



やさしい
Uniswap

DEMO

間に誰も介さず ether と ERC20
トークンを交換できる Ethereum
上の仕組み

1. 基本的な交換の仕組み
2. 価格決定の仕組み
3. 貯蓄の提供の仕組み
4. 価格変動曲線
5. フロントランニングリスク

1. 基本的な交換の仕組み

ERC20トークンごとにコントラ
クトがあり、コントラクトに
etherとERC20トークンが貯蓄さ
れている

Etherを送ることによってERC20を得ることができ、逆にERC20を送ることによってEtherを得られる

ERC20トークンごとの交換の場合、Etherがブリッジとして交換される

DAI \rightleftharpoons ETH

ETH \rightleftharpoons MKR

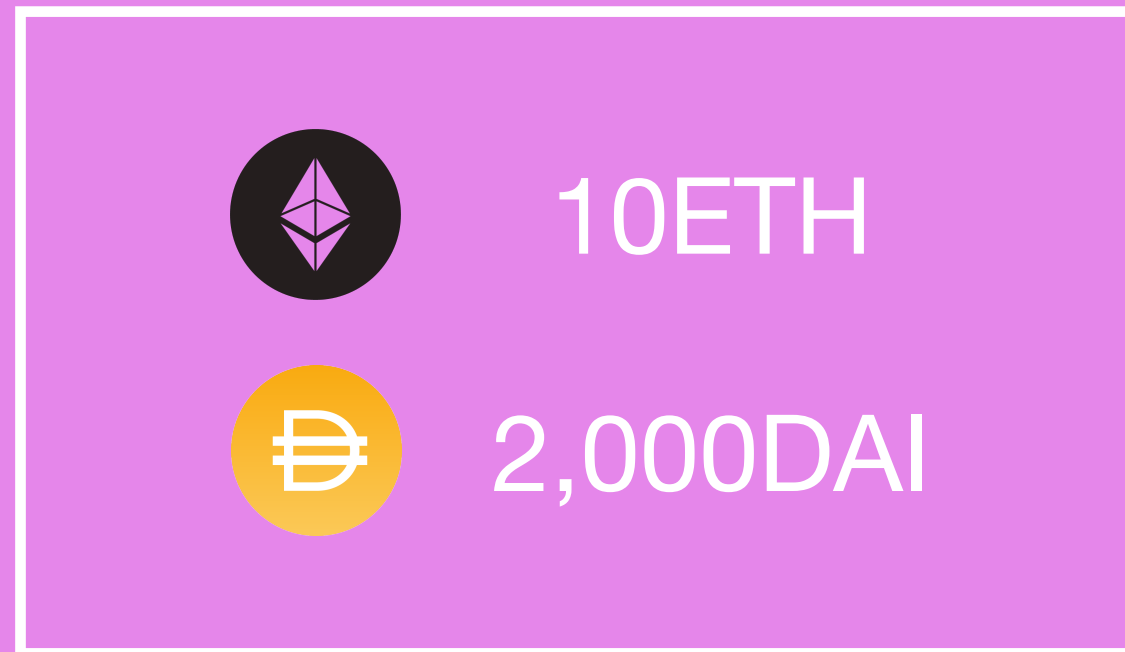
貯蓄モデルなので、買い手と売り
手をマッチングする必要がない

2. 価格決定の仕組み

$$x \times y = k \text{ 式}$$

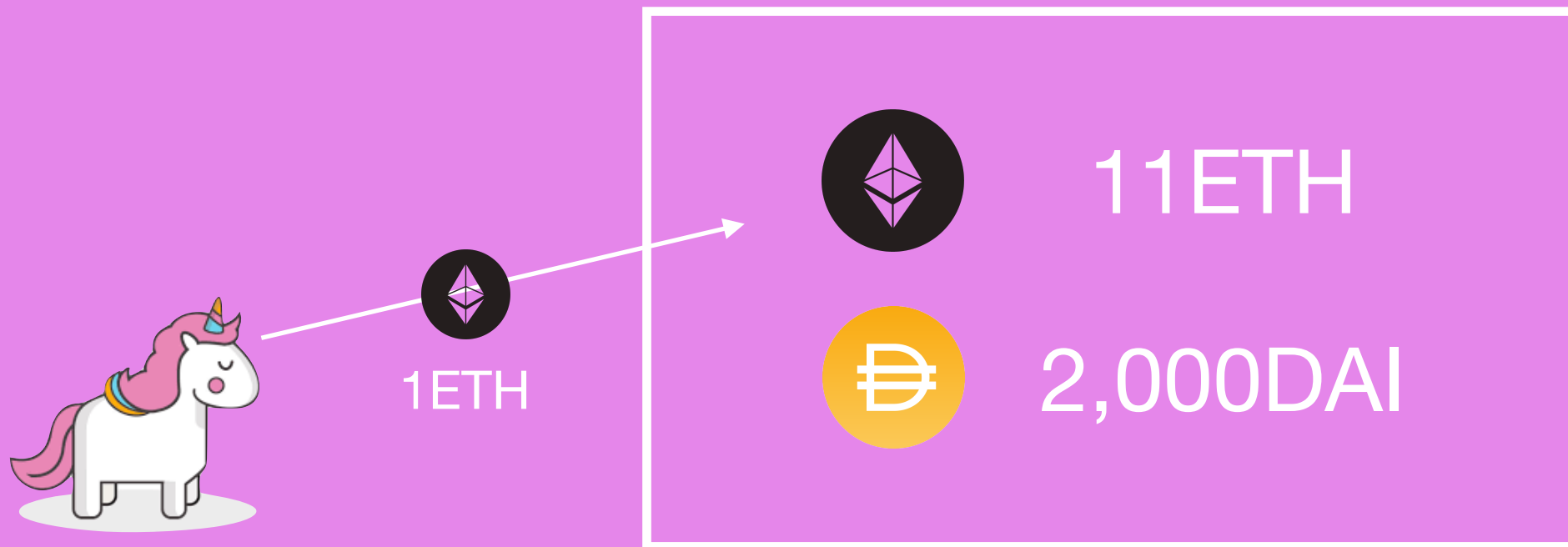
交換コントラクト内のetherの量と
ERC20トークンの量の積があるトランズ
アクションで常に一定になるように価格
が計算される

