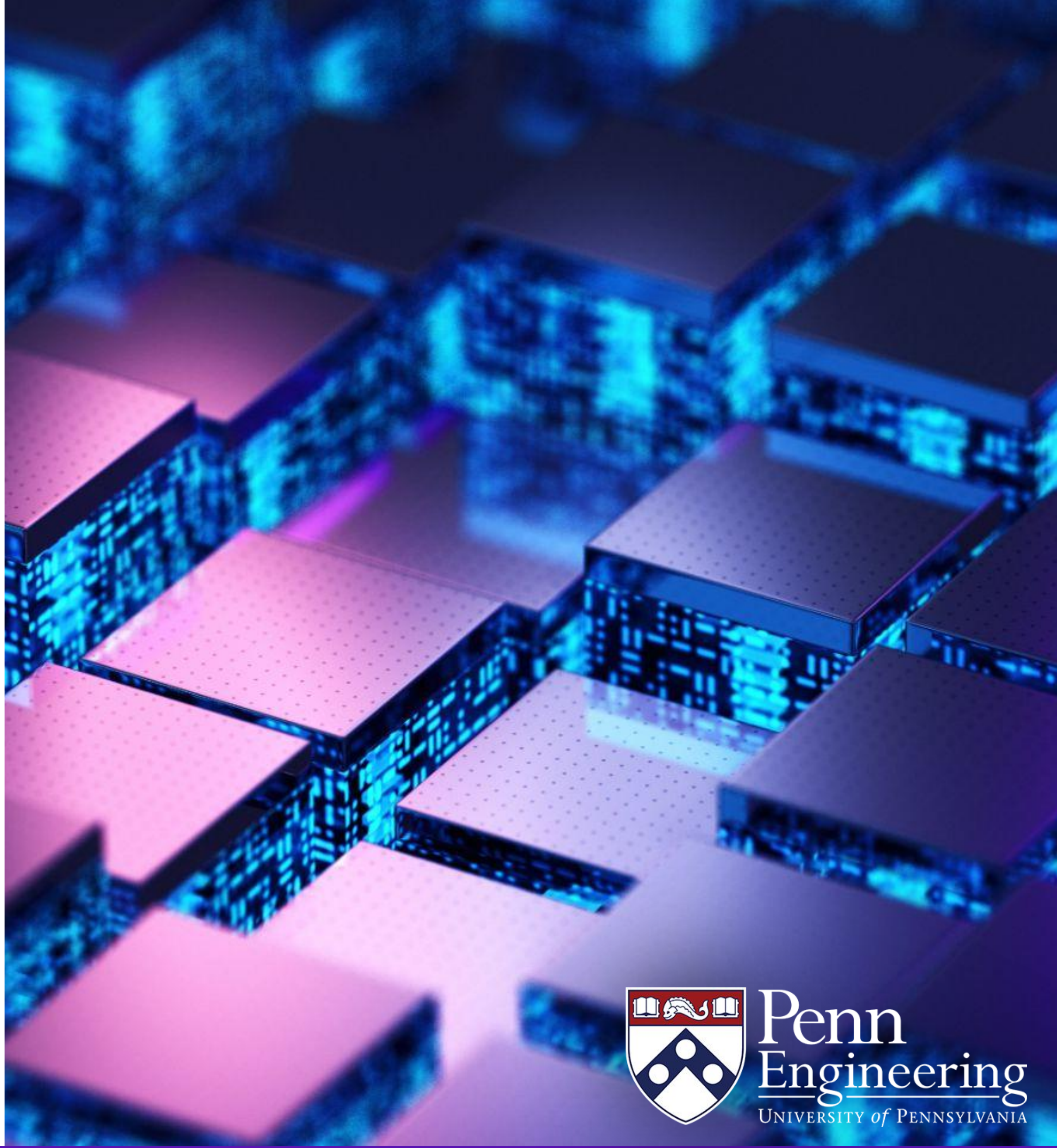
EAS 5830: BLOCKCHAINS

Uniswap v2

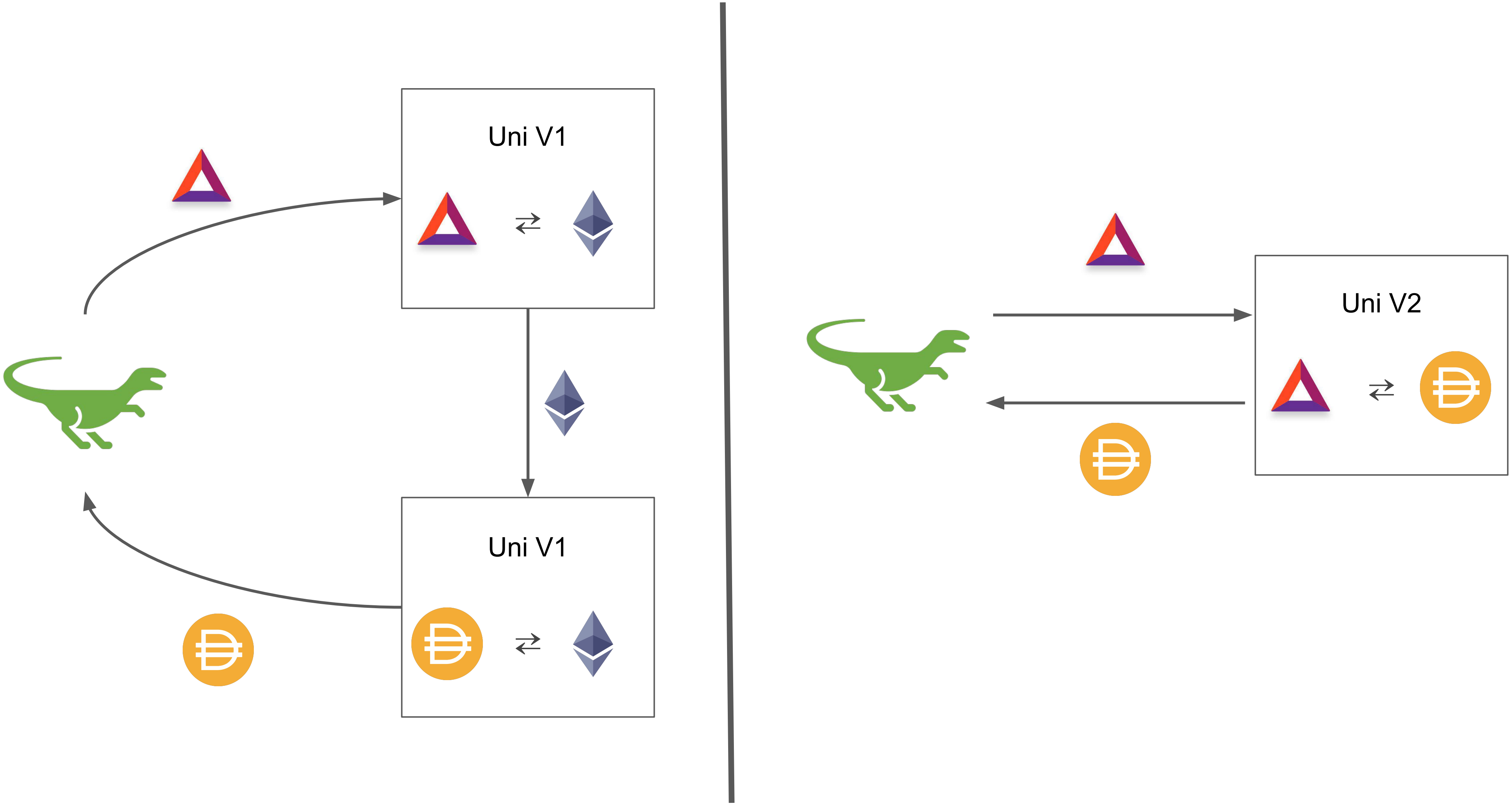
Professor Brett Hemenway Falk



Uniswap V2

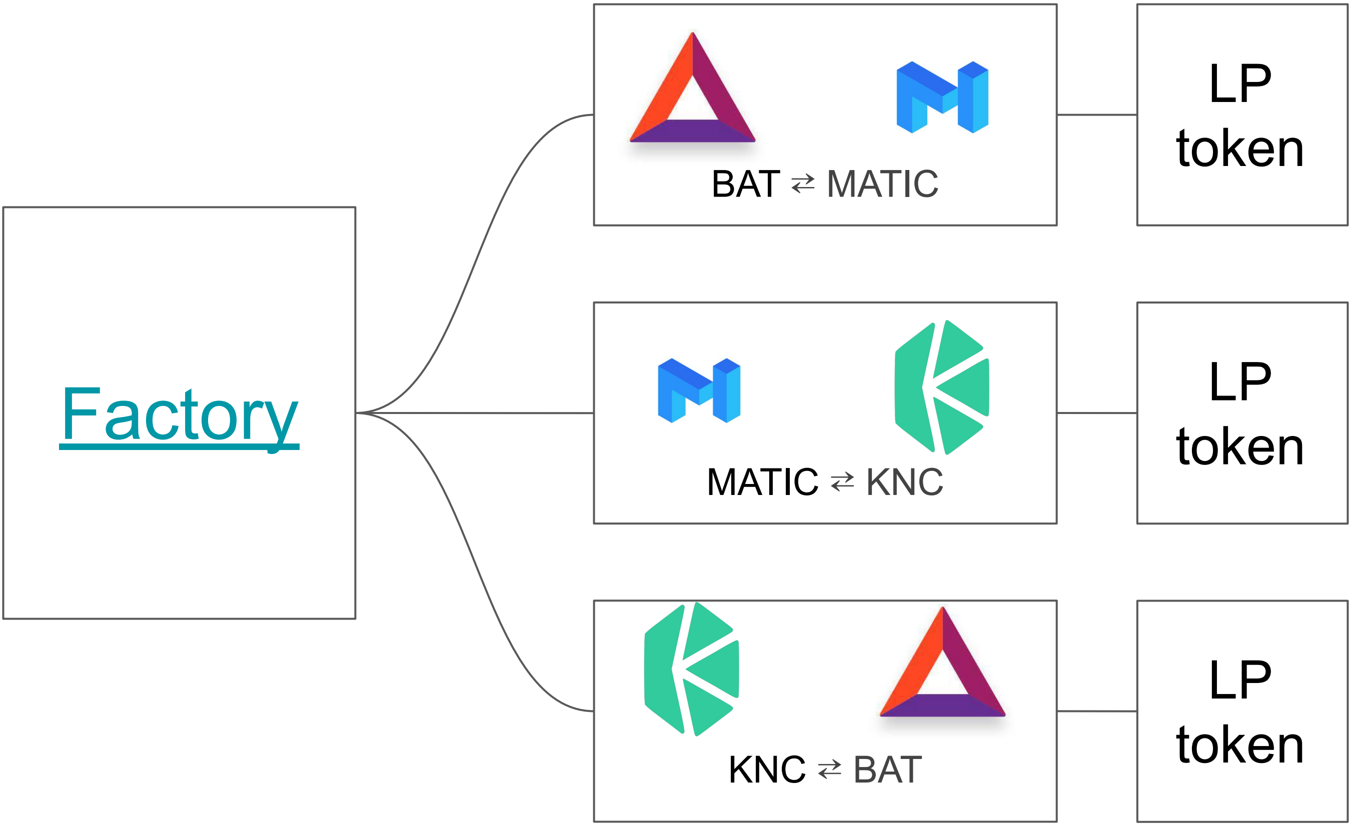
- Launched in 2020
- Exchanges trade ERC20 ⇄ ERC20
  - (not ETH / ERC20 as in Uniswap V1)
- Price Oracles
- Flash swaps

V2 has one exchange per pair



Uniswap V2 Architecture

- Trade ERC20 ⇄ ERC20
- One contract for each ERC20 Pair
- Factory creates / records exchange contracts
- Exchanges issue LP tokens to track balances
  - Exchange contract is also ERC20 contract for its own LP tokens



