# DO BITCOIN ÀS CBDCS

*João Pedro Alonso*

# Overview

- *Contexto Histórico: 2008 e crise financeira*
- *Origem do Bitcoin*
- *Por que Blockchain é importante?*
- *Origem do Ethereum*
- *Ethereum, DeFi e novas possibilidades*
- *DeFi*
- *Dinheiro Digital e novos paradigmas*
- *E o Governo?*
- *Blockchains Centralizadas*
- *CBDCs*
- *DREX e o cenário atual no Brasil*

# Contexto Histórico
# Crise de 2008

- Não é coincidência que o Whitepaper do Bitcoin surgiu em meados de 2008, em meio a uma das maiores crises financeiras dos EUA;
- O povo havia perdido a confiança no governo e nos Bancos para gerenciar seu dinheiro, e isso abriu espaço para novas alternativas e quebras de paradigmas.

# 31 de Outubro de 2008

# NASCE O BITCOIN

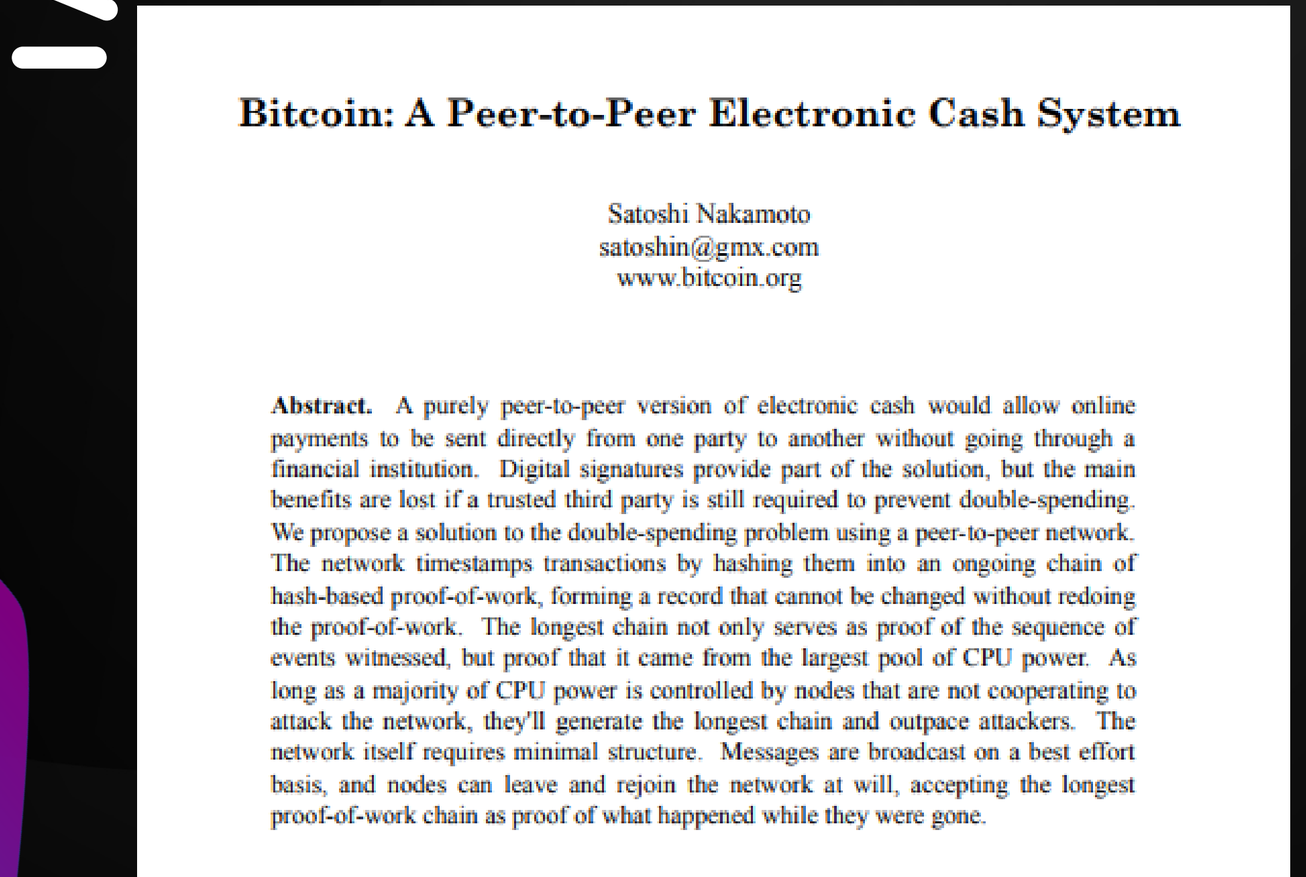
## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