DAI交換コントラクト

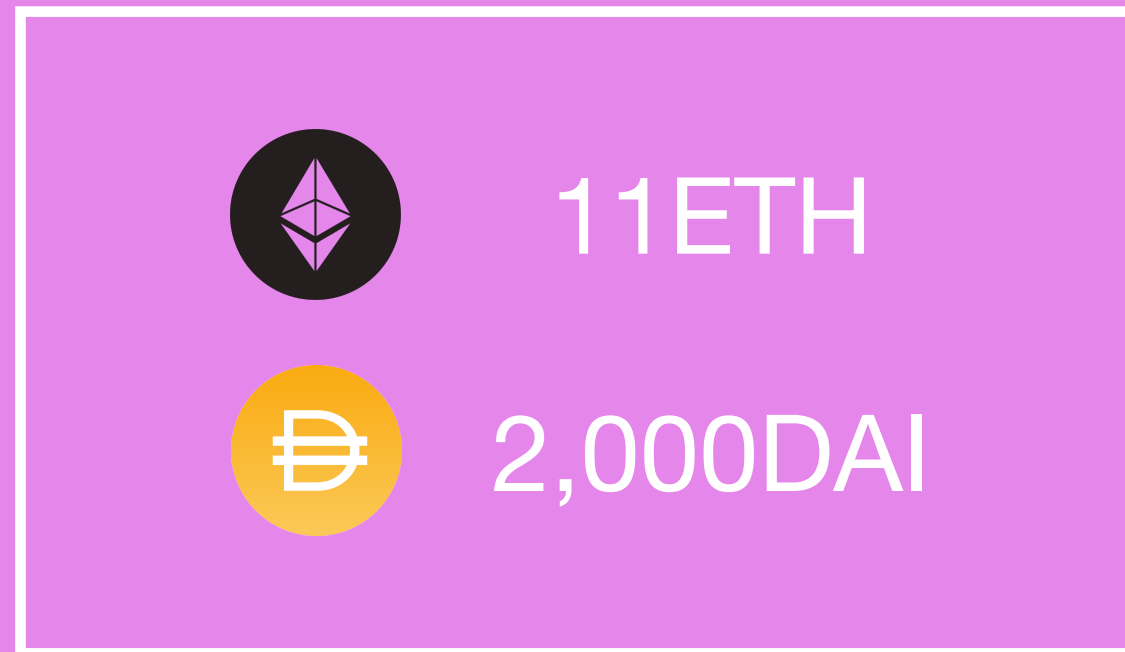


$$10(\text{ETHの量}) \times 2,000(\text{DAIの量}) = 20,000(\text{定数})$$

DAI交換コントラクト

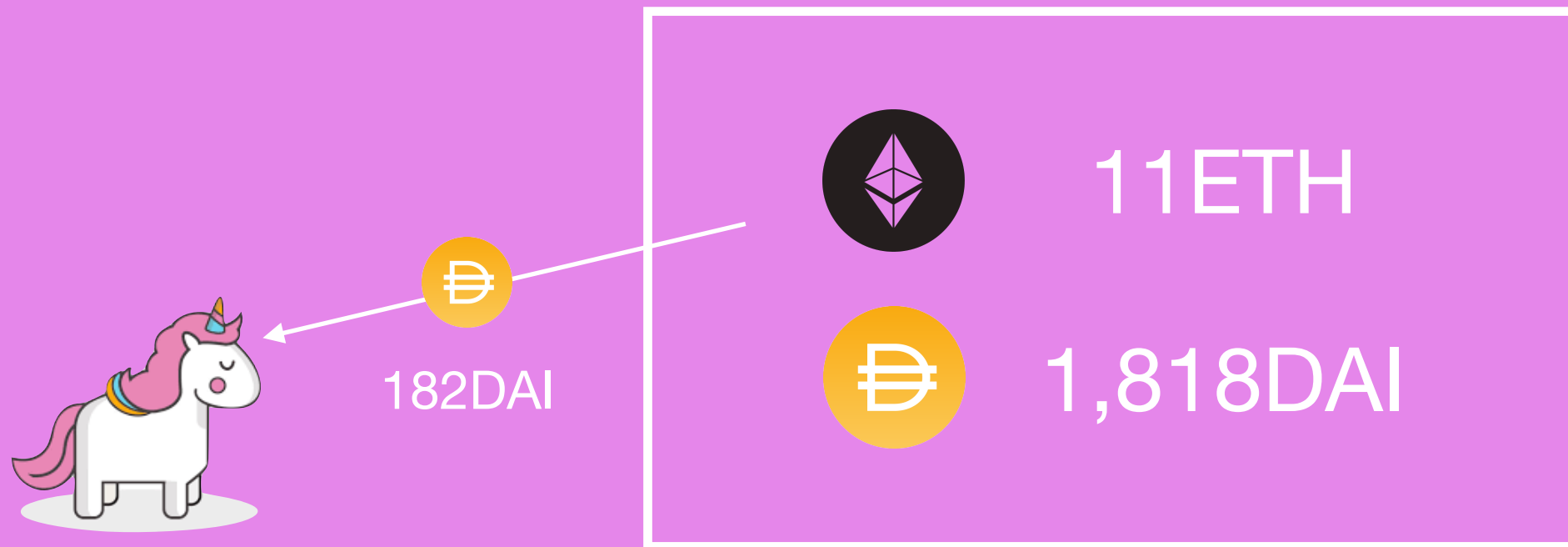


DAI交換コントラクト



$20,000(\text{定数}) \div 11(\text{ETHの量}) =$
 $1,818(\text{コントラクトの必要なDAIの量})$

DAI交換コントラクト



$2,000(\text{元々のDAIの量}) - 1,818(\text{コントラクトに必要なDAIの量})$
 $= 182(\text{購入されたDAI})$

