Blockchain Module

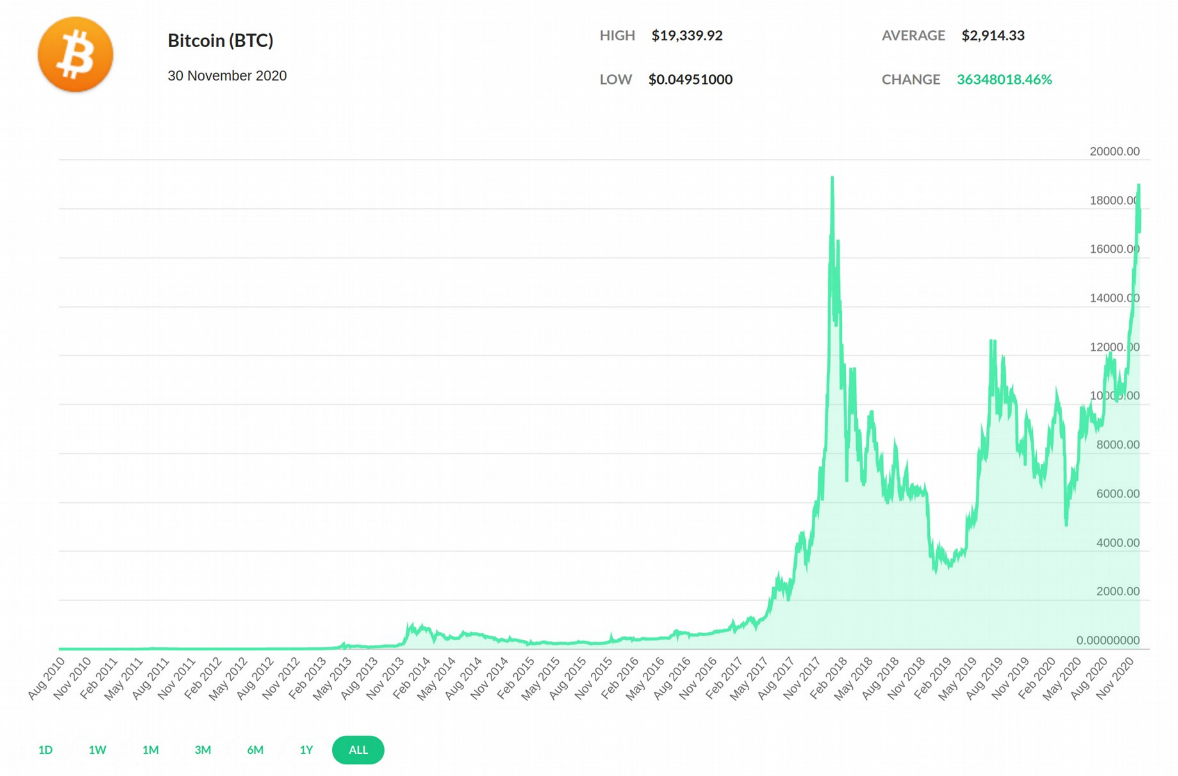
Current Usage of Blockchain

Speculation and Investment

- Vast majority of blockchain usage today is speculation
- 2017 rise was a retail phenomenon
- Current rise has more institutional investment (and manipulation)
  - Paypal *
  - Grayscale **
  - Square ***
  - Tether ****
- Driven partly by view that cryptocurrency is hedge against inflation, potentially large upside due to immaturity of market and low liquidity

* https://www.forbes.com/sites/billybambrough/2020/10/23/paypal-just-gave-346-million-people-a-new-way-to-buy-bitcoin-but-theres-a-nasty-catch/
** https://decrypt.co/resources/everything-you-need-to-know-about-the-grayscale-bitcoin-trust
*** https://www.cnbc.com/2020/10/08/square-buys-50-million-in-bitcoin-says-cryptocurrency-aligns-with-companys-purpose.html
**** https://amycastor.com/2020/11/21/are-pixie-fairies-behind-bitcoins-latest-bubble/

Speculation and Investment



Bitcoin (BTC)

