchain do *Ethereum*, porém outras plataformas como o *Binance Smart Chain* conseguem oferecer uma experiência mais versátil, eficiente e escalável.

III. BENEFÍCIOS DA DEFI

Como esperado, este protocolo por ser tão adotado no de 2020, deverá ter algum tipo de benefícios. Vamos ver quais os edifícios principais cujo *DeFi* oferecem e justifique a sua adoção:

- Transparência - Os termos, condições e operações financeiras tradicionais acontecem com base na necessidade de saber, mas a menos que esteja do lado do banco, não precisa de saber. *DeFi* divide a cortina utilizando contratos inteligentes baseados em cadeias de bloqueio, colocando ambas as partes num acordo financeiro em pé de igualdade.

- Segurança - Há muito valor em cima da mesa quando se utilizam serviços financeiros. Os seus dados pessoais, para não mencionar dinheiro, são colocados nas mãos de organizações centralizadas que podem ser pirateados, roubados, ou enganados por *hackers* bem colocados que agem maliciosamente. Estes elementos tornar-se-ão progressivamente menos possíveis no mundo da *DeFi*, porque tudo funciona utilizando *smart contracts* altamente seguros.

- Direto - O financiamento descentralizado retira a necessidade de um *middleman* através da organização de um acordo direto entre as partes que é garantido através de *smart contracts* baseados em *blockchain*, permitindo assim acesso a empréstimos sem necessidade de aprovações e operações tradicionais de bancos

IV. INTRODUÇÃO A *BINANCE SMART CHAIN*

Considerando o que vimos sobre o uso do protocolo *DeFi*, vimos que *Ethereum* é um exemplo popular de uma plataforma que permite o uso do protocolo tendo já vários *DeFi* em fase de produção como por exemplo: o *UniSwap* ou *SushiSwap*.

Porém existe outras plataformas existentes para o uso desenvolvimento deste mesmo protocolo, cujo neste caso iremos investigar o *Binance Smart Chain* (BSC).

Antes da conceção da BSC, *Binance* criou em 2017 uma criptomoeda, *Binance Coin* (BNB), cujo utilizava o *Ethereum* como base. Hoje, *Binance* conta com um projeto maior e independente do *Ethereum*, com o objectivo de ser mais eficaz e seguro para o utilizador e o *developer*, projeto este que foi denominado *Binance Chain*. Este foi uma aplicação descentralizada, cujo a *Binance* chama de *dApp*, com o objectivo de tornar a troca de criptomoedas rápida e segura. Porém, *Binance Chain* não incluía os *smart contracts*, logo não permitindo empréstimos e outras soluções cujo *Ethereum* mostraria ser possível. Foi assim que em abril de 2020, *Binance* lança o *Binance Smart Chain*

Vamos verificar alguns dos princípios fundamentais de design que BSC foi contruída:

1. *Standalone Blockchain*: BSC pretende ser um *blockchain* independente, em vez de ser uma solução de duas camadas como se apresentava inicialmente. é importante que as técnicas e funções fundamentais sejam contidas nelas próprias de modo que não exista cortes de serviço.
2. Compatibilidade com *Ethereum*: A primeira plataforma de *Smart Contracts* prática e popular foi o *Ethereum*. Para permitir a continuidade e suporte a aplicações e comunidades mais modernas, BSC escolhe a compatibilidade com *Ethereum*.
3. Aposta envolvida Consenso e Governação: O consenso baseado na estaca é mais amigo do ambiente e deixa opções mais flexíveis para a governação comunitária. Espera-se que este consenso permita um melhor desempenho da rede em relação à prova total de trabalho, ou seja, um tempo de bloqueio mais rápido e uma maior capacidade de transação.
4. *Native Cross-Chain Communication*: tanto a BC como a BSC serão escritas com apoio nativo para a comunicação entre as duas cadeias de bloqueio. O protocolo de comunicação deverá ser bidirecional, descentralizado, e sem confiança. Concentrar-se-á na movimentação de bens digitais entre BC e BSC, ou seja, fichas BEP2, e eventualmente, outras fichas BEP introduzidas mais tarde. O protocolo deve cuidar do mínimo de outros itens armazenados no estado das cadeias de bloqueio, com apenas algumas exceções.

V. O QUE É PANCAKESWAP?

PancakeSwap foi desenvolvida por um grupo anonimo de *developers*, com base na *Binance Smart Chain* e lançada a 20 de setembro de 2020, com o objetivo de criar uma moeda de imagem simpática e simples, e que fosse direta e factual. Por este motivo em vários documentos que verificamos sobre a *PancakeSwap* não iremos notar grandes descrições ou explicações sobre como funciona ou como são feitas as mais diferentes transações ou funções.

Assim seguindo a filosofia da *PancakeSwap*, ou seja, em poucas palavras e de maneira direta:

"*PancakeSwap* é uma troca descentralizada para a troca de fichas BEP-20." (Binance,2021)

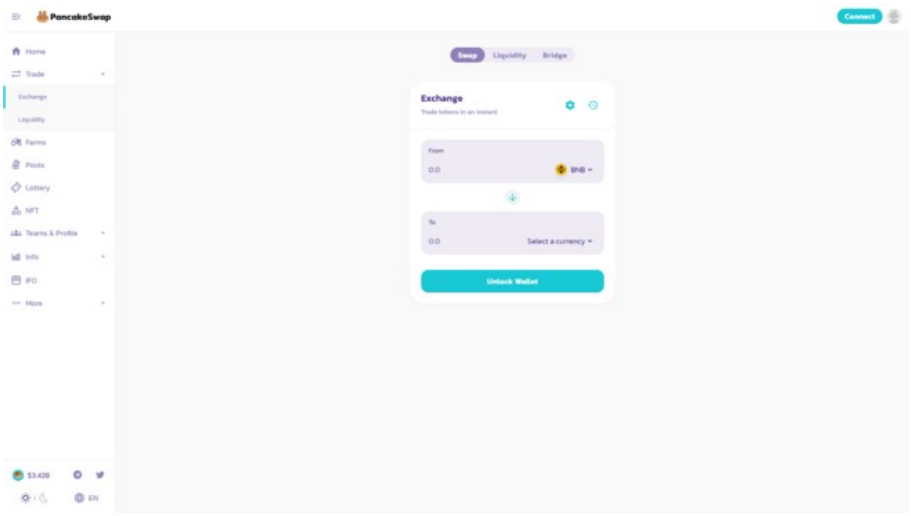
VI. A *PANCAKESWAP EXCHANGE*

Nos protocolos *DeFi*, é comum existir estas plataformas de troca e modelos de como o fazê-lo. No caso do *PancakeSwap*, é usado um modelo *automated market maker(AMM)*, e o que isto significa é que, em vez de um utilizador ter que ser combinado com outro utilizador para executar uma troca de moedas, num AMM os utilizadores usam o que se chama de *Liquidity pools*.

Estas "piscinas" são cheias com fundos de todo o tipo de utilizadores. Ao depositar os seus fundos, os utilizadores recebem um *token* proveniente do fornecedor da piscina (LP).

São com estes *tokens* que o utilizador poderá utilizar as trocas, ou pode deixar os *tokens* na *liquidity* pool para ganhar todo o tipo de prémios.

Em poucas palavras, os utilizadores podem trocar BEP-20 *tokens*, ou adicionar *liquidity* e ganhar variados prémios.



Interface da Pancake Swap Exchange

VII. CULTIVAR E STAKING NA PANCAKESWAP

A *PancakeSwap* dá oportunidade aos utilizadores de cultivarem a sua própria *token* de governação, denominada por CAKE.

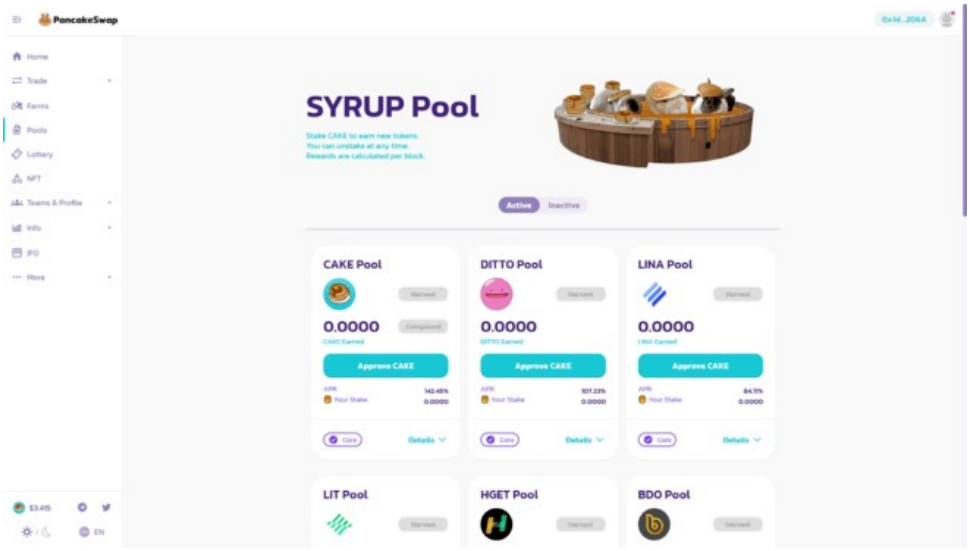
É na horta que o utilizador pode depositar as suas *tokens* LP, trancando-as no processo que dará CAKE ao utilizador. *PancakeSwap* dá uma grande variedade de LP que se pode cultivar, mas uma lista das mais populares pode ser encontrada no guia oficial:

- CAKE – BNB LP
- BUSD – BNB LP
- BETH – ETH LP
- USDT – BUSD LP
- USDC – BUSD LP
- DAI – BUSD LP
- LINK – BUSD LP
- TWT – BNB LP

Para além da *PancakeSwap* dar a possibilidade de ganhar a própria *token* deles através da cultivação de *tokens* LP, também existe outra funcionalidade que permite ganhar mais prémios: *Staking*.