# 31 de Outubro de 2008

# NASCE O BITCOIN



**Bitcoin: A Peer-to-Peer Electronic Cash System**

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

**Curiosidade: a tecnologia blockchain (inaugurada com o bitcoin) não traz praticamente nenhuma tecnologia nova! Apenas combinou diferentes primitivas de criptografia de um jeito genial nunca antes visto!**

# Mas o que tem de especial nesse tal Bitcoin?

# Mas o que tem de especial nesse tal Bitcoin?

## “Permissionless”

Não é necessário pedir autorização para nenhuma autoridade para criar uma carteira digital e começar a fazer transações na rede; conexões peer-to-peer conectam usuários diretamente sem necessitar de bancos ou outras instituições financeiras;

# Mas o que tem de especial nesse tal Bitcoin?

## “Permissionless”

Não é necessário pedir autorização para nenhuma autoridade para criar uma carteira digital e começar a fazer transações na rede; conexões peer-to-peer conectam usuários diretamente sem necessitar de bancos ou outras instituições financeiras;

## Resistente a Censura

É praticamente impossível bloquear, alterar, ou reverter transações na rede, devido à estrutura da blockchain;

# Mas o que tem de especial nesse tal Bitcoin?

## “Permissionless”

Não é necessário pedir autorização para nenhuma autoridade para criar uma carteira digital e começar a fazer transações na rede; conexões peer-to-peer conectam usuários diretamente sem necessitar de bancos ou outras instituições financeiras;

## Resistente a Censura

É praticamente impossível bloquear, alterar, ou reverter transações na rede, devido à estrutura da blockchain;

## Descentralizado

A rede é mantida por milhares de computadores ao redor do mundo e nenhum deles tem controle central sobre a rede;

# Mas o que tem de especial nesse tal Bitcoin?

## “Permissionless”

Não é necessário pedir autorização para nenhuma autoridade para criar uma carteira digital e começar a fazer transações na rede; conexões peer-to-peer conectam usuários diretamente sem necessitar de bancos ou outras instituições financeiras;

## Resistente a Censura

É praticamente impossível bloquear, alterar, ou reverter transações na rede, devido à estrutura da blockchain;

## Descentralizado

A rede é mantida por milhares de computadores ao redor do mundo e nenhum deles tem controle central sobre a rede;

