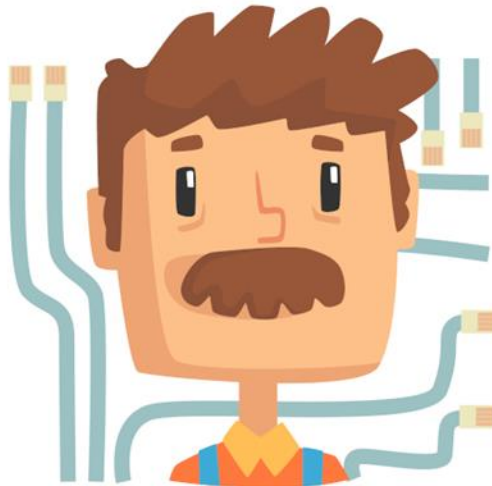


Gawęda o kryptowalutach część trzecia



Gawędę sponsoruje słowo „uproszczenie”

**Nie kupuj kryptowalut mając
tylko wiedzę z tej prelekcji.
Ucz się i ćwicz na małych
kwotach! Używaj testnetu!**

Did I just lose half a million dollars by sending WETH to WETH's contract address?

3,427 points • 2,085 comments • submitted 20 hours ago * (last edited<\$>lastedited</\$>) by basubadelmevt to r/ethereum 🐼 2 🏆 3 🙏 5 🌶️ 2 & 81 more

Please tell me that I didn't :(

<https://etherscan.io/tx/0x96a7155b44b77c173e7c534ae1ceca536ba2ce534012ff844cf8c1737bc54921>^[1]

Edit: Full story. Sent ETH to WETH contract and got WETH back (after some googling I found this is how the contract works). Assumed it works the same way backwards and sent WETH back to the contract. No ETH back. Apparently you have to use a frontend to get the ETH back. ETH lost forever.

Edit 2: Thanks strangers. I am really happy to see lots of kind hearted people in the comments and chat. This is a significant amount of money for anyone to lose and it was the case for me as well. I was under the stress of some other things in my life and made a bigger mistake by making assumptions in this wild early technology. But, I will be OK.

Edit 3: I am also sorry that this was a negative event for the perception of cryptocurrencies. The last thing I would want in this world :(A life-changing lesson for me, but definitely something to work on as a community as well.

Krótkie przypomnienie

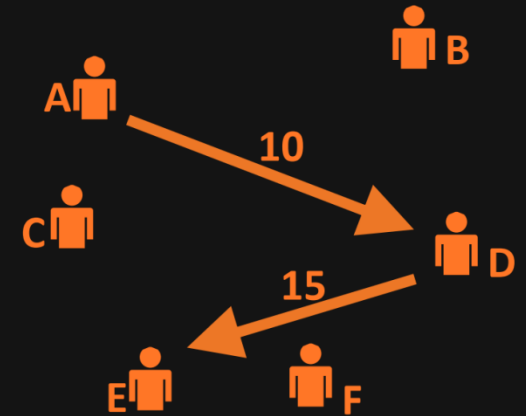
części 1

Składniki Bitcoina

1. Rozproszony rejestr kryptografia, P2P

A → D, 10
D → E, 15
... → ..., ...
... → ..., ...
... → ..., ...

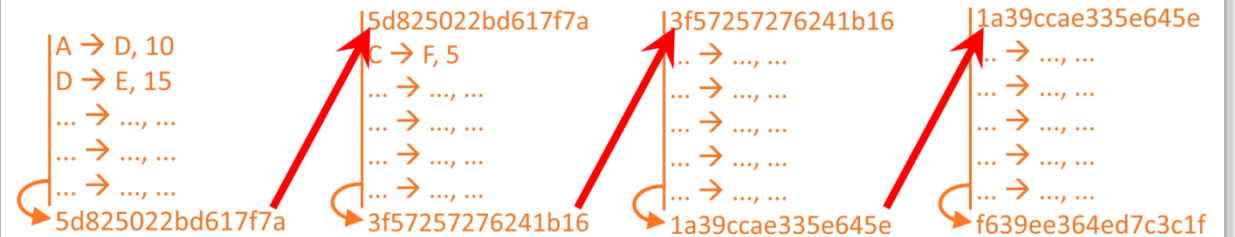
Rejestr pożyczek



Grupa znajomych

Składniki Bitcoina

1. Rozproszony rejestr
2. Blockchain
zapobieganie fałszerstwom



Składniki Bitcoina

1. Rozproszony rejestr
2. Blockchain
3. Generowanie jednostek kryptowaluty
limitowana podaż itp.

900 tys. zł



Składniki Bitcoina

1. Rozproszony rejestr
2. Blockchain
3. Generowanie jednostek kryptowaluty

oraz: konsensus, regulacja trudności, kryptografia klucza publicznego itd.

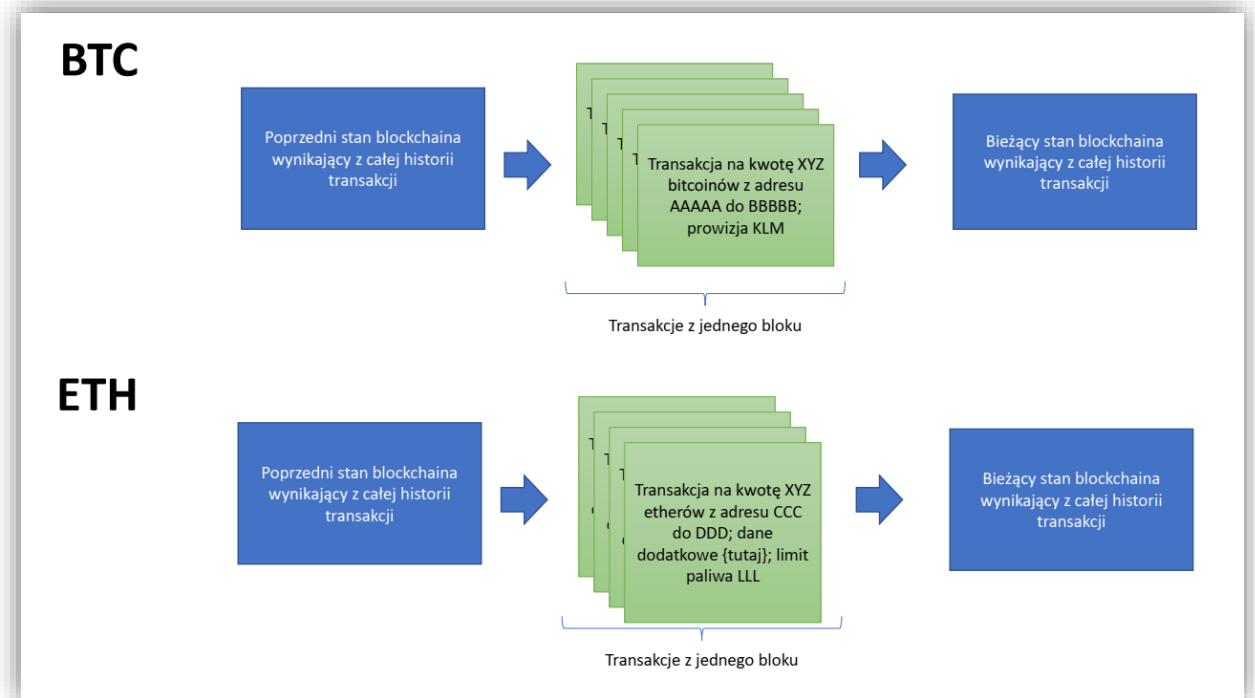


Krótkie przypomnienie

części 2

Składniki Ethereum

1. W blockchainie Ethereum możemy rejestrować nie tylko przelewy, ale dowolne dane



Składniki Ethereum

1. W blockchainie Ethereum możemy rejestrować nie tylko przelewy, ale dowolne dane
2. Możemy też publikować w blockchainie programy, aktywowane przelewem na konto programu