30 November 2020

HIGH $19,339.92

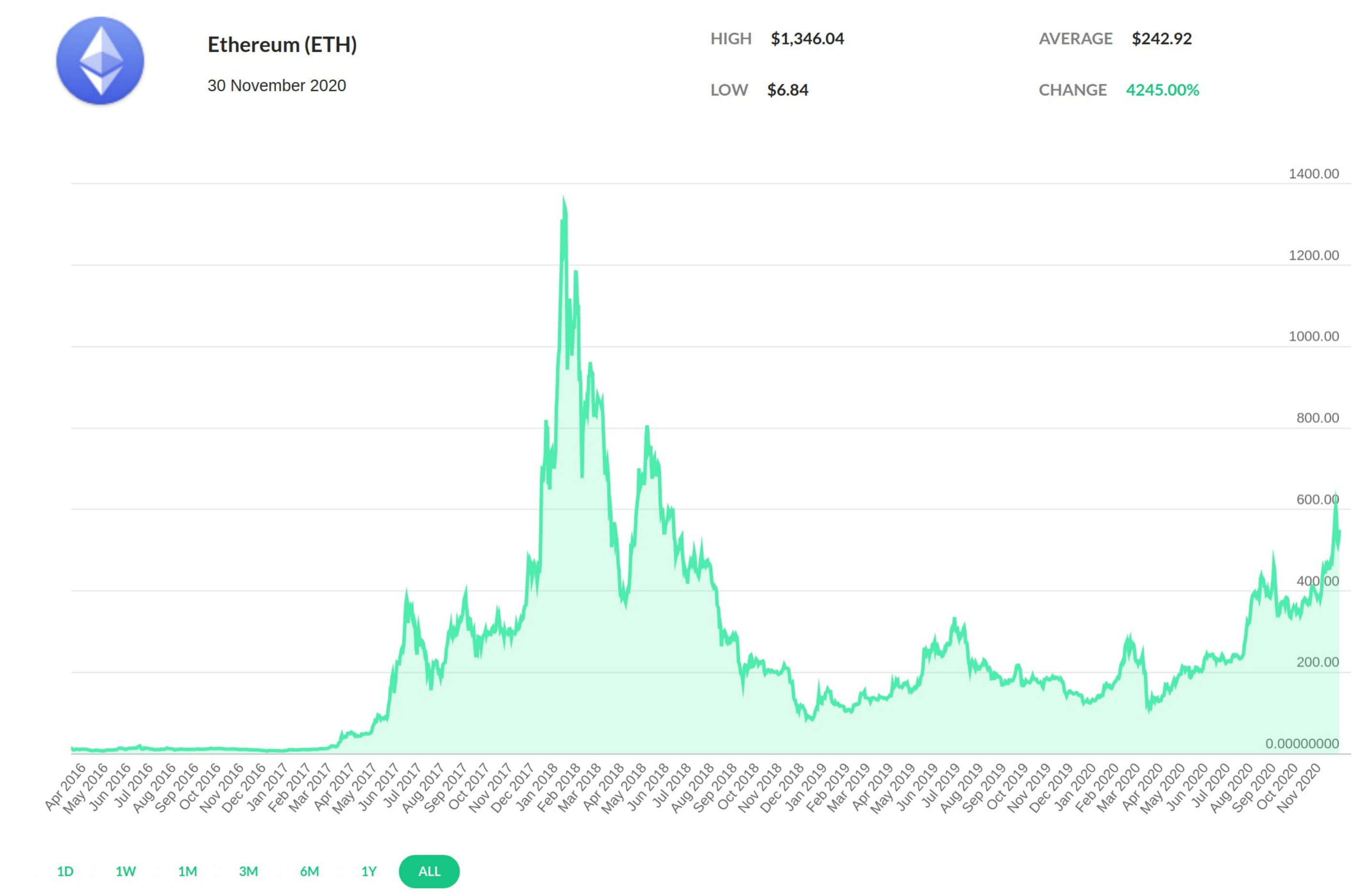
LOW $0.04951000

AVERAGE $2,914.33

CHANGE 36348018.46%

Source: coincap.io (30 Nov, 2020)

Speculation and Investment



Ethereum (ETH)

