Blockchain Credentials and Introduction to Ethereum

19 Feb 2025

Handy Bong (handy@hku.hk)

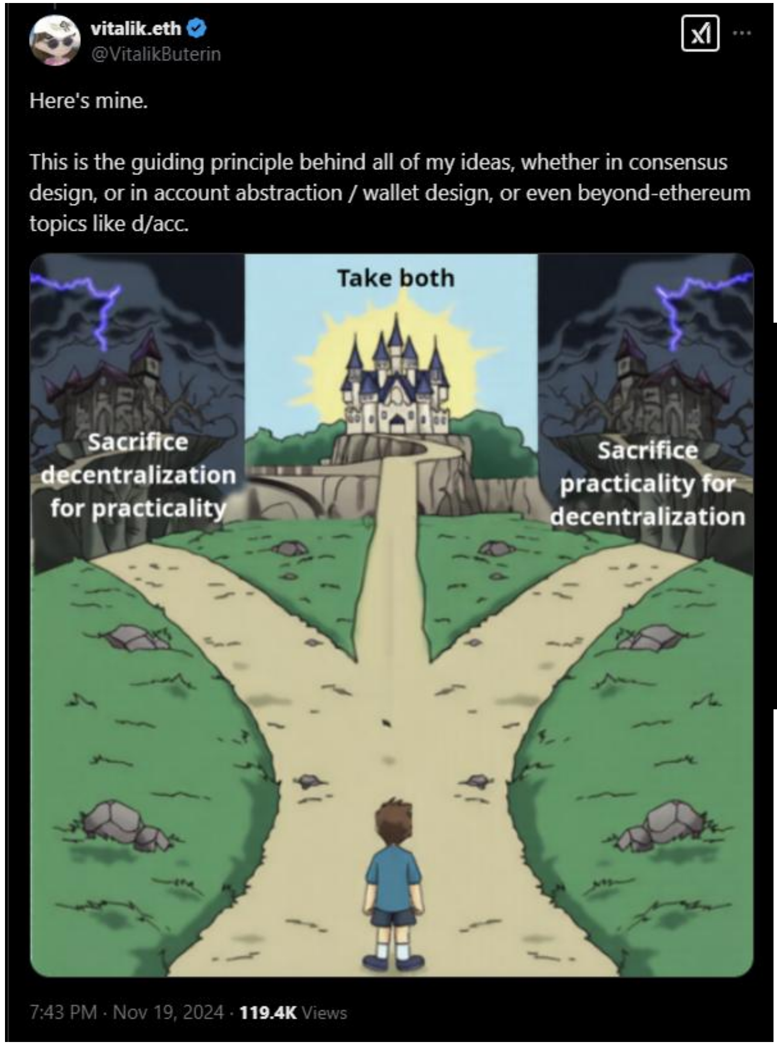
Outlines

- Why use blockchain?
- Blockchain credentials
- Introduction to Ethereum
- Mini workshop: using blockchain explorer with Etherscan
    - Basic features of blockchain explorer
    - Read blockchain transaction

Why use blockchain?

- Blockchain properties:
  - **Decentralized**
  - Transparent
  - Immutability
- Public?
  - What data safe to put into public space? (encrypted or plain text)
  - Do we need monetary feature? (payment system)
- Private/permissioned?
  - Do we need monetary feature?
  - Do we want full ownership of data?
- Can we do some trade-off?
  - L2-blockchain: start *slightly* centralized (decentralize on architecture)

Decentralization Obligatory



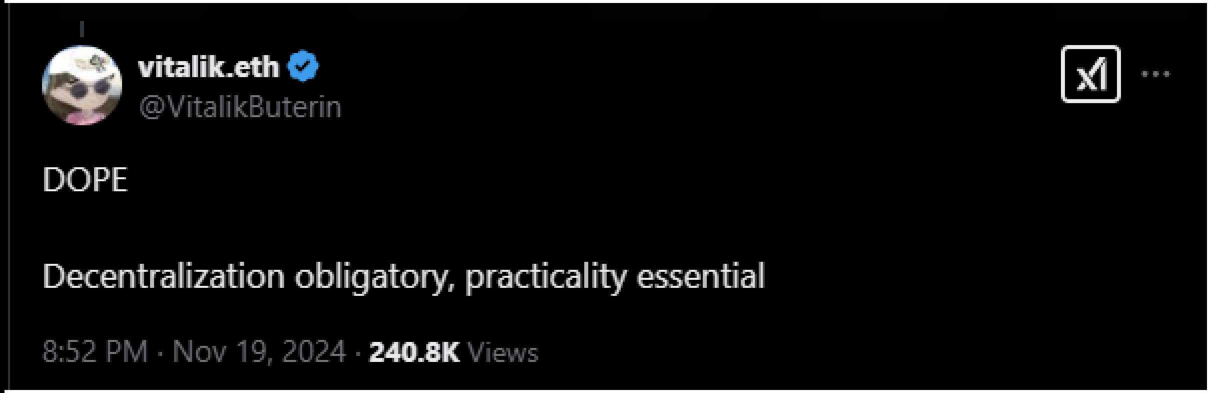
vitalik.eth
@VitalikButerin

Here's mine.

This is the guiding principle behind all of my ideas, whether in consensus design, or in account abstraction / wallet design, or even beyond-ethereum topics like d/acc.

Take both
Sacrifice decentralization for practicality
Sacrifice practicality for decentralization