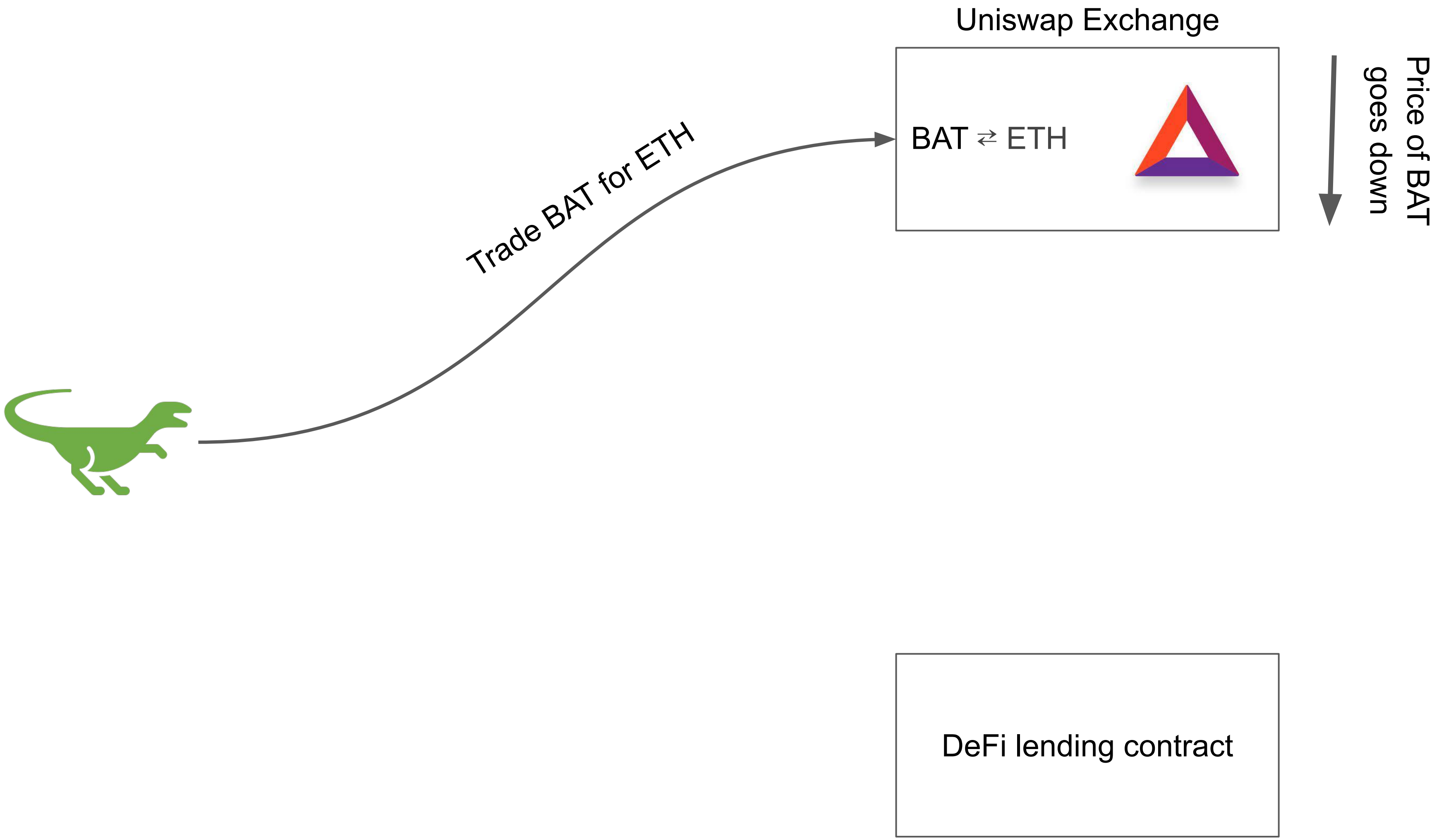
One exchange per pair

- ETH exposure
  - In V1 liquidity providers must have exposure to ETH
    - Risk of impermanent loss
  - In V2 liquidity providers can create pairs without holding ETH
- Reduced trading fees
  - In V1 trading ERC20 ⇄ ERC20 requires two steps
  - In V2 trading ERC20 ⇄ ERC20 requires one step
- Fragmented liquidity
  - More exchanges
    - ~50,000 Uniswap V2 exchanges
    - ~4,000 Uniswap V1 exchanges

Price Oracle

- Price discovery is the central role of a marketplace
- How can Uniswap make exchange rate data available to other contracts?
  - Current balances reflect exchange rate
  - Contracts can query Uniswap balances