30 November 2020

HIGH $1,346.04

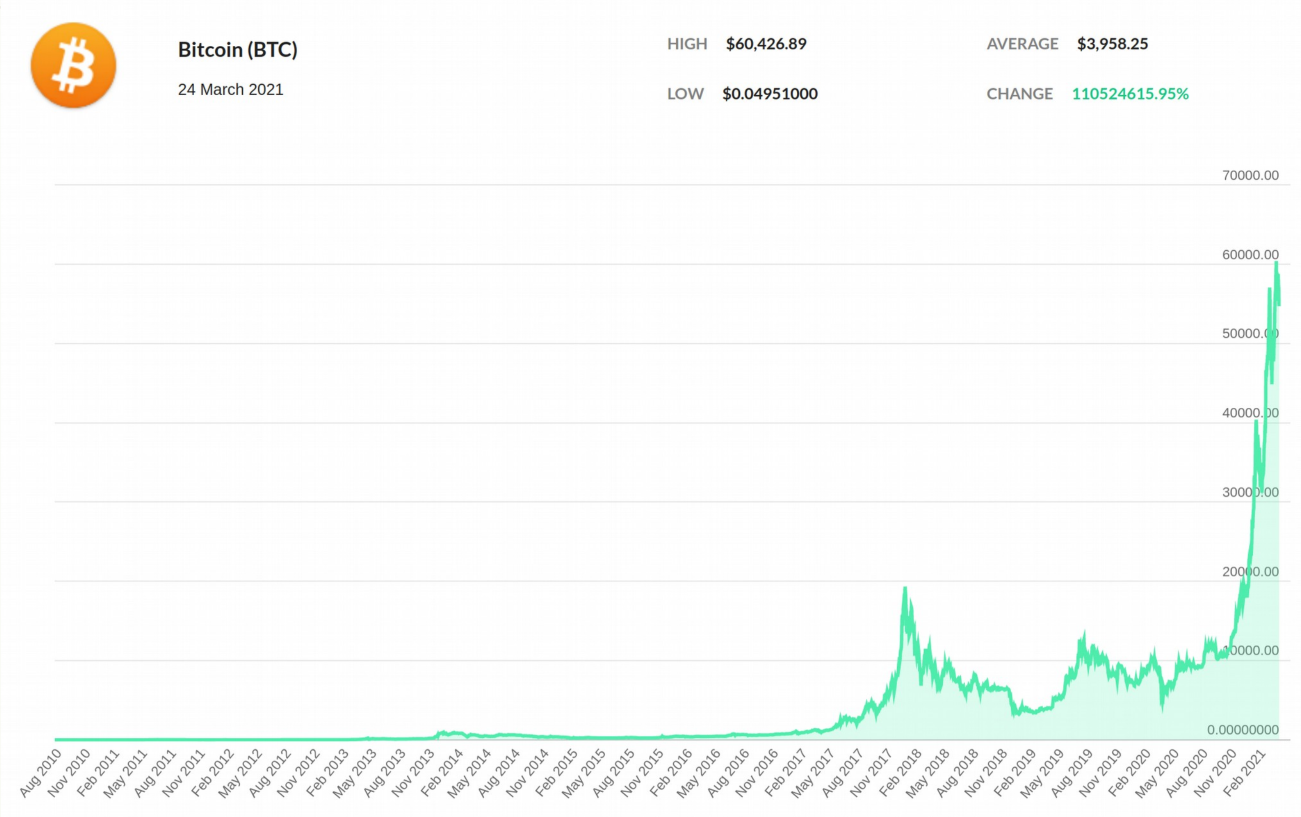
LOW $6.84

AVERAGE $242.92

CHANGE 4245.00%

Source: coincap.io (30 Nov, 2020)

Speculation and Investment



Bitcoin (BTC)