3. 貯蓄の提供の仕組み

Liquidity Provider

コントラクトにetherとERC20
トークンを提供することで利益を
得られるようになっている

Liquidity Provider

同価値のetherとERC20と一緒に
プールする

供給量に応じて利益を得られる

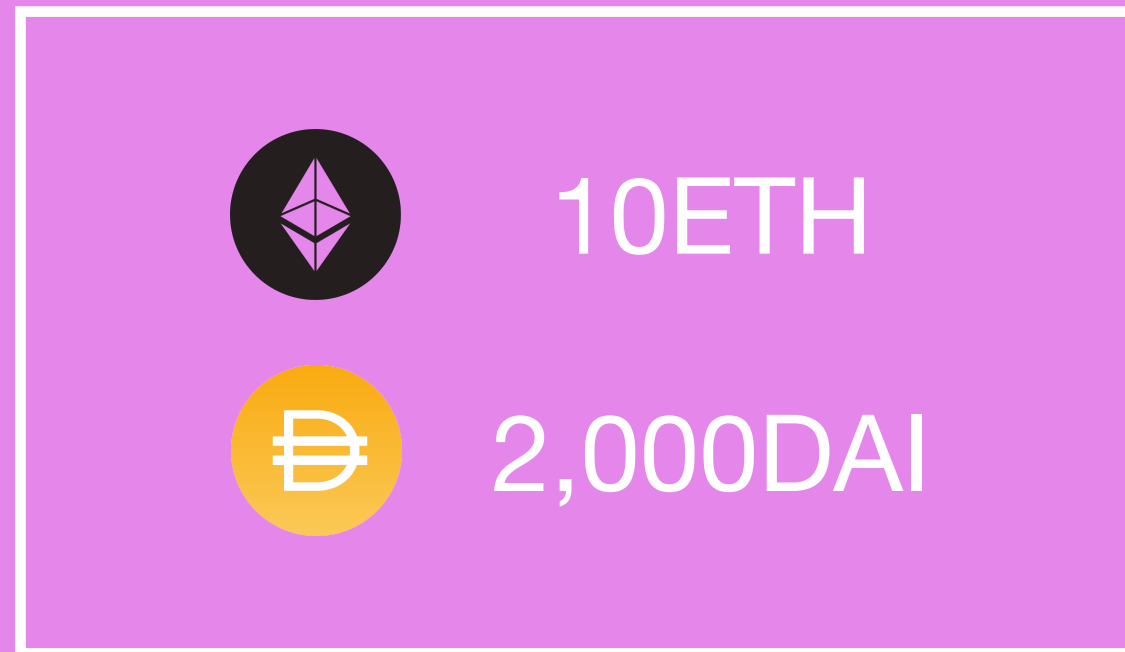
Liquidity Provider

供給した分に応じてLiquidity
トークンを得ることができる
トークンを交換することで供給し