Price oracle manipulation



Uniswap Exchange

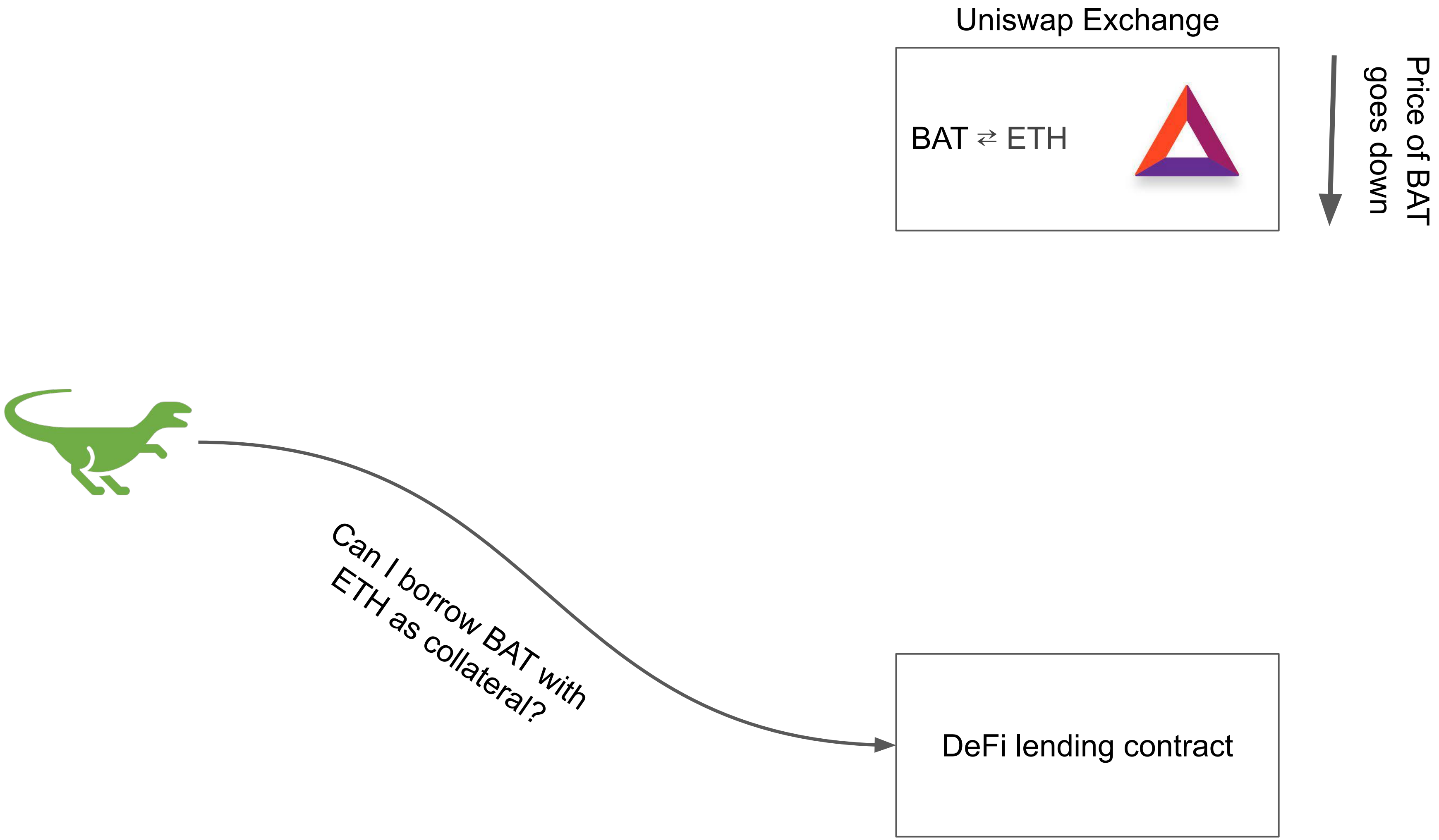
BAT ⇄ ETH

Price of BAT goes down

Trade BAT for ETH

DeFi lending contract

Price oracle manipulation



Uniswap Exchange

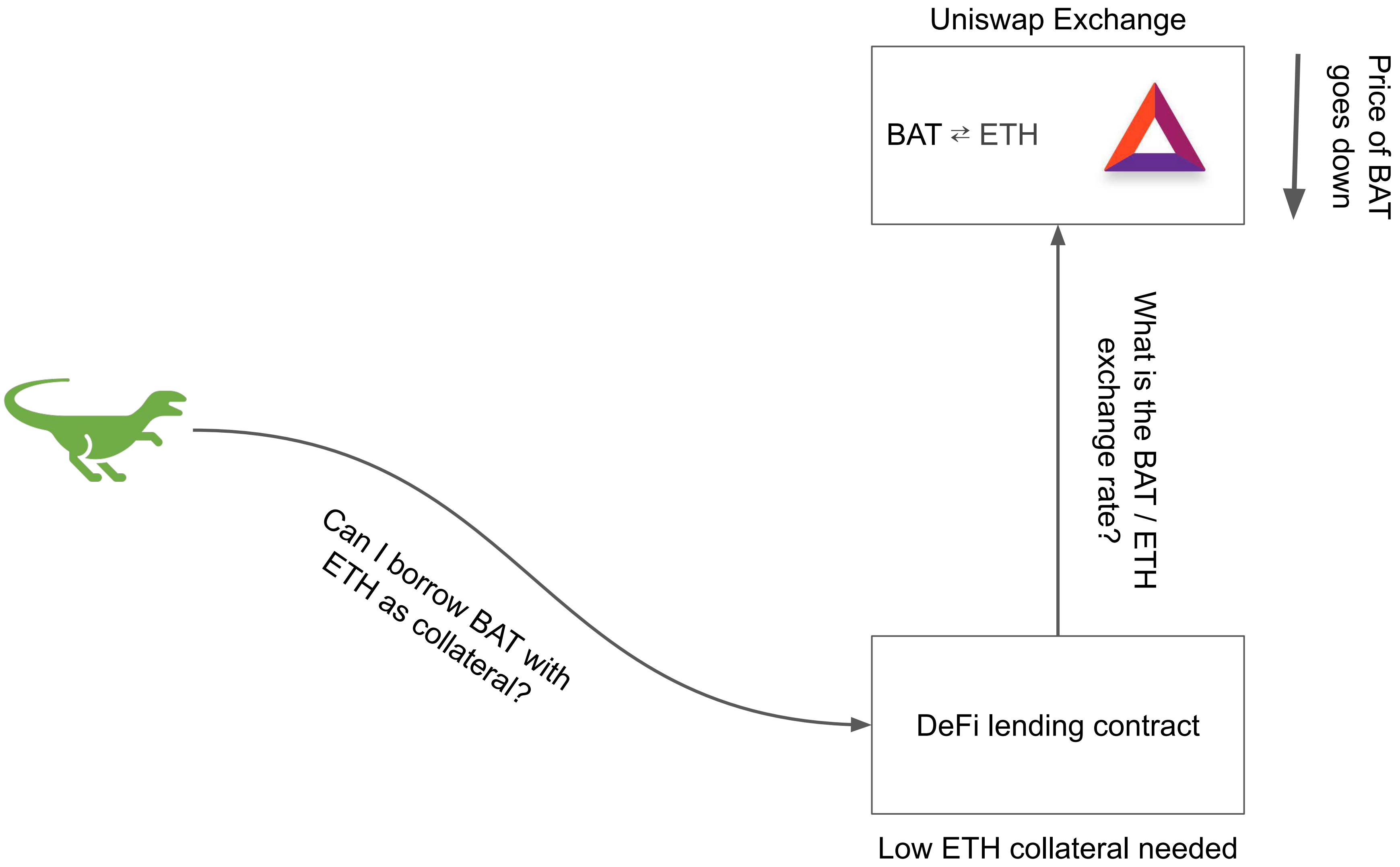
BAT ⇄ ETH

Price of BAT goes down