Smart contract

- Żeby uruchomić program w rozproszonym komputerze, musimy go w osobnej transakcji rozesłać do całej sieci ETH
- Programy to **kontrakty**
- **Kontrakt** jest tworzony przez transakcję pokrywającą koszt zapisania go w blockchainie
- Każdy kontrakt dostaje unikalny **adres publiczny**



```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.4.16 <0.9.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

Składniki Ethereum

1. W blockchainie Ethereum możemy rejestrować nie tylko przelewy, ale dowolne dane
2. Możemy też publikować w blockchainie programy, aktywowane przelewem na konto programu
3. Mamy rozproszony komputer: obliczenia są deterministyczne, wyniki zapisane w blockchainie i chronione przez konsensus

Czym są kontrakty w sieci Ethereum?

Przykłady za chwilę

- Kontrakt to taki automat, który będzie coś robił tylko, gdy będzie adresatem transakcji (nadanej przez człowieka) lub wiadomości (praktycznie to samo, ale nadanej przez inny kontrakt)
- Kontrakt ma dostęp do historii blockchajna i prawie niczego innego (żadnych plików, sieci, urządzeń – tylko blockchain i dane z transakcji)
- Kontrakt jest umieszczany w blockchainie raz na zawsze, nie da się zmienić jego działania (możliwe jest samozniszczenie, z bonusem!)
- Ale można zrobić kontrakt z dynamicznym przekierowaniem

Część trzecia

- Dwa słowa o wydajności Ethereum
- Co to są tokeny
- Co to jest ICO
- Co to jest NFT
- Co to jest Proof of Stake (oraz Space)
- Inne częste pytania

slido.com
#76766



Wydajność Ethereum VM

„Any given block of the Ethereum blockchain represents a maximum amount of execution, currently 30 million gas. And the system adds a new block every 15 seconds, which means the total compute of the Ethereum network as 2 million gas/second, since that is the amount of computation that gets recorded into the Ethereum ledger.

Estimating the cost (measured in ‘gas’) of an arbitrary computation is complex but let’s assume that we are only interested in the most simple operation: 256 bit integer addition. Each addition costs 3 gas each. So on a worldwide basis this system rates at 600,000 adds per second.”

<https://www.usenix.org/publications/loginonline/web3-fraud>

Wydajność Ethereum VM

„Any given block of the Ethereum blockchain represents a maximum amount of execution, currently 30 million gas. And the system adds a new block every 15 seconds, which means the total compute of the Ethereum network is 2 million gas/second. This is the amount of computation that gets recorded into the Ethereum ledger.

Estimating the cost (measured in ‘gas’) of any arbitrary computation is complex but let’s assume that the gas used by the most simple operation: 256 bit integer addition. Each addition costs 3 gas each. So on a worldwide basis this system rates at 600,000 adds per second.”

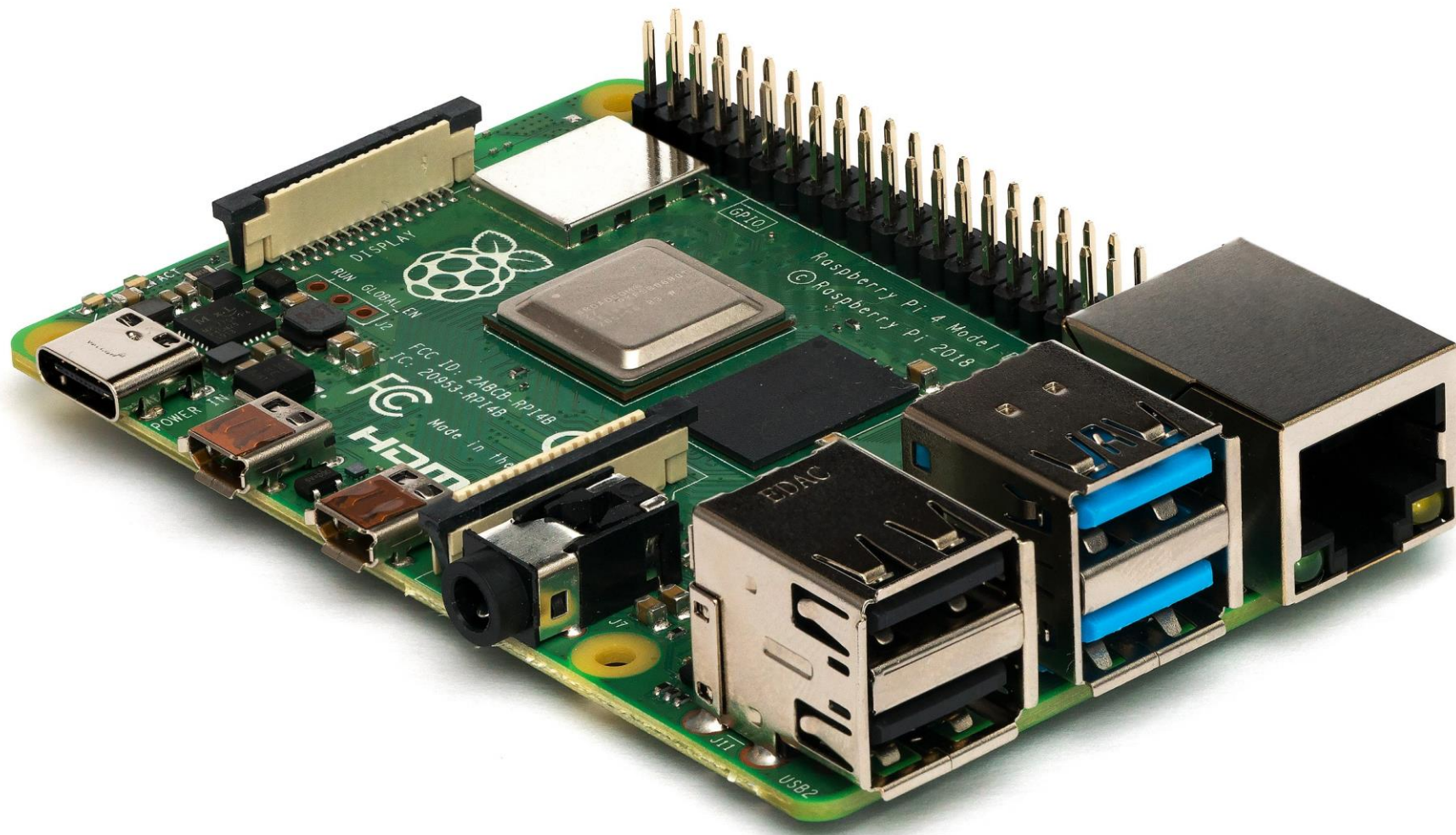
<https://www.usenix.org/publications/loginonline/web3-fraud>

Wydajność Ethereum VM

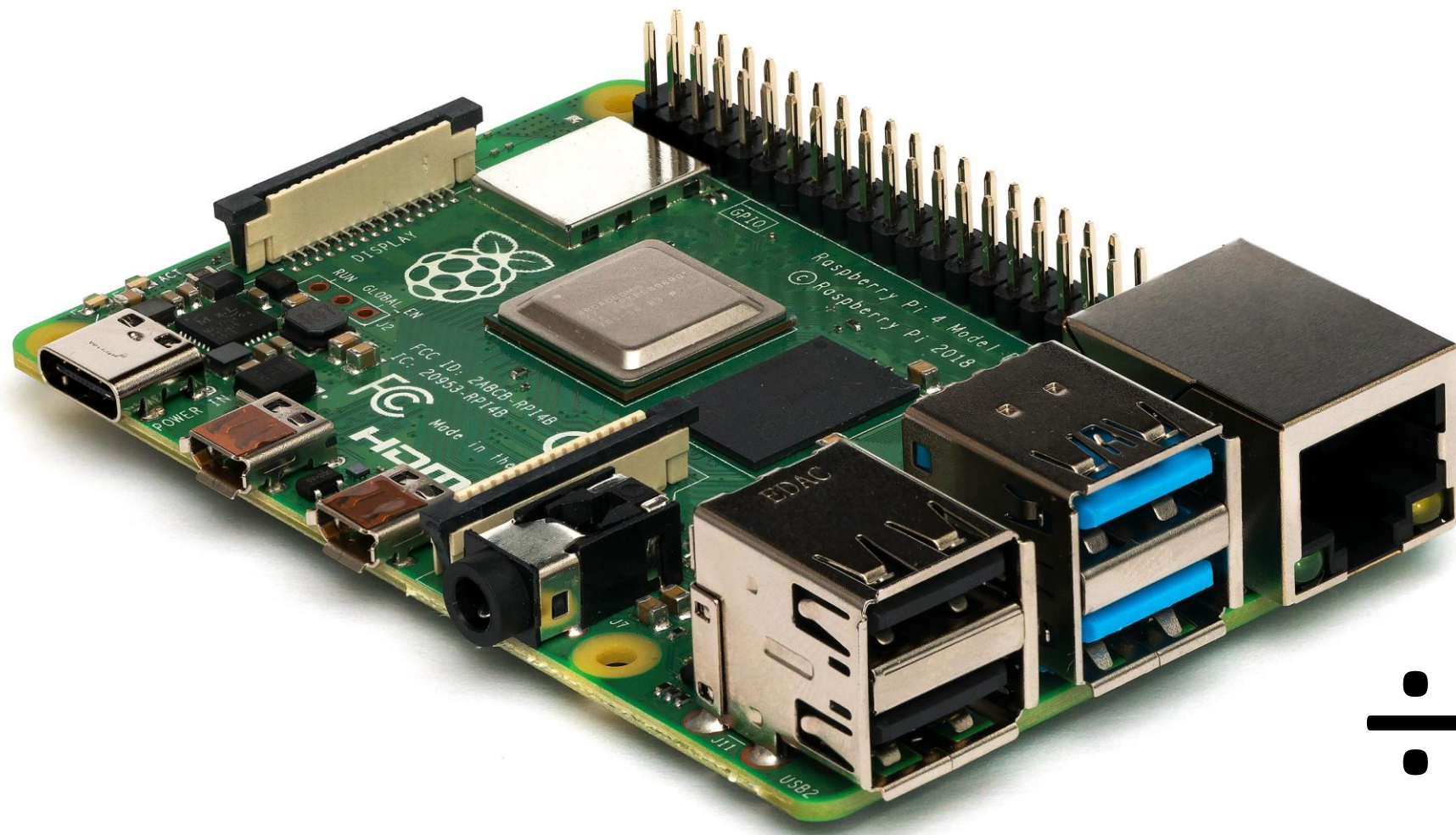


x 20

Wydajność Ethereum VM



Wydajność Ethereum VM



÷ 5000

Część trzecia

- Dwa słowa o wydajności Ethereum
- Co to są tokeny
- Co to jest ICO
- Co to jest NFT
- Co to jest Proof of Stake (oraz Space)
- Inne częste pytania

slido.com
#76766



Tokeny

na razie nie chodzi o NFT, cierpliwości!

slido.com

#76766



Dygresja

- Wyobraźmy sobie automat z autografami
- Wrzucasz 2 x 100 zł
- Automat wypłuka 1 x 100 zł, ale zwrócona stułotówka ma odręczny autograf Supergwiazdy
- Autograf jest warty 100 zł



Dygresja



- Wyobraźmy sobie automat z autografami
- Wrzucasz 2 x 100 zł
- Automat wypłaca 1 x 100 zł, ale zwrócona stułotówka ma odręczny autograf Supergwiazdy
- Liczba autografów jest ograniczona do 100 a Supergwiazda umiera
- Autograf jest wart ~~100 zł~~ 100000 zł

Dygresja



- Wyobraźmy sobie automat z autografami
- Wrzucasz 2 x 100 zł
- Automat wypłuka 1 x 100 zł, ale zwrócona stużłotówka ma odręczny autograf Supergwiazdy
- **Liczba autografów jest ograniczona do 100 a Supergwiazda umiera**
- Autograf jest warty ~~100 zł~~ **nie wiadomo ile milionów zł**
- **Wartość autografu jest oderwana od wartości banknotu**
- **Autografem można zapłacić za rzeczy niedostępne za złotówki**

Tokeny

- Kontrakty w sieci Ethereum mogą zapisywać dane w blockchainie
- Kontrakt wie, z jakiego adresu pochodzą środki, które go aktywowały

Tokeny

- Kontrakty w sieci Ethereum mogą zapisywać dane w blockchainie
- Kontrakt wie, z jakiego adresu pochodzą środki, które go aktywowały
- Kontrakt może zapisywać sobie informację, ile dziesiątek ETH wpłynęło z danego adresu.
- Nazwijmy tę nową jednostkę „TomekToken”. 10 ETH to 1 TomekToken.

Tokeny

- Kontrakty w sieci Ethereum mogą zapisywać dane w blockchainie
- Kontrakt wie, z jakiego adresu pochodzą środki, które go aktywowały
- Kontrakt może zapisywać sobie informację, ile dziesiątek ETH wpłynęło z danego adresu.
- Nazwijmy tę nową jednostkę „TomekToken”. 10 ETH to 1 TomekToken.
- Zróbmy dodatkową funkcję do przelewania TomekTokenów.

Tokeny

- Kontrakty w sieci Ethereum mogą zapisywać dane w blockchainie
- Kontrakt wie, z jakiego adresu pochodzą środki, które go aktywowały
- Kontrakt może zapisywać sobie informację, ile dziesiątek ETH wpłynęło z danego adresu.
- Nazwijmy tę nową jednostkę „TomekToken”. 10 ETH to 1 TomekToken.
- Zróbmy dodatkową funkcję do przelewania TomekTokenów.

To już prawie Bitcoin! Jest kreacja tokenów, są przelewy między portfelami

Tokeny – przykład uproszczony

- Podczas tworzenia kontraktu definiujemy, ile tokenów należy do twórcy kontraktu.
- Oprócz tego mamy tylko funkcję do przelewania tokenów.

Tokeny – przykład uproszczony

- Podczas tworzenia kontraktu definiujemy, ile tokenów należy do twórcy kontraktu.
- Oprócz tego mamy tylko funkcję do przelewania tokenów.
- Spostrzeżenie 1: takich tokenów nigdy nie przybędzie.
- Spostrzeżenie 2: tokenów nigdy nie ubędzie, ale można je „spalić” przelewając je na losowy adres.