た資産と手数料を得られる

4. 価格変動曲線

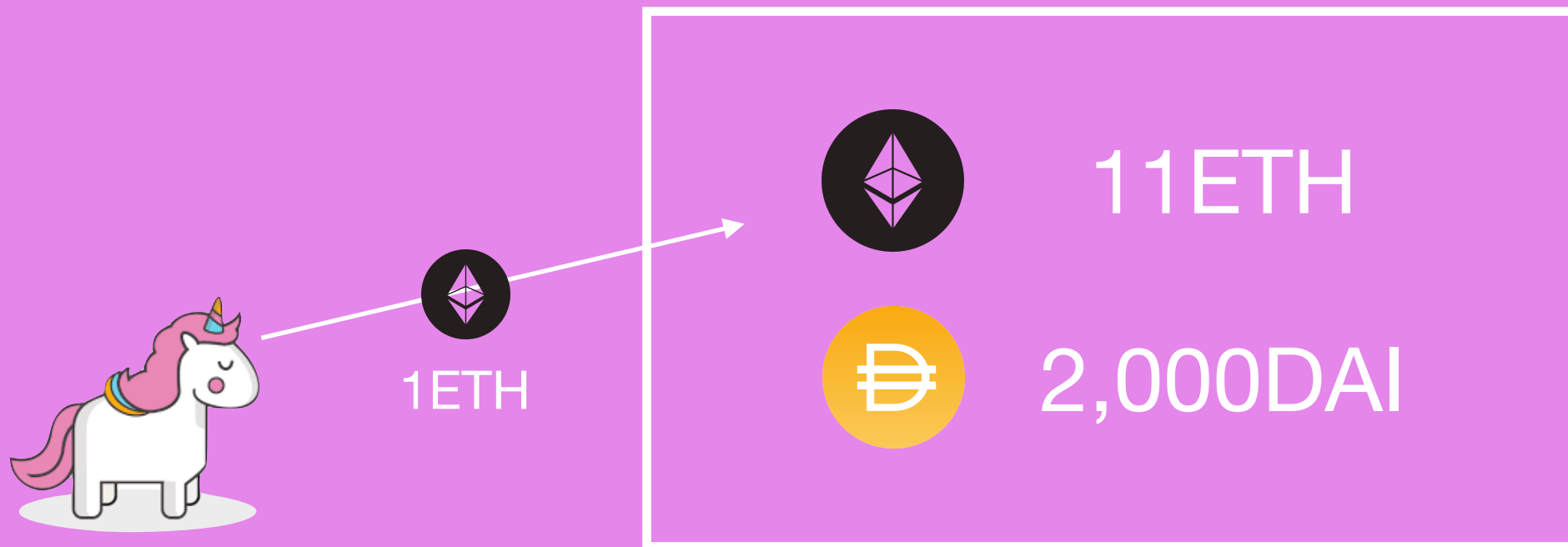
供給量に応じて価格が変動する

DAI交換コントラクト@Tx 0

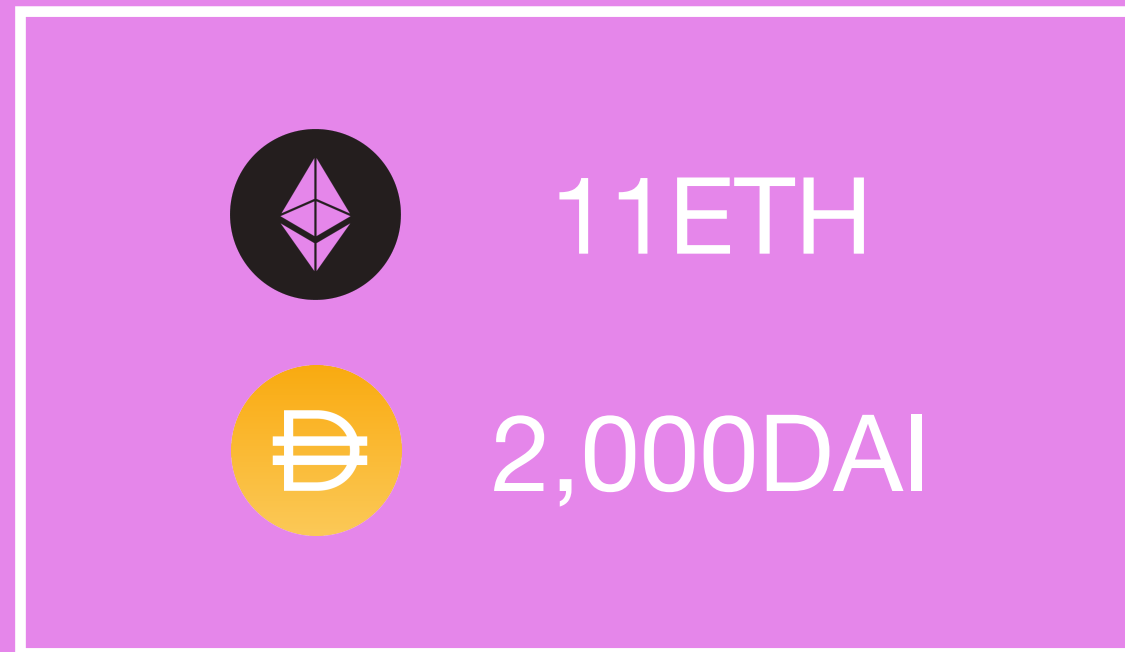


$$10(\text{ETHの量}) \times 2,000(\text{DAIの量}) = 20,000(\text{定数})$$

DAI交換コントラクト@Tx 0

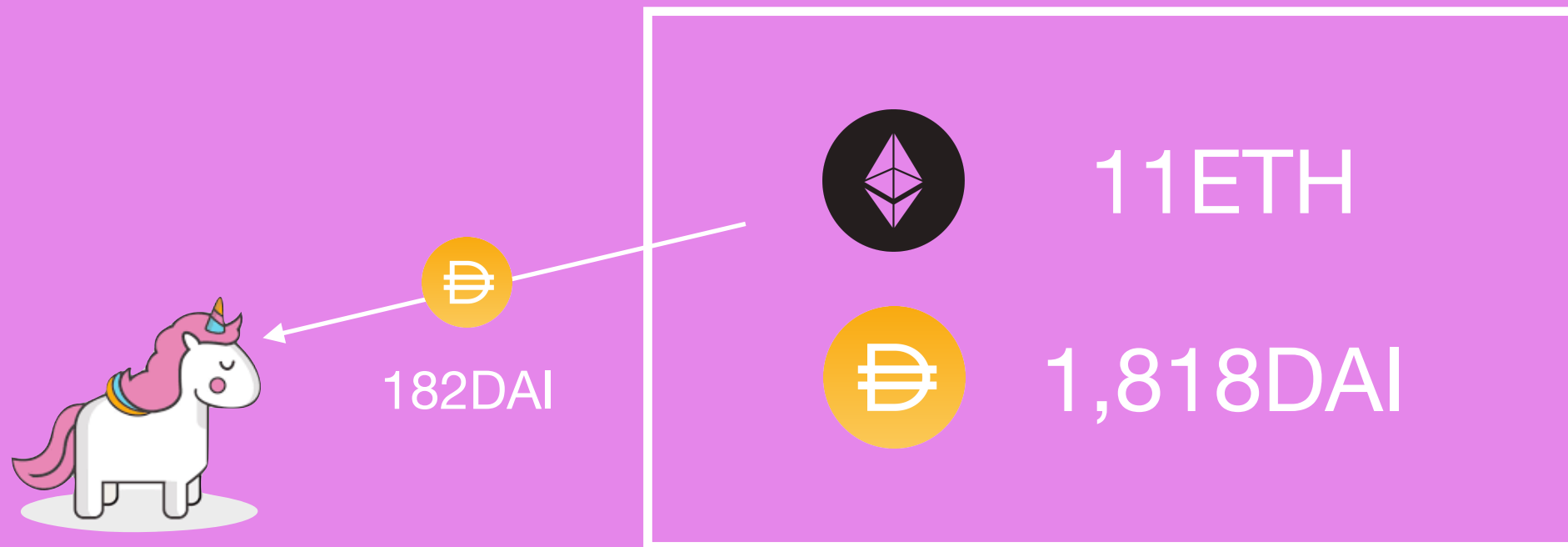