24 March 2021

HIGH $60,426.89

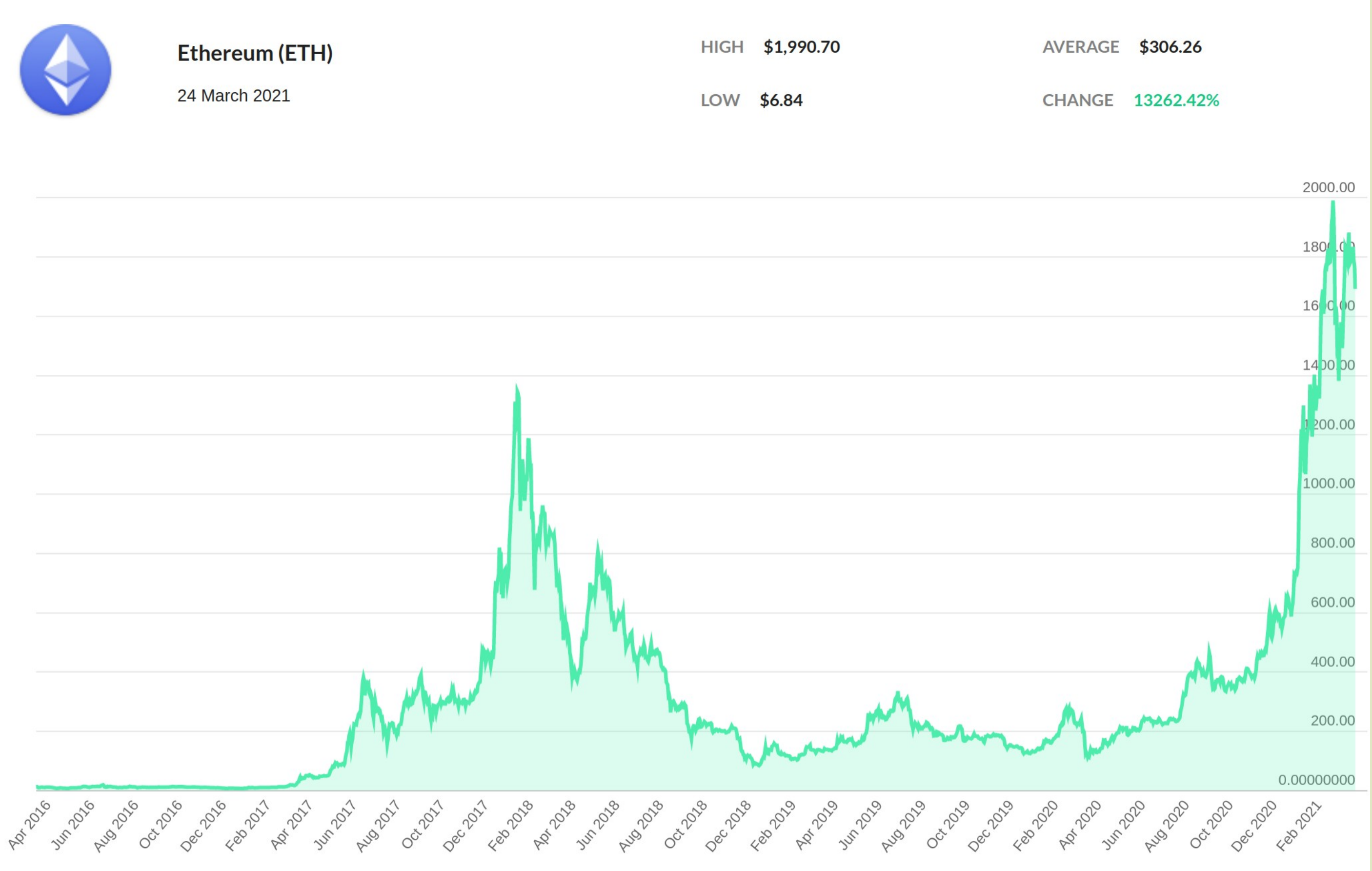
LOW $0.04951000

AVERAGE $3,958.25

CHANGE 110524615.95%

Source: coincap.io (24 Mar, 2021)

Speculation and Investment



Ethereum (ETH)

24 March 2021

HIGH **$1,990.70**

LOW **$6.84**

AVERAGE **$306.26**

CHANGE 13262.42%

Source: coincap.io (24 Mar, 2021)

What can you do with BTC

- Store it (HODLing) and wait for moon
- Sell it via OTC trades or through exchanges
- Wrap it (wBTC) and use it on Ethereum decentralised finance
- Use it as a medium of exchange in return for goods or services (rare)
- Use the chain as a timestamp record (opentimestamps)

What can you do with ETH

- Store it (HODLing) and wait for moon
- Sell it via OTC trades or through exchanges
- Use it as a medium of exchange in return for goods or services (rare)
- Use it on Ethereum decentralised finance
- Stake 32 ETH on the ETH 2.0 Beacon Chain and get 7-8% return