Depois de ganhar CAKE nas *liquidity pools*, existe a possibilidade cujo envolve outras piscinas maiores, ao que a *PancakeSwap* chama de SYRUP pools, que servem para que o utilizador empilhe CAKE para ganhar outras *tokens*.

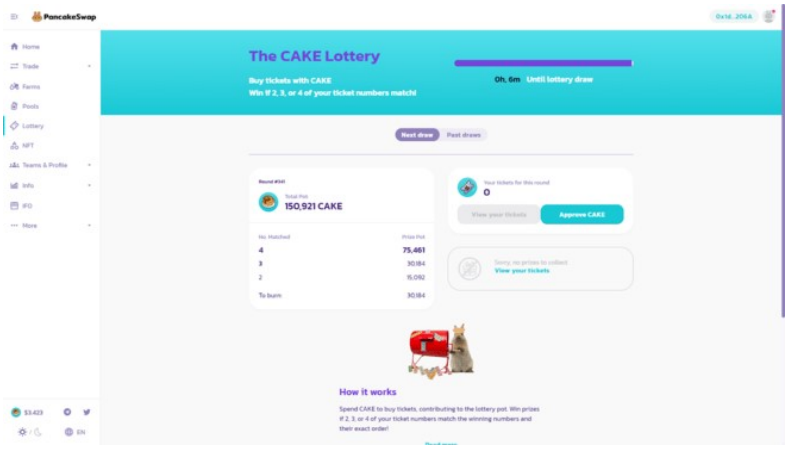
A maior SYRUP pool é de CAKE, ou seja, ao empilhar CAKE *tokens* numa SYRUP pool de CAKE, dará ao utilizador muitas mais CAKE *tokens* cujo ele poderá usufruir, mas existem mais *tokens* que o utilizador pode receber.



Interface da Pancake Swap SYRUP pool

VIII. LOTARIA E NFTS NA PANCAKESWAP

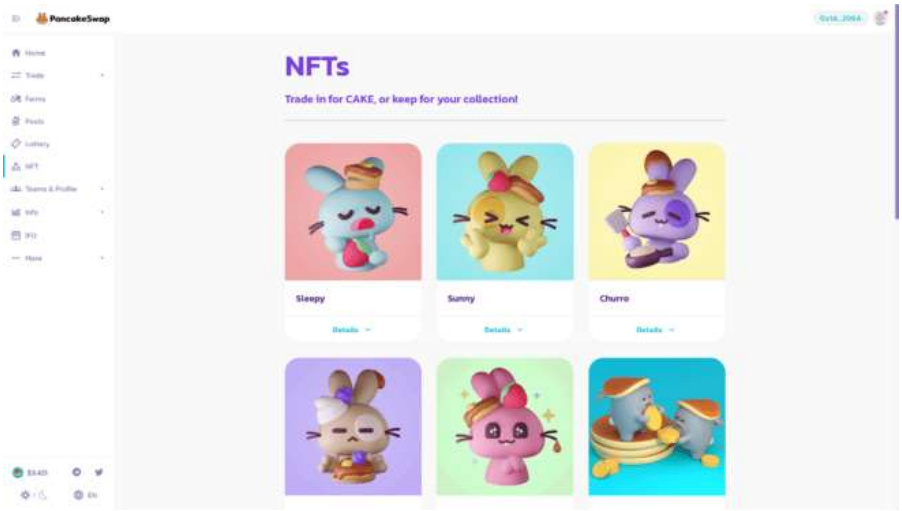
Cada sessão de lotaria leva 6 horas. Um bilhete custa 10 CAKE, que lhe dará ao utilizador uma combinação aleatória de quatro dígitos de números entre 1 e 14, por exemplo, 10-5-8-3. Para ganhar o *jackpot* (50% de toda a lotaria), os números do seu bilhete precisam de corresponder aos quatro números na mesma posição que o bilhete vencedor. Caso os números não corresponderem, também ganha prémios se dois ou mais dos seus números estiverem na mesma posição que os números do bilhete premiado.



Interface da Pancake Swap Lottery

Com *PancakeSwap* também é possível ganhar NFTs vindos da BSC. Se for escolhido como vencedor de um NFT, pode trocá-lo pelo valor CAKE que representa ou manter o NFT na sua carteira como peça de coleção. Para terem uma chance de ganhar,

os utilizadores terão de apenas registar, e ficam automaticamente legíveis para serem selecionados.



Interface da Pancake Swap NFTs

IX. CONCLUSÃO

São com estas mais variáveis características que *PancakeSwap*, em pouco menos de um ano, tornou-se uma das principais *Tokens DeFi* da plataforma BSC. A sua simplicidade no usos e toda a integração com tecnologias emergentes como a própria plataforma da *Binance* como também o recente boom das NFTs como também do todo o mercado das criptomoedas, fazem com que a *PancakeSwap* não só tenha já algum reconhecimento, mas também angaria grande potencial para se tornar uma das caras das criptomoedas, junto com *Ethereum* ou *Binance Coin*.

Toda a comunicação e arte da *PancakeSwap* também sugere a grande expansão das criptomoedas. Entre várias moedas onde se tentam destacar ao parecerem grandes moedas do futuro, *PancakeSwap* vai atrás de arte quase pixel com influências japonesas, possivelmente tentando atrair um publico mais jovem, que neste momento descobre o mundo cripto.

Por fim, o sucesso da *PancakeSwap* deixa a porta aberta e afirma que apesar de grandes nomes como *Bitcoin* e *Ethereum* tenham destaque como grandes inovadores e populares, é extremamente possível e viável a criação de novas *criptomoedas* inovadoras que possam ocupar ou usar tecnologias já existentes.

Deixo assim o valor da CAKE, no dia de conclusão deste documento:


PancakeSwap Token (Cake)
$15.90 ↓1.26%
Add Liquidity
Trade
LIQUIDITY
$340.07M
↓0.79%
VOLUME 24H
$48.41M
↑0.56%
VOLUME 7D
$362.21M
TRANSACTIONS 24H
49K
Volume
Liquidity
Price
$15.90
Jun 17, 2021
18.00
17.50
17.00
16.50
15.90
15.50
15.00
06/13 1:00 AM
06/14 1:00 AM
06/15 1:00 AM
06/16 1:00 AM
06/17 1:00 AM
06/17 7:00

REFERÊNCIAS BIBLIOGRÁFICAS

A Guide to PancakeSwap. (n.d.). Binance Academy. Retrieved 13 June 2021, from https://academy.binance.com/en/articles/a-guide-to-pancakeswap

Binance Chain Community Releases Whitepaper for Enabling Smart Contracts. (n.d.). Binance Blog. Retrieved 13 June 2021, from https://www.binance.com/en/blog/421499824684900520/Binance-Chain-Community-Releases-Whitepaper-for-Enabling-Smart-Contracts

Binance Coin (BNB)—Overview, History and Uses, ICO. (n.d.). Corporate Finance Institute. Retrieved 13 June 2021, from https://corporatefinanceinstitute.com/resources/knowledge/other/binance-coin-bnb/

DeFi explained: The guide to decentralized finance. (2020, December 30). *Forkast*. https://forkast.news/explainer-decentralized-finance-defi-guide/

Pancake Swap Review: Everything You NEED To Know!! (2021, February 26). *Coin Bureau*. https://www.coinbureau.com/review/pancakeswap-cake/

PancakeSwap Intro. (n.d.). Retrieved 3 June 2021, from https://docs.pancakeswap.finance/

PancakeSwap: What it is and how it works. (2021, January 3). *The Cryptonomist*. https://en.cryptonomist.ch/2021/01/03/pancakeswap-what-it-is-how-it-works/

What Is Pancakeswap? | Shrimpy Academy. (n.d.). Retrieved 3 June 2021, from https://academy.shrimpy.io/post/what-is-pancakeswap

Whitepaper_ Binance Smart Chain.pdf. (n.d.). Retrieved 13 June 2021, from https://dex-bin.bnbstatic.com/static/Whitepaper_%20Binance%20Smart%20Chain.pdf

Capítulo 5

Shiba Inu

Costa, André

Resumo

A criação desta cripto moeda começou com uma simples pergunta: "O que aconteceria se um projeto de cripto moeda fosse cem por cento administrado pela sua comunidade?". Projetos construídos nesta base são a natureza selvagem do nosso futuro, já que, à medida que nos afastamos da mentalidade das estruturas financeiras tradicionais e inflexíveis, tornamo-nos livres para descobri novas maneiras de resolver problemas e nos relacionarmos com os outros. Estes projetos são mais do que uma mudança de ritmo, são uma forma de praticar a aceitação radical dos outros. Quando o sucesso de um projeto depende da força partilhada de todos os indivíduos que o compõem, todos são forçados a mudar as suas perspetivas, por forma a alinharem-se com as pessoas à sua volta. Percebe-se assim que a verdadeira força não vem de uma só pessoa, mas sim de quando várias trabalham juntas e em harmonia. Foi com este pensamento que o Ecossistema Shiba Inu foi desenvolvido, demonstrando assim a importância de demolir este paradigma há muito estabelecido.

Palavras-Chave: comunidade, cripto moeda, Ecossistema, projeto

Abstract

The creation of this cryptocurrency started with a simple question: "What would happen if a cryptocurrency project were one hundred percent managed by your community?" Projects built on this foundation are the wild nature of our future, as as we move away from the mindset of traditional, inflexible financial structures, we become free to discover new ways to solve problems and connect with others. These projects are more than a change of pace, they are a way to practice radical acceptance of others. When the success of a project

depends on the shared strength of all the individuals that comprise it, everyone is forced to change their perspectives, in order to align themselves with the people around them. It can be seen that true strength does not come from just one person, but when several work together in harmony. It was with this in mind that the Shiba Inu Ecosystem was developed, thus demonstrating the importance of demolishing this long-established paradigm.

Keywords: community, cryptocurrency, Ecosystem, project

Shiba Inu

I. INTRODUÇÃO

A *Shiba Inu* (柴犬) (Código: SHIB) é uma cripto moeda descentralizada, criada em agosto de 2020 por um cidadão anónimo conhecido apenas como "*Ryoshi*". O seu nome provém de uma raça de cães japonesa com o mesmo nome.