7:43 PM · Nov 19, 2024 · 119.4K Views



vitalik.eth
@VitalikButerin

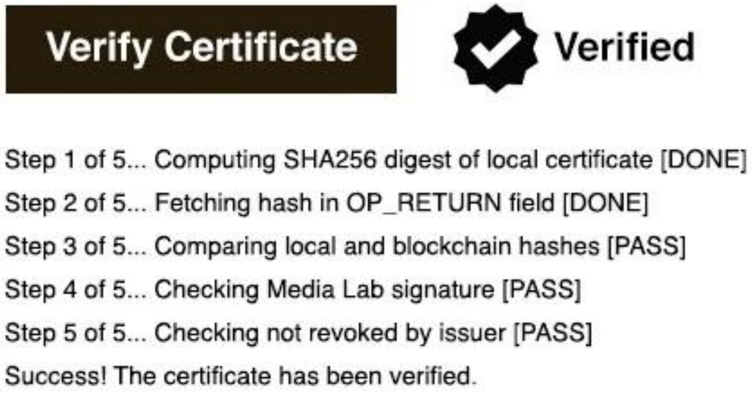
DOPE

Decentralization obligatory, practicality essential

8:52 PM · Nov 19, 2024 · 240.8K Views

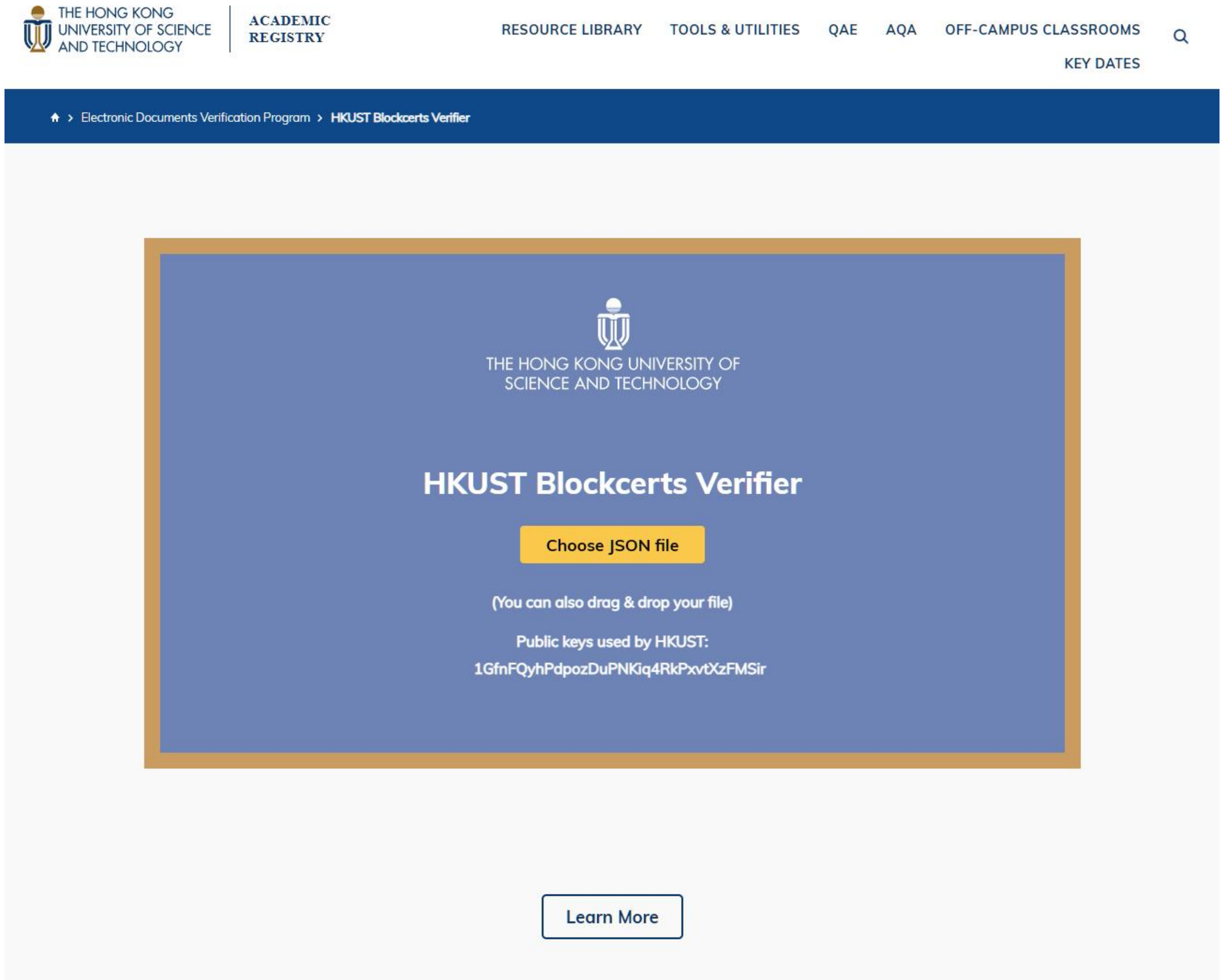
Blockchain Credentials

- Blockcerts
  - Open standard for blockchain credentials.
  - Open source, every one can verify credential.
- Why we need blockchain credential?
  - Decentralize verification
  - Ownership of credential
  - Prevent fraud
- Require credential issuer to **disclose** their *signature*.



```
Step 1 of 5... Computing SHA256 digest of local certificate [DONE]
Step 2 of 5... Fetching hash in OP_RETURN field [DONE]
Step 3 of 5... Comparing local and blockchain hashes [PASS]
Step 4 of 5... Checking Media Lab signature [PASS]
Step 5 of 5... Checking not revoked by issuer [PASS]
Success! The certificate has been verified.
```

HKUST Blockcert

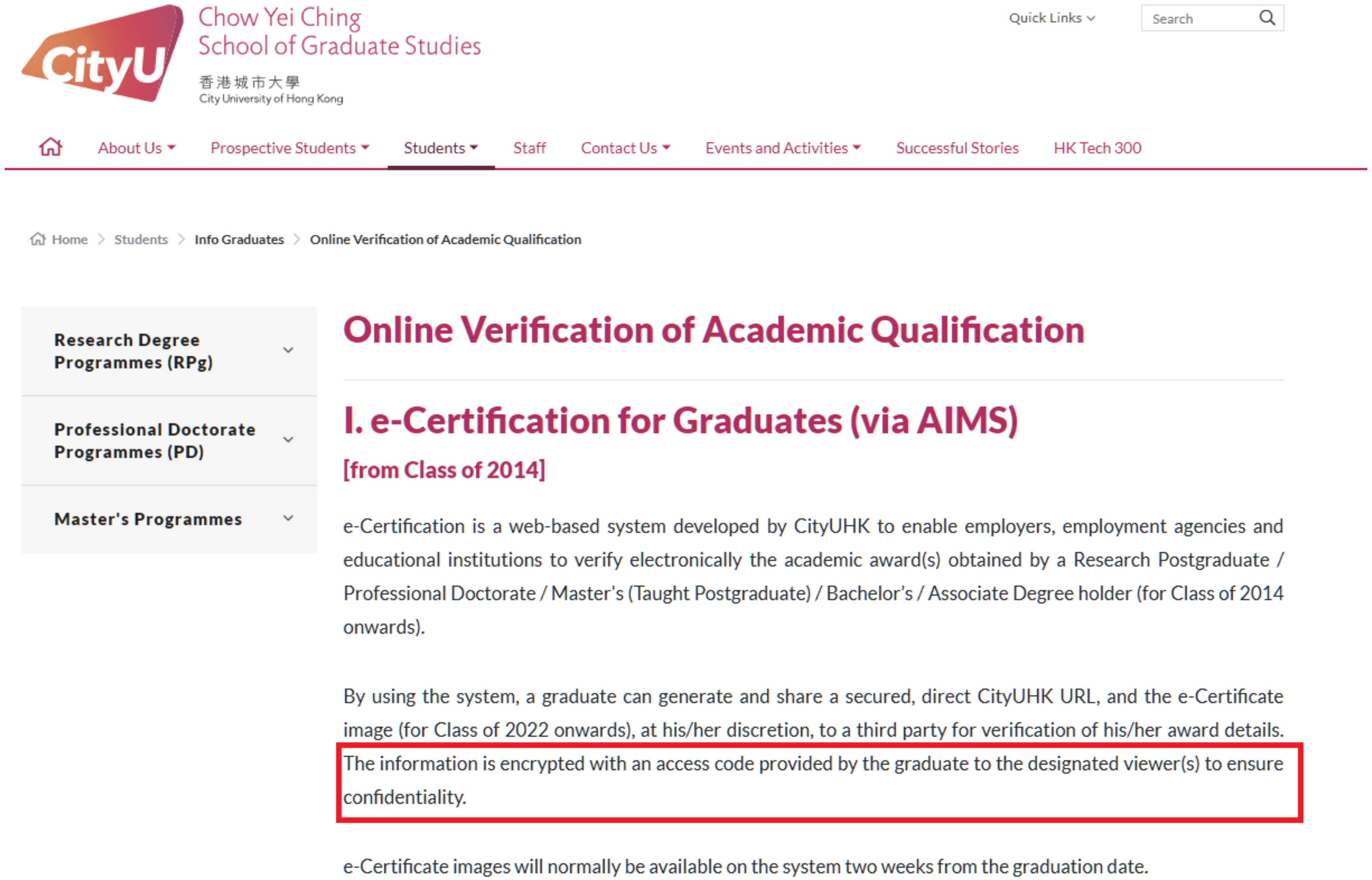

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY
ACADEMIC REGISTRY
RESOURCE LIBRARY
TOOLS & UTILITIES
QAE
AQA
OFF-CAMPUS CLASSROOMS
KEY DATES
Electronic Documents Verification Program > HKUST Blockcerts Verifier
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY
Choose JSON file
Learn More