ETH Beacon Chain

- Proposed as Phase 0 for move to Proof of Stake
- In operation since Dec 2020 (required 16,384 validators to stake)
- 32 ETH stake deposited on ETH 1.0 chain smart contract
- Need to run ETH 2.0 validator client + ETH 1.0 chain
- Have separate validator key and withdrawal key
- As of Mar 2021 ETH beacon chain has ~111K validators

- If your validator is running, you get REWARDS
- If your validator is down, you get PENALTIES *(50% uptime to break even)*
- If you do nefarious things, you get SLASHED *(1/32 of your STAKE)*

ETH Beacon Chain

- 12-second SLOT where a random validator can propose a BLOCK
- A BLOCK can contain graffiti (‘*Mr F was here*’)
- A SLOT might not contain a BLOCK!
- BLOCK is signed by 128 other random validators (COMMITTEE)
- 2/3 of COMMITTEE must sign to validate BLOCK
- 32 BLOCKS are aggregated into EPOCHs
- EPOCHS are signed by all validators (66% required)
- (TLDR: complex COMMITTEE splitting per BLOCK in EPOCH)
- See https://beaconcha.in/ for live stats

https://ethos.dev/beacon-chain/

ETH Beacon Chain & BLS

- With 111K validators, each EPOCH might have 111K signatures?
- @ 64 bytes per signature, that would be ~ 7MB per EPOCH
- But no, each epoch only has a single signature
- It is a BLS signature (BLS12_381)
- BLS signatures have a cool superpower:
  - M BLS signatures can be aggregated into a single BLS signature
  - This signature can be validated if all M public keys are provided
  - BLS also have a threshold signature scheme where you can validate that N of M of the public keys signed the message

https://www.youtube.com/watch?v=DpV0Hh9YajU

Decentralised Finance

- **Tokens**
  - ICO (fund raising)
  - Governance Token (voting)
  - Liquidity Rewards
  - Utility Tokens
  - Stablecoins
  - Enterprise Tokens (for interaction with mainnet)

Decentralised Finance

- **Yield Farming**
  - Providing liquidity in return for rewards
  - Rewards can be used to provide liquidity
  - Obtaining more rewards
  - Chance to obtain tokens early and hope for moon
  - Examples: Compound, Aave, Yearn Finance

    (30 Nov 2020): YFI 783M, AAVE 853M, COMP 456M
  -

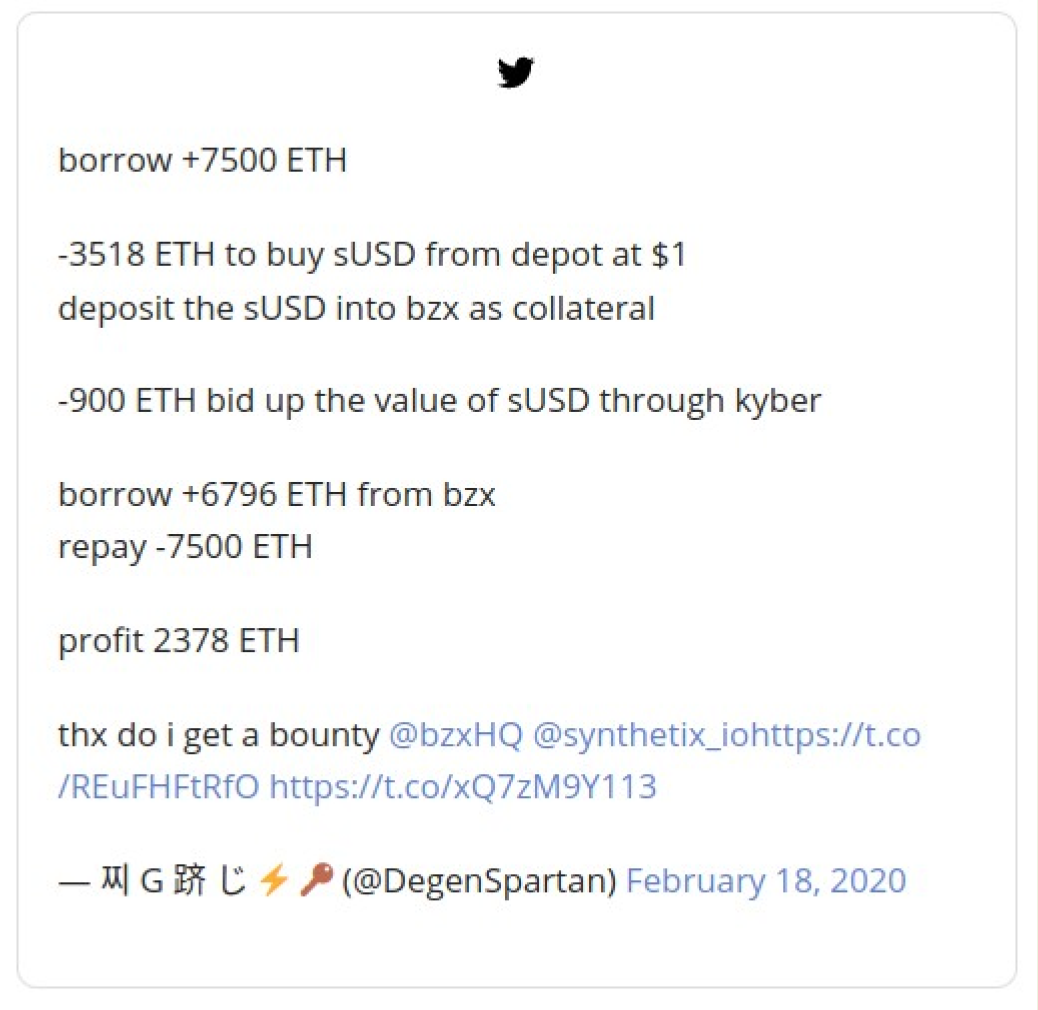
* https://decrypt.co/resources/what-is-yield-farming-beginners-guide