DAI交換コントラクト@Tx 0



$20,000(\text{定数}) \div 11(\text{ETHの量}) =$
 $1,818(\text{コントラクトの必要なDAIの量})$

DAI交換コントラクト@Tx 0

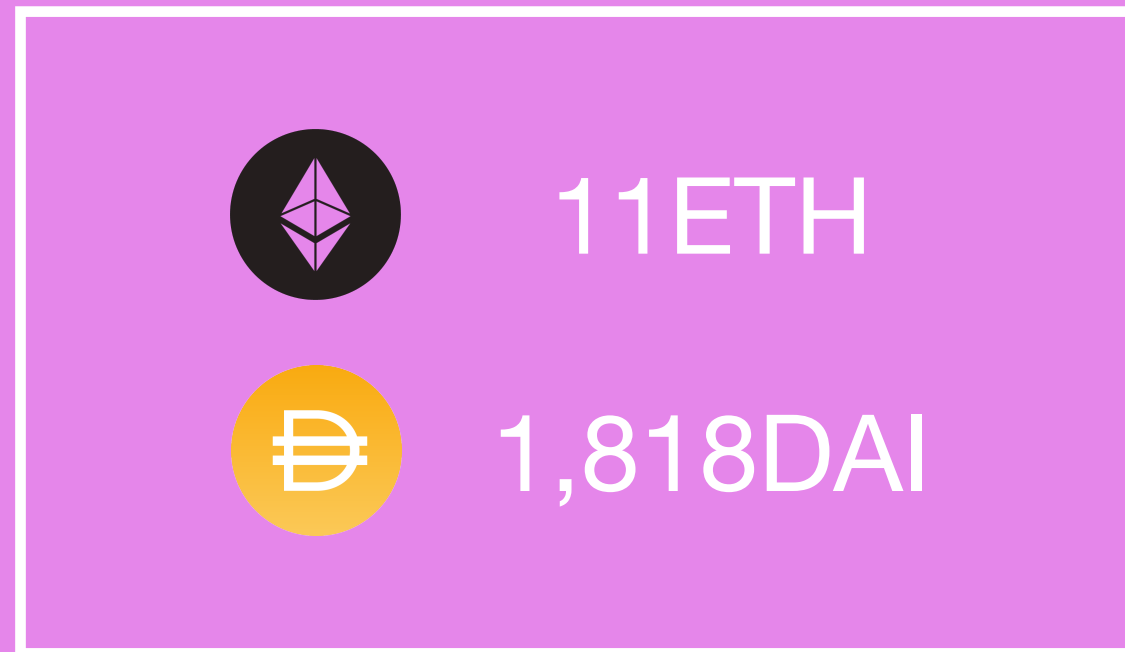


$2,000(\text{元々のDAIの量}) - 1,818(\text{コントラクトに必要なDAIの量})$
 $= 182(\text{購入されたDAI})$