HKUST Blockcerts Verifier

(You can also drag & drop your file)

Public keys used by HKUST:
1GfnFQyhPdpozDuPNKiq4RkPxvtXzFMSir

CityU e-Certification


Chow Yei Ching
School of Graduate Studies
香港城市大學
City University of Hong Kong
Quick Links
Search
About Us
Prospective Students
Students
Staff
Contact Us
Events and Activities
Successful Stories
HK Tech 300
Home > Students > Info Graduates > Online Verification of Academic Qualification
Research Degree Programmes (RPg)
Professional Doctorate Programmes (PD)
Master's Programmes

Online Verification of Academic Qualification

I. e-Certification for Graduates (via AIMS)

[from Class of 2014]

e-Certification is a web-based system developed by CityUHK to enable employers, employment agencies and educational institutions to verify electronically the academic award(s) obtained by a Research Postgraduate / Professional Doctorate / Master's (Taught Postgraduate) / Bachelor's / Associate Degree holder (for Class of 2014 onwards).

By using the system, a graduate can generate and share a secured, direct CityUHK URL, and the e-Certificate image (for Class of 2022 onwards), at his/her discretion, to a third party for verification of his/her award details. The information is encrypted with an access code provided by the graduate to the designated viewer(s) to ensure confidentiality.

e-Certificate images will normally be available on the system two weeks from the graduation date.

What the challenges?

- How can certificate holder prevent leak of access?
  - In HKUST Blockcert and CityU, anyone with JSON and access code can view the certificate.
- Decentralize verification
- Decentralize certificate issuing
- Scope
  - Type of academic institution: university, secondary school?
- Ideal solution:
  - Use blockchain account (wallet) to send “credentials”
  - Can everyone manage blockchain account?
- Trade-off?
  - Credentials hold by trusted platform

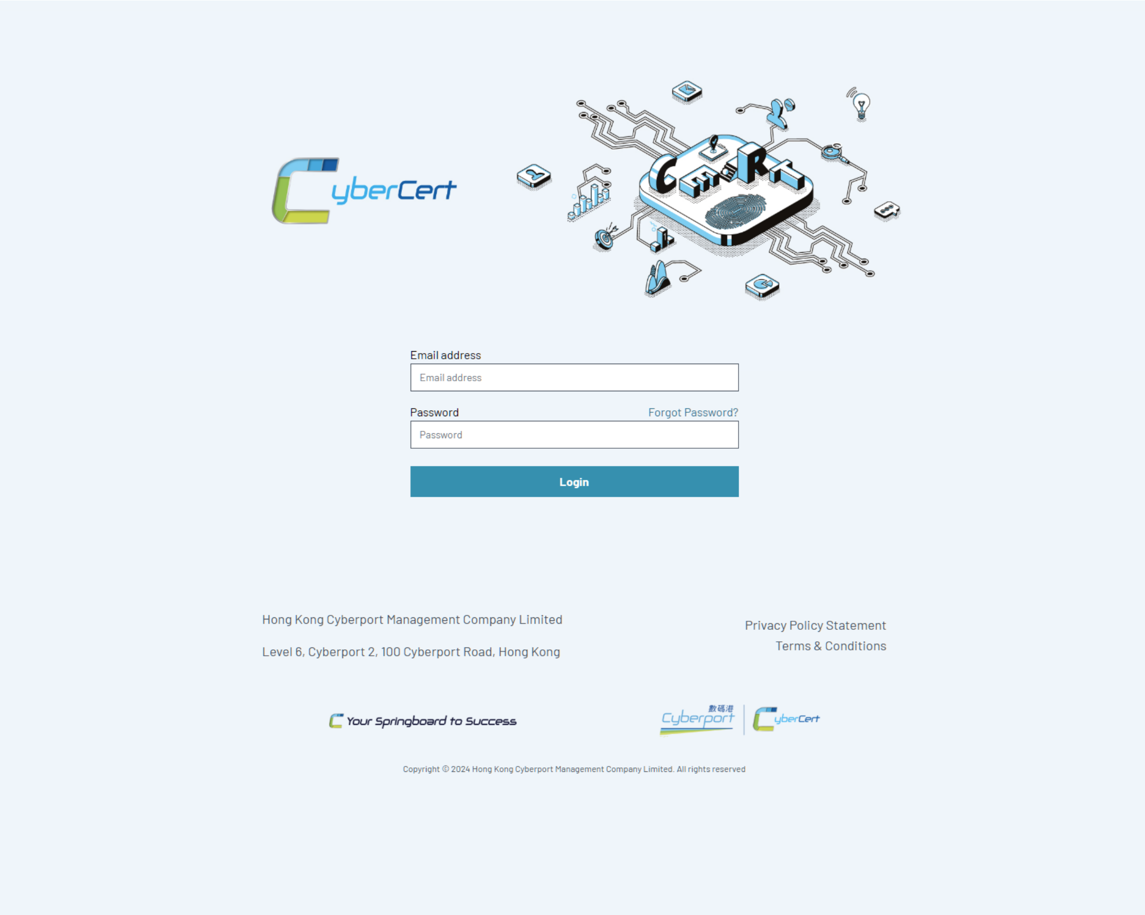
Introduce CyberCert

- CyberCert is Cyberport initiative for **e-Certification platform for local academic institution**.
- Currently launch for limited users.
- Features:
  - Certificate holder can track and manage access restriction to share certificate.
  - Academic institution can issue certificate through the platform.

CyberCert Design Overview

- **Decentralization** on roadmap
  - Getting academic institution on-board
- Permissioned blockchain: Hyperledger
  - Full ownership of data for privacy. Certificate may have private information.
  - Not require any monetary features.
  - Open source.

CyberCert Homepage



CyberCert

Email address

Email address

Password

Forgot Password?