```
contract MyBitcoin {

    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyBitcoin(uint256 initialSupply) public {
        balanceOf[msg.sender] = initialSupply;
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) public {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                     // Subtract from the sender
        balanceOf[_to] += _value;                             // Add the same to the recipient
    }
}
```

```
contract MyBitcoin {
```

```
/* This creates an array with all balances */  
mapping (address => uint256) public balanceOf;
```

Tutaj jest rejestr stanu tokenów
na poszczególnych adresach

```
/* Initializes contract with initial supply tokens to the creator of the contract */  
function MyBitcoin(uint256 initialSupply) public {  
    balanceOf[msg.sender] = initialSupply;  
}
```

Utworzenie Smart Kontraktu, założyciel
dostaje wszystkie tokeny

```
/* Send coins */  
function transfer(address _to, uint256 _value) public {  
    require(balanceOf[msg.sender] >= _value); // Check if the sender has enough  
    require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows  
    balanceOf[msg.sender] -= _value; // Subtract from the sender  
    balanceOf[_to] += _value; // Add the same to the recipient  
}
```

Każdy posiadacz tokenów może
przekazywać je na inne adresy

```
}
```


Tokeny w blockchainie Ethereum ERC-20

- kryptowaluta ETH to tylko „papier” na którym „wydrukowano” rejestr tokenów
- wartość tokenów nie musi mieć związku z wartością ETH
- wszystkie dane o posiadaczach tokenów „pamięta” kontrakt

```
contract MyBitcoin {  
  
    /* This creates an array with all balances */  
    mapping (address => uint256) public balanceOf;  
  
    /* Initializes contract with initial supply tokens to the creator of the contract */  
    function MyBitcoin(uint256 initialSupply) public {  
        balanceOf[msg.sender] = initialSupply;  
    }  
  
