

DeFi

Ivan Sendin

DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

# DeFi

Ivan Sendin

FACOM - Universidade Federal de Uberlandia  
ivansendin@yahoo.com, sendin@ufu.br

10 de outubro de 2024

# DeFi

## DeFi

Ivan Sendin

### DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)











Sandwich

DeX- Solidity...

- Queridinha do momento  
(se Fintech já chama atenção...)
- Finanças Descentralizadas
- Qualquer serviço financeiro oferecido por  
mecanismos descentralizados
- Serviços equivalentes aos tradicionais
- Serviços novos...
- Movimentam milhões e milhões

## DeFi

## Geral

#	NAME	CHAIN	SECTOR	TVL (USD) ▾
1 🏆	 <b>Maker</b>	Ethereum	Lending	\$16.16B
2 🦊	 <b>Curve Finance</b>	Ethereum	DEXes	\$11.14B
3 🦊	 <b>Convex Finance</b>	Ethereum	Assets	\$9.05B
4	 <b>Aave</b>	Multichain	Lending	\$8.47B
5	 <b>Compound</b>	Ethereum	Lending	\$6.29B
6	 <b>InstaDApp</b>	Ethereum	Lending	\$5.28B
7	 <b>yearn.finance</b>	Ethereum	Assets	\$2.81B
8	 <b>Balancer</b>	Ethereum	DEXes	\$2.19B
9	 <b>Bancor</b>	Ethereum	DEXes	\$1.84B
10	 <b>SushiSwap</b>	Ethereum	DEXes	\$1.43B

Fonte: DeFi Pulse (ANTIGO)

# Tokens

DeFi

Ivan Sendin

DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

- ERC20
  - “Moedas”
- ERC721
  - Non-Fungible Token
  - [Crypto Kitties](#)
  - Cada contrato ERC721 mantém uma coleção de tokens (uint256) associados a uma URI...
  - Regras para criação (mint) de novos tokens

# Exchanges

DeFi

Ivan Sendin

DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

- Como obter Bitcoin? Ether? Litecoin?
- Você pode minerar...
- Exchanges... Casa de Câmbio e Bolsa de criptomoedas  
Pix, transferência, cartão de crédito(?)
- Muitas
- Muitos golpes, acidentes de percurso
- Muitas taxas!!!

# Algumas...

## DeFi

Ivan Sendin

### DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

- Binance
- Mercado Bitcoin
- Foxbit
- Coinbase
- (não é um endosso **cuidado!!!**)
- Em geral elas são **donas** das suas criptomoedas!!!

# Algumas...

## DeFi

Ivan Sendin

## DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

- Em geral elas são **donas** das suas criptomoedas!!!
- Quando voce compra Bitcoin/Ethereum não é registrado na Blockchain
- Vantagem: diminui a responsabilidade do usuário
- Perdeu a senha (de acesso) o dinheiro ainda pode ser recuperado
- Desvantagem: golpes (em vários níveis) e erros operacionais
- “Solvencia”: a corretora tem mesmo os bitcoin que ela alega ter ?
- Quanto ela alega ter...corresponde a realidade??
- Existem protocolos...

# Funcionamento

DeFi

Ivan Sendin

DeFi

Geral

Tokens

**Exchanges**

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

- Funcionam usando “Order Book”
- (Bolsa de Valores.. igual aos filmes)