Password

Login

Hong Kong Cyberport Management Company Limited

Level 6, Cyberport 2, 100 Cyberport Road, Hong Kong

Privacy Policy Statement

Terms & Conditions

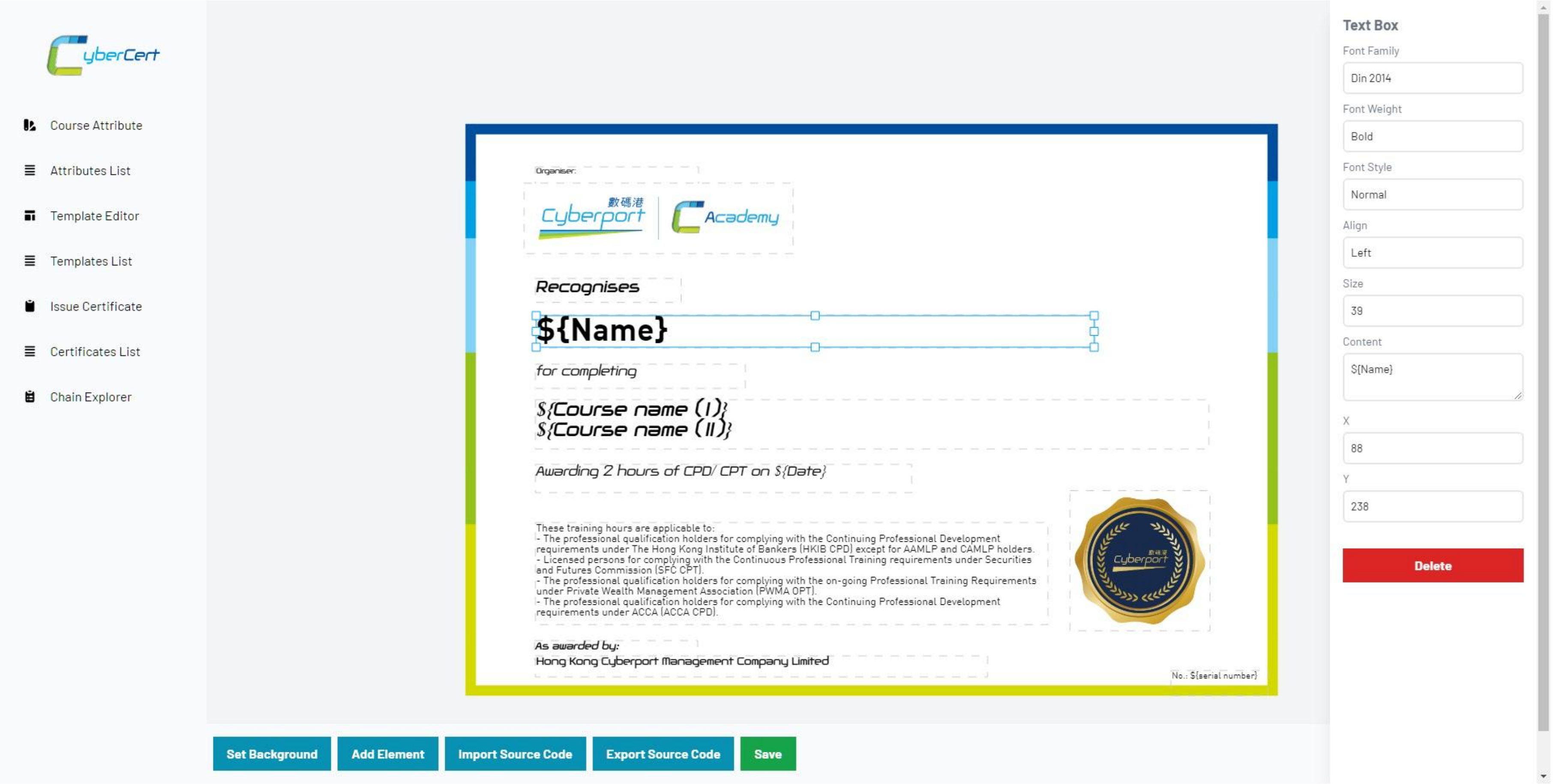
Your Springboard to Success

Cyberport 數碼港 | CyberCert

Copyright © 2024 Hong Kong Cyberport Management Company Limited. All rights reserved

https://cybercert.cyberport.hk/

Certificate Template



Organiser:

Recognises

${Name}

for completing

${Course name (I)}
${Course name (II)}

Awarding 2 hours of CPD/ CPT on ${Date}

These training hours are applicable to:
- The professional qualification holders for complying with the Continuing Professional Development requirements under The Hong Kong Institute of Bankers (HKIB CPD) except for AAMLP and CAMLP holders.
- Licensed persons for complying with the Continuous Professional Training requirements under Securities and Futures Commission (SFC CPT).
- The professional qualification holders for complying with the on-going Professional Training Requirements under Private Wealth Management Association (PWMA OPT).
- The professional qualification holders for complying with the Continuing Professional Development requirements under ACCA (ACCA CPD).

As awarded by:
Hong Kong Cyberport Management Company Limited

No.: ${serial number}

Text Box

Font Family: Din 2014

Font Weight: Bold

Font Style: Normal

Align: Left

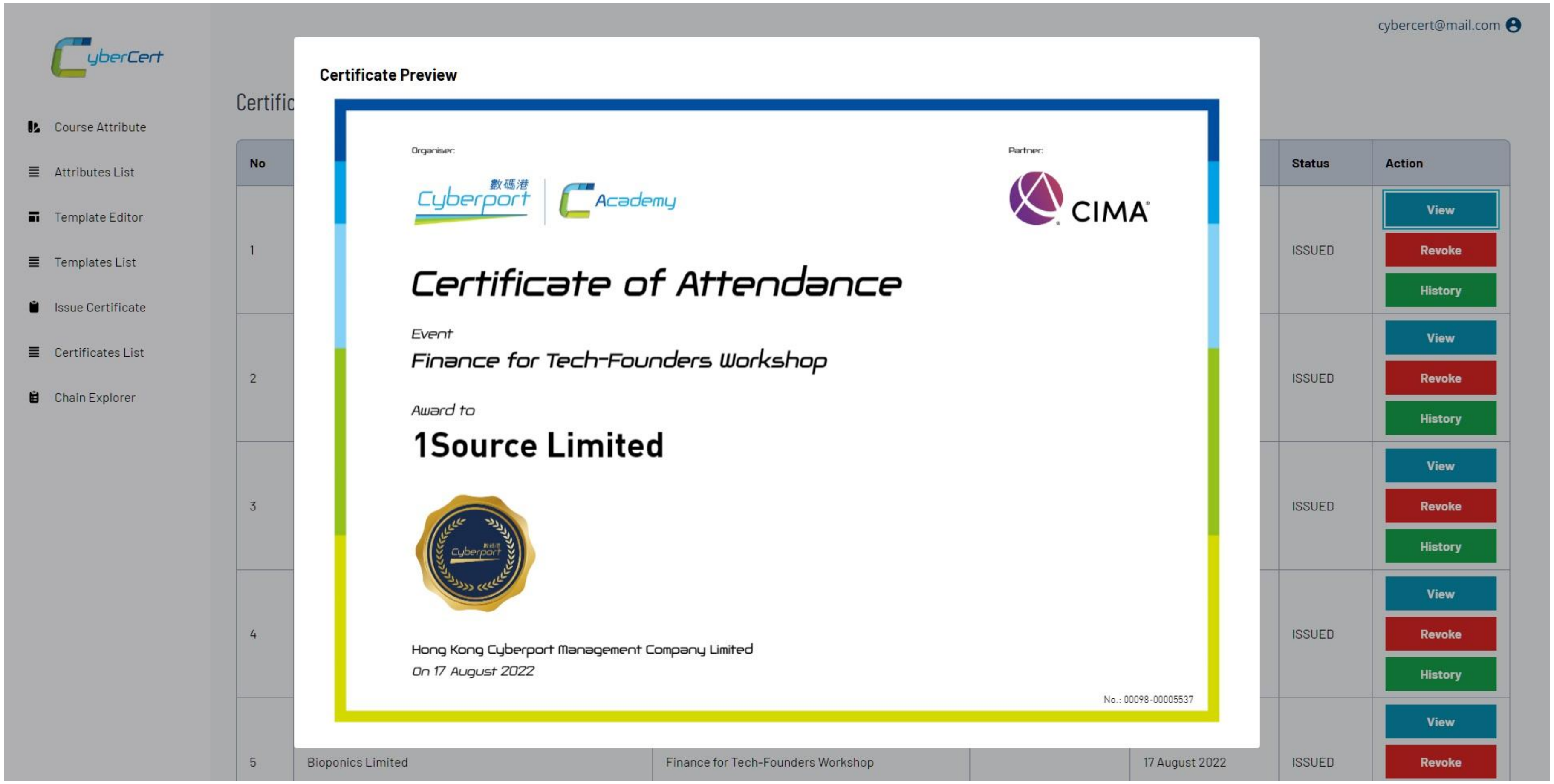
Size: 39

Content: ${Name}

X: 88

Y: 238

Certificate Preview



Certificate Preview

Organiser:

Cyberport 數碼港 | Academy

Partner:

CIMA

Certificate of Attendance

Event

Finance for Tech-Founders Workshop

Award to

1Source Limited

Hong Kong Cyberport Management Company Limited

On 17 August 2022

No.: 00098-00005537

No					Status	Action
1					ISSUED	View Revoke History
2					ISSUED	View Revoke History
3					ISSUED	View Revoke History
4					ISSUED	View Revoke History
5	Bioponics Limited	Finance for Tech-Founders Workshop		17 August 2022	ISSUED	View Revoke

Ethereum

- Proof-of-Work (PoW) to Proof-of-Stake (PoS) in 2022.
- In PoS, instead of mining, user *vote* for validator to propose the block.
- Block is produced in 1 **slot**.
- In each **slot** (**12 seconds**), one validator is randomly selected to be a block proposer, who can create new block.
- In each slot, a committee of validators is randomly selected, who vote to support/deny validity of the block.
- 1 epoch = ~32 slots = 6.4 minutes.
- Transaction finality takes **2 epochs** (~13 minutes).
- **Q: why not make it faster block time?**

Ethereum Accounts

- There are 2 types of Ethereum account:
    - Externally-owned account (EOA)
        - Account controlled by public/private keypair.
    - Contract account
        - Account of contract deployed to Ethereum network.
        - Doesn’t have private key. Controlled by logic of smart contract code.
        - Example: multi-signature wallet
        - Multi-signature wallet
            - Wallet with multiple *owners*
            - To perform operation such *deposit* and *withdraw*, require N of M signatures (approval) for owner to execute. Example: Withdraw 1 ETH require 3 signatures from available 5 owners.

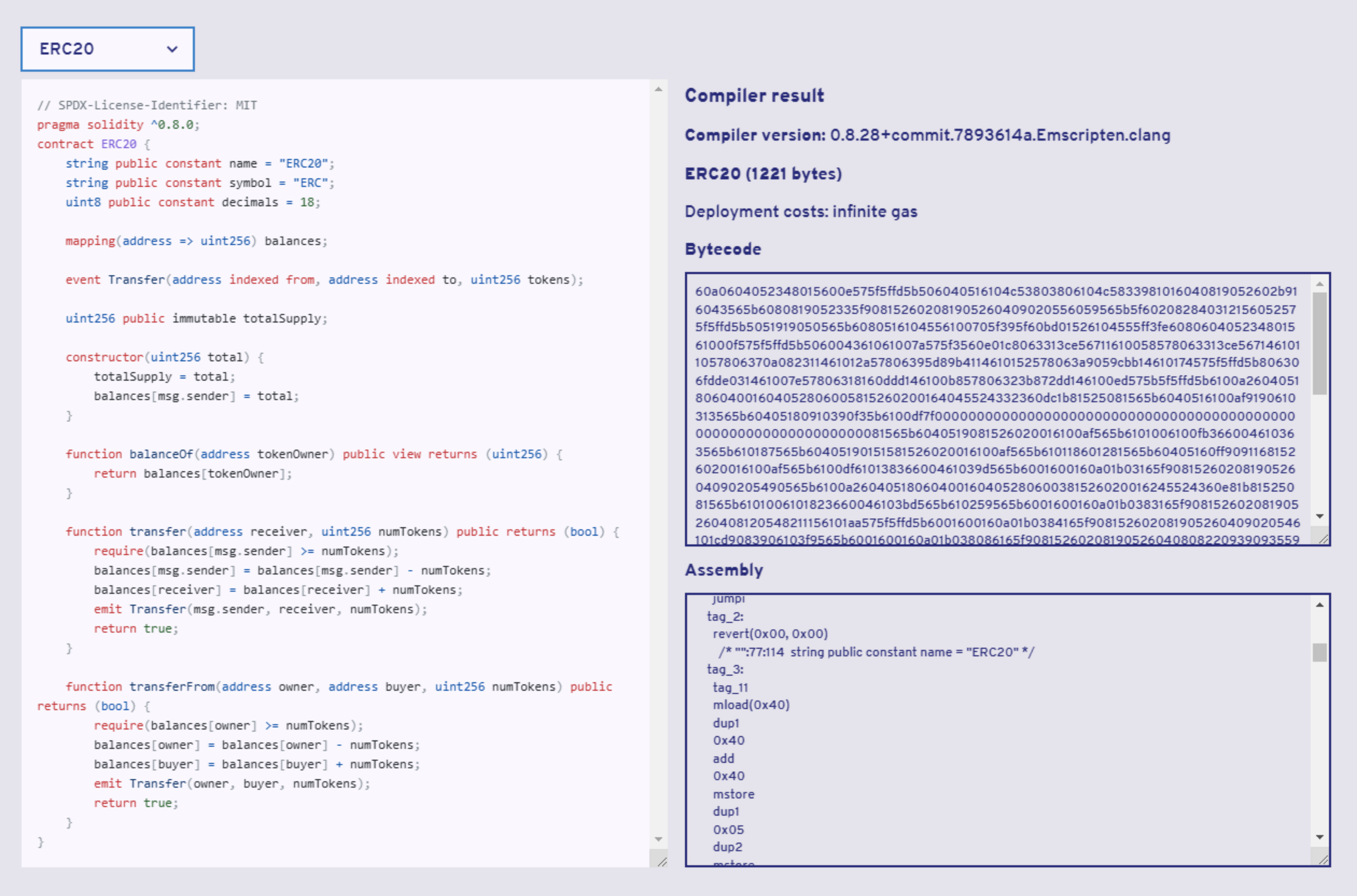
Gas

- *Gas* refers to the **unit** that measures the amount of computational effort required to execute specific operations on the Ethereum network.
- The *gas fee* is the amount of gas used to do some operation, multiplied by the cost per unit gas. The fee is paid regardless of whether a transaction succeeds or fails.
- With gas, it will prevent infinite loops and computational waste.