交換レート@Tx 0

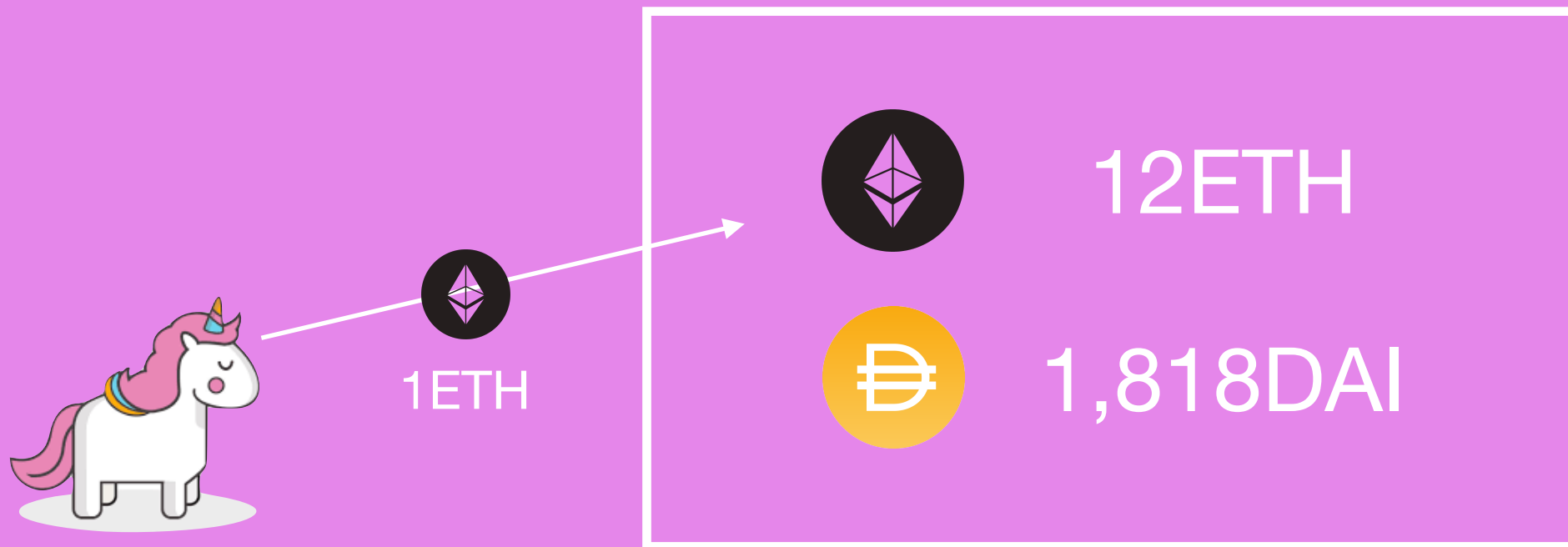
1ETH \rightleftharpoons 182DAI

DAI交換コントラクト@Tx 1

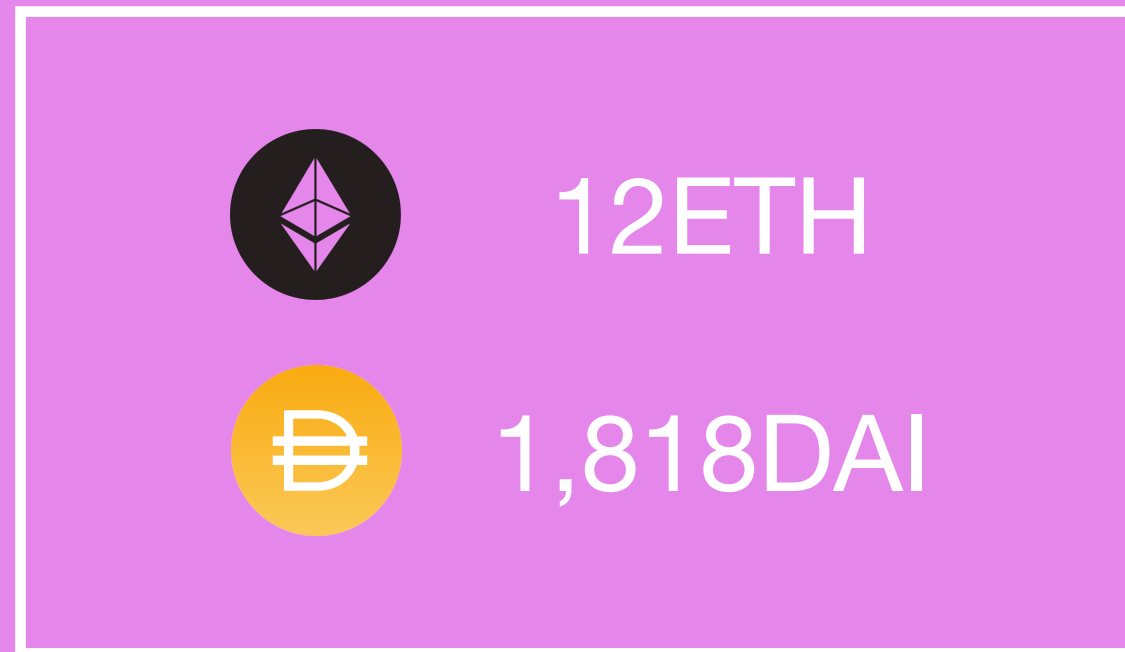


$$11(\text{ETHの量}) \times 1,818(\text{DAIの量}) = 20000(\text{定数})$$

DAI交換コントラクト@Tx 1