Ela é baseada noutra cripto moeda, a *Dogecoin*. O objetivo da *Shiba Inu* é ultrapassar a *Dogecoin*, e por isso autodenomina-se "*The Dogecoin Killer*" ("A Assassina do *Dogecoin*").

Esta cripto moeda, também conhecida como *Shiba Token*, é um *token* (moeda) ERC-20 no *blockchain Ethereum*. Não tem qualquer utilidade contratual nem é apoiada por nenhum ativo, é simplesmente um *token* transferível. Estes *tokens* podem ser transacionados nas seguintes plataformas: *ShibaSwap*, *Kucoin*, *CoinBene*, *Probit Global*, *Coin*DCX, *Wazir*X, *Binance*, *Crypto.com*, *Huobi* e OKEx.

II. A HISTÓRIA

O fundador "*Ryoshi*" abordou a criação desta comunidade através de uma perspetiva única: *"Acreditamos que através do poder da descentralização coletiva, podemos construir algo que seja mais forte do que o que uma equipa centralizada jamais possa criar. Um token administrado pela sua comunidade não é nada sem a união dos indivíduos que lhe fornecem o objetivo."*.

Desde os primeiros dias após a sua criação, todos os membros desta comunidade são conhecidos como *Shib Army* (Exército *Shib*), que se tornou mais do que uma expressão, sendo agora utilizado em nomes de utilizador e identificadores de fotos de perfil ou avatares em diferentes plataformas.

Quem quiser tornar-se um novo recruta deste "exército", deverá abraçar os princípios fundamentais desta comunidade:

1. Começámos do zero, e com zero. Esse é o espírito do nosso projeto, criar algo do nada.
2. Não fomos fundados a partir de uma comunidade existente ou uma equipa pré-concebida. As mentes brilhantes por detrás da *Shib* nunca tinham trabalhado juntas anteriormente. Eles eram uma nova equipa de desenvolvedores, designers, moderadores, profissionais de marketing e estimuladores de participação. Quando você se juntou à *Shib Army*, de qualquer ponto do mundo, você encontrou um local onde os seus talentos foram utilizados da melhor forma, e começou a trabalhar.
3. Nós amamos o cães *Shiba Inu*.

Presentemente, a comunidade é constituída por mais de 120 000 membros.

III. O PORQUÊ DA DESCENTRALIZAÇÃO

Até agora, a centralização tem sido um pré-requisito para todas as estruturas oficiais de cripto moeda. Nelas, os sistemas políticos, educacionais e financeiros foram elaborados de forma a que não haja uma distribuição equivalente e ética do poder, para quem com eles opere. Houve momentos na nossa história em que este tipo de modelo desempenhou um papel importante, mas numa época como a de agora, em que as informações do mundo estão disponíveis num simples clique de um botão, tornou-se necessário repensar este modelo.

O ano de 2021 deu-nos um exemplo disso, como foi o caso do *WallStreetBets*, que nos mostrou como seria dispersar o controlo para os consumidores e investidores inexperientes. Contudo, apesar de inovador, este movimento teve pouca margem de progresso, já que foi "estrangulado" pela burocracia da "Sociedade Centralizada" no preciso momento em que parecia estar à beira do sucesso.

Meses antes deste caso ter-se tornado público, o fundador da *Shiba Inu*, "*Ryoshi*" já estava a colocar em prática o seu projeto de criar uma cripto moeda 100% baseada numa comunidade.

As cripto moedas em si, são uma ideia de redefinir o conceito de riqueza e como ela pode ser adquirida, o que vai contra todos os processos tradicionais. Nas palavras do fundador da *Shiba Inu*, *"No cenário económico, sempre em constante mudança, as cripto moedas que não conseguem ser independentes lutam por uma existência ténue."*. "*Ryoshi*" acrescenta que *"Quando as regras do jogo são alteradas em se desfavor, os sistemas não têm outra opção senão aceitar, independentemente das consequências."*.

IV. *BLOCKCHAIN* *ETHEREUM*

Desde o início desta jornada, o fundador "*Ryoshi*" esteve sempre inclinado para utilizar o *blockchain Ethereum*, já que é um serviço seguro e estável, e que proporciona a descentralização pretendida pelo mesmo. Desta forma, todos os membros da comunidade podem ter os seus *tokens* numa "carteira" e recolher os seus pagamentos, de qualquer parte do mundo, sem qualquer interferência ou legislação externa.

"*Ryoshi*" decidiu doar 50% das cripto moedas *Shiba Inu* ao co-fundador do *Ethereum Vitalik Buterin*, porque nas suas palavras *"Não existe nenhuma grandeza sem um ponto vulnerável, e enquanto o Vitalik Buterin não nos deixe vulneráveis, a Shiba irá crescer e sobreviver."*.

As características do *Ethereum* foram a base perfeita para a criação do *ShibaSwap*, uma plataforma de transação de *tokens* totalmente descentralizada, onde se pode negociar, comprar, vender e HODL (guardar para sempre), ganhando assim recompensas que ultrapassam em muito o valor de outras plataformas.

Com o iminente aparecimento do *Ethereum* V.2, que trará transações mais rápidas e baratas, espera-se que a *ShibaSwap* se torne o intercâmbio mais popular e de maior volume.

V. *SHIBASWAP*

Empenhados em construir o melhor Ecossistema Descentralizado no mundo, a *Shiba Inu* foi uma das "sementes" da qual este ecossistema "brotou", e a *ShibaSwap* foi como eles "cavaram as suas raízes".

O objetivo da *ShibaSwap* é fornecer um lugar seguro e descentralizado para a transação das suas cripto moedas. Para tal, uma equipa de desenvolvimento está a trabalhar afincadamente para desenvolver tanto esta plataforma, como o próprio ecossistema, por forma a alcançarem novos patamares de desenvolvimento.

Uma troca descentralizada (DEX) é um mercado ponto a ponto (P2P) que conecta os compradores e os vendedores de cripto moedas. Ao contrário das plataformas centralizadas (CEXs), as plataformas descentralizadas não têm qualquer tipo de custódia, ou seja, o utilizador controla todas as suas chaves privadas aos efetuar transações nestas plataformas.

Os principais *tokens* da *ShibaSwap* são: *Shiba Inu* ($*SHIB*), *Leash Dogecoin Killer* ($*LEASH*) e *Bone* ($*BONE*).

Recorrendo a uma analogia "canina", esta é a forma de funcionamento da *ShibaSwap*:

- Os utilizadores ao adquirirem uma das *tokens*, colocam os seus *Shibs* (*tokens* adquiridos) a escavar (apostar), ou optam por enterrar (guardar) os seus *tokens*.
- Os melhores "treinadores" (utilizadores) ensinam as suas *Shibas* (tokens) a *swap* (troca), que permite trocar um *token* por outro.
- Quando as *Shibas* "escavam", "enterram" ou "trocam", são gerados "retornos" que são distribuídos para as "contas" onde os utilizadores têm os seus *tokens*.

Quando os *tokens* são "enterrados" ficam com a seguinte designação:

Os *ShibaSwap Liquidity Pairs* (Pares de Liquidez da *ShibaSwap*) (SSLP) são:

Serão distribuídas recompensas, de forma proporcional, intituladas de *Bone* (Osso), aos detentores de conjuntos de *tokens* mencionados anteriormente. Enquanto os *tokens* apostados recebem uma percentagem fixa de *Bone*, os SSLP são distribuídos como *Bone Per Block* (Osso por Bloco) (BPB), com base nos pontos alocados de cada "conta de utilizador". Algumas "contas" são "premiadas" para receberem o dobro ou o triplo dos retornos.

VI. *SHIBA INU TOKEN*

Este *token* surgiu em agosto de 2020.

Depois de terem sido cunhados mil biliões de *tokens*, metade foi colocado na *Uniswap* (Protocolo financeiro descentralizado, utilizado para trocar cripto moedas), tendo as chaves privadas desses *tokens* sido apagadas, e a outra metade foi dada para a "carteira" do *Vitalik Buterin*, tendo atingido o primeiro lugar de *token* mais valioso, superando até o valor do próprio *Ethereum*.

Esta cripto moeda foi o marco zero para muitos dos projetos populares de hoje, já que foi a primeira a permitir que um utilizador pudesse ter na sua "carteira" biliões, ou até mesmo triliões,

de *tokens*, para além de ter sido a primeira comunidade em ambiente descentralizado.

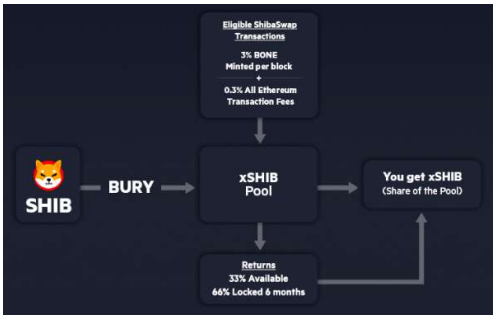
Ganhou o apelido de "*The Dogecoin Killer*" ("A Assassina do *Dogecoin*"), já que os seus membros acreditam que ela tem a capacidade de ultrapassar o valor do *Dogecoin*, de forma exponencial, sem nunca ultrapassar a marca dos $0,01.

A *Shiba Inu* é o primeira cripto moeda a ser listada e incentivada na *ShibaSwap*, imortalizando-a assim na história para sempre.

Em 29 de abril de 2021 estes eram os dados estatísticos da *Shiba Inu*: 124.250 titulares e 2.507.392,4% de valorização.

Um dos incentivos para a aquisição desta cripto moeda são o dobro dos retornos.

O modelo *Bury* (Guardar) deste *token* para devolução de retornos processa-se da seguinte forma:



O modelo *Dig* (Apostar) processa-se da seguinte forma:

VII. *LEASH DOGECOIN KILLER*

O *Leash* é o segundo *token* no ecossistema *Shiba Inu*.