Smart Contract

- Small, autonomous application run on Ethereum Virtual Machine (EVM)
- Programming language:
  - Solidity (C++, Javascript-like)
  - Vyper (Python-like)
- The smart contract code will be interpreted into *machine code* that can be execute by EVM.
- Executing the code will incur additional *gas* (unit) in transaction.
- Smart contract has *function* and *storage*.
- **Q: what are smart contract limitations?**
- **A: One of limitations, smart contract cannot read/access external information (today's weather, stock price, etc).**

Smart Contract: Example



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract ERC20 {
    string public constant name = "ERC20";
    string public constant symbol = "ERC";
    uint8 public constant decimals = 18;

    mapping(address => uint256) balances;

    event Transfer(address indexed from, address indexed to, uint256 tokens);

    uint256 public immutable totalSupply;

    constructor(uint256 total) {
        totalSupply = total;
        balances[msg.sender] = total;
    }

    function balanceOf(address tokenOwner) public view returns (uint256) {
        return balances[tokenOwner];
    }

    function transfer(address receiver, uint256 numTokens) public returns (bool) {
        require(balances[msg.sender] >= numTokens);
        balances[msg.sender] = balances[msg.sender] - numTokens;
        balances[receiver] = balances[receiver] + numTokens;
        emit Transfer(msg.sender, receiver, numTokens);
        return true;
    }

    function transferFrom(address owner, address buyer, uint256 numTokens) public
returns (bool) {
        require(balances[owner] >= numTokens);
        balances[owner] = balances[owner] - numTokens;
        balances[buyer] = balances[buyer] + numTokens;
        emit Transfer(owner, buyer, numTokens);
        return true;
    }
}
```

Compiler result

Compiler version: 0.8.28+commit.7893614a.Emscripten.clang

ERC20 (1221 bytes)

Deployment costs: infinite gas

Bytecode