DeFi

Ivan Sendin

DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market

Maker

Constant Sum Market

Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

## LIVRO DE OFERTAS

Preço (R\$)	Quantidade (BTC)	Total (BTC)
28.673,69	62.124	3.591.924
28.673,69	9.622	4.416.095
28.673,69	69.742	3.353.912
28.674,69	1.051	3.187.766
28.673,69	139.350	3.117.970
28.673,69	168.021	2.909.929
28.673,69	10.213	2.602.552
28.673,69	512	2.591.924
28.673,69	62.124	3.591.924
28.673,69	259.622	4.416.095
28.673,69	69.742	3.353.912
28.673,69	201.051	3.187.766
28.673,69	139.350	3.117.970
28.673,69	168.021	2.909.929
28.673,69	10.213	2.602.552
28.673,69	1.912	2.591.924
28.431,69		
Spread 163,48 (0,57%)		
28.510,21	1.296.163	1.296.163
28.510,21	20.110	1.316.275
28.510,21	9.919	1.325.464
28.509,21	24.742	1.350.206
28.509,21	78.532	1.428.671
28.509,21	207.422	1.636.902
28.508,21	129.546	1.751.431
28.507,21	419.905	2.184.544
28.507,21	78.532	1.428.671
28.507,21	207.422	1.636.902
28.506,21	129.546	1.751.431
28.506,21	419.905	2.184.544
28.506,21	78.532	1.428.671
28.506,21	207.422	1.636.902
28.506,21	129.546	1.751.431
28.506,21	419.905	2.184.544

# Funcionamento

## DeFi

Ivan Sendin

### DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

- Quando existe um matching de valor de venda/compra a exchange faz a negociação
- (altera uma tabela no Banco de dados)
- E cobra uma porcentagem

# Exchanges

DeFi

Ivan Sendin

DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

- Spread
- Falta de liquidez
- In business, economics or investment, market liquidity is a market's feature whereby an individual or firm can quickly purchase or sell an asset without causing a drastic change in the asset's price. Liquidity involves the trade-off between the price at which an asset can be sold, and how quickly it can be sold. (Fonte: Wikipedia)

# Order Book

DeFi

Ivan Sendin

DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

- O modelo Order Book nao funciona muito bem em smart contracts
- É normal colocar/reposicionar/tirar ordens...
- Muito lento em SC
- Muito caro: GAS!!
- (nas exchanges é de graça)

# DEX

## DeFi

Ivan Sendin

### DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

- Uma DEX consegue implementar - de forma algorítmica - alternativas ao Order Book
- **Automated Market Makers**  
Algoritmos de definem o preço dos tokens conforme o mercado se movimenta.  
A relação de preço é estabelecida dinamicamente
- Liquidity Pools/Liquidity Providers
- Os usuários depositam tokens
- Ficando “socios” de um pool de liquidez
- Recebe uma fração das taxas cobradas “LP Tokens”

- Constant Product Market Maker - CPMM
- $Saldo_x.Saldo_y = k$
- Estabelece o preço do  $X$  e  $Y$  respeitando a oferta e procura

- Em um contrato estão depositados 100 ethers e 50 tokens  $X$
- $100.50 = 5000$
- Se eu tenho 10 Ethers para comprar em tokens  $X$
- O saldo do pool em Ether será de 110
- O saldo em  $X$ :

$$110 \cdot Saldo_x = 5000$$

$$Saldo_x = \frac{5000}{110}$$

$$Saldo_x = 45$$

- Logo o contrato me paga 5 tokens (arredondamento e sem taxas)

- Se eu depositar mais 10 Ethers para comprar mais token:

$$x' = \frac{5000}{120}$$

$$x' = 41$$

- Agora eu recebo 4 tokens...subiu o preço!!
- Normal??



## DeFi

Ivan Sendin

### DeFi

Geral

Tokens

Exchanges

DeX

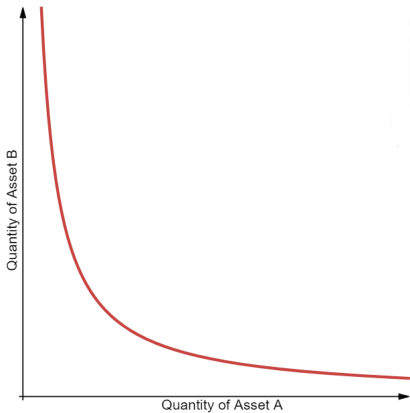
Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...