    /* Send coins */  
    function transfer(address _to, uint256 _value) public {  
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough  
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows  
        balanceOf[msg.sender] -= _value;                     // Subtract from the sender  
        balanceOf[_to] += _value;                             // Add the same to the recipient  
    }  
}
```

Także inne blockchaine,
np. Binance Smart Chain

ICO

Initial Coin Offering

slido.com

#76766



Initial Coin Offering

- Pomysł na finansowanie startupu

Initial Coin Offering

- Pomysł na finansowanie startupu
- Inwestorzy wpłacają ETH, dostają tokeny

Initial Coin Offering

- Pomysł na finansowanie startupu
- Inwestorzy wpłacają ETH, dostają tokeny
-
- Pojawia się popyt na tokeny

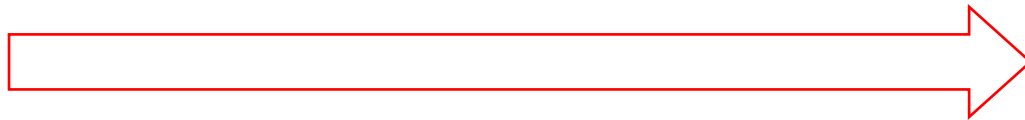
Initial Coin Offering

- Pomysł na finansowanie startupu
- Inwestorzy wpłacają ETH, dostają tokeny
-
- Pojawia się popyt na tokeny
- Jest Handel, cena Rośnie, wszyscy są Zadowoleni

Initial Coin Offering

- Pomysł na finansowanie startupu
- Inwestorzy wpłacają ETH, dostają tokeny

- ????



Token do płacenia za usługi startupu
Token „akcjonariusza”
Token „udziałowca”

- Pojawia się popyt na tokeny
- Jest Handel, cena Rośnie, wszyscy są Zadowoleni

Initial Coin Offering **Wariant realistyczny**

- Pomysł na finansowanie startupu
- Inwestorzy wpłacają ETH, dostają tokeny
- (wariant A) Startup przez lata pozoruje działalność i przejada ETH
- (wariant B) Startup znika, twórcy znikają, ETH też znika

Initial Coin Offering **Wariant realistyczny**

- Pomysł na finansowanie startupu
 - Inwestorzy wpłacają ETH, dostają tokeny
 - (wariant A) Startup przez lata pozoruje działalność i przejada ETH
 - (wariant B) Startup znika, twórcy znikają, ETH też znika
-
- 2017 – setki ICO, setki milionów USD, setki przewałów
 - 2018 – ban na reklamy ICO w Google, Twitrze, Facebooku, MailChimp
 - Lata lecą a jakoś się nie słyszy o rzeczywistych sukcesach

Initial Coin Offering **Wariant realistyczny**

- Pomysł na finansowanie startupu
 - Inwestorzy wpłacają ETH, dostają tokeny
 - (wariant A) Startup przez lata pozoruje działalność i przejada ETH
 - (wariant B) Startup znika, twórcy znikają, ETH też znika
-
- 2017 – setki ICO, setki milionów USD, setki przewałów
 - 2018 – ban na reklamy ICO w Google, Twitterze, Facebooku, MailChimp
 - Lata lecą a jakoś się nie słyszy o rzeczywistych sukcesach
 - (za to popyt na specjalistów od ICO był dziki)

Initial Coin Offering **Wariant jeszcze bardziej realistyczny**

- Pomysł na finansowanie startupu
- Założyciele startupu mają wielką pulę tokenów gratis
- Insiderzy mają równie wielką pulę za ~~poł~~ dziesięć procent ceny
- Inwestorzy płacą pełną cenę
- Pump & dump

NFT

Non-Fungible Token

slido.com

#76766



Non-Fungible Token

- Wszystkie tokeny (ERC-20) są nieodróżnialne, Smart Contract przechowuje informację o saldzie
- NFT (ERC-721) to po prostu ponumerowane tokeny
- I już



Informatyk Zakładowy @InfZakladowy · 13 min

...

Trzecia gawęda o kryptowalutach, będzie [m.in.](#) o NFT. Szanowna publiczności, ten kawałek ma być:

jechany po całości

51,9%

wyważony i obiektywny

30,8%

czysto techniczny

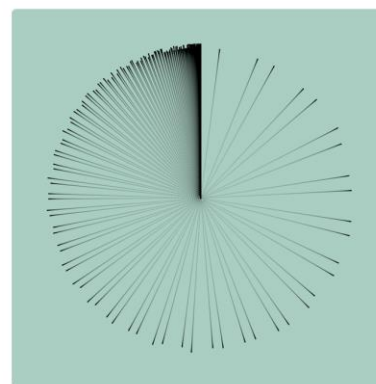
17,3%

52 głosy · Pozostało 8 godzin

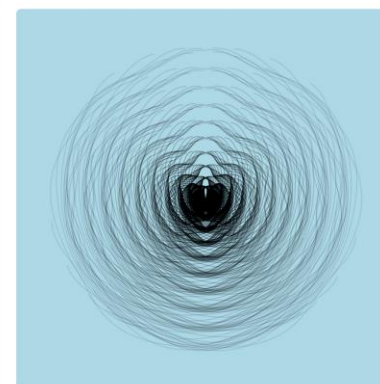


Non-Fungible Token

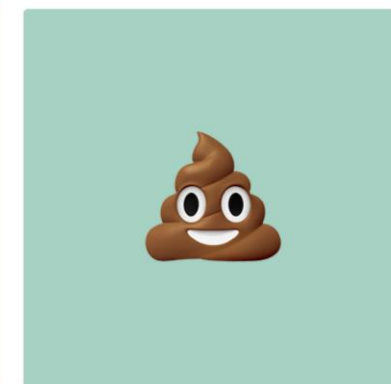
- Kupowanie numerów nie jest ciekawe, więc NFT to zazwyczaj obrazki mające jakiś numer (np. *seryjny*) albo wygenerowane w oparciu o *hash* czegoś (np. *transakcji tworzącej tokena*)
- Jest gorzej – na platformach typu OpenSea „kupujesz” URL pokazujący, co kupiłeś/aś. Możliwe dowcipy: co innego zobaczysz kupując, co innego w portfelu
- Nie ma tu trwałości blockchajna, jest tylko platforma



NFT on OpenSea