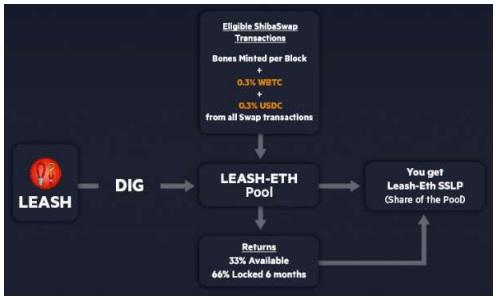
Originalmente, este *token* foi concebido para estabelecer um novo nível base, vinculado ao preço do *Dogecoin*. Mais tarde, foi decidido abandonar essa função, tendo as chaves privadas que permitiam o novo nível base sido apagadas para garantir isso. Desta forma, o *Leash* continuou como um simples token ERC-20.

Ao contrário da *Shiba Inu*, o *Leash* tem apenas 107.647 *tokens* cunhados. O baixo fornecimento de *tokens*, junto com a demanda e recompensa por manter esta cripto moeda, levou a uma ascensão meteórica, semelhante à *Shiba Inu*, podendo apenas ser o início da sua valorização.

Em 29 de abril de 2021 estes eram os dados estatísticos do *Leash*: 5.137 titulares e 6.499.900% de valorização.

O modelo *Bury* (Guardar) deste *token* para devolução de retornos processa-se da seguinte forma:

O modelo *Dig* (Apostar) processa-se da seguinte forma:



VIII. *BONE*

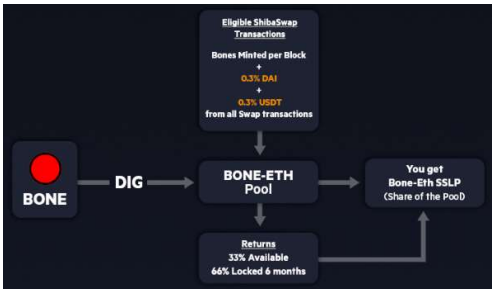
Este *token* está disponível apenas na *ShibaSwap*, tendo sido cunhados 250.000.000 *tokens*.

O *Bone* foi projetado para se encaixar perfeitamente entre os dois *tokens* anteriormente referidos, no que diz respeito ao fornecimento de circulação.

Para além disso, este é um *token* de governação, já que permitirá a quem o possuir votar nas propostas para 2022, bem como quais os *tokens* que serão adicionados à *ShibaSwap*. Desta forma, quantos mais *tokens* um membro tiver, maior o seu peso na votação de decisões futuras.

O modelo *Bury* (Guardar) deste *token* para devolução de retornos processa-se da seguinte forma:

O modelo *Dig* (Apostar) processa-se da seguinte forma:



IX. A LISTA GRRR

Fazer parte da comunidade *Shiba* traz benefícios aos seus membros. Para tal existe este recurso, uma espécie de *Blacklist* (Lista Negra), exclusivo da *ShibaSwap*, que garante que os titulares das transações que queiram aceder aos seus retornos, não tenham que se preocupar com a possibilidade de a transação estar a apostar os seus *tokens*, "congelando" assim a sua retirada.

Esta funcionalidade foi parametrizada, já que se verificaram "congelamentos" suspeitos em plataformas de transações centralizadas.

X. O FUTURO

Para garantir a longevidade da *ShibaSwap* e do ecossistema *Shiba Inu*, 5% de todos os *Bone Per Block* (Osso por Bloco) (BPB) serão alocados numa "carteira de desenvolvimento", ativada com várias assinaturas, que será dividida ao meio da seguinte forma:

- 50% (6.250.000 *Bones*), destinado ao alívio financeiro que os Desenvolvedores, Administradores e a equipa de *Marketing* necessitam para se focarem a tempo inteiro neste ecossistema. Estes 50% serão repartidos da seguinte maneira:
  - Desenvolvedores (4.000.000 *Bones*) – Para compensar cada um dos desenvolvedores pelo seu investimento inicial na *ShibaSwap*, e também para oferecer salários para que possam trabalhar exclusivamente neste ecossistema nos próximos anos;
  - Administradores (1.250.000 *Bones*) – Para que haja um grupo confiável de administradores, implantados em vários canais, para proteger um espaço seguro, onde os fãs da *Shiba* constroem uma comunidade sem qualquer tipo de problemas;
  - *Marketing* (1.000.000 *Bones*) – Até agora, o ecossistema *Shiba Inu* foi bem-sucedido sem ter sido gasto um dólar em *marketing*. Este fundo permitirá que sejam implementadas estratégias internacionais de marketing, que tornarão a cripto moeda *Shiba Inu* um *token* mais valorizado, rivalizando assim com a *Bitcoin* e a *Ethereum*.
- 50% (6.250.000 *Bones*), destinado ao Fundo de Desenvolvimento do Ecossistema *Shiba Inu*, para que os avanços registados se mantenham. Este financiamento também permitirá elaborar planos e estratégias para o restante ano de 2021, e concluir projetos confirmados para 2022 e 2023.

Foi revelado que a próxima cripto moeda deste ecossistema será a *Shiba Treat*, a ser lançada brevemente.

XI. CONCLUSÃO

Pelas palavras do seu fundador "*Ryoshi*" *"A comunidade Shiba começou com a semente de uma ideia: O que poderia acontecer se não houvesse uma equipa centralizada, sem qualquer tipo de financiamento e sem uma liderança direta? Poderia a descentralização realmente funcionar? Poderíamos seguir a tempestade perfeita de cripto moedas como a Bitcoin ou a Dogecoin, mas desta vez com algo totalmente voltado para a comunidade? (...) Este é o início de uma nova era para as comunidades descentralizadas. Quando for a hora certa (porque não devemos apressar as coisas boas), a ShibaSwap será o ponto crucial de contacto entre o mundo descentralizado e as comunidades globais, permitindo-nos atualizar a nossa visão*

de adoção generalizada da cripto moeda financeiramente descentralizada.”.

REFERÊNCIAS

[1] “Ryoshi”. Shiba Inu Ecosystem, Shiba Inu, Versão 1, Abr. 29, 2021. [Online]. Disponível: https://www.shibatoken.com/, Acedido em: Jun. 12, 2021

Capítulo 6

Ripple - XRP

Gonçalves, José

Resumo

Embora existam vários algoritmos de consenso para os Byzantine Generals Problem, especificamente quando diz respeito aos sistemas de pagamento distribuídos, muitos sofrem de alta latência induzida pela exigência que todos os nós dentro da rede comuniquem de forma síncrona. A "confiança" exigida a estas sub-redes é de facto mínima e pode ser ainda mais reduzida com a escolha de princípios dos nós membros. Além disso, é necessária uma conectividade mínima para manter o acordo em toda a rede. O resultado é um algoritmo de consenso de baixa latência que ainda mantém a robustez face às falhas bizantinas. A moeda utilizada pelo Protocolo Ripple é chamada de XRP, esta moeda é muito utilizada em transações bancárias e é geralmente mais rápida que a BitCoin.

Palavras-Chave: criptomoeda, transações, Ripple, XRP, token e BitCoin

Abstract

Although there are several consensus algorithms for the Byzantine Generals Problem, specifically when it comes to distributed payment systems, many suffer from high latency induced by the requirement that all nodes within the network communicate synchronously. The "trust" required of these subnets is in fact minimal and can be further reduced with the choice of principles of the member nodes. In addition, minimal connectivity is required to maintain agreement across the entire network. The result is a low-latency consensus algorithm that still maintains robustness against Byzantine failures. The currency used by the Ripple Protocol is called XRP, this currency is widely used in banking

transactions and is generally faster than BitCoin.

Keywords:criptocurrency, transaction, Ripple, XRP, token e BitCoin

Ripple - XRP

I. INTRODUÇÃO

Este *token* foi escolhido devido a ser uma criptomoeda que é capaz de fazer transações de bancos, onde os próprios bancos aderem a essa própria moeda, algo pouco comum, entre as demais criptomoedas.

Esta moeda XRP funciona através de um Sistema de pagamentos distribuídos, em que permite ao utilizador tranferir valores sem preocupação pelo mundo. Funciona ainda com as redes ponto a ponto e por isso tem os mesmos desafios que as demais moedas digitais, como a prevenção de duplo gasto de fundos e assegurando um consenso pela rede ao estado das contas e dos balanços.

Isto foi primeiramente implementado por Schwartz o algoritmo por detrás do XRP resolve problemas com uso de um protocolo de tolerância e aceitação a falhas Bizantinas. Fazendo isso por colectar sub-redes confiáveis, isto ficou com a nomenclatura de XRP *Ledger Consensus Protocol*. (*Chase e MacBrough - 2018 - Analysis of the XRP Ledger Consensus Protocol.pdf*)

Abstratamente a rede do XRP é replicada em uma máquina. O estado replicado é mantido por cada nó inserido na rede e o estado da transação corresponde às transações por clientes na rede.Se os nós estiverem de acordo a transação será implementada ao estado e a transação processa o protocolo e regras para ordenar cada conjunto. A função do XRP LCP é fazer a rede chegar a um acordo no conjunto de transações feitas. Assim desde que exista aceitação nos nós a transação gera registos constantemente.

Diferente dos algoritmos *proof-of-work* e *proof-of-stake*, XRP LCP tem fornecido menos latência nas transações e maior taxa de transferência aos seus utilizadores. Por isto os utilizadores tem que definir uma lista de nós única, cuja lista será a única que a rede ouvirá em relação ao seu estado.

Foi verificado com diversos operadores de rede, o XRP é seguro e não pode ficar "parado" sem continuar o seu progresso.