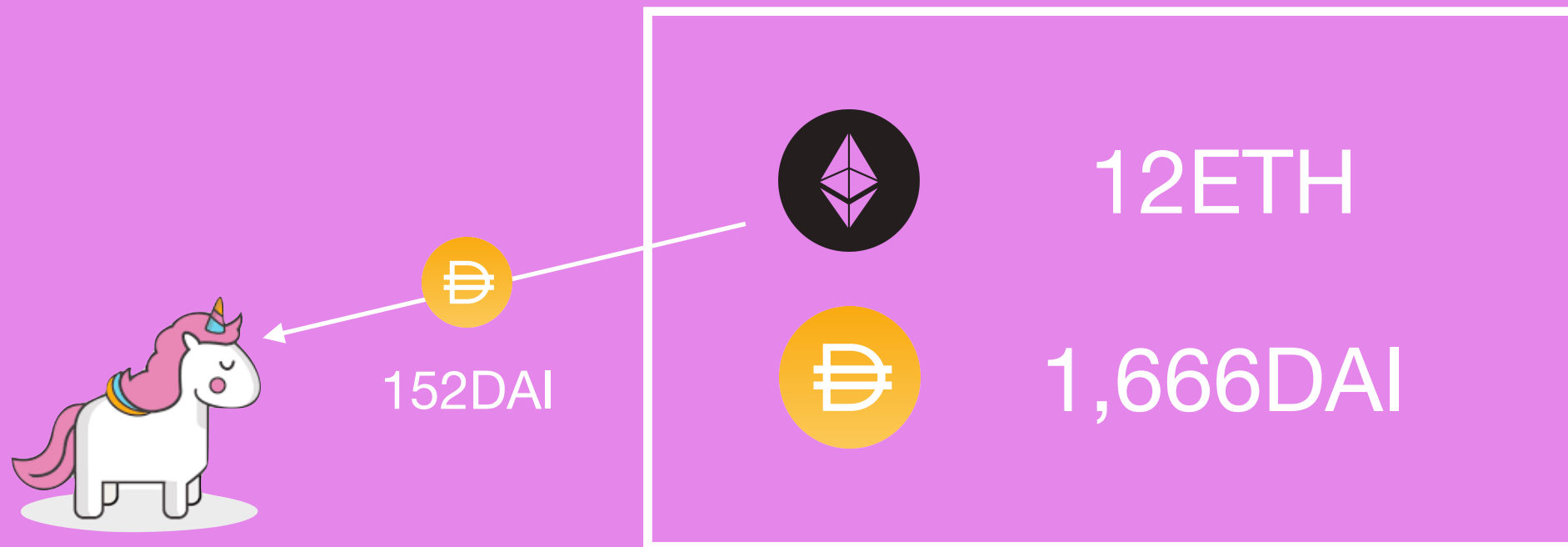


DAI交換コントラクト@Tx 1



$20000(\text{定数}) \div 12(\text{ETHの量}) =$
 $1,666(\text{コントラクトに必要なDAIの量})$

DAI交換コントラクト@Tx 1



$1,818(\text{元々のDAIの量}) - 1,666(\text{コントラクトに必要なDAIの量})$
 $= 152(\text{購入されたDAI})$