## Oferta limitada

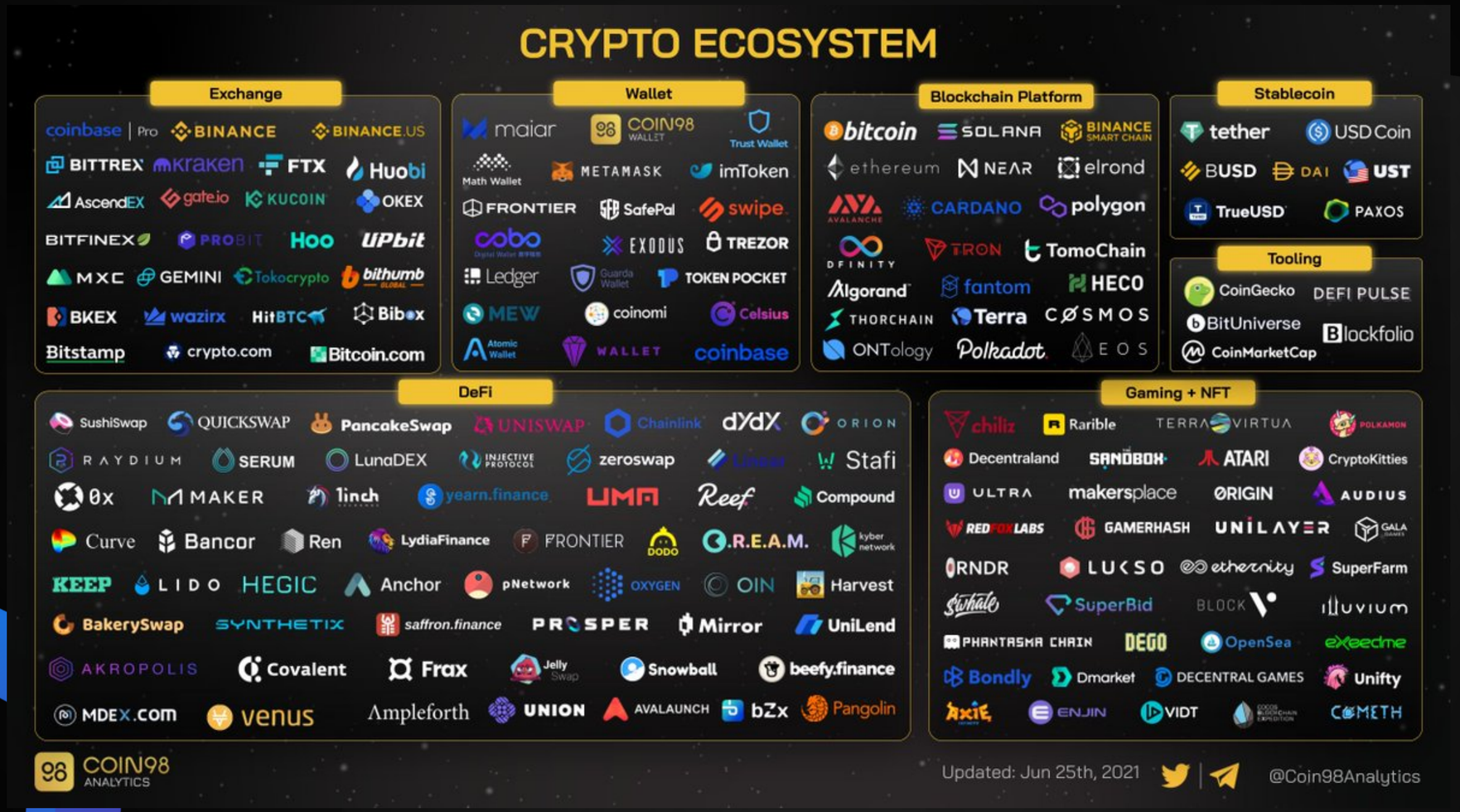
A quantidade de bitcoins que pode ser minerada é limitada em 21 milhões, algo definido algoritmicamente no protocolo do Bitcoin - impedindo um cenário de inflação desenfreada decorrido de políticas de governo irresponsáveis;

# Ok, mas e depois?

**Esse conjunto único de atributos foi algo revolucionário para a época, mas apesar da tremenda inovação que trouxe, o Bitcoin foi apenas o primeiro passo de algo muito maior!**

# Ok, mas e depois?

**Esse conjunto único de atributos foi algo revolucionário para a época, mas apesar da tremenda inovação que trouxe, o Bitcoin foi apenas o primeiro passo de algo muito maior!**



# Ok, voltando um pouco

Beleza, a rede do bitcoin tem todos aqueles atributos super bacanas (decentralização, resistência à censura, “permissionless”, etc), mas ela, por fatores de implementação e objetivo dos criadores, se limita apenas a ser uma rede cujo único objetivo é manter um registro de transações.

# Ok, voltando um pouco

Beleza, a rede do bitcoin tem todos aqueles atributos super bacanas (decentralização, resistência à censura, “permissionless”, etc), mas ela, por fatores de implementação e objetivo dos criadores, se limita apenas a ser uma rede cujo único objetivo é manter um registro de transações.

Porém algumas pessoas começaram a perceber que a estrutura da blockchain poderia ser utilizada para outras aplicações!!! Pois é apenas um banco de dados distribuído, mantido por uma rede de computadores que seguem algumas regras específicas!