II. SURGIMENTO DO XRP

O XRP diferente da maioria das outras criptomoedas é controlada por uma empresa privada a *Ripple Labs*. Antes disso o desenvolvedor de *web* Ryan Fugger desenvolveu em 2004 o *Ripplepay*. Este desenvolvedor conceptualizou esta ideia depois de trabalhar em um sistema de transações em *Vancouver*, a intenção era de criar um sistema monetário descentralizado e permitir com efetividade que individuos e comunidades criassem seu próprio dinheiro. A primeira utilização deste sistema foi o *RipplePay.com*, estreou-se em 2005 como um serviço financeiro fornecendo uma opção de pagamento seguro aos membros através de uma rede global. (Peck, 2013)

Um novo sistema foi conceptionado por Jed McCaleb, projectado e construído por Arthur Britto e David Schwartz. O desenvolvimento foi iniciado de um sistema de moeda digital que as transações seriam verificadas por consenso entre os membros da rede em vez da mineiração que é usada pelo *BitCoin*, dependendo da *Blockchain*. Isto foi

desenvolvido para eliminar depência do *BitCoin* em trocas centralizadas, usando menos electricidade e fazer suas transações bastante mais rápido que o *BitCoin*. (*Ripple*, 2017)

A equipa criou uma empresa *Open Coin*, que começou a desenvolver o protocolo de transação *Ripple* (RTXP). Criando também o seu próprio *Token* XRP, fazendo também com que os bancos pudessem fazer transferências com tempos entre as mesmas muito reduzidos. (Andrews, 2013)

O protocolo *Ripple* anunciou também a ligação com o pioneiro dos *tokens Bitcoin*, fazendo uma ligação entre os dois protocolos permitiu que fosse enviado pagamentos com qualquer moeda para endereço *Bitcoin*. Isto é feito com o uso de uma *Bitcoin Bridge*. (Gilson, 2013)

A empresa mudaria o nome de *Open Coin* para o nome actual *RippleLabs*, a empresa que está por detrás do surgimento do XRP. Com o seu sistema de verificação por consenso que pode ser integrados às redes dos bancos. (Andrews, 2013)

III. FUNCIONAMENTO DO RIPPLE/XRP

A rede *Ripple Technology* é um facilitador de transações, feito para transferir qualquer tipo de bens, em tempo real e sem custos adicionais. Não tem centralização, sendo corrido por vários operadores, com diversos pagamentos feitos em consenso, podendo ser feitos pagamentos entre bancos e moedas virtuais com relativa facilidade.

A diferença para a tecnologia *Blockchain*, para a tecnologia *Ripple* é similar em fazer transações, porém a quantidade de possibilidades do *Blockchain* é mais limitada, enquanto *Ripple* tem maiores possibilidades de transação. Podendo também fazer isso com maior velocidade e maior quantidade de transações, sendo feito somente poucas transações com o *Blockchain*, enquanto muitas transações feitas pela *Ripple* é feita em poucos segundos.(IIF, 2014)

A rede é descentralizada na teoria, porém tem um foco de um centralização quase universal onde os servidores em vez de estarem somente em um local, estariam espalhados um pouco por todo o mundo, pelo menos essa seria a ideia de uma descentralização. Ainda que a empresa por detrás da tecnologia *Ripple* e do *token* XRP ainda tenha controlo sobre a produção de *Tokens* e também sobre a sua valorização ou desvalorização tendo em conta a sua oferta ou procura.

Precisamente por isso a empresa criadora e gestora do XRP tem sofrido com muitas acções legais que foram contra a moeda XRP, que é dito ser controlada pela empresa. Por isso a centralização existe sendo localizadas as linhas de crédito e balanços. Isto que ao contrário do idealizado pelos seus pioneiros seria, uma descentralização e uso de sistemas distribuidos cada individuo ser tratado como um próprio banco, tendo suas dividas, pagamentos e créditos.

Alguns dos problemas iniciais foram sendo solucionados, com a moeda XRP onde foi deixado de somente tratar as pessoas como bancos com dividas, pagamentos ou créditos as pessoas passaram a poder ter uma carteira de *tokens* XRP e podendo enviar essa moeda para pessoas com *Bitcoin* e vice-versa através do já mencionado *Bitcoin Bridge*. Mantendo alguma de sua descentralização a *Ripple* permite tanto a troca de pagamentos dividas, como também as transferências mais normais de uma criptomoeda para outra criptomoeda com o *Bitcoin*.

A principal vantagem de poder ter ambas as hipóteses é que mesmo que não utilize o XRP poderá utilizar a tecnologia *Ripple* para fazer transições através do protocolo onde fica com a dívida que será paga pela pessoa credora. Podendo fazer isso com qualquer criptomoeda, moeda real ou até mesmo bens. Ainda que possa haver o problema da

confiança em relação a essa pessoa. Para isso somente é necessário uma porta de acesso e pessoas que validem por consenso a transação.(Vitalik, 2013)

IV. COMPARAÇÃO COM OUTRA MOEDA

Gráfico 1 - Gráfico Ripple (Valor do Token)

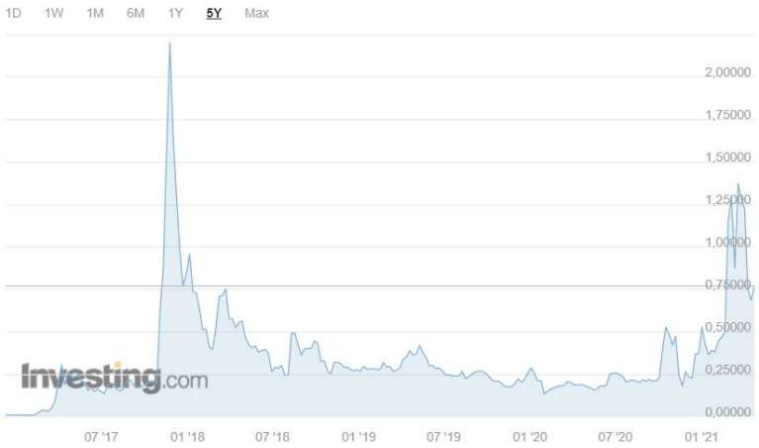
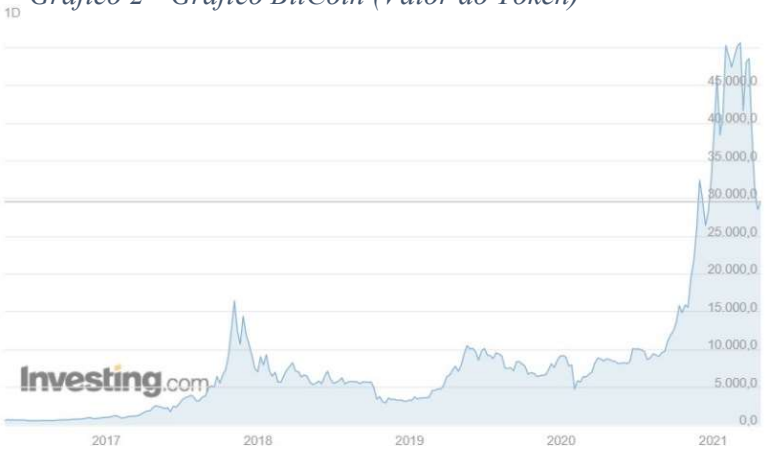


Gráfico 2 - Gráfico BitCoin (Valor do Token)



A nível de comparação podemos notar que as escalas são diferentes sendo a do XRP entre 0 e 2 euros, enquanto a do *BitCoin* poderá ir de 0 a 45 euros, por aí pode-se ver que o preço da *Bitcoin* pode flutuar de alto para baixo de acordo com o mercado. Sendo a XRP com um valor geralmente menor, mas mais constante tendo somente o seu pico de valor no principio do ano 2018 com valorização de maior de 2 euros e actualmente onde andou entre os 0.75 e 1.25 euros aproximadamente.

No caso da *BitCoin* a moeda sempre teve uma valorização alta como a criptomoeda pioneira é também a mais valorizada e com maior história de aumento chegando neste ano a passar os 45 € por *token* e estando actualmente perto dos 30 € por *token*, o que faz dela uma moeda bastante valorizada, mesmo com a ascenção de outras moedas.

A XRP tem um valor de *token* baixo, pois foca-se nas transações com um valor similar ao monetário utilizado no mundo tentando ser uma opção para os sistemas bancários e sendo utilizado por alguns bancos actualmente. A XRP não é minerável o que faz com que não possa ter tanto variação de valores como o *BitCoin* e outras criptomoedas

têm, isso tem a vantagem de alguma estabilidade, mas também aparentemente não tem a possibilidade de haver um grandes acrescimo como no caso do *BitCoin*.

Figure 1 - Dados Gerais Token XRP

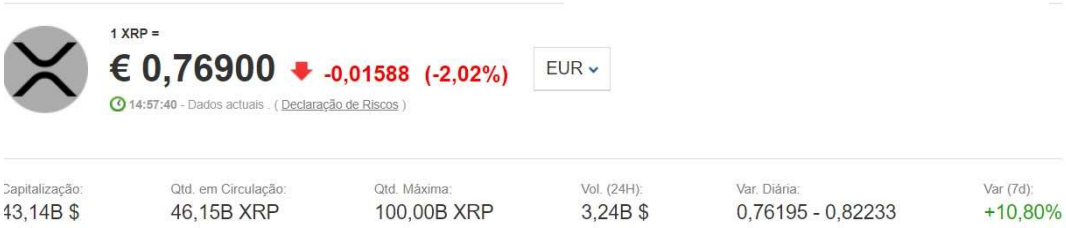
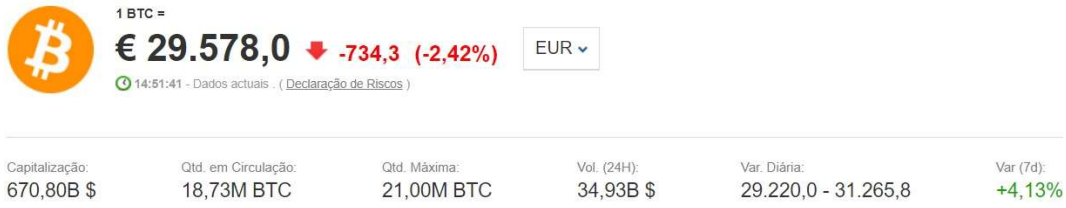


Figure 2 - Dados Gerais Token BitCoin



O token XRP tem uma capitalização muito inferior ao líder de mercado *BitCoin*, tendo o *BitCoin* 670 Bilhões de Euros, enquanto o XRP não chega sequer a 50 Bilhões. Porém a quantidade em circulação em circulação do *token* XRP é maior em quase muito mais o líder do mercado, algo que acontece devido à maior rapidez de transação que é feita pelo uso do protocolo *Ripple*. Sendo de 46 Bilhões, enquanto o *BitCoin* é de somente 18 Milhões.