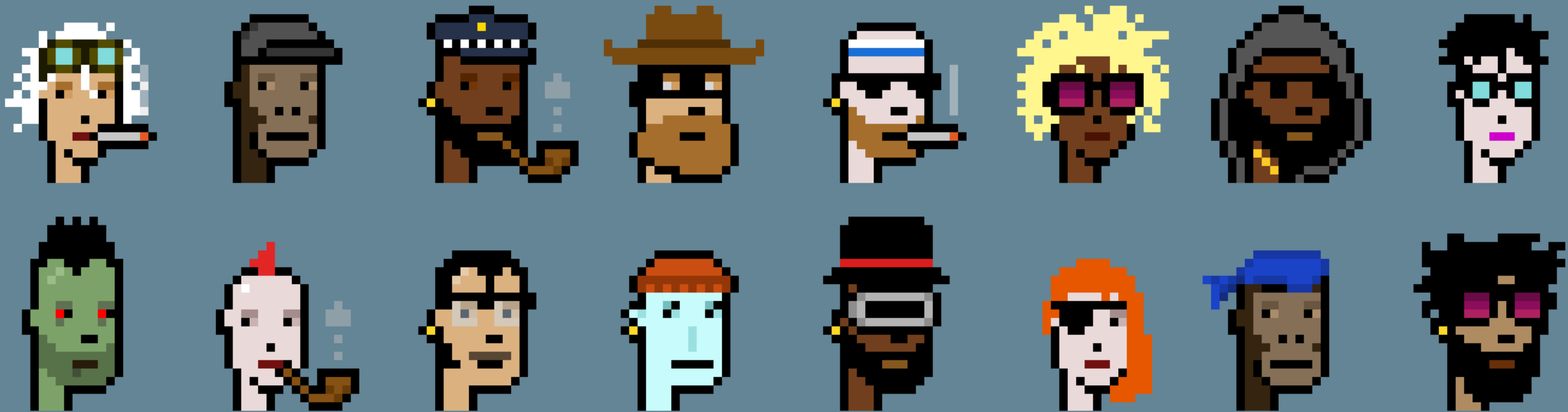
Same NFT on Rarible



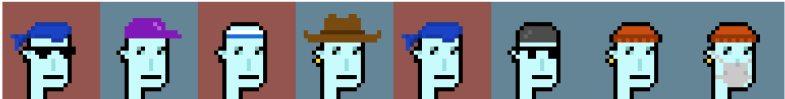
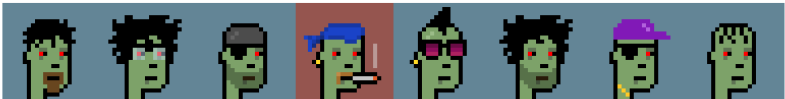
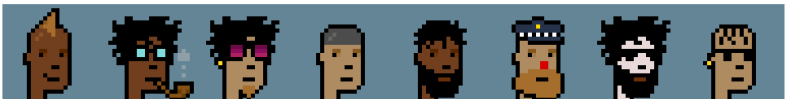
Same NFT in a wallet

<https://moxie.org/2022/01/07/web3-first-impressions.html>

CryptoPunks (2017)



Punk Types

Attribute	#	Avail	Avg Sale ⓘ	Cheapest ⓘ	More Examples
Alien	9	3	0	 23KΞ	
Ape	24	2	0	 15KΞ	
Zombie	88	7	1.48KΞ	 1.9KΞ	
Female	3840	535	247.08Ξ	 80Ξ	
Male	6039	858	110.10Ξ	 82.95Ξ	

Attributes

Attribute	#	Avail	Avg Sale ⓘ	Cheapest ⓘ	More Examples
Beanie	44	8	387Ξ	 800Ξ	
Choker	48	12	199Ξ	 222Ξ	
Pilot Helmet	54	13	357.25Ξ	 300Ξ	

Cryptopunks / 3100



CryptoPunk 3100

One of 9 Alien punks.

Bid	0x319aae	0.11Ξ (\$366)	Sep 14, 2021
Offered		35KΞ (\$111.16M)	Aug 30, 2021
Offered		38.89KΞ (\$126.19M)	Aug 28, 2021
Bid	0xeea014	0.10Ξ (\$311)	Aug 08, 2021
Offered		35KΞ (\$90.5M)	Aug 01, 2021
Bid	"meta".e...	<0.01Ξ (\$<0.01)	Jul 05, 2021
Sold	0x6611fe	0x7b8961	4.2KΞ (\$7.58M) Mar 11, 2021
Bid	0x7b8961	4.2KΞ (\$7.58M)	Mar 11, 2021
Bid Withdrawn	0x51657	1.4KΞ (\$2.19M)	Mar 04, 2021
Bid	0x51657	1.4KΞ (\$2.17M)	Mar 02, 2021
Bid Withdrawn	0xa...	1.39KΞ (\$2.14M)	Mar 02, 2021
Bid	0xa...	1.39KΞ (\$2.11M)	Mar 01, 2021

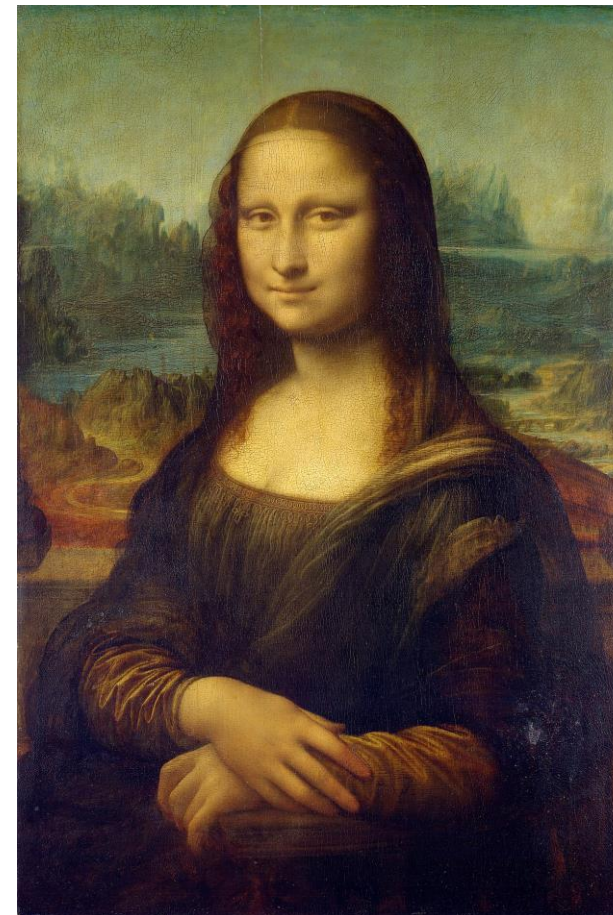
NFT

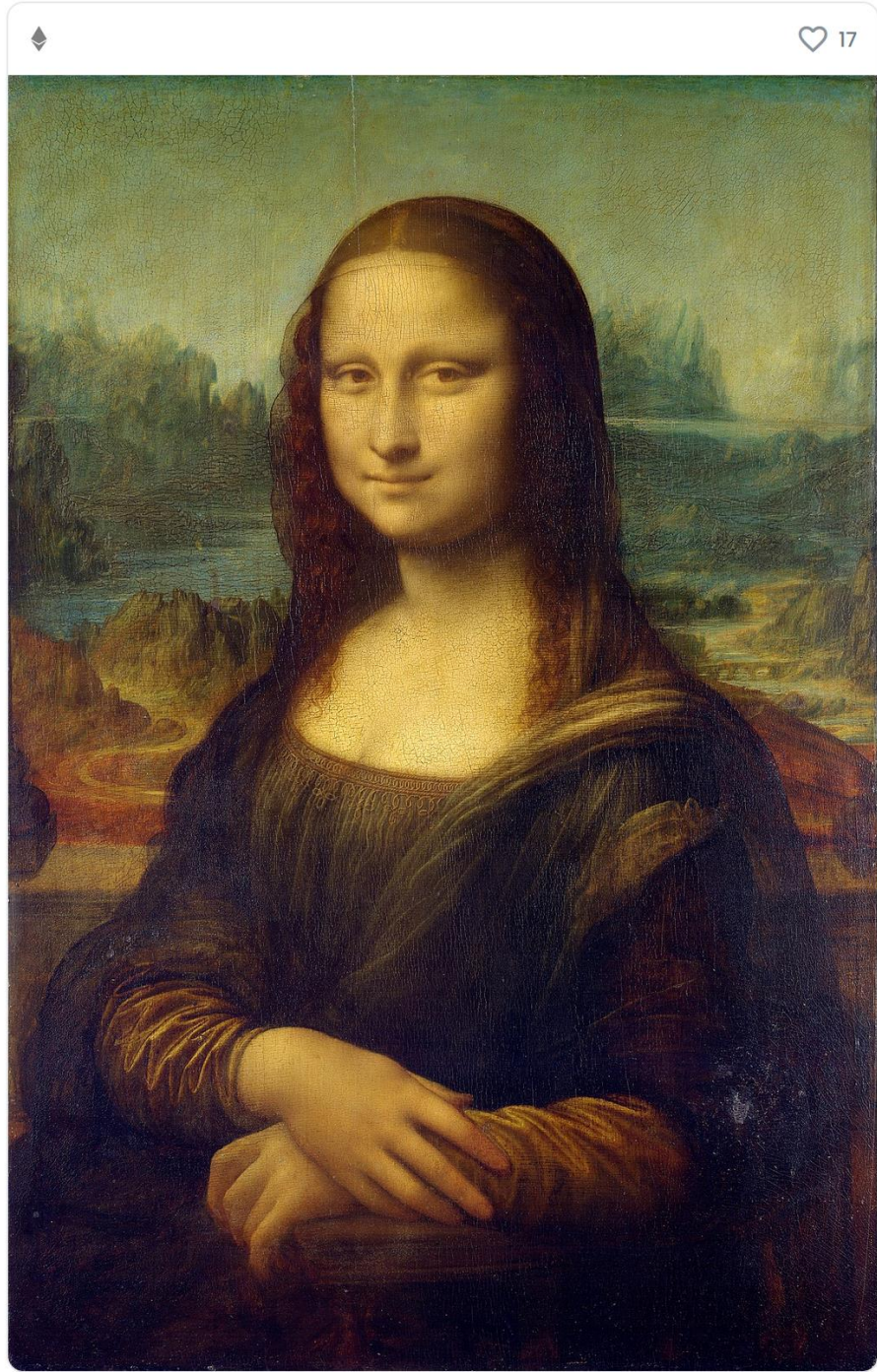


Jeśli kupisz NFT z Mona Lisą, to:

- sprzedawcą nie był rząd Francji
- obraz nie staje się twoją własnością
- nie nabywasz praw majątkowych do dzieła
- nie nabywasz praw autorskich do dzieła
- twój NFT nie ma gwarancji unikalności

Płacisz jedynie za napis „NFT *abc* przynależy do portfela *xyz*” umieszczony w rozproszonej bazie danych





17

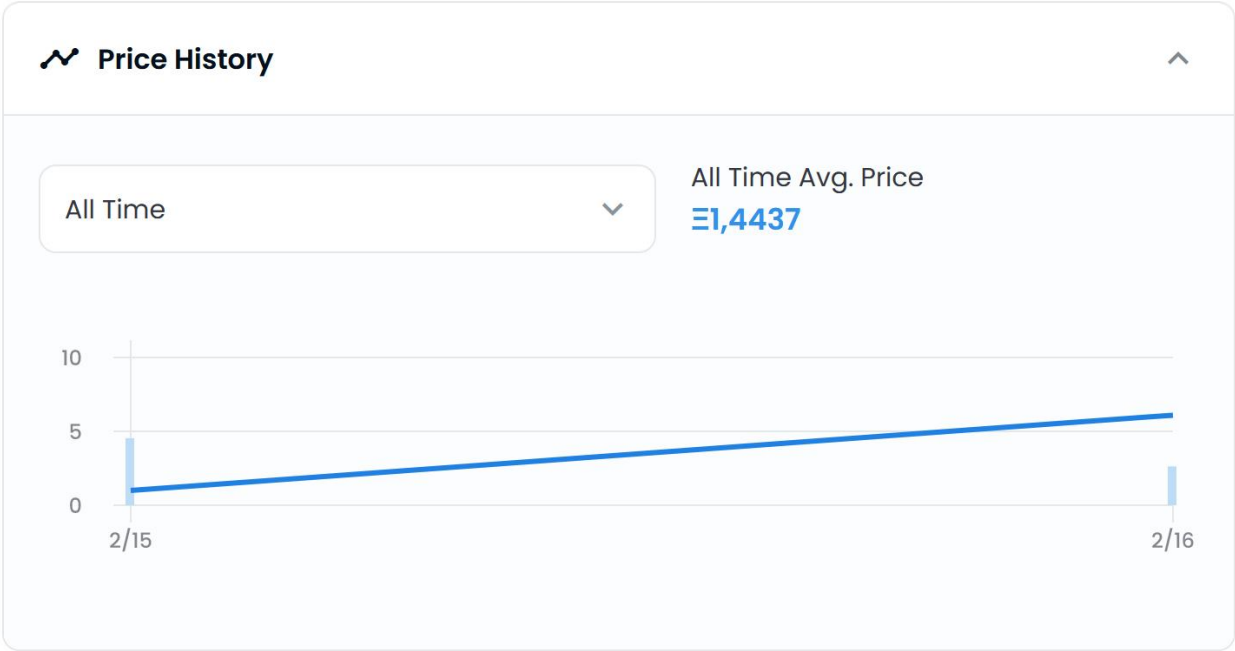
CryptoMasterpieces



Mona Lisa

Owned by 89798E 17 favorites

 [Make offer](#)



 **Listings** 

 **Offers** 



♥ 0

Mona Lisa Painting NFT

↺

↻

⋮

The very first Mona Lisa NFT (The Untouched Image)

Owned by [BusinessFactory](#)

 [Make offer](#)

Price History

All Time 



No item activity yet

Listings

Offers

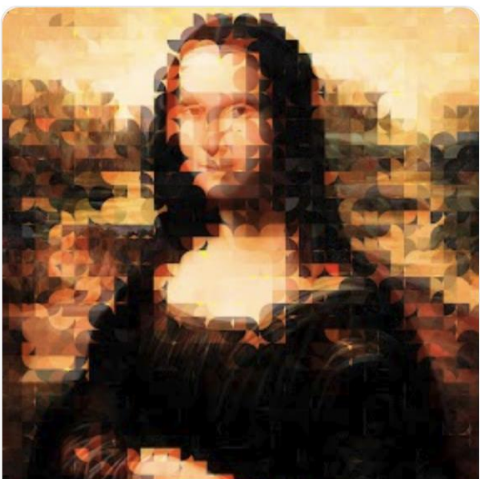


Digital Mona Lisa ...
Digi Mona Lisa I

Price
0.04

Buy now

1



Digital Mona Lisa ...
Digi Mona Lisa IV

Price
0.04

3



Digital Mona Lisa ...
Digi Mona Lisa X

Price
0.04

2



Digital Mona Lisa ...
Digi Mona Lisa III

Price
0.05

2



Digital Mona Lisa ...
Digi Mona Lisa VIII

Price
0.05

2



Digital Mona Lisa ...
Digi Mona Lisa II

Price
0.05



Digital Mona Lisa ...
Digi Mona Lisa VI

Price
0.06



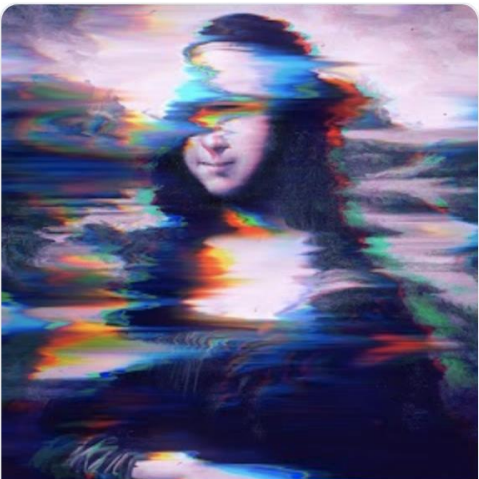
Digital Mona Lisa ...
Digi Mona Lisa V

Price
0.06



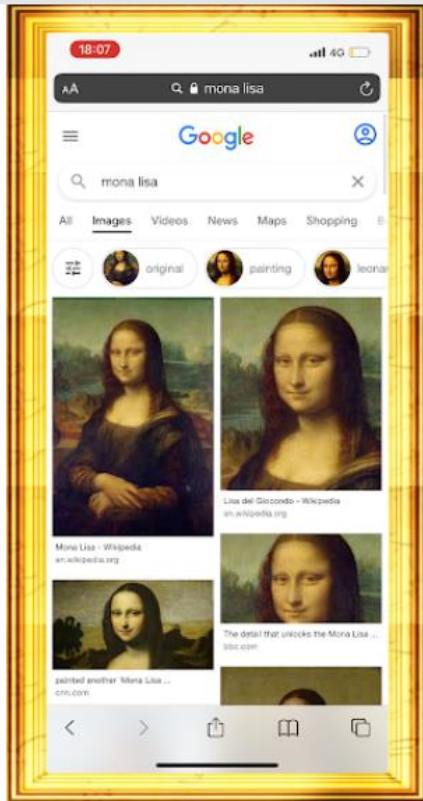
Digital Mona Lisa ...
Digi Mona Lisa IX

Price
0.06



Digital Mona Lisa ...
Digi Mona Lisa VII

Price
0.1



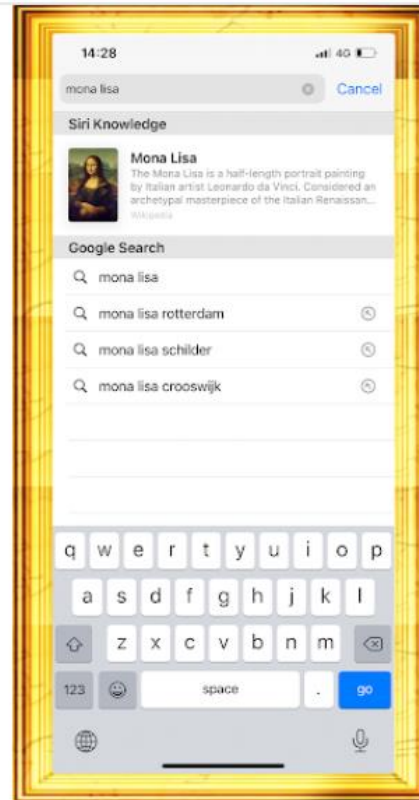
Mona Lisa NFT

Mona_Lisa_NFT_SS_v1:

Price

0.35

Buy now

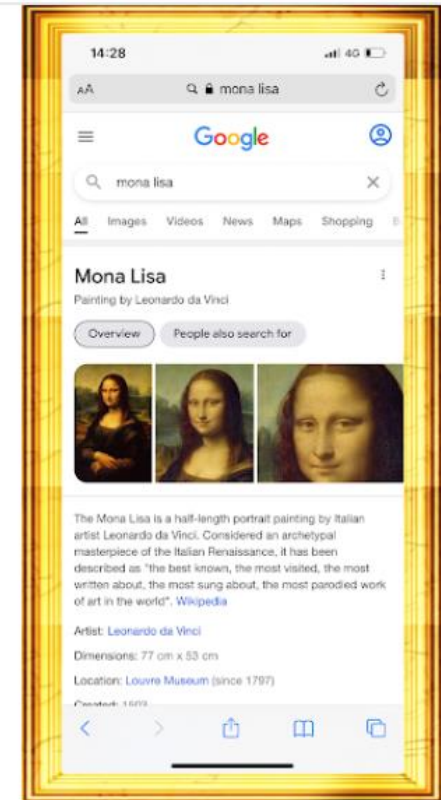


Mona Lisa NFT

Mona_Lisa_NFT_SS_v3:

Price

0.45



Mona Lisa NFT

Mona_Lisa_NFT_SS_v4

Price

0.55



NFT

Chcesz wspomóc pieniędzem ulubionego artystę?

- Kup płytę, książkę, obraz
- Pójdź na koncert
- Przelej datek na jego/jej fundację

Nie marnuj megawatów energii, nie buduj piramid finansowych, nie kupuj kawałków piosenek.



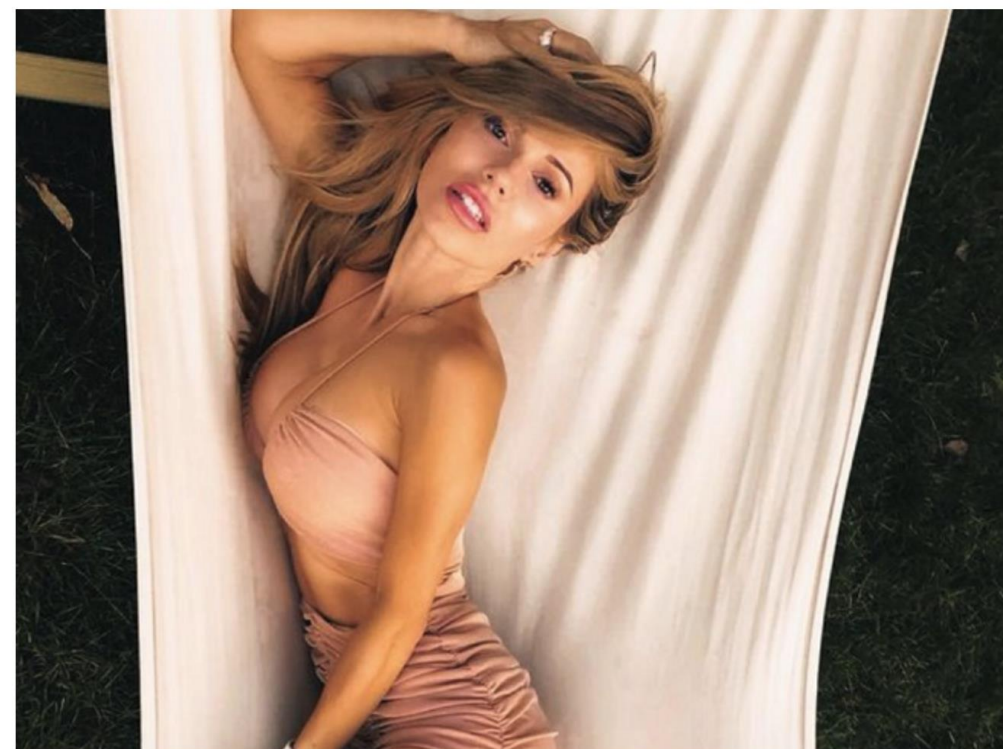
Wirtualnedia.pl > Technologie > aplikacje mobilne

Doda sprzedaje swoje ciało jako NFT. „Jego wartość będzie rosła wraz z moją popularnością”

Piosenkarka Dorota „Doda” Rabczewska zapowiedziała, że będzie sprzedawać części skanu 3D swojego ciała w formie tokenów NFT. - Każde moje NFT i jego wartość będą rosły wraz z moją popularnością. Zestawiając to z moimi planami na przyszłość moi fani pierwszy raz będą mieli okazję wzbogacić się - zapewnia.



komentarze 19





O co tu chodzi?

Kolejny sposób na to, aby ludzie mający dolary kupowali kryptowaluty za dolary