Eis que um dia alguém se perguntou:

Eis que um dia alguém se perguntou:

E se eu pegasse essa mesma estrutura da blockchain, que nada mais é que um banco de dados descentralizado mantido por vários computadores, e usasse essa mesma rede para rodar uma máquina virtual global descentralizada em cima da blockchain??

Eis que um dia alguém se perguntou:

E se eu pegasse essa mesma estrutura da blockchain, que nada mais é que um banco de dados descentralizado mantido por vários computadores, e usasse essa mesma rede para rodar uma máquina virtual global descentralizada em cima da blockchain??

# Pare pra pensar um pouco sobre isso...

# Pare pra pensar um pouco sobre isso...

**Uma máquina virtual decentralizada mantida por milhares de computadores, cuja estrutura de armazenamento de dados é uma blockchain.**

# Pare pra pensar um pouco sobre isso...

**Uma máquina virtual decentralizada mantida por milhares de computadores, cuja estrutura de armazenamento de dados é uma blockchain.**

**Ou seja:**

Além de apenas transacionar criptomoedas, pessoas poderiam fazer upload de programas de computador nessa  super máquina virtual, e outras pessoas poderiam rodar esses programas

# Pare pra pensar um pouco sobre isso...

## Uma máquina virtual decentralizada mantida por milhares de computadores, cuja estrutura de armazenamento de dados é uma blockchain.

### Ou seja:

Além de apenas transacionar criptomoedas, pessoas poderiam fazer upload de programas de computador nessa  super máquina virtual, e outras pessoas poderiam rodar esses programas

Essa nova camada de Máquina Virtual permitiria automação de transações através de funções autoexecutáveis;

# Pare pra pensar um pouco sobre isso...

## Uma máquina virtual decentralizada mantida por milhares de computadores, cuja estrutura de armazenamento de dados é uma blockchain.

### Ou seja:

Além de apenas transacionar criptomoedas, pessoas poderiam fazer upload de programas de computador nessa  super máquina virtual, e outras pessoas poderiam rodar esses programas

Essa nova camada de Máquina Virtual permitiria automação de transações através de funções autoexecutáveis;

Tudo isso seria feito em ambiente descentralizado e imutável, então uma vez que um código de computador fosse registrado na rede blockchain, aquele código não poderia sofrer alterações maliciosas no futuro

# Extremamente útil, não é?

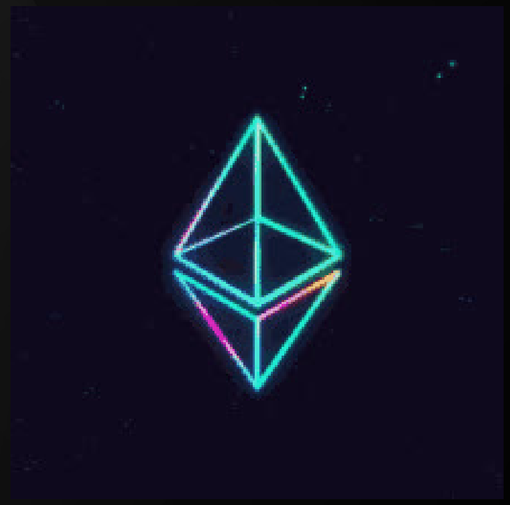
# Extremamente útil, não é?

O bom é que essa ideia já foi implementada! E é um dos projetos mais bem sucedidos do mundo crypto!

# Extremamente útil, não é?

O bom é que essa ideia já foi implementada! E é um dos projetos mais bem sucedidos do mundo crypto!

A primeira rede a implementar essa ideia foi a **Ethereum**! Hoje sua moeda nativa, o Ether (ETH), possui o segundo maior Market Cap dentre as criptomoedas atuais, somente atrás do Bitcoin!