```
60a0604052348015600e575f5ffd5b506040516104c53803806104c583398101604081905 2602b91
6043565b6080819052335f90815260208190526040902055605956 5b5f6020828403121560525 7
5f5ffd5b5051919050565b608051610455610070 5f395f60bd01526104555ff3fe6080604052348015
61000f575f5ffd5b50600436106100 7a575f3560e01c8063313ce5671161005857806331 3ce567146101
1057806370a082311461012a57806395d89b41146101525780 63a9059cbb14610174575f5ffd5b80630
6fdde031461007e57806318160ddd146100b857806323b872dd146100ed575b5f5ffd5b6100a2604051
806040016040528060058152602001640455243323 60dc1b81525081565b604051 6100af9190610
313565b60405180910390f35b6100df7f0000000000000000000000000000000000000000000000
000000000000000000081565b6040519081526020016100af565b6101006100fb36600461036
3565b610187565b6040519015158152602001 6100af565b610118601281565b60405160ff909116 8152
6020016100af565b6100df610138366004610 39d565b6001600160a01b03165f9081526020819052 6
04090205490565b6100a26040518060400160405280600381526020016245524360e81b815250
81565b6101006101823660046103bd565b610259565b6001600160a01b0383165f90815260208 1905
2604081205482111561 01aa575f5ffd5b6001600160a01b0384165f908152602081905260409020546
101cd9083906103f9565b6001600160a01b038086165f9081526020819052604080822093909355 9
```

Assembly

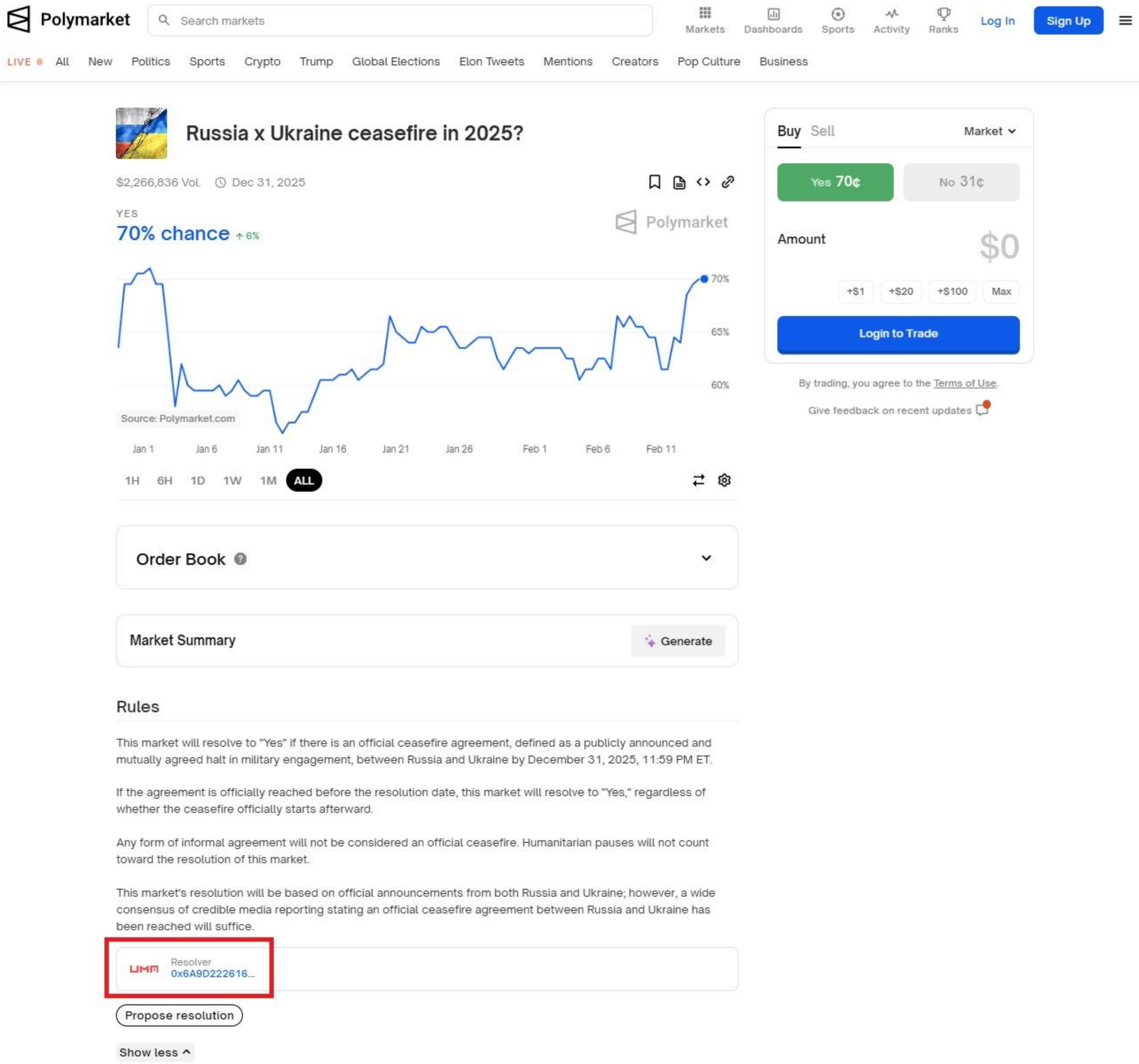
```
  jumpi
tag_2:
  revert(0x00, 0x00)
    /* "":77:114  string public constant name = "ERC20" */
tag_3:
  tag_11
  mload(0x40)
  dup1
  0x40
  add
  0x40
  mstore
  dup1
  0x05
  dup2
  mstore
```

Smart Contract: ERC-20

- ERC-20 is standard of fungible token contract.
- ERC-20 token doesn’t have real value until listed on crypto exchange
- Why use standard? **Interoperability**
  - Token can be listed in multiple crypto exchange.
  - Seamless contract to contract interaction.

Smart Contract: Oracles

- By default, smart contract cannot *read* off-chain (external) information (weather, stock price, etc) to process.
- Oracles source off-chain information to allow smart contract to use external information.
- Example: Polymarket
  - Prediction market for betting on future events.



Russia x Ukraine ceasefire in 2025?

Source: Polymarket.com

By trading, you agree to the Terms of Use.

Give feedback on recent updates

Market Summary

Rules

This market will resolve to "Yes" if there is an official ceasefire agreement, defined as a publicly announced and mutually agreed halt in military engagement, between Russia and Ukraine by December 31, 2025, 11:59 PM ET.

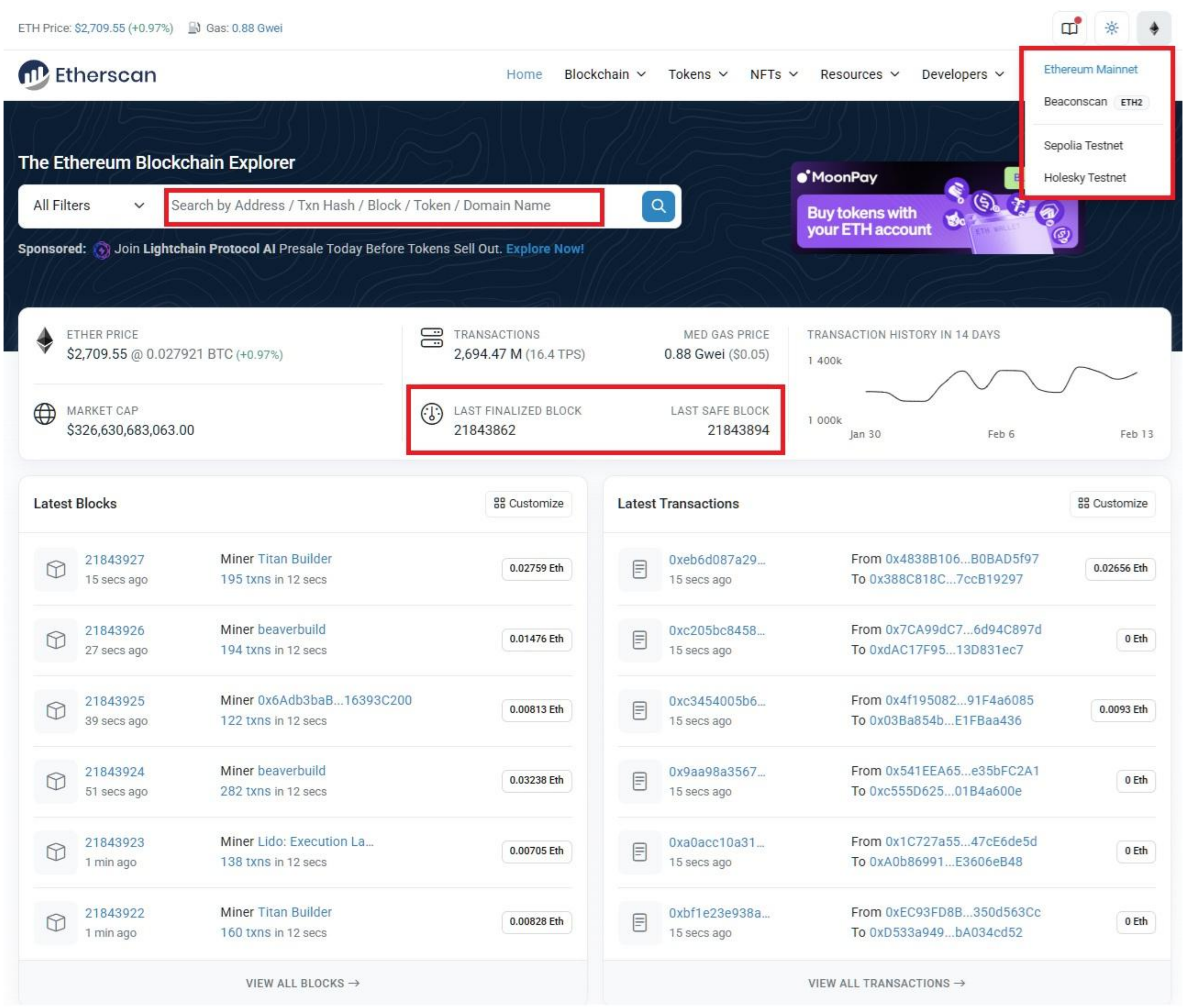
If the agreement is officially reached before the resolution date, this market will resolve to "Yes," regardless of whether the ceasefire officially starts afterward.

Any form of informal agreement will not be considered an official ceasefire. Humanitarian pauses will not count toward the resolution of this market.

This market's resolution will be based on official announcements from both Russia and Ukraine; however, a wide consensus of credible media reporting stating an official ceasefire agreement between Russia and Ukraine has been reached will suffice.

Mini Workshop: Using Blockchain Explorer with Etherscan