PS: umiecie znaleźć te NFT z kawałkami Dody? Ja nie.



itch.io  @itchio · 8 g.

A few have asked about our stance on NFTs:

NFTs are a scam. If you think they are legitimately useful for anything other than the exploitation of creators, financial scams, and the destruction of the planet the we ask that please reevaluate your life choices.

Peace 🕊️



2



21,9 tys.



92,3 tys.



itch.io  @itchio · 8 g.

Also fuck any company that says they support creators and also endorses NFTs in any way. They only care about their own profit and the opportunity for wealth above anyone else.

Especially given the now easily available discourse concerning the problems of NFTs.



1



2,9 tys.



19,4 tys.



Obserwacja bez związku z NFT:

Czy zauważyliście, że koparek do kryptowalut
nie da się kupić od producentów za kryptowaluty?

Patrz także: gorączka złota, sprzedawcy łopat

Proof of Stake

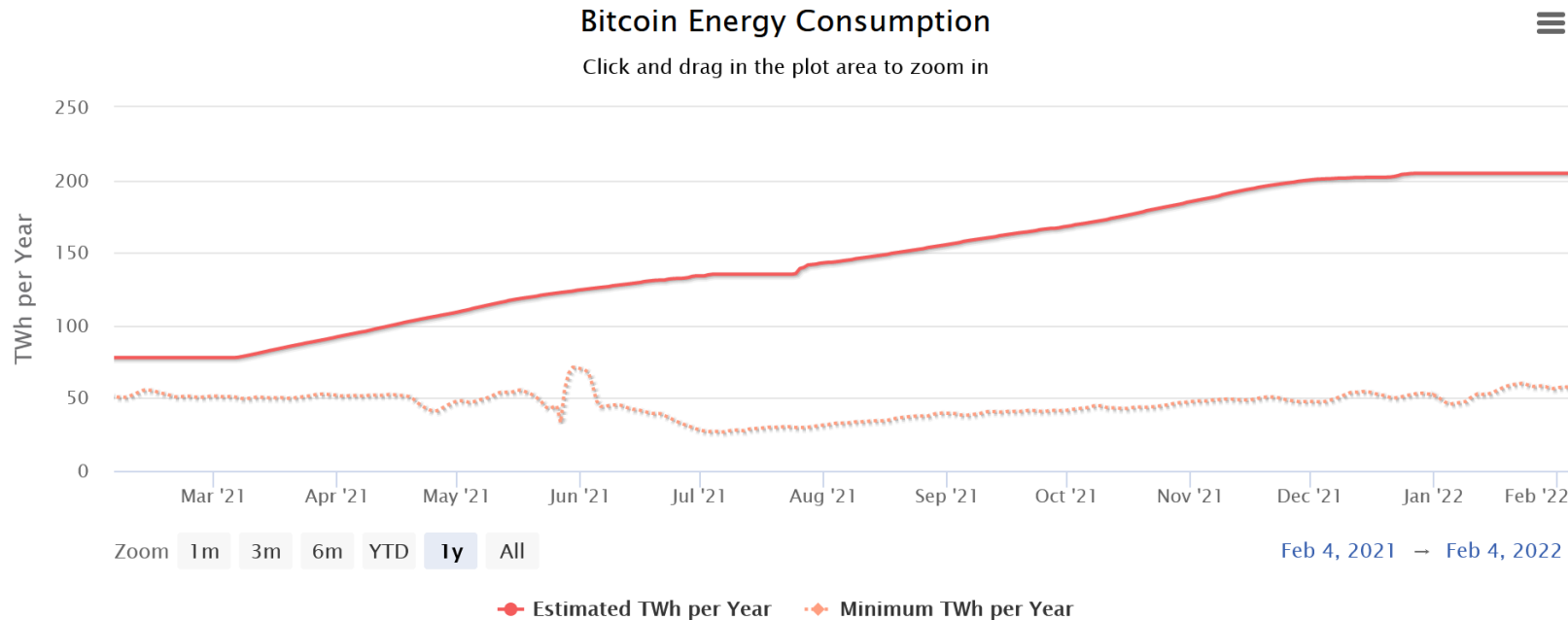
slido.com

#76766



Najpierw był Proof of Work

PoW = dowód, że górnik poniósł
nakłady aby wykopać blok



Antminer T19

- 95 Thps
- 3300 W
- \$5000



Elektrownia Bełchatów, roczna produkcja 28TWh, autor: PGEGiEK (CC BY-SA 4.0)

Proof of Stake

- Uczestnicy rynku zamrażają stawkę (32EHT / \$100.000) lub jej wielokrotność aby otrzymać status *walidatora*
- Sieć losowo wyznacza walidatora, który utworzy kolejny blok
- Inni losowo wyznaczeni walidatorzy sprawdzają prawidłowość bloku
- Kto kantuje, traci stawkę
- Kto tworzy prawidłowe bloki, zgarnia nagrodę

Kiedy?

Proof-of-stake (PoS) | ethereum

← → ↻ ∞

https://ethereum.org/en/developers

Szukaj



Proof-of-stake >



Last edit: [@wackerow](#), January 26, 2022

See contributors

 Edit page

On this page >

Ethereum is moving to a consensus mechanism called proof-of-stake (PoS) from [proof-of-work \(PoW\)](#). This was always the plan as it's a key part in the community's strategy to scale Ethereum via [upgrades](#). However getting PoS right is a big technical challenge and not as straightforward as using PoW to reach consensus across the network.

PREREQUISITES

To better understand this page, we recommend you first read up on [consensus mechanisms](#).

Kiedy?

W połowie 2017 roku PoS miał wejść
w życie za kilka miesięcy

Proof-of-stake (PoS) | ethereum X

← → ↺ ∞ 🛡️ 🔒 https://ethereum.org/en/developers 📄 📌 ☆ 🖨️ 🔍 Szukaj 🗑️ ⬇️ ⏏️ ☰

🔍 ☰

Proof-of-stake >

 Last edit: [@wackerow](#), January 26, 2018 [See contributors](#) [Edit page](#)

>

...to a consensus mechanism called proof-of-stake (PoS) from [proof-of-work \(PoW\)](#).
...was always the plan as it's a key part in the community's strategy to scale Ethereum via [upgrades](#).
However getting PoS right is a big technical challenge and not as straightforward as using PoW to reach consensus across the network.

PREREQUISITES

To better understand this page, we recommend you first read up on [consensus mechanisms](#).

Skąd taka zwłoka?

- Proof of Work dzieje się w „prawdziwym świecie”
- Proof of Stake to coś, co działa w ramach kryptowaluty

Skąd taka zwłoka?

- Proof of Work dzieje się w „prawdziwym świecie”
 - Proof of Stake to coś, co działa w ramach kryptowaluty
1. rejestr transakcji mówi nam, kto ma środki w blockchainie
 2. *cośtam cośtam*
 3. ludzie mający środki w blockchainie decydują o kolejnych transakcjach w blockchainie

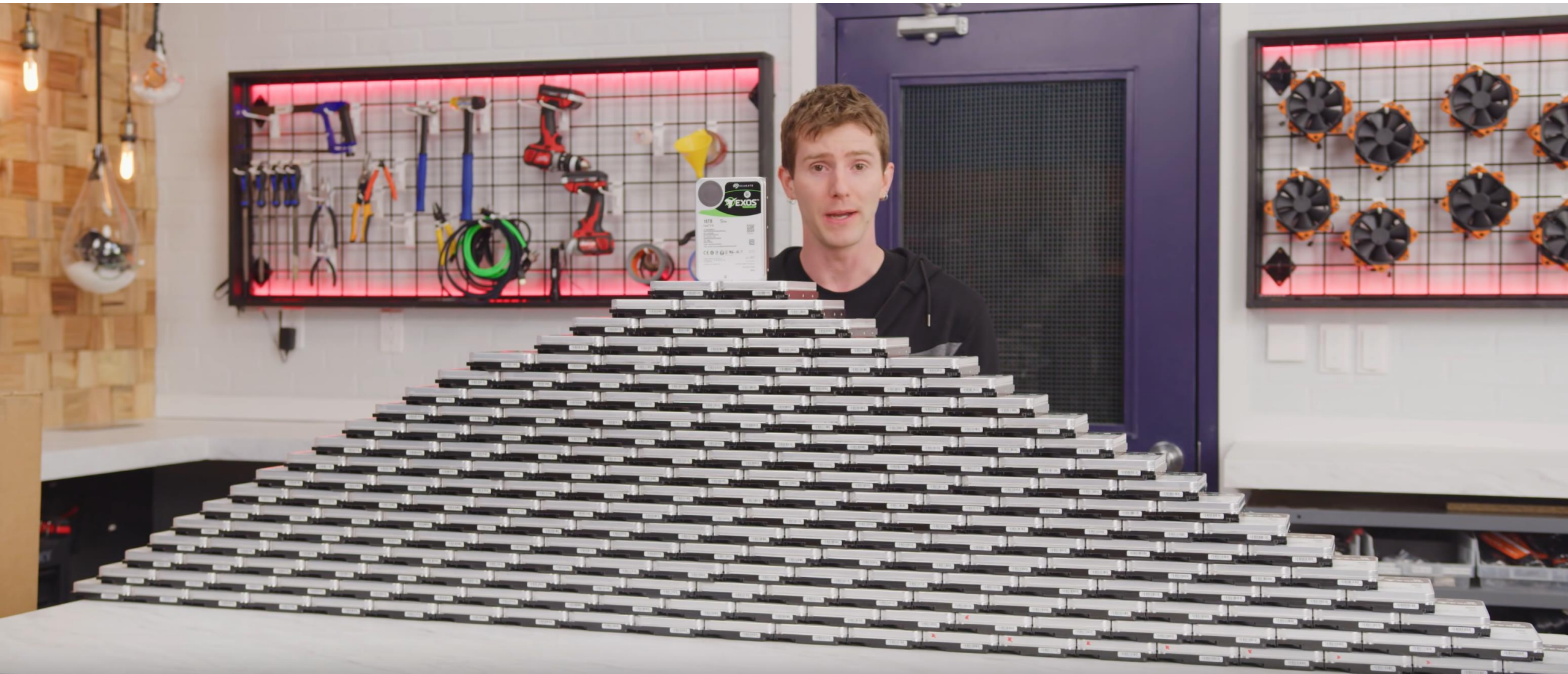
Coś jest nie tak?

- Bogaci staną się jeszcze bogatsi
- Hard fork? Bogaci pozostaną bogaci w obu wariantach

Coś jest nie tak?

- Bogaci staną się jeszcze bogatsi
- Hard fork? Bogaci pozostaną bogaci w obu wariantach
- Ale: jeśli zamiast jednej kryptowaluty będziemy mieli dziesięć lub sto
- ... a w każdej z nich tych samych bogaczy...
- ... to chętnych na zakup kryptowaluty za dolary może braknąć.