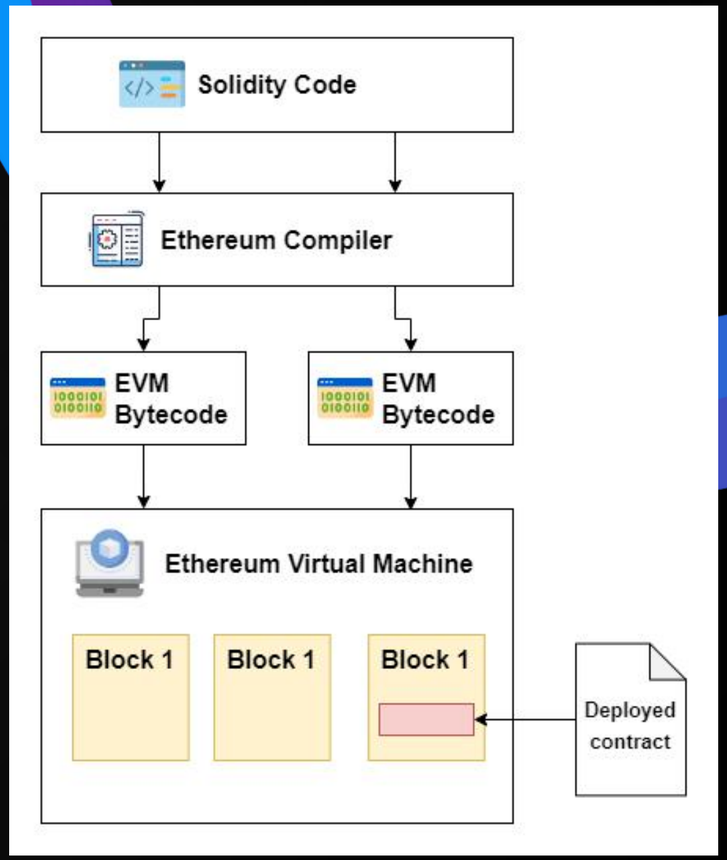
# Ethereum e novas possibilidades

A **Ethereum Virtual Machine** (EVM) é essa máquina virtual que roda “em cima” da rede blockchain do Ethereum;

# Ethereum e novas possibilidades

A **Ethereum Virtual Machine** (EVM) é essa máquina virtual que roda “em cima” da rede blockchain do Ethereum;

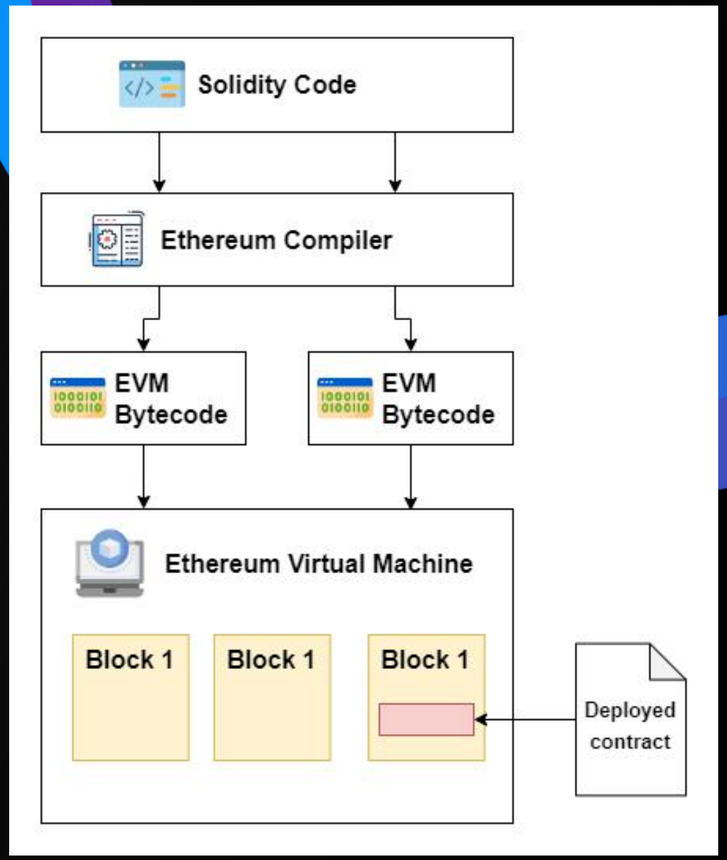
Códigos de computador armazenados na rede Ethereum são chamados de **Smart Contracts**, que são códigos autoexecutáveis que garantem que acordos firmados sejam cumpridos;