Decentralised Finance

- **Flash Loans**
  - A loan that is taken out and repaid in the same block, meaning the borrower only pays gas for the transaction.
  - Used to provide more collateral for defi actions
  - If the downstream transactions fail, the loan never occurred

* https://blog.coincodecap.com/what-are-flash-loans-on-ethereum

Decentralised Finance



borrow +7500 ETH

-3518 ETH to buy sUSD from depot at $1
deposit the sUSD into bzx as collateral

-900 ETH bid up the value of sUSD through kyber

borrow +6796 ETH from bzx
repay -7500 ETH

profit 2378 ETH

thx do i get a bounty @bzxHQ @synthetix_iohttps://t.co/REuFHFtRfO https://t.co/xQ7zM9Y113

— 찌 G 跻 じ ⚡🔑 (@DegenSpartan) February 18, 2020

Decentralised Finance

- **Oracles**
  - Provide a feed of real-world data to blockchain
  - e.g. ETH USD price
  - Used by MakerDao to stabilise the price of DAI
    - If the ETH/USD rate goes down, loans that are no longer sufficiently collateralised are liquididated
    - If the ETH/USD rate goes up, additional DAI can be withdrawn from collateralised loan
  - Useful for prediction markets (who won the election?)

* https://ethereum.org/en/developers/docs/oracles/

Decentralised Finance

- **Governance Tokens**
  - Governance of protocols driven by voting with blocks of tokens
  - Key component of decentralised governance
  - e.g. Uniswap

* https://uniswap.org/blog/uni/

Decentralised Finance

- **Stablecoins**
  - Non-volatile (ish) tokens pegged to a fiat currency (USD)
    - e.g. DAI, USDC, USDT
  - DAI is algorithmic, smart contract operated based on collateralised loans
  - USDC is based on bank deposits
  - USDT is also based on bank deposits *(allegedly)*

[*] https://uniswap.org/blog/uni/

Decentralised Finance

- **Uniswap vs Sushiswap**
  - Copied Uniswap code
  - Offered Sushi token for providing liquidity on Sushiswap
  - Created by pseudonymous Chef Nomi
  - Who sold all his Sushi
  - And then bought it back
  - And then Uniswap released UNI, airdropping to Uniswap LPs for free
  - SUSHI (225M), Uniswap (800M) as of 30 Nov 2020
  - Update: SUSHI (2B), UNI (15B) as of 24 Mar 2021

* https://uniswap.org/blog/uni/