- Proof of Stake pozwala bogaczom zapobiegać decentralizacji

Proof of Space



Proof of Space

Wykres Chia na PLN

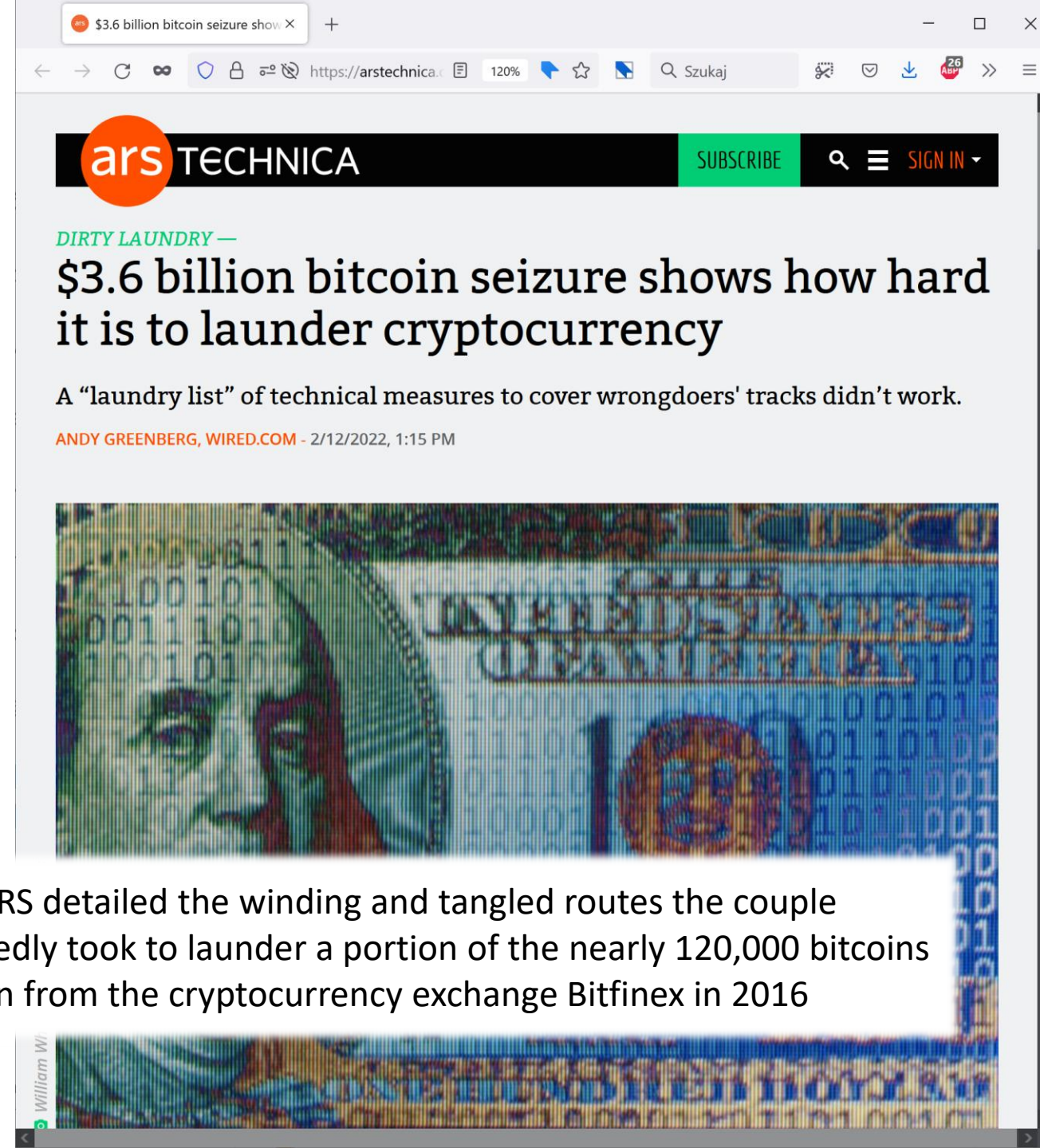


Czy kryptowaluty dają anonimowość?

- To zależy (np. BTC kontra Monero)
- Blockchain jest jawny, w BTC i ETH wszystko widać
- Okup w kryptowalucie można śledzić w obu kierunkach
- Istnieją miksery kryptowalut
- Na końcu przestępcy chcą dostać dolary
- Najłatwiej ograniczyć początek i koniec łańcucha (AML/ KYC, limity transakcji, zgłoszenia do regulatorów, wyrzucanie poza obręb cywilizacji itd.)

Czy miksery działają

- To często nie jest legalna działalność
- Właściciel miksera może oddalić się z mikserem (i jego zawartością)



Pranie brudnych pieniędzy



The centralization of Ethereum's mining pools and exchanges enabled Poly Network to persuade them to blacklist the addresses involved. This made it very difficult for the miscreant to escape with the loot, much of which was returned. But it also vividly demonstrated that in most blockchains it is the mining pools that decide which transactions make it into a block, and are thus executed.

Problemy z mempool

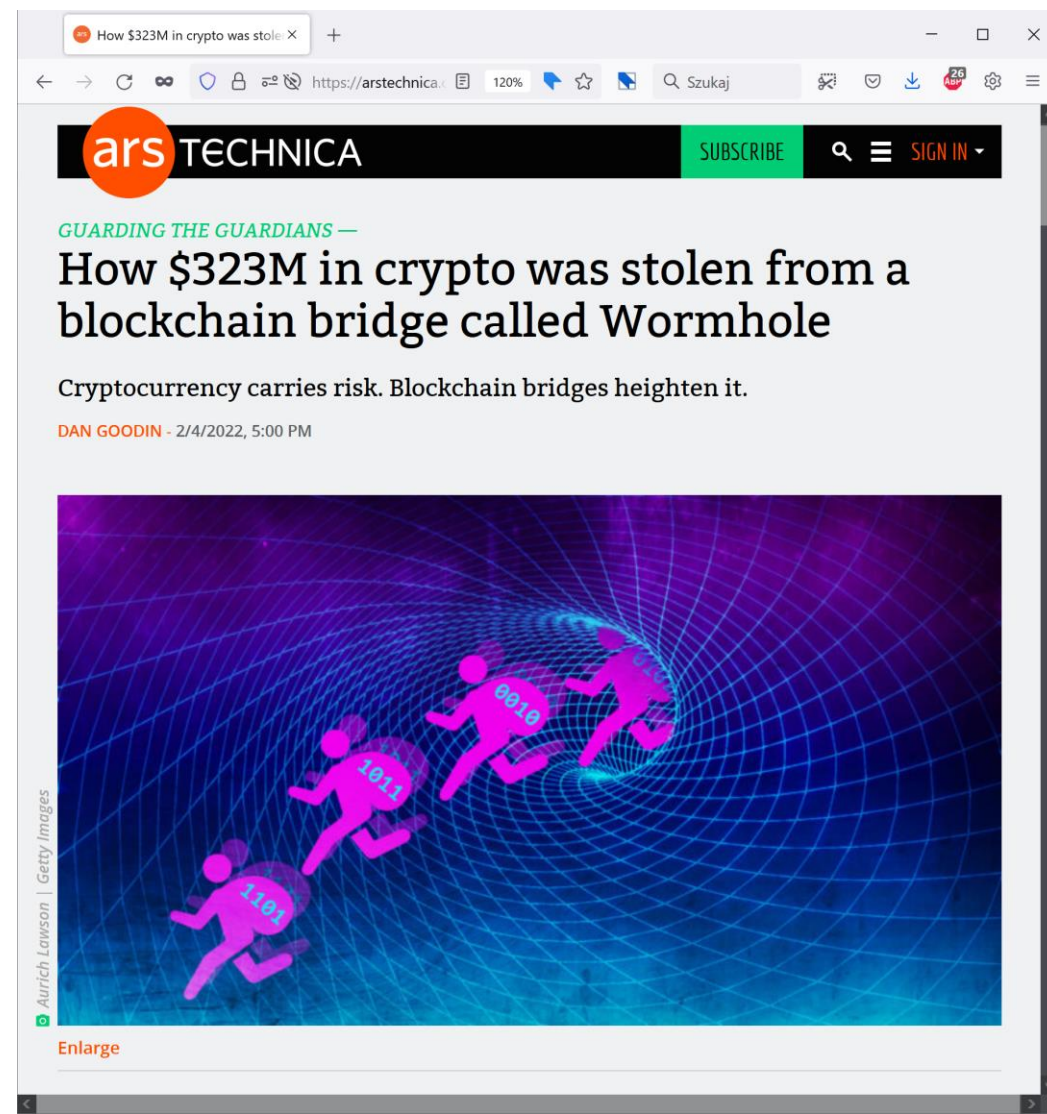
[...] after the group spotted the vulnerability and built a transaction to rescue the funds, they could not put the rescue transaction in the public mempool because it would have been front-run by a bot. They had to find a miner who would put the transaction in a block *without* it appearing in the mempool

In other words, their transaction needed a dark pool. And they had to trust the cooperative miner not to front-run it. [...]

<https://blog.dshr.org/2022/02/ee380-talk.html>

Jak działa wymiana między różnymi kryptowalutami?

- Nie ma tu żadnej magii
- Jeśli dwa blockchainya się nie stykają, potrzebujesz pośrednika któremu zaufasz
- Pośrednik przyjmie środki typu A, wyda ci środki typu B
- Jeśli „nośnik” jest wspólny (np. ETH dla tokenów ERC-20), możliwe jest tworzenie smart kontraktów z kantorem



Co to jest „wrapped BTC/ETH”

- W uproszczeniu – reprezentacja środków z jednego blockchajna w innym blockchainie
- Np. „wrapped BTC” może być tokenem w sieci ETH
- Musisz zaufać emitentowi wBTC, że nie oddali się w nieznanym kierunku z powierzonymi BTC

Co to jest stablecoin

- Kryptowaluta, której wartość jest powiązana z prawdziwymi pieniędzmi przekazanymi emitentowi stablecoina
- Zwiększają płynność giełd kryptowalutowych, bo ktoś planujący sprzedaż może przechować środki bez straty w stablecoinie
- Trzeba zaufać emitentowi, że zapewnia pokrycie wszystkich coinów prawdziwymi pieniędzmi w prawdziwym banku

Co to jest shitcoin

- Kryptowaluta o niskiej płynności, popularności, wartości
- Przykład: Dogecoin z czasów, zanim napisał o niej na Twitterku Elon Musk (ten od Tesli i SpaceX)



Elon Musk 
@elonmusk

Tesla merch buyable with Dogecoin

[Przetłumacz Tweeta](#)

7:18 AM · 14 sty 2022 · Twitter for iPhone

52 tys. Tweetów podanych dalej 7 607 Cytatów z Tweeta 333,6 tys. Polubień

Co to jest DAO

Decentralized Autonomous Organization

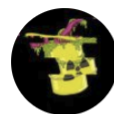
Zdecentralizowana autonomiczna organizacja

Czyli... smart kontrakt?

Czy coś w rodzaju spółki/spółdzielni?

Co to jest DeFi

„termin odnoszący się do systemów i aplikacji zbudowanych w oparciu o technologię blockchain, służących ich użytkownikom do korzystania z usług i produktów finansowych **nie regulowanych w przepisach prawa i nie objętych nadzorem właściwych organów**”



Jacob Silverman 
@SilvermanJacob

...

Imagine if big banks were getting hacked for tens or hundreds of millions of \$\$ each week but also nothing was insured, there were no systems in place to mitigate fallout, and half of the hacks were inside jobs. That's basically DeFi.

[Przetłumacz Tweeta](#)

2:15 AM · 3 lut 2022 · Twitter Web App