Can I borrow BAT with ETH as collateral?

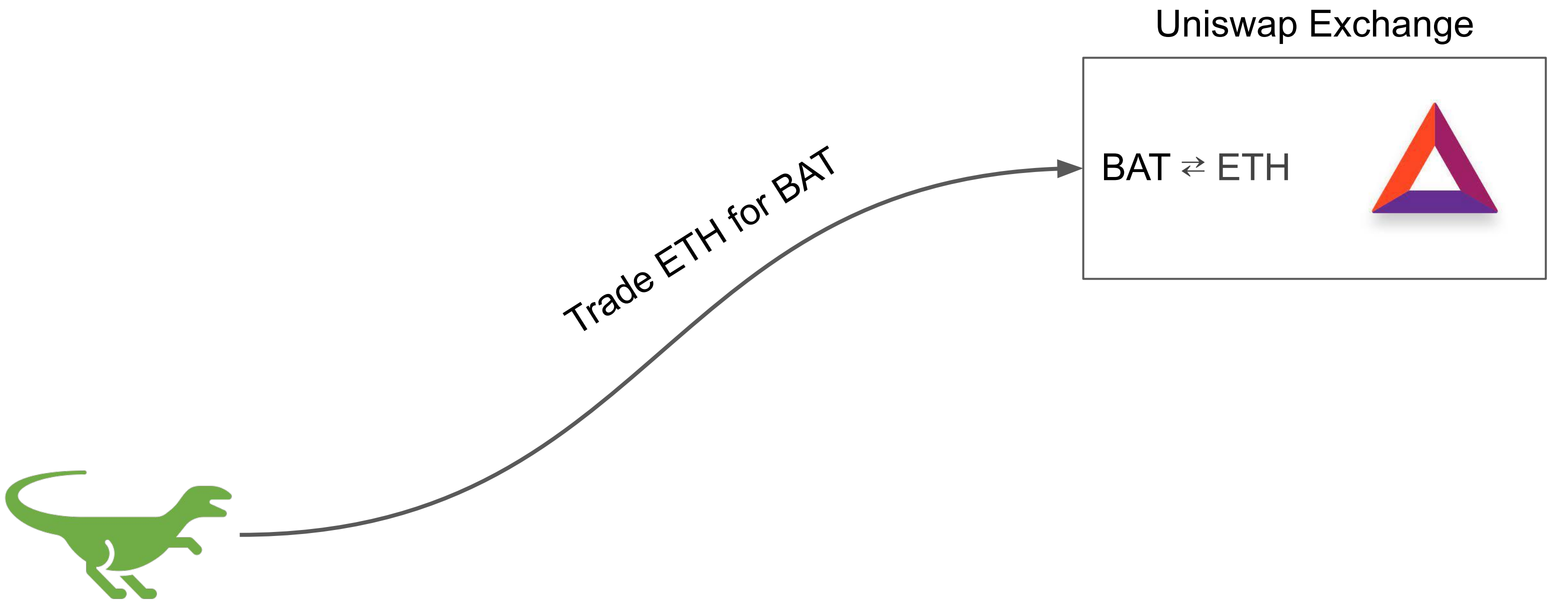
DeFi lending contract

Price oracle manipulation



Uniswap Exchange
BAT ⇄ ETH
Price of BAT goes down
What is the BAT / ETH exchange rate?
Can I borrow BAT with ETH as collateral?
DeFi lending contract
Low ETH collateral needed