# Ethereum e novas possibilidades

A **Ethereum Virtual Machine** (EVM) é essa máquina virtual que roda “em cima” da rede blockchain do Ethereum;

Códigos de computador armazenados na rede Ethereum são chamados de **Smart Contracts**, que são códigos autoexecutáveis que garantem que acordos firmados sejam cumpridos;




- Exemplo -

**Venda de um NFT somente quando as duas partes submeterem seus ativos para realizar a troca automática**

# E o que DeFi tem a ver com isso?

Decentralized Finance (DeFi) é toda a classe de serviços financeiros baseados em Smart Contracts na Blockchain;

# E o que DeFi tem a ver com isso?

Decentralized Finance (DeFi) é toda a classe de serviços financeiros baseados em Smart Contracts na Blockchain;

---

Agora, transações em redes Blockchain não se limitam a apenas envio e recebimento de criptomoedas. Com DeFi, é possível:

Realizar e receber empréstimos;

Receber juros de empréstimos feitos;

Trocar criptomoedas por outras (swap);

# E o que DeFi tem a ver com isso?

Decentralized Finance (DeFi) é toda a classe de serviços financeiros baseados em Smart Contracts na Blockchain;

---

Agora, transações em redes Blockchain não se limitam a apenas envio e recebimento de criptomoedas. Com DeFi, é possível:

Realizar e receber empréstimos;

Receber juros de empréstimos feitos;

Trocar criptomoedas por outras (swap);

---

Tudo isso de forma Descentralizada e sem a presença de nenhuma instituição financeira! Apenas indivíduos com carteiras digitais e bastante programação!

# Aplicações DeFi

## Plataformas de Empréstimo

- Funcionam como bancos e financeiras, e dão aos usuários a possibilidade de pegar empréstimos em criptomoedas.
- **A diferença é que não há intermediários, e tudo é regido pelos smart contracts.**
- No geral, é preciso deixar ativos digitais como garantia para ter acesso aos recursos. MakerDAO e Compound são alguns exemplos.


Fonte: Infomoney

# Aplicações DeFi

## Stablecoins

- São criptomoedas pareadas em algum ativo, como ouro, prata ou moedas fiduciárias (dólar, euro, real e outras).
- **Dois exemplos são o Tether (USDT) e o USD Coin (USDC).**
- Cada unidade equivale a um dólar. Essa classe de ativo, portanto, busca a estabilidade, e não é volátil como Bitcoin, Ethereum e outros criptoativos.

**Fonte: Infomoney**

# Aplicações DeFi

## Exchanges Descentralizadas

- As DEX, como também são chamadas, são corretoras nas quais os usuários podem negociar criptomoedas entre si (peer-to-peer) sem intermediários.
- **Nessas plataformas, tudo é controlado por algoritmos e contratos inteligentes.**
- Elas são diferentes de exchanges centralizadas, que têm uma equipe e uma empresa no controle, como é o caso do Mercado Bitcoin e da Binance, por exemplo. Dois exemplos de DEX são a Uniswap (UNI) e a PancakeSwap (CAKE).


Fonte: Infomoney

# E o Governo? e os bancos?

**Diante de todas essas transformações no ambiente financeiro global, os governos e os bancos não ficaram de parados!**

**Cada vez mais, instituições financeiras tradicionais e governos têm voltado seus olhos para esse novo paradigma do mundo crypto, para poderem se adaptar a esse novo ambiente, e não serem passados para trás.**

“Mas se blockchain é descentralizada e não precisa de intermediários, como os bancos podem se beneficiar dessa tecnologia?”

**“Mas se blockchain é descentralizada e não precisa de intermediários, como os bancos podem se beneficiar dessa tecnologia?”**

Aí que está a questão:
**não necessariamente uma Blockchain precisa ser descentralizada!**

# Como assim???

Exatamente! O primeiro caso de uso de uma Blockchain, o Bitcoin, foi completamente descentralizado, não havendo nenhuma instituição havendo um papel central na coordenação da rede.

Mas isso não quer dizer que toda rede Blockchain deve seguir esse formato!

# Como assim???

Exatamente! O primeiro caso de uso de uma Blockchain, o Bitcoin, foi completamente descentralizado, não havendo nenhuma instituição havendo um papel central na coordenação da rede.