Co to jest DeFi

„Opierająca się na zyskach pośredników klasyczna bankowość, jest zazwyczaj niedostępna w regionach charakteryzujących się niskimi dochodami. Dzięki temu, że koszty DeFi są stosunkowo niewielkie, opłacalne staje się udostępnianie Zdecentralizowanych Aplikacji Finansowych osobom o mniejszych zarobkach.”

Czy DeFi są bezpieczne?

Cream hack early analysis

1. Using account A, Flash Borrow 500m DAI
2. Deposit 500m dai into yDAI
3. Deposit ~500m yDAI into yUSD
4. Deposit ~500m yUSD into yUSDVault
5. Mint ~\$500m crYUSD (it used yUSDVault as underlying)
6. Account A now has \$500m crYUSD
7. Using account B, flash borrow \$2b ETH
8. Mint cETHER
9. Borrow 500m yUSDVault
10. Mint \$500m crYUSD
11. Transfer \$500m crYUSD to account A
12. Borrow 500m yUSDVault
13. Mint \$500m crYUSD
14. Transfer \$500m crYUSD to account A
15. Borrow 500m yUSDVault
16. Transfer 500m yUSDVault to account A
17. Account A now has \$1.5b crYUSD and \$500m yUSDVault
18. Using account A, Redeem \$500m yUSDVault
19. Transfer 8m yUSD to yUSDVault to ~double its' share value (1 to 2)
20. Since yUSDVault is now worth double, cream now thinks that the account A's \$1.5b crYUSD is worth \$3b
21. Borrow \$2b ETH
22. Account A now has \$2 ETH, \$500m yUSD, and \$1b in Cream collateral.
23. The ETH and yUSD can be used to pay back the blas loans while the \$1b collateral can be used to drain Cream

These are my raw notes of the exploit. I usually translate these to English before posting a thread but it's getting late here and I might go to bed before finishing the detailed thread so enjoy these to-the-point notes till then.

Ile kryptowalut ukradziono w 2022 roku?

- Równowartość 559 milionów dolarów (sprawdzono: dziś o 16:42)
- źródło: web3isgoinggreat.com
- Różne formy:
 - pump and dump
 - zniknięcie twórcy ICO/DeFi/NFT
 - wydrenowanie giełdy
 - konwencjonalna kradzież haseł/kluczy

Co takiego dały nam te kryptowaluty?



Co takiego dały nam te kryptowaluty?

CI Crypto miners are killing free CI

CI providers like LayerCI, GitLab, TravisCI, and Shippable are all worsening or shutting down their free tiers due to cryptocurrency mining attacks.



COLIN CHARTIER

25 APR 2021 • 3 MIN READ

ASUS GeForce RTX 3090 ROG STRIX OC WHITE 24GB GDDR6X

★★★★★ (4 opinie) od: ASUS | kod producenta: ROG-STRIX-RTX3090-O24G-WHITE | kod x-kom: 628032



Oszczędź 1 000,00 zł
~~15 199,00 zł~~ **14 199,00 zł**

1 ▾

Dodaj do koszyka



Dostępny

Dowiedz się więcej



Kup teraz, otrzymasz w środę

Dowiedz się więcej



Darmowy odbiór w salonie

Koszty dostawy



Rata tylko 437,80 zł

Oblicz ratę



Salon: Wrocław Pasaż

Zamów na środę (16 lutego)



+5

Układ: GeForce RTX 3090

Pamięć: 24 GB

Na zakończenie #1



Jackson Palmer
@ummjackson



Cryptocurrency is like taking the worst parts of today's capitalist system (eg. corruption, fraud, inequality) and using software to technically limit the use of interventions (eg. audits, regulation, taxation) which serve as protections or safety nets for the average person.

[Przetłumacz Tweeta](#)

6:54 PM · 14 lip 2021 · Twitter Web App

3 436 Tweetów podanych dalej **389** Cytatów z Tweeta **18,2 tys.** Polubień

Na zakończenie #2



Richard Gaywood

@PenLlawen



W odpowiedzi do [@mathieuisabel](#) i [@markrussinovich](#)

Bitcoin is 14 years old.

14 years after Berners-Lee compiled the first web browser, we had Google, CSS, Wordpress, Safari, Firefox, Flickr, and MySpace.

14 years isn't "just getting started".

[Przetłumacz Tweeta](#)



Richard Gaywood @PenLlawen · 28 sty

The Bitcoin paper was published in 2008, 14 years ago. Ethereum was released in 2015, 6 years ago.

Berners-Lee's first web browser was prototyped in 1990, and published in Comms of the ACM in 1993.

1/

[Pokaż ten wątek](#)



**INFORMATYK
ZAKŁADOWY.PL**