Price oracle manipulation



- Obtained under-collateralized loan
- Entire sequence can happen in one transaction
- Default on loan and sell excess BAT on another (more liquid) market

The BZX Attack

- Feb 15, 2020
  - hackers use a flash loan to manipulate prices on Uniswap to steal 1,271 ETH from BZX
- May 17, 2020
  - Uniswap V2 is launched with better price oracle mechanism

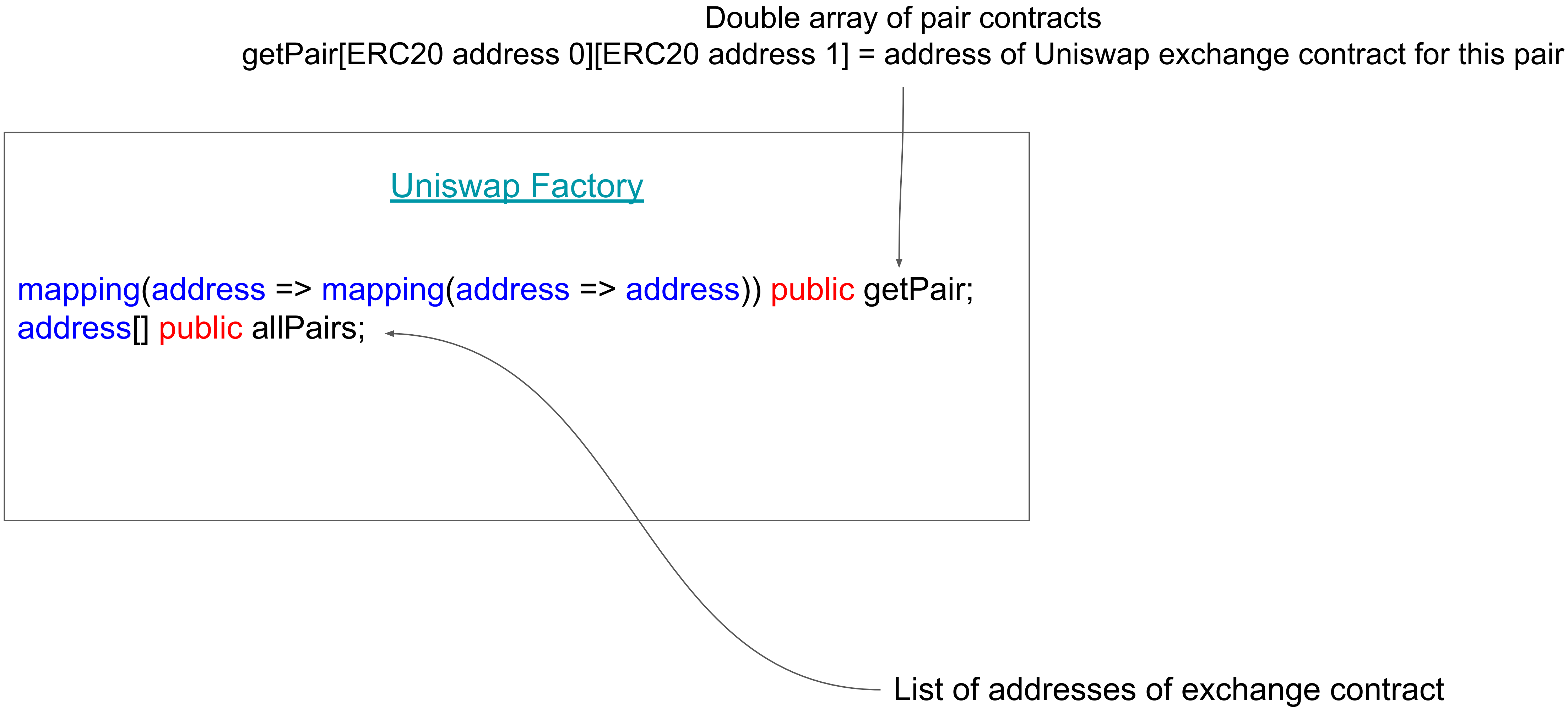
Avoiding Price Oracle Manipulation

- Have Uniswap report the price from the *last block*
- Manipulating price across block boundary is very risky
  - Transactions can’t span blocks, so you must separate transactions
  - If you drive the price of BAT down in one block another actor can buy BAT at this low price before you call the oracle
- For the first transaction in a block, Uniswap records the price
  - Uniswap also records the time since the last recorded price
  - This allows the contract to create Time-Weighted Average Price (TWAP) for any time interval

Flash Loans

- Users can “borrow” ERC20 token from Uniswap pair pools, as long as the loan is repaid in the same transaction