Mas isso não quer dizer que toda rede Blockchain deve seguir esse formato!

Poderia existir uma rede Blockchain cujos nós são os bancos de um país, sendo que haveria um nó central (Ex: Banco Central) que controlaria a emissão da moeda dessa rede;

“Mas se a vantagem principal do uso de blockchain era a descentralização, qual a vantagem então de se usá-la nesse caso?”

**“Mas se a vantagem principal do uso de blockchain era a descentralização, qual a vantagem então de se usá-la nesse caso?”**

Aí que está uma outra questão muito importante:

**O uso de blockchain (e de Smart Contracts), mesmo se mantida por algumas poucas organizações centralizadoras, permite a tokenização do dinheiro e de ativos financeiros!**

Não se pode esquecer de todos os ativos financeiros tradicionais, além do dinheiro fiduciário, que são incompatíveis com o ambiente descentralizado do DeFi, mas que mesmo assim podem se beneficiar das automações que a tecnologia blockchain pode trazer para instituições tradicionais!

# O que são Ativos Tokenizados?

São tokens (qualquer ativo digital transferível em Blockchain) que representam ativos do mundo real

## Fracionalizáveis

Podem ser facilmente subdivididos em pedaços menores, representando propriedade parcial

## Programáveis

Ativos digitais podem ser programáveis para executar diferentes rotinas a partir do uso de Smart Contracts

## Tecnologia Agnóstica

Qualquer ativo, financeiro ou não, pode ser digitalizado e transformado em um token na Blockchain

# Casos de uso de Tokenização de Ativos

### Ativos Imobiliários

Permite posse fracional de imóveis de maneira muito mais simples, além de trazer mais liquidez ao mercado imobiliário;

### Arte

Permite a digitalização da posse de uma certa peça de arte. Isso pode trazer mais segurança e agilidade para transações com esse tipo de ativo;

### Tokenização de Commodities


Da mesma forma que com ativos imobiliários, a tokenização de Commodities traz mais agilidade e liquidez em transações, além de permitir novas modalidades de posse de ativos;

# CBDC

## "Criptomoedas" dos Governos

Central Bank Digital Currency (CBDC) é o termo utilizado para o uso de tecnologia DLT (Distributed Ledger Technology) para a criação de moedas digitais controladas por Bancos Centrais;

# CBDC
## "Criptomoedas" dos Governos

**Central Bank Digital Currency** (CBDC) é o termo utilizado para o uso de tecnologia DLT (Distributed Ledger Technology) para a criação de moedas digitais controladas por Bancos Centrais;

Da mesma forma que com ativos tokenizados, os principais benefícios de uma CBDC estão relacionados à programabilidade do dinheiro e maior agilidade e inovação em serviços financeiros

# CBDC Brasileiro!

## O que é o DREX?

- **É o real**, a moeda brasileira oficial, **em formato digital**
- Tem o **mesmo valor** e a **mesma aceitação** do real tradicional
- **Regulado pelo Banco Central** e **emitido** somente **em sua plataforma**
- Tem as **mesmas garantias e segurança** do real tradicional
- **Depende de um banco** ou de **outra instituição** para seu uso pelo cidadão