- Constant Sum Market Maker - CSMM
- $Saldo_x + Saldo_y = k$
- É possível “drenar” um recurso
- Facilita a arbitragem
- Não é utilizado

## DeFi

Ivan Sendin

### DeFi

Geral

Tokens

Exchanges

DeX

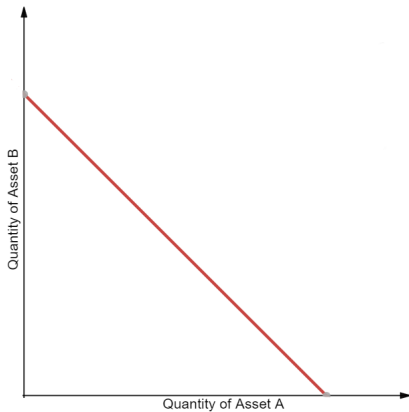
Constant Product Market  
Maker

**Constant Sum Market  
Maker**

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...



- Constant Mean Market Maker (CMMM)
- Permite mais de 2 tokens
- $(S_x \cdot S_y \cdot S_z)^{1/3} = k$
- 3 pares de tokens em um unico pool

- Uma micro implementação em Python...
- Prova de conceito do ataque de Sandwich
- Um pool de liquidez
- T1 e T2

## DeFi

Ivan Sendin

### DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market

Maker

Constant Sum Market

Maker

Constant Mean Market

Maker (CMMM)

Sandwich

DeX- Solidity...

```
# buy ?? tokens t2 using qt1 of t1  
# return (t1balance,t2balance, t2 delta)
```

```
def buy(t1,t2,qt1):  
    k=t1*t2  
    nt1 = t1+qt1  
    nt2 = k/nt1  
    return (nt1,nt2, t2-nt2)
```

## DeFi

Ivan Sendin

### DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market

Maker

Constant Sum Market

Maker

Constant Mean Market

Maker (CMMM)

Sandwich

DeX- Solidity...

```
# Sell ?? tokens t2 using qt1 of t1  
# return (t1balance,t2balance, t2 delta)  
def sell(t1,t2,qt1):  
    tmp = buy(t1,t2,-qt1)  
    return (tmp[0],tmp[1],-tmp[2])
```

```
def simpleTest():  
    t1=100.0  
    t2=100.0  
  
    q=10.0  
    #Compra t2 usando q unidades de t1  
    (t1,t2,d) = buy(t1,t2,q)  
  
    print (t1,t2,d)  
    #110.0 90.9090909090909 9.090909090909093  
  
    #Compra t2 usando q unidades de t1  
    q=10.0  
    (t1,t2,d) = buy(t1,t2,q)  
    print (t1,t2,d)  
    #120.0 83.33333333333333 7.575757575757578  
  
    q=20.0  
    (t1,t2,d) = sell(t1,t2,q)  
    print (t1,t2,d)  
    #100.0 100.0 16.666666666666667
```

## SEM COBRANÇA DE TAXAS



## DeFi

Ivan Sendin

### DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

```
t1 = 1000.0
```

```
t2 = 1000.0
```

```
# Legit user
```

```
q=100.0
```

```
(t1,t2,d) = buy(t1,t2,q)
```

```
print ('Gastou ',q,' T1 para comprar ',d, ' T2',t1,t2)
```

```
#Gastou 100.0 T1 para comprar 90.90909090909088 T2 1100.0 909.0909090909091
```

- Vamos supor que um usuário *Sand1* tenha capacidade de “olhar” a rede P2P  
Razoável
- Vamos supor que um usuário *Sand1* tenha capacidade de “furar a fila”  
Razoável: Gas, Eclipse

## DeFi

Ivan Sendin

DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market

Maker

Constant Sum Market

Maker

Constant Mean Market

Maker (CMMM)