A nível de uma quantidade máxima de tokens o XRP também tem uma grande vantagem de ter uma quantidade maior, com 100 Bilhões do *token* XRP que poderão ser produzidas, enquanto somente poderá ser feito 21 Milhões de *BitCoins*.

O Volume nas últimas 24 horas (à data de 5/6/2021) foi de 3 Bilhões aproximadamente para o XRP, para o *BitCoin* foi 34, quase 35 Bilhões, o que é praticamente dez vezes mais que o XRP. O *BitCoin* é o líder de mercado das criptomoedas diáriamente, ainda que a nível de percentagem a variação do XRP tenha sido de mais de 10 %, em relação a somente 4 % por parte do *BitCoin*, porém isso representa menos em quantidade, pois o valor por XRP é muito menor que o *BitCoin*.

(*Todas as criptomoedas - Investing.com Portugal*, 2021)

V. CONCLUSÃO – CONSIDERAÇÕES FINAIS

Relativamente ao XRP não é das criptomoedas utilizadas pelas pessoas comuns, pois os ganhos caso aconteçam não poderão ser elevados. Por isso fazendo uma comparação geral uma moeda como o *BitCoin* que é mais variável no valor poderá ter maior retorno em poucos dias, como também um maior prejuízo, sendo uma aposta com o dinheiro do investidor. Estes factores podem ser mitigados com um pouco de conhecimento sobre o mercado actual e também em relação a fatores como o que a empresa *Ripple* pode fazer em relação a desvalorização da moeda, também é algo muito perigoso, ainda que o valor não seja tão variável, quando for em grandes quantidades poderá fazer uma grande diferença.

A vantagem principal do protocolo *Ripple* é mais tida em consideração por parte de empresas do ramo bancário que podem ter grandes vantagens em transacções muito rápidas feitas por esse protocolo mais directo do que o sistema actual em diversos bancos. Funcionando como centralizado através de diversos bancos que já estão a utilizar o protocolo, quantos mais utilizarem o protocolo, mais ele será eficaz em transações de crédito e débito entre esses diversos bancos.

Em uma visão dde investimento, como consideração um pouco conservadora, não seria conselhado o investimento em nenhuma das duas caso tenha falta de experiência ou conhecimento do mercado. Sendo arriscado, mas se estivesse já com algum conhecimento relativo de um maior aumento diário e com alguma investigação sobre o progresso diário nos últimas semanas para perceber o aumento constante ou irregular da criptomoeda.

REFERÊNCIAS

Andrews, E. (2013, Setembro 24). *Chris Larsen: Money Without Borders | Stanford Graduate School of Business*. https://www.gsb.stanford.edu/insights/chris-larsen-money-without-borders

Chase e MacBrough—2018—Analysis of the XRP Ledger Consensus Protocol.pdf. (2018). Obtido 3 de Junho de 2021, de https://ripple.com/files/ripple_consensus_whitepaper.pdf

Gilson, D. (2013, Julho 3). *OpenCoin: Ripple users can send payments to bitcoin addresses*. https://www.coindesk.com/opencoin-ripple-users-can-send-payments-to-bitcoin-addresses

IIF. (2014, Outubro 14). *IIF Technology Showcase: Ripple Labs*. https://www.youtube.com/watch?v=DvBns7XLLxo&ab_channel=IIF

Peck, M. (2013, Janeiro 14). *Ripple Credit System Could Help or Harm Bitcoin—IEEE Spectrum*. https://spectrum.ieee.org/telecom/internet/ripple-credit-system-could-help-or-harm-bitcoin

Ripple, T. (2017, Maio 11). *How We Are Further Decentralizing the XRP Ledger to Bolster Robustness for Enterprise Use | Ripple*. https://ripple.com/insights/how-we-are-further-decentralizing-the-ripple-consensus-ledger-rcl-to-bolster-robustness-for-enterprise-use/

Todas as criptomoedas—*Investing.com Portugal*. (2021, Junho 5). https://pt.investing.com/crypto/currencies

Vitalik, B. (2013, Fevereiro 26). *Introducing Ripple—Bitcoin Magazine: Bitcoin News, Articles, Charts, and Guides*. https://bitcoinmagazine.com/business/introducing-ripple

Capítulo 7

Cardano ADA

Nunes, Ivo

Resumo

Com a descredibilização do setor Bancário diversas pessoas procuram formas alternativas seguras e credíveis de realizar os seus investimentos financeiros. Em 2009 surge a primeira alternativa a Bitcoin com o passar do tempo diversos outros projetos surgem para melhorar e fortalecer os problemas e a dificuldade de escalabilidade da Bitcoin, com isso surgiram diversas outras redes e moedas que visam complementar aquilo que a primeira moeda não conseguiu e uma dessas redes tem o nome de Cardano e a sua moeda ADA a primeira cadeia de blocos ou blockchain que consiste em PoS, com este paper tenho como objetivo principal mostrar um pouco do que consegui captar e preservar na revisão de literatura que efetuei, mostrarei um pouco da sua história, a rede em si qual o propósito da criação e forma de atuar as suas vantagens do ponto de vista interno e externo, a sua posição no mercado e a forma como interpreto a sua posição no mercado atual e até onde penso que pode atingir. Terminarei o paper com as conclusões a que cheguei durante este intenso e agradável estudo.

Palavras-Chave: Bitcoin, Blockchain, Cardano, PoS, ADA

Abstract

With the discrediting of the banking sector, many people are looking for safe and credible alternative ways to make their financial investments. In 2009, Bitcoin was the first alternative to Bitcoin. As time went by, several other projects emerged to improve and strengthen Bitcoin's scalability problems and difficulties. As a result, several other networks and currencies emerged that aimed to complement what the first currency could not. One of these networks is called Cardano and its currency ADA, the first blockchain or blockchain that

consists of PoS, With this paper my main goal is to show a little of what I managed to capture and preserve in the literature review that I performed, I will show a little of its history, the network itself which the purpose of creation and how to act its advantages from the internal and external point of view, its market position and how I interpret its position in the current market and how far I think it can go. I will end the paper with the conclusions I reached during this intense and pleasant study.

Keywords: Bitcoin, Blockchain, Cardano, PoS, ADA

CARDANO - ADA

i. INTRODUÇÃO

Antes de abordar o tema deste trabalho acho que seria importante começar a falar de dinheiro. Dinheiro não são apenas moedas e notas que estão no banco são também coisas que uma pessoa utiliza que possui um valor para outra e que origina uma possível troca, há cerca de quatro mil anos por toda a África e Ásia eram búzios, os mesmos possuem o mesmo valor hoje em dia mas se quisermos efetuar algum tipo de compra com búzios atualmente, será obviamente impossível e isto acontece porque nos dias de hoje ninguém acredita no valor do búzio, nestas primordiais versões do dinheiro usava-se como moeda produtos que possuíam valor intrínseco sejam elas cabeças de gado, peles, sal, cereais, grãos de café ainda hoje em ambientes de privação exterior como as prisões a moeda de troca são cigarros.

Mas utilizar uma mercadoria como moeda de troca tem as suas limitações uma delas é a logística imaginemos que recebíamos o nosso salário em batatas não teríamos forma de transportar o mesmo pelo menos de uma vez só. O segundo problema era geográfico em diferentes partes do globo a valorização do alimento era diferente, os Maias valorizavam muito o sal mas porventura um país que conseguisse sal facilmente talvez não o valorizasse tanto e isso poderia dificultar a troca, no entanto este sistema foi cada vez tornando-se mais credível para as pessoas, fiável e sofisticado e à medida que este sistema se tornou global nasceu a necessidade de trocar as mercadorias por algo mais conveniente e fácil de transportar o maior avanço aconteceu quando as pessoas começaram a depositar a sua confiança em dinheiro que não tinha qualquer valor foi aí que ao avançar dos anos chegámos às notas de cindo euros dos dias de hoje.

Esta fase trouxe uma enorme vantagem que mesmo pessoas que não se conheciam podiam efetuar trocas o que nos leva a afirmar que o dinheiro é um sistema de confiança mútua só tem valor porque acreditamos no mesmo como diria Buddha *"Money is the worst discovery of human life. But it is the most trusted material to test human nature."*.

O sistema monetário tornou-se então o sistema mais credível a nível global para comprar e vender e é originário da Banca em todos os países seja qual for a moeda existe uma autoridade central que garante que temos dinheiro na conta e confirma que a transação é válida a grande vantagem de existir esta autoridade central é que esta é incumbida de garantir que estamos a realizar negócio com uma pessoa séria, mas nem tudo é ouro sob azul esta mediação realizada pelos Bancos origina enormes taxas que inviabilizam muitas vezes o negócio por exemplo em muitos comércios locais que pretendemos utilizar o cartão multibanco para efetuarmos compras de valor menor que cinco euros não nos é permitido pelo comerciante, pois a taxa inviabiliza o lucro do comerciante.

Uma das grandes desvantagens deste sistema é a privacidade a Banca tem acesso a toda informação de compras vendas e demais que eu realizar, esta foi uma das razões pelas quais *Satoshi Nakamoto* que ninguém sabe se é um grupo de pessoas ou uma pessoa singular em 2009 lançou a Bitcoin segundo o(s) próprio(s) tem como objetivo substituir a confiança do dinheiro por criptografia, utilizando um sistema eletrónico descentralizado ou seja é um treinador que acredita no onze titular, independente do banco, governos e politiquices.