**Fonte: Banco Central do Brasil**

# CBDC Brasileiro!

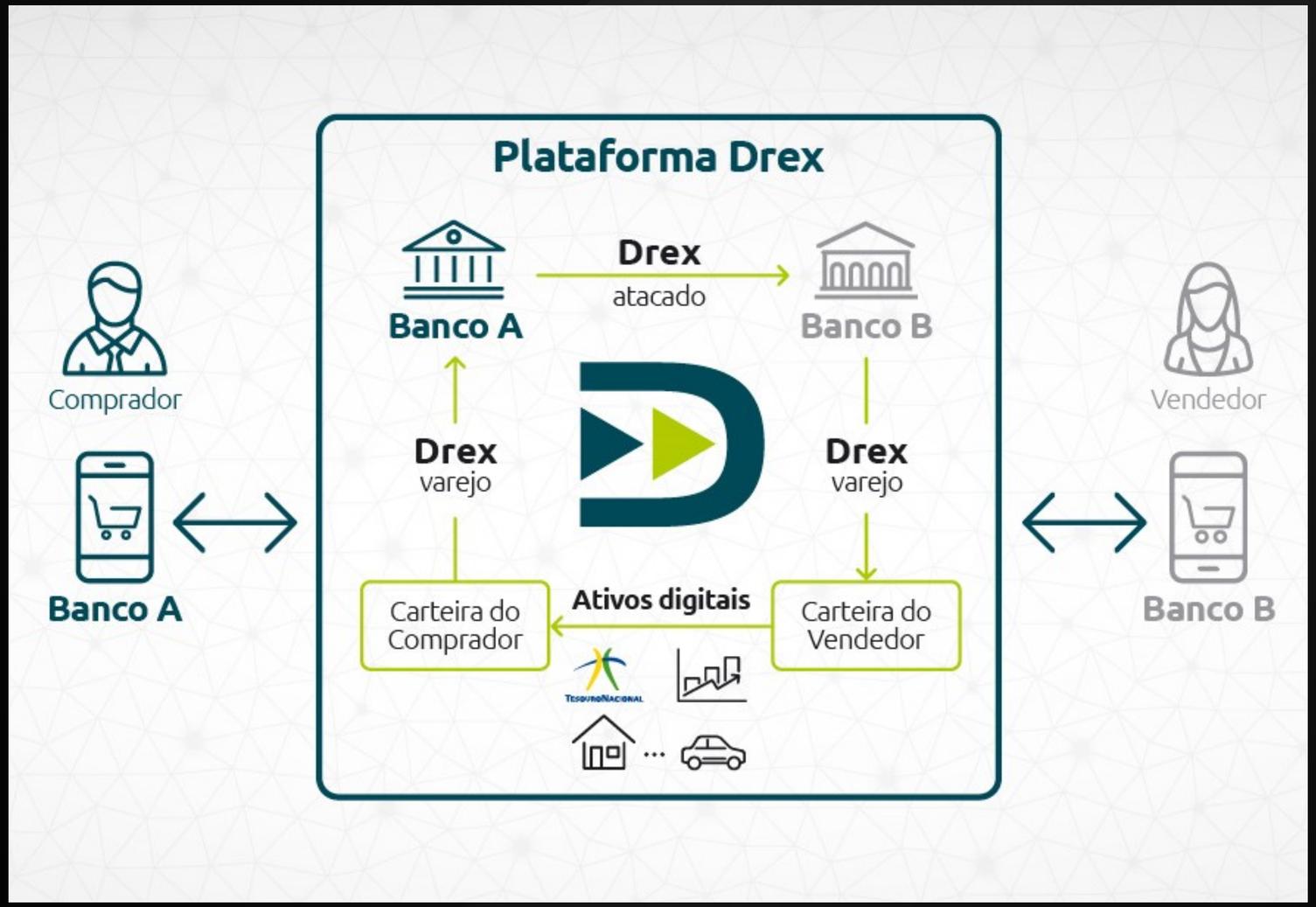
**Como vai funcionar?**

**O Drex vai permitir que vários tipos de transações financeiras seguras com ativos digitais e contratos inteligentes estejam à sua disposição. Esses serviços financeiros inteligentes serão liquidados pelos bancos dentro da Plataforma Drex do Banco Central (BC), que é um ambiente em desenvolvimento utilizando a tecnologia de registro distribuído (em inglês Distributed Ledger Technology – DLT).**

**Para ter acesso à Plataforma Drex, você precisará de um intermediário financeiro autorizado, como um banco. Esse intermediário fará a transferência do seu dinheiro depositado em conta para sua carteira digital do Drex, para que você possa realizar transações com ativos digitais com total segurança.**

**Fonte: Banco Central do Brasil**

# CBDC Brasileiro!




Fonte: Banco Central do Brasil

# Porém existe o outro lado da moeda...

- Governo com muito mais controle e (possivelmente) vigilância sobre movimentações financeiras de indivíduos;
- Governo com autoridade de reverter transações, em caso de comprovação de fraude;

**Será que é interessante o governo ter esse tipo de poder de vigilância sobre os indivíduos de um país?**

# Dúvidas?

Muito obrigado pela atenção!