Uniswap V2 Factory Contract



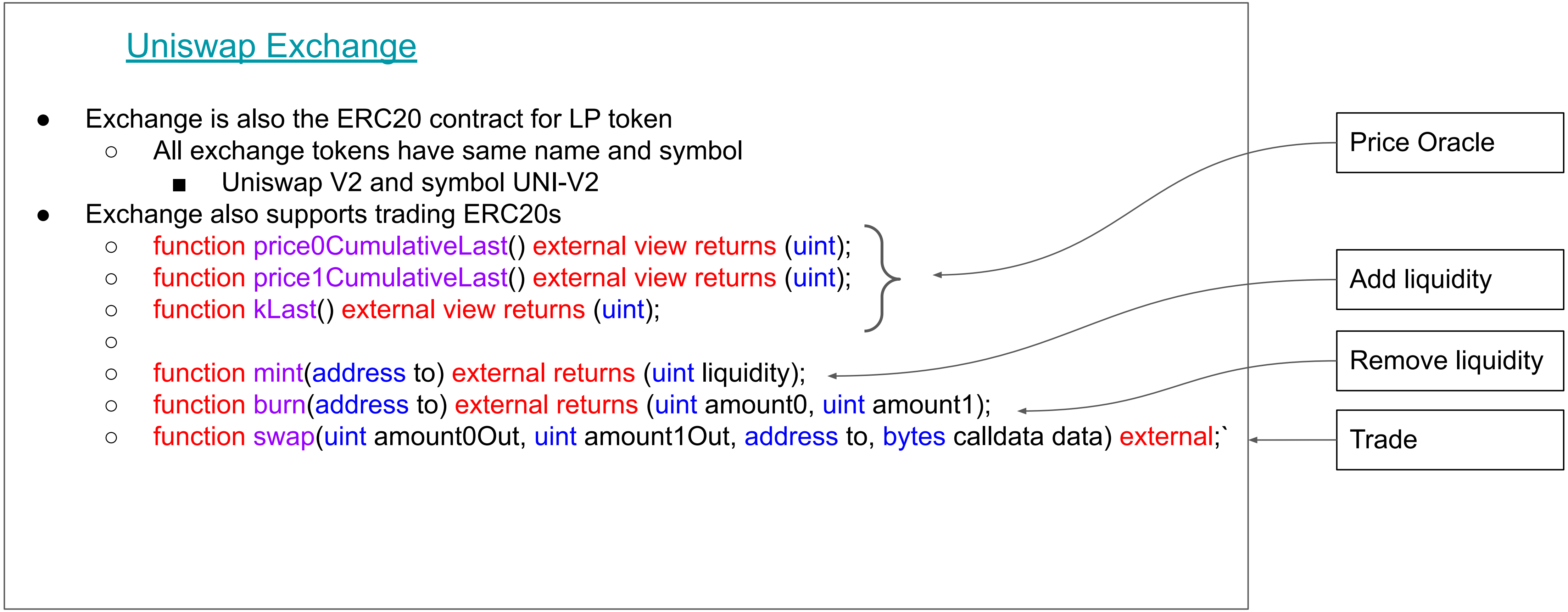
Double array of pair contracts
getPair[ERC20 address 0][ERC20 address 1] = address of Uniswap exchange contract for this pair

Uniswap Factory

```
mapping(address => mapping(address => address)) public getPair;
address[] public allPairs;
```

List of addresses of exchange contract

Uniswap V2 Exchange Contract



Uniswap Exchange

- Exchange is also the ERC20 contract for LP token
  - All exchange tokens have same name and symbol
    - Uniswap V2 and symbol UNI-V2
- Exchange also supports trading ERC20s
  - function price0CumulativeLast() external view returns (uint);
  - function price1CumulativeLast() external view returns (uint);
  - function kLast() external view returns (uint);
  -
  - function mint(address to) external returns (uint liquidity);
  - function burn(address to) external returns (uint amount0, uint amount1);
  - function swap(uint amount0Out, uint amount1Out, address to, bytes calldata data) external;`

Uniswap V2 Router

```
function addLiquidity( address tokenA, address tokenB, uint amountADesired, uint
amountBDesired, uint amountAMin, uint amountBMin, address to, uint deadline)
```

```
function swapExactTokensForTokens( uint amountIn, uint amountOutMin,
address[] calldata path, address to, uint deadline )
```

```
function swapTokensForExactTokens( uint amountOut, uint amountInMax,
address[] calldata path, address to, uint deadline )
```

Conclusion

- Uniswap v2 is still live and active on Ethereum
- The contracts are excellent examples of clean solidity programming
- Uniswap v2 Whitepaper