Sandwich

DeX- Solidity...

```
# Agora com sandwich
```

```
t1 = 1000.0
```

```
t2 = 1000.0
```

```
#Atacante
```

```
q=50
```

```
(t1,t2,qd) = buy(t1,t2,q)
```

```
print ('Sand1 Gastou ',q,' T1 para comprar ',qd, ' T2 ',t1,t2)
```

```
#Sand1 Gastou 50 T1 para comprar 47.61904761904759 T2 1050.0 952.3809523809524
```

```
# Legit user
```

```
q=100.0
```

```
(t1,t2,d) = buy(t1,t2,q)
```

```
print ('Gastou ',q,' T1 para comprar ',d, ' T2 ',t1,t2)
```

```
#Gastou 100.0 T1 para comprar 82.81573498964804 T2 1150.0 869.5652173913044
```

```
#Atacante
```

```
(t2,t1,d) = buy(t2,t1,qd)
```

```
print ('Sand1 conseguiu ',d,' T1 vendendo ',qd, ' T2 ',t1,t2)
```

```
#Sand1 conseguiu 59.70654627539511 T1 vendendo 47.61904761904759 T2 1090.29345372460
```

- Ataque de sandwich
- Depende da capacidade de “interceptar” uma transação
- Rede P2P
- Criar uma transação que será executada antes
- Um tipo de Arbitragem
- Risco quase zero
- Pode ser automatizada
- Ganhos pequenos....

## DeFi

Ivan Sendin

### DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

```
contract tinyDeX {  
  
    address owner;  
  
    struct PoolType {  
        address poolOwner;  
        ERC20 x;  
        ERC20 y;  
    }  
  
    mapping (string=>PoolType) pools;  
  
    constructor() public {  
        owner = msg.sender;  
    }  
  
    function createPool(string memory name, ERC20 x, ERC20 y) public {  
        require (pools[name].poolOwner == address(0), "This pool already exists!");  
        require (x.allowance(msg.sender, address(this)) > 0, "Show me the token!");  
        require (y.allowance(msg.sender, address(this)) > 0, "Show me the token!");  
  
        x.transferFrom(msg.sender, address(this), x.allowance(msg.sender, address(this)));  
        y.transferFrom(msg.sender, address(this), y.allowance(msg.sender, address(this)));  
  
        pools[name].poolOwner = msg.sender;  
        pools[name].x = x;  
        pools[name].y = y;  
    }  
}
```

## DeFi

Ivan Sendin

### DeFi

General

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

```
// buy y token using x token
function buy(string memory name) public {
    require (pools[name].poolOwner != address(0), "This pool doesnt exist!");
    require (pools[name].x.allowance(msg.sender, address(this)) > 0, "Show me the token!");
    uint256 xamount = pools[name].x.allowance(msg.sender, address(this));
    uint256 xbalance = pools[name].x.balanceOf(address(this));
    uint256 ybalance = pools[name].y.balanceOf(address(this));

    uint256 yamount = (ybalance*xamount)/(xbalance+xamount);

    pools[name].x.transferFrom(msg.sender, address(this), xamount);
    pools[name].y.transfer(msg.sender, yamount);
}
```

## DeFi

Ivan Sendin

### DeFi

General

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

```
function sell(string memory name) public {
    require (pools[name].poolOwner != address(0), "This pool doesnt exist!");
    require (pools[name].y.allowance(msg.sender, address(this)) > 0, "Show me the token!");
    uint256 yammount = pools[name].y.allowance(msg.sender, address(this));
    uint256 ybalance = pools[name].y.balanceOf(address(this));
    uint256 xbalance = pools[name].x.balanceOf(address(this));

    uint256 xammount = (xbalance*yammount)/(ybalance+yammount);

    pools[name].y.transferFrom(msg.sender, address(this), yammount);
    pools[name].x.transfer(msg.sender, xammount);

}

}
```

# tinyDeX

## DeFi

Ivan Sendin

### DeFi

Geral

Tokens

Exchanges

DeX

Constant Product Market  
Maker

Constant Sum Market  
Maker

Constant Mean Market  
Maker (CMMM)

Sandwich

DeX- Solidity...

- Gostaríamos que o dono do contrato e o dono do pool recebessem uma taxa por cada transação
- Possibilidade de extinguir o pool
- Quantidade mínima de token que eu aceito reber por transação
- (Tem um bug que se manifesta quando tivermos diversos pools)