Mas o Banco não tem só coisas más uma das suas grandes vantagens é poder garantir que uma pessoa não gasta os mesmos cinco euros duas vezes, e para igualar essa vantagem da banca *Satoshi Nakamoto* teve de criar uma rede e essa rede é chamada Blockchain e a ideia utilizada foi para uma pessoa enviar *Bitcoin* da pessoa A para a pessoa B cada pessoa terá uma chave pública e outra privada a pública como o próprio nome indica é visível por todos e a privada funciona como uma password que deve ser mantida em sigilo e esta assinatura digital é alterada a cada transação então mas sem um banco como controlamos isto sem erros, a ideia destas moedas digitais é substituir esta confiança por poder computacional ao invés de confiarmos na pessoa do banco confiamos nos computadores que estão na rede ou seja a pessoa A e B estão a efetuar a transação e a rede (computadores C,D,E,F..) estão a competir entre si para decifrar esta transação organizá-la num bloco de informação encriptado e enviá-la para todos os integrantes da rede, quanto mais potente for o computador maior é a probabilidade de decifrar essa equação/transação estas cadeias de blocos são guardados de forma cronológica na rede.

O valor das criptomoedas depende logicamente da oferta, procura e do numero de competidores mas sobretudo de vários outros fatores exógenos difíceis de calcular que influenciam a sua performance ao longo do tempo é por isso que é um ativo de alto risco.

ii. CARDANO

Cardano é uma plataforma pública de código aberto ou "*opensource*" que se orgulha da sua própria moeda criptográfica chamada ADA. Um dia, a rede também suportará contratos inteligentes também conhecidos como "*smart contracts*", que são contratos que executam automaticamente os seus próprios termos ou acordos. Este último tema abordado sobre a rede Cardano ainda se encontra em fase de construção, pelo que ainda não está amplamente disponível para utilização. No entanto, Cardano orgulha-se de ter algumas mentes muito brilhantes a trabalhar no seu sistema, com cientistas de universidades como a Universidade de Edimburgo e o Instituto de Tecnologia de Tóquio a ajudar.

O livro de valores da conta de Cardano é a Camada de Liquidação de Cardano. Esta é a parte da plataforma da cadeia de bloqueio que hospeda a ADA. O seu objetivo é melhorar algumas das questões de escala que existem com Bitcoin, Ethereum e outras moedas criptográficas de primeira e segunda geração. É também emparelhado separadamente com a Camada de Computação Cardano, que permite aos utilizadores personalizarem as regras das suas transações individualmente.

Pelas palavras de um dos seus criadores Chales Hoskinson *"Cardano is an open platform that seeks to provide economic identity to the billions who lack it by providing decentralized applications to manage identity, value and governance"*.

iii. HISTÓRIA

Durante a década de 2010, a primeira década da moeda criptográfica, foi largamente dominada pelo Bitcoin e pelo Ethereum. O Bitcoin foi pioneiro no espaço criptográfico desde o início como o ativo original baseado na cadeia de bloqueio ou blockchain, enquanto o Ethereum redefiniu os parâmetros do que é possível, introduzindo contratos inteligentes e acolhendo milhares de novos protocolos ERC20 que continuam a fazer avançar a indústria até aos dias de hoje.

Devido ao domínio e quota de mercado do Ethereum, a maioria dos programadores optaram por trabalhar na sua rede, com o objetivo de melhorar projetos anteriores ou construir novos campos excitantes como o DeFi que é a variedade de aplicações e projetos no espaço público da blockchain orientado para perturbar o mundo financeiro tradicional, em cima da robusta infraestrutura do Ethereum. Contudo, existem alternativas ambiciosas disponíveis, tais como Cardano (ADA).

Cardano (ADA) pode ser considerada uma iniciativa global da blockchain, dado que é a primeira que é proof of stake, conceito que declara que uma pessoa pode extrair ou validar transações em bloco de acordo com o número de moedas que possui foi desenvolvida academicamente por um grupo de peritos na matéria. A equipa Cardano é composta por engenheiros, académicos e um cofundador do Ethereum Charles Hoskinson sendo o mesmo e Jeremy Wood as principais figuras da moeda e da rede. O grupo eclético escolheu fazer algo diferente em 2015 e construir uma cadeia de bloqueio nativa a partir do zero.

Juntos, estão extremamente focados para assegurar que Cardano cumpre o propósito para o qual foi criado: gerir uma plataforma digital livre de intermediários financeiros, uma que seja mais inclusiva e sustentável do que outras plataformas da cadeia de blocos.

A plataforma recebeu o nome do polimaturgo e matemático italiano Gerolamo Cardano. Fascinantemente, o seu ativo nativo ADA tem o nome da influente matemática britânica Ada King, Condessa de Lovelace e a única filha do famoso poeta Lord Byron.

Ada Lovelace foi uma brilhante matemática, escritora e é agora reconhecida como um dos primeiros programadores informáticos de sempre. Lovelace reconheceu o potencial matemático dos computadores no início e publicou o primeiro algoritmo em 1843 que uma máquina deste tipo poderia realizar. Diz-se que sem o trabalho de Lovelace, os computadores como os conhecemos hoje não existiriam.

iv. PROPÓSITO E FORMA DE ATUAR

Cardano é uma plataforma construída para um futuro sustentável, para ajudar as pessoas a trabalhar melhor em conjunto, confiar umas nas outras, e construir soluções globais para problemas globais.

Cardano é um garfo na estrada. Leva-nos de onde estivemos até onde estamos destinados: uma sociedade global segura, transparente e justa, e que serve tanto a muitos como a poucos. Tal como as revoluções tecnológicas anteriores, oferece um novo modelo de como trabalhamos, interagimos, e criamos, como indivíduos, empresas e sociedades.

Cardano começou com uma visão de um mundo sem intermediários, em que o poder não é controlado por uns poucos responsáveis, mas sim por muitos com poder. Neste mundo, os indivíduos têm controlo sobre os seus dados e sobre a forma como interagem e transacionam. As empresas têm a oportunidade de crescer independentemente das estruturas de poder monopolistas e burocráticas. As sociedades são capazes de perseguir a verdadeira democracia: autogovernada, justa e responsável. Trata-se de um mundo tornado possível por Cardano.

A primeira geração de cadeias de bloqueio (como a Bitcoin) oferecia livros de contabilidade descentralizados para a transferência segura de moedas criptográficas. Contudo, tais cadeias de bloqueio não proporcionavam um ambiente funcional para a liquidação de transações complexas e o desenvolvimento de aplicações descentralizadas. À medida que a tecnologia das cadeias de bloqueio amadurecia, a segunda geração (como o Ethereum) proporcionava soluções mais aperfeiçoadas para a escrita e execução de contratos inteligentes, desenvolvimento de aplicações, e a criação de diferentes tipos de fichas. Por outro lado, a segunda geração de cadeias de bloqueios enfrenta frequentemente problemas em termos de escalabilidade.

Cardano é concebido como a terceira geração de cadeias de bloqueio, uma vez que combina as propriedades das gerações anteriores e evolui para satisfazer todas as necessidades emergentes dos utilizadores. Ao comparar as propriedades da cadeia de bloqueio, muitos aspetos devem ser considerados. Assim, a melhor solução deve garantir a mais alta segurança, escalabilidade (rendimento das transações, escala de dados, largura de banda da rede), e funcionalidade (para além do processamento das transações, a cadeia de bloqueios deve fornecer todos os meios para a liquidação de transações comerciais). Além disso, é importante assegurar que a tecnologia da cadeia de bloqueio esteja em constante desenvolvimento em termos de sustentabilidade e seja interoperável com outras cadeias de bloqueio e instituições financeiras.

Para responder a estas necessidades, Cardano concentra-se em conceitos centrais como:

Escalabilidade - assegura que o livro razão Cardano seja capaz de processar um grande número de transações sem afetar o desempenho da rede. A escalabilidade também proporciona capacidades de maior largura de banda para permitir que as transações transportem uma quantidade significativa de dados de apoio que podem ser facilmente geridos dentro da rede. Para estas necessidades, Cardano está a implementar várias técnicas (como a compressão de dados, por exemplo) e está a trabalhar para introduzir Hydra, que permitirá a funcionalidade de cadeias laterais múltiplas.

Interoperabilidade - assegura o ambiente mais multifuncional para operações financeiras, comerciais ou comerciais, permitindo aos utilizadores interagir não só com um tipo de moeda, mas com múltiplas moedas através de várias cadeias de blocos. Além disso, a interoperabilidade com entidades bancárias centralizadas é tão importante para conceder legitimidade e conveniência de utilização. Cardano está a ser desenvolvido para apoiar transferências entre cadeias, tipos de fichas múltiplas, e línguas de contratos inteligentes comummente utilizadas.

Sustentabilidade - conceber uma cadeia de bloqueios de prova de aceitação significa que é vital assegurar que o sistema é autossustentável. Para impulsionar o crescimento e maturidade de uma forma verdadeiramente descentralizada, Cardano é construído para permitir à comunidade manter o seu desenvolvimento contínuo, participando, propondo, e implementando melhorias do sistema. Para assegurar a sustentabilidade, o sistema de tesouraria é controlado pela comunidade e é constantemente recarregado a partir de potenciais fontes, tais como moedas recentemente cunhadas a serem retidas como financiamento, uma percentagem das recompensas do pool de participações, e taxas de transação.

v. VANTAGENS

Abordarei neste capítulo sobre as vantagens mais sonantes desta rede e moeda face às restantes no mercado:

Investigação académica - métodos formais, tais como especificações matemáticas, testes baseados em propriedades, e provas, são a melhor forma de fornecer sistemas de software de alta garantia e dar confiança aos utilizadores para a gestão de fundos digitais. Cardano foi construído utilizando métodos formais para obter fortes garantias sobre a correção funcional dos componentes nucleares do sistema. Todas as pesquisas e especificações técnicas que sustentam Cardano estão disponíveis ao público, e toda a atividade de desenvolvimento de Cardano é publicada online.

Conceção do sistema - Cardano é escrito em Haskell, uma linguagem de programação funcional segura que encoraja a construção de um sistema utilizando funções puras, o que leva a uma conceção onde os componentes são convenientemente testados isoladamente. Além disso, as características avançadas de Haskell permitem-nos empregar toda uma gama de métodos poderosos para assegurar a correção do código, tais como basear a implementação em especificações formais e executáveis, testes extensivos baseados em propriedades, e testes em execução em simulação.