交換レート@Tx 1

1 ETH \rightleftharpoons 152 DAI

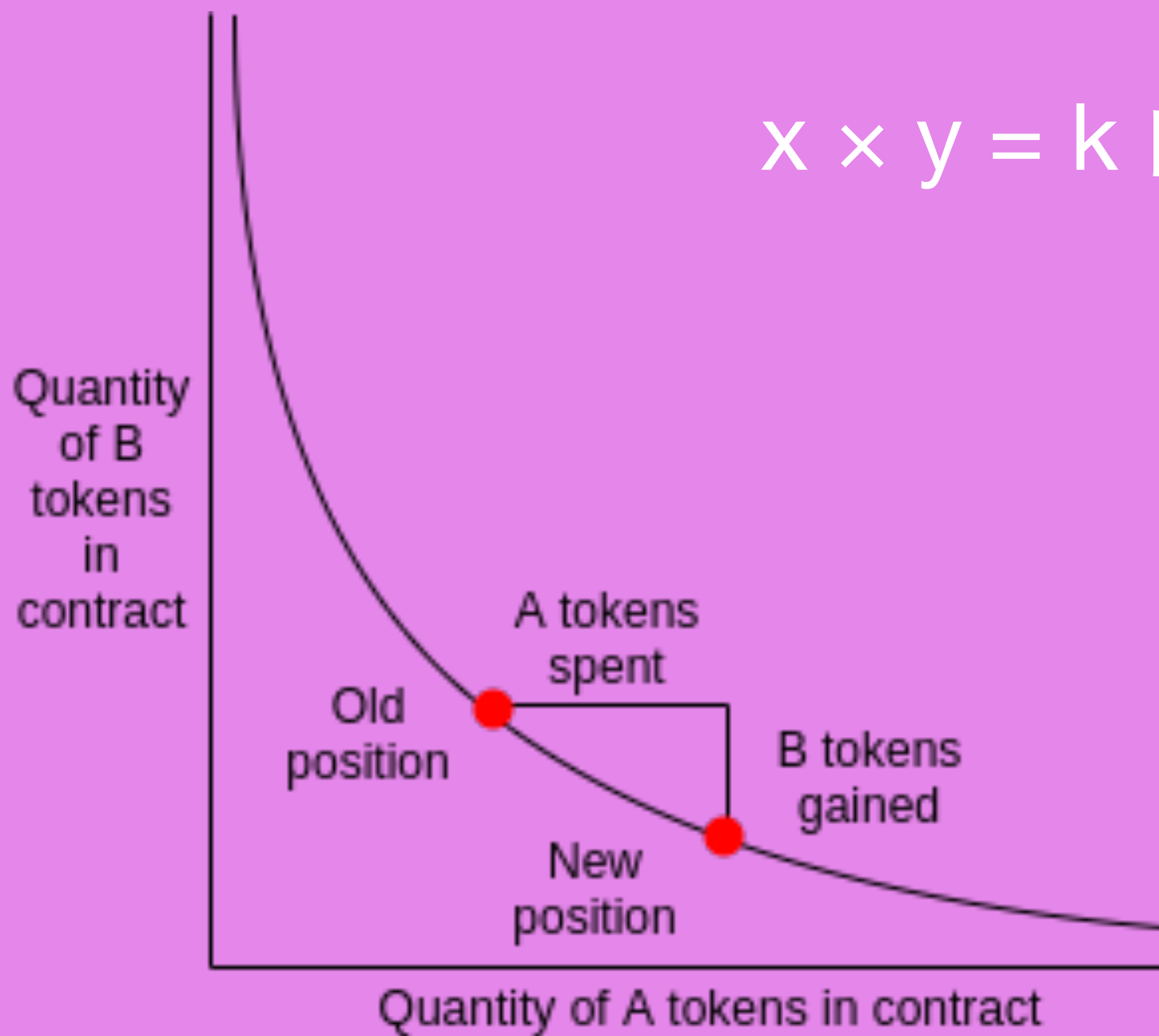
DAIの供給量が減ったので、ETHに対するDAIの価格がはね上がった

@Tx 0 1ETH \rightleftharpoons 182DAI

@Tx 1 1ETH \rightleftharpoons 152DAI

*実際のプールは12000ETH + 2,400,000DAI以上なので1ETHの取引ではほとんど変動しない

$$x \times y = k \text{ 曲線}$$



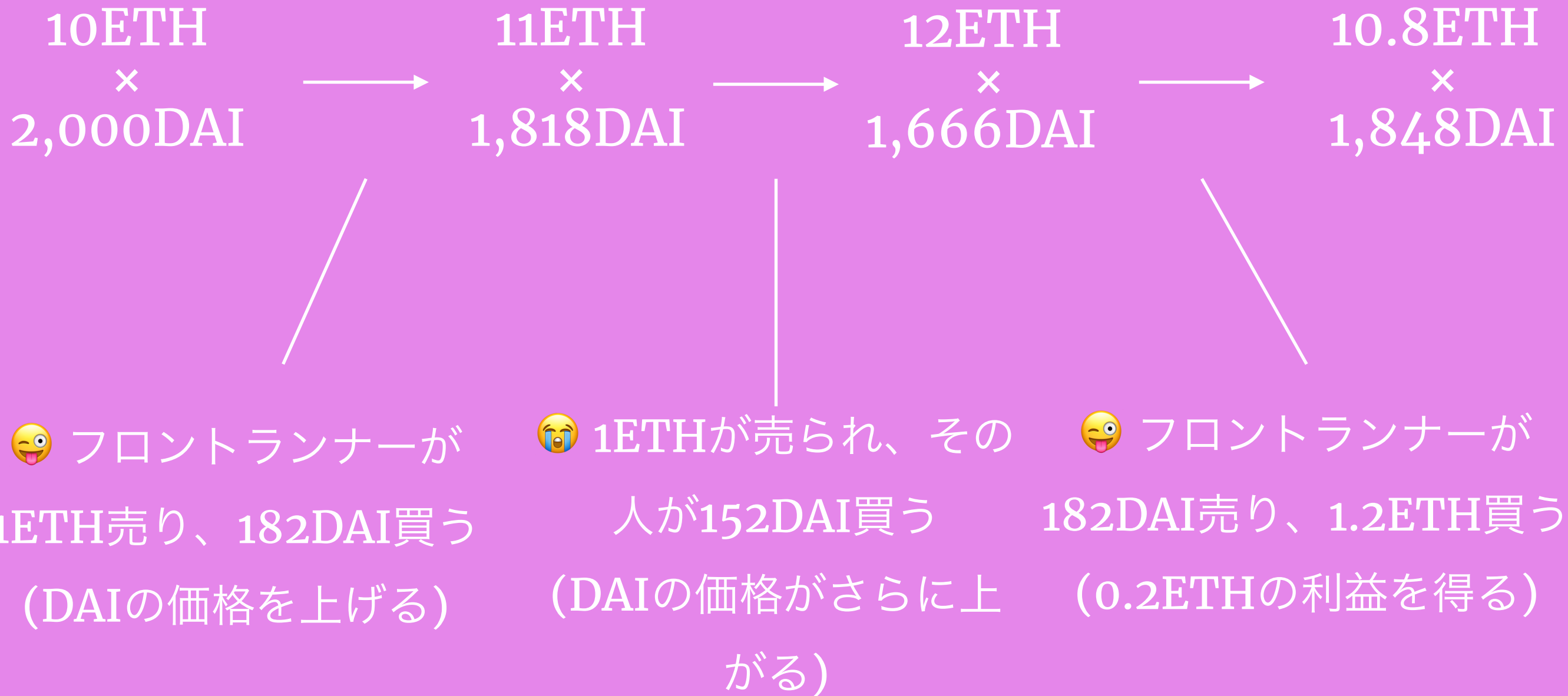
5. フロントランニングリスク

フロントランニング

GasPriceをうまく設定することでトランザクションの順番を変えて価格操作し、利益を上げる手法

フロントランナーが
1ETHを売るTxを見つけた場合

DAI交換コントラクトの状態変化(定数20000)と フロンランニングの流れ



フロントランニング緩和策

- 交換したい最小のトークンと締め切りを指定することで回避
- 最小のトークン量でない場合、もしくは締め切り以内でない場合、Txが失敗

Thank You! 😊

Follow me on Twitter
@taisuke_mino_JP