Segurança - Oroboros (o protocolo Cardano proof-of-stake) estabelece garantias rigorosas de segurança; foi entregue com vários artigos revistos por pares apresentados em conferências e publicações de topo na área da ciber-segurança e criptografia.

Consumo de energia - Cardano é uma cadeia de prova de consumo de energia. Em contraste com as correntes de bloqueio de prova de trabalho, Cardano requer muito menos energia e potência computacional. A rede Bitcoin cresce através de computadores que fazem cálculos cada vez mais intensivos em energia - prova de trabalho - o que é insustentável a longo prazo. A Universidade de Cambridge tem uma ferramenta online que mostra que os computadores que alimentam o Bitcoin já consomem duas vezes mais energia do que a Suíça todos os anos.

Actualizações contínuas - tradicionalmente, as cadeias de blocos são actualizadas utilizando garfos duros. Ao conduzir um garfo duro, o protocolo actual deixaria de funcionar, novas regras e mudanças seriam implementadas, e a cadeia seria reiniciada - com a sua história anterior a ser apagada. Cardano trata os garfos rígidos de forma diferente. Em vez de implementar mudanças radicais, a tecnologia do combinador de forquilhas Cardano assegura uma transição suave para um novo protocolo, ao mesmo tempo que guarda o histórico dos blocos anteriores e não causa quaisquer perturbações para os utilizadores finais.

Descentralização - O Cardano é mantido por mais de 2.000 conjuntos de estacas distribuídas operados pela comunidade. Todos os blocos e transações são validados pelos participantes da rede sem qualquer dependência de uma autoridade centralizada.

Ambiente funcional para casos de utilização empresarial - Cardano está a estabelecer uma base para finanças globais descentralizadas para desenvolver uma gama de DApps que podem funcionar utilizando contratos inteligentes funcionais e específicos do domínio, fornecendo fichas multi-ativos para quaisquer necessidades. Com um livro razão multi-ativos já disponível, a Cardano está a trazer apoio a contratos inteligentes em 2021.

vi. ADA VS WORLD

Cardano não se encontra classificado em 4º devido apenas à sua acessibilidade económica. Tem várias outras características essenciais que o colocaram muito à frente de outros. Uma destas várias outras características é que é uma das primeiras moedas a ter usado com sucesso a prova do mecanismo de aposta o tão famoso Proof of Stake. A energia consumida pelo PoS é menor em comparação com a energia consumida pelo mecanismo de PoW. Mesmo antes da atualização do PoS na cadeia de bloqueio do Ethereum, a ADA tem funcionado numa rede de PoS em pleno.

Outro benefício que a rede Cardano tem em relação a outras é que toda a tecnologia desenvolvida está sujeita a uma investigação concentrada de revisão pelos integrantes. Cada transação realizada na cadeia de bloqueio pode ser contestada mesmo antes de ser executada. Este nível de avanço deu à cadeia de

bloqueio Cardano estabilidade e resiliência, assegurando que os problemas são notados e corrigidos antes de se tornarem um revés.

Com 57% do fornecimento total de ADA foi inicialmente distribuído num ICO (Initial Coin Offerings) onde a rede Cardano angariou 62 milhões de dólares. Ao contrário de outras moedas, ADA é utilizado para fazer transações na cadeia de bloqueio Cardano e como uma moeda digital. Da mesma forma que é necessário ETH para fazer transações na cadeia de bloqueio Ethereum, o ADA é utilizado na rede Cardano. Face à minha experiência em pequenos investimentos diria que a Cardano para ganho de capital é uma opção bastante interessante. Em vez de comparar o Cardano com outras moedas criptográficas, deve compreender como funciona a rede para facilitar a maximização da utilização.

Quando comparado com Bitcoin ou Ethereum, o Cardano pode não valer a pena, especialmente quando o preço é usado como medida de comparação. Contudo, é de notar que a Cardano é atualmente a melhor opção quando se trata de custos transacionais, PoS e rapidez. A primeira e segunda geração de criptomoedas não estão à altura deste símbolo, uma vez que utilizou as suas limitações e usou isso como base para a sua atualização. Graças a Charles, o criador das redes Cardano.

Cardano é uma das moedas mais seguras para investir, o preço da moeda Bitcoin pode ser demasiado elevado ou demasiado caro, e as taxas de transação Ethereum são assustadoras mesmo após os esforços recentes de Vitalik Buterin.

Penso que o interessante na rede Cardano é a forma altruísta como Charles Hoskinson fala sobre a mesma *"If you see me trying to boost the price of Ada, then I've been compromised and sell all your Ada. Cardano will be valuable based upon hard work, real world use and the utility of the platform. I'm not here to make day traders rich. I'm here to change the world"* aconselho também a visualização deste vídeo do IOHK com o tema Cardano whiteboard; overview with Charles Hoskinson pois possui informação extremamente interessante na comparação entre Cardano e as outras redes e moedas.

vii. MERCADO E INVESTIMENTOS

A moeda criptográfica Cardano (CCC:ADA) tem registado um aumento de preço ultimamente e as previsões dos especialistas em alta têm-no feito subir ainda mais.

O impressionante rally do preço de Cardano vem depois de uma atualização significativa da sua cadeia de bloqueio. A atualização Goguen 'Mary' permite aos utilizadores criar fichas personalizadas na cadeia que são 'nativas' da rede, tornando a ADA uma cadeia de bloqueios multi-ativos.

O chamado "Ethereum killer" tem estado em chamas ao longo de 2020. O preço Cardano viu pela primeira vez um aumento de 600% no seu valor de mercado entre Março e Julho de 2020. Depois a ficha subiu mais 130% com o fim do ano.

Só em 2021, o valor de mercado da ADA aumentou em 300%. Com a equipa de engenheiros da IOHK

FIGURA VII-1

FIGURA VII-1

Como pequeno investidor de algumas moedas e acreditando no projeto Cardano fico extremamente contente por ele começar a ganhar alguma força, neste momento estou a realizar stacking de 100 moedas Cardano como podem ver na figura VII-3 com juros a sete dias que rondam entre os 7 e 17% e assim vou continuar pois acredito no projeto a longo prazo irá ser extremamente rentável e penso ser inevitável a

substituição do modelo financeiro atual para algo similar ao implementado nas cripto moedas.

Moeda	Quantia total	7-Day APY	Data de inscrição	Período de Bloqueio (Dias)	Data Final dos Juros	Dias de Acumulação	Juros acumulado
ADA	25.07816338	17.79%	2021-06-08	15 Dias	2021-06-24	5 Dias	0.06111545
ADA	20.86947611	7.79%	2021-05-19	60 Dias	2021-07-19	25 Dias	0.11134900
ADA	16.33272133	7.79%	2021-05-17	60 Dias	2021-07-17	27 Dias	0.09411452
ADA	39.50046000	7.79%	2021-05-09	60 Dias	2021-07-09	35 Dias	0.29505646

FIGURA VII-3

Acredito solenemente que com a introdução dos contratos inteligentes em Agosto do presente ano a moeda atingirá números nunca antes vistos.

viii. CONCLUSÃO

Num mundo onde a desconfiança no sistema financeiro tradicional cresce dia após dia conheci um projeto que poderá revolucionar o mundo.

Cardano é um projeto inovador e único que visa fornecer uma nova forma de infraestrutura de blockchain que combina as vantagens de muitos conceitos matemáticos e tecnológicos de ponta. Este projeto de blockchain de terceira geração tem potencial para se tornar uma plataforma de contrato inteligente líder do setor, mas ainda há muito desenvolvimento a ser feito. Para um projeto verdadeiramente ambicioso, só o tempo provará o impacto duradouro de Cardano no mundo da criptografia e no mundo inteiro, mas o futuro é certamente brilhante.

REFERÊNCIAS

ADA USD Binance Análise Técnica—Investing.com. (sem data). Investing.com Brasil. Obtido 8 de Junho de 2021, de https://br.investing.com/crypto/cardano/ada-usd-technical

Barroso, R. (sem data). *O outro lado da corrida ao «ouro digital»*. 6.

Blockchain 101. (sem data). CoinDesk. Obtido 8 de Junho de 2021, de https://www.coindesk.com/learn/blockchain-101/what-is-blockchain-technology

Cardano. (sem data). TradingView. Obtido 9 de Junho de 2021, de https://br.tradingview.com/ideas/cardano/

Cryptocurrency Prices, Charts And Market Capitalizations. (sem data). CoinMarketCap. Obtido 10 de Junho de 2021, de https://coinmarketcap.com/

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. Em J. Katz & H. Shacham (Eds.), *Advances in Cryptology – CRYPTO 2017* (Vol. 10401, pp. 357–388). Springer International Publishing. https://doi.org/10.1007/978-3-319-63688-7_12

Kiyosaki, R. T., & Lechter, S. L. (2011). *Rich dad, poor dad: What rich teach their kids about money - that the poor and middle class do not*. Plata Pub.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (sem data). *Bitcoin and Cryptocurrency Technologies*. 308.

Salman, A., & Razzaq, M. G. A. (2018). Bitcoin and the World of Digital Currencies. Em G. Kucukkocaoglu & S. Gokten (Eds.), *Financial Management from an Emerging Market Perspective*. InTech. https://doi.org/10.5772/intechopen.71294

technology, F. B. F. L. R. S. is a writer with 8+ years of experience about the intersection between, investing, business R. is an expert in, business, blockchain, & Sharma, cryptocurrencies L. about our editorial policies R. (sem data). *Cardano Aims to Create a Stable Cryptocurrency Ecosystem*. Investopedia. Obtido 11 de Junho de 2021, de https://www.investopedia.com/news/introduction-cardano/

What is Cardano (ADA)? Here's what you should know about this crypto. (2018, Junho 17). EToro. https://www.etoro.com/news-and-analysis/trading/what-is-cardano-ada-heres-what-you-should-know-about-this-crypto/