- Introduction of features and network (mainnet, beacon chain, and test-net)
- Read basic transaction information: tx status, gas, calldata
- Read public smart contract



ETH Price: $2,709.55 (+0.97%) Gas: 0.88 Gwei

Etherscan

Home | Blockchain | Tokens | NFTs | Resources | Developers

- Ethereum Mainnet
- Beaconscan ETH2
- Sepolia Testnet
- Holesky Testnet

The Ethereum Blockchain Explorer

All Filters | Search by Address / Txn Hash / Block / Token / Domain Name

Sponsored: Join **Lightchain Protocol AI** Presale Today Before Tokens Sell Out. **Explore Now!**

MoonPay Buy tokens with your ETH account

ETHER PRICE
$2,709.55 @ 0.027921 BTC (+0.97%)

MARKET CAP
$326,630,683,063.00

TRANSACTIONS
2,694.47 M (16.4 TPS)

MED GAS PRICE
0.88 Gwei ($0.05)

LAST FINALIZED BLOCK
21843862

LAST SAFE BLOCK
21843894

TRANSACTION HISTORY IN 14 DAYS

Latest Blocks Customize

21843927 15 secs ago	Miner Titan Builder 195 txns in 12 secs	0.02759 Eth
21843926 27 secs ago	Miner beaverbuild 194 txns in 12 secs	0.01476 Eth
21843925 39 secs ago	Miner 0x6Adb3baB...16393C200 122 txns in 12 secs	0.00813 Eth
21843924 51 secs ago	Miner beaverbuild 282 txns in 12 secs	0.03238 Eth
21843923 1 min ago	Miner Lido: Execution La... 138 txns in 12 secs	0.00705 Eth
21843922 1 min ago	Miner Titan Builder 160 txns in 12 secs	0.00828 Eth

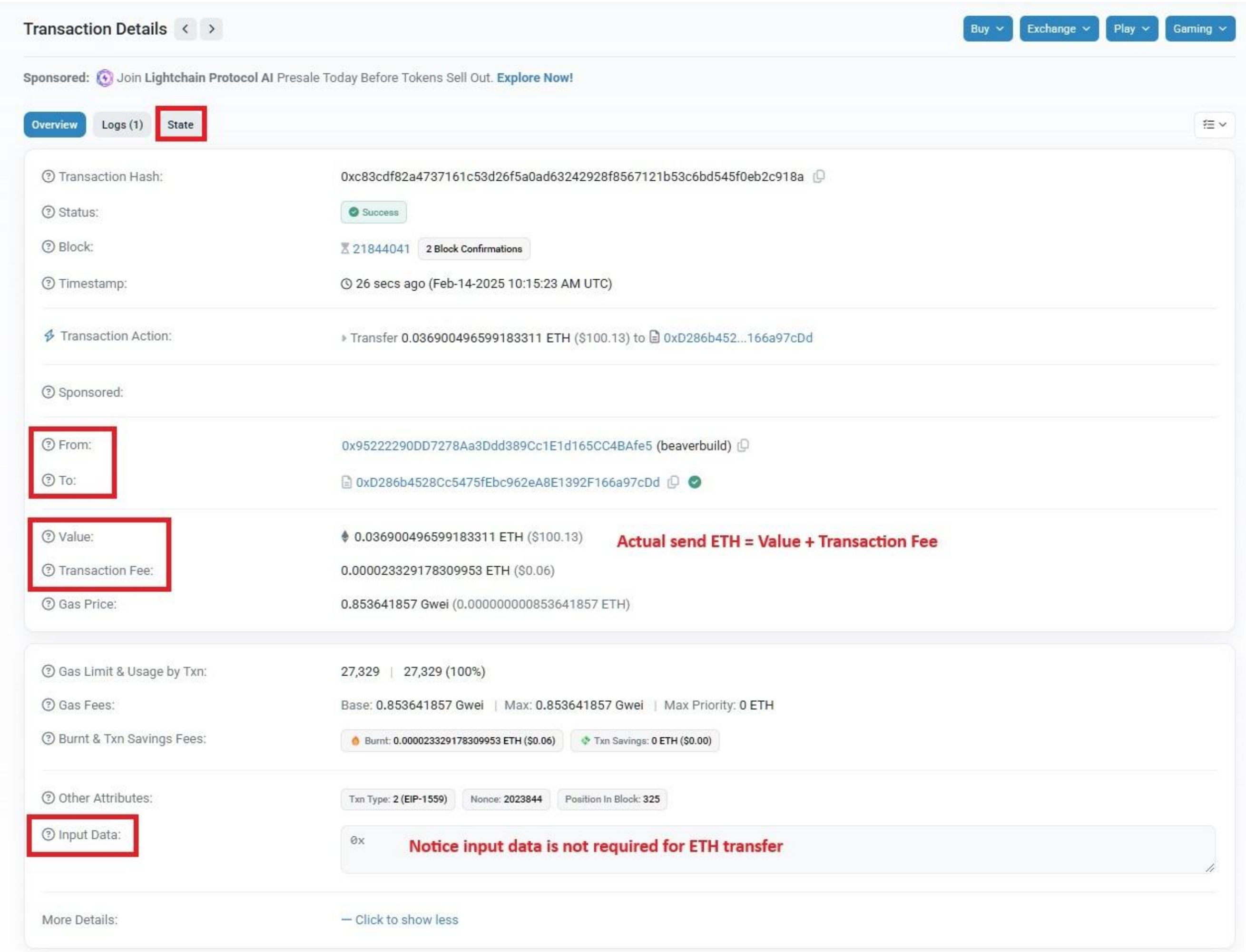
VIEW ALL BLOCKS →

Latest Transactions Customize

0xeb6d087a29... 15 secs ago	From 0x4838B106...B0BAD5f97 To 0x388C818C...7ccB19297	0.02656 Eth
0xc205bc8458... 15 secs ago	From 0x7CA99dC7...6d94C897d To 0xdAC17F95...13D831ec7	0 Eth
0xc3454005b6... 15 secs ago	From 0x4f195082...91F4a6085 To 0x03Ba854b...E1FBaa436	0.0093 Eth
0x9aa98a3567... 15 secs ago	From 0x541EEA65...e35bFC2A1 To 0xc555D625...01B4a600e	0 Eth
0xa0acc10a31... 15 secs ago	From 0x1C727a55...47cE6de5d To 0xA0b86991...E3606eB48	0 Eth
0xbf1e23e938a... 15 secs ago	From 0xEC93FD8B...350d563Cc To 0xD533a949...bA034cd52	0 Eth

VIEW ALL TRANSACTIONS →

Transaction: Send ETH



Sponsored: Join **Lightchain Protocol AI** Presale Today Before Tokens Sell Out. **Explore Now!**

Transaction Hash: 0xc83cdf82a4737161c53d26f5a0ad63242928f8567121b53c6bd545f0eb2c918a

Status: Success

Block: 21844041 2 Block Confirmations

Timestamp: 26 secs ago (Feb-14-2025 10:15:23 AM UTC)

Transaction Action: Transfer 0.036900496599183311 ETH ($100.13) to 0xD286b452...166a97cDd

Sponsored:

From: 0x95222290DD7278Aa3Ddd389Cc1E1d165CC4BAfe5 (beaverbuild)

To: 0xD286b4528Cc5475fEbc962eA8E1392F166a97cDd

Value: 0.036900496599183311 ETH ($100.13)

Actual send ETH = Value + Transaction Fee

Transaction Fee: 0.000023329178309953 ETH ($0.06)

Gas Price: 0.853641857 Gwei (0.000000000853641857 ETH)

Gas Limit & Usage by Txn: 27,329 | 27,329 (100%)

Gas Fees: Base: 0.853641857 Gwei | Max: 0.853641857 Gwei | Max Priority: 0 ETH

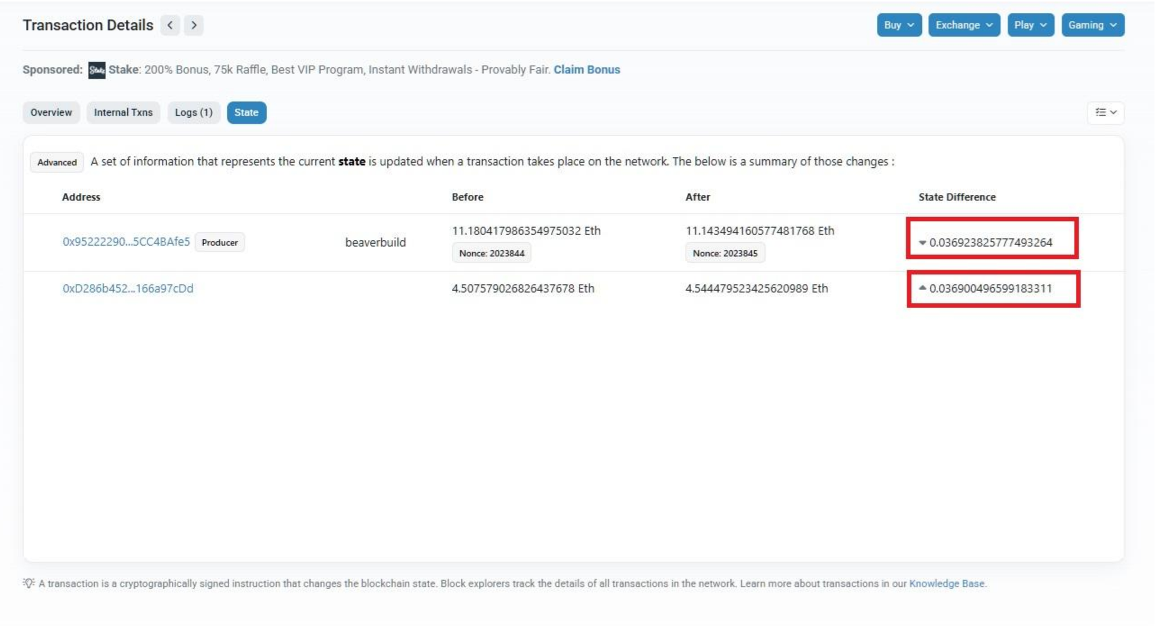
Burnt & Txn Savings Fees: Burnt: 0.000023329178309953 ETH ($0.06) Txn Savings: 0 ETH ($0.00)

Other Attributes: Txn Type: 2 (EIP-1559) Nonce: 2023844 Position In Block: 325

Input Data: 0x

Notice input data is not required for ETH transfer

More Details: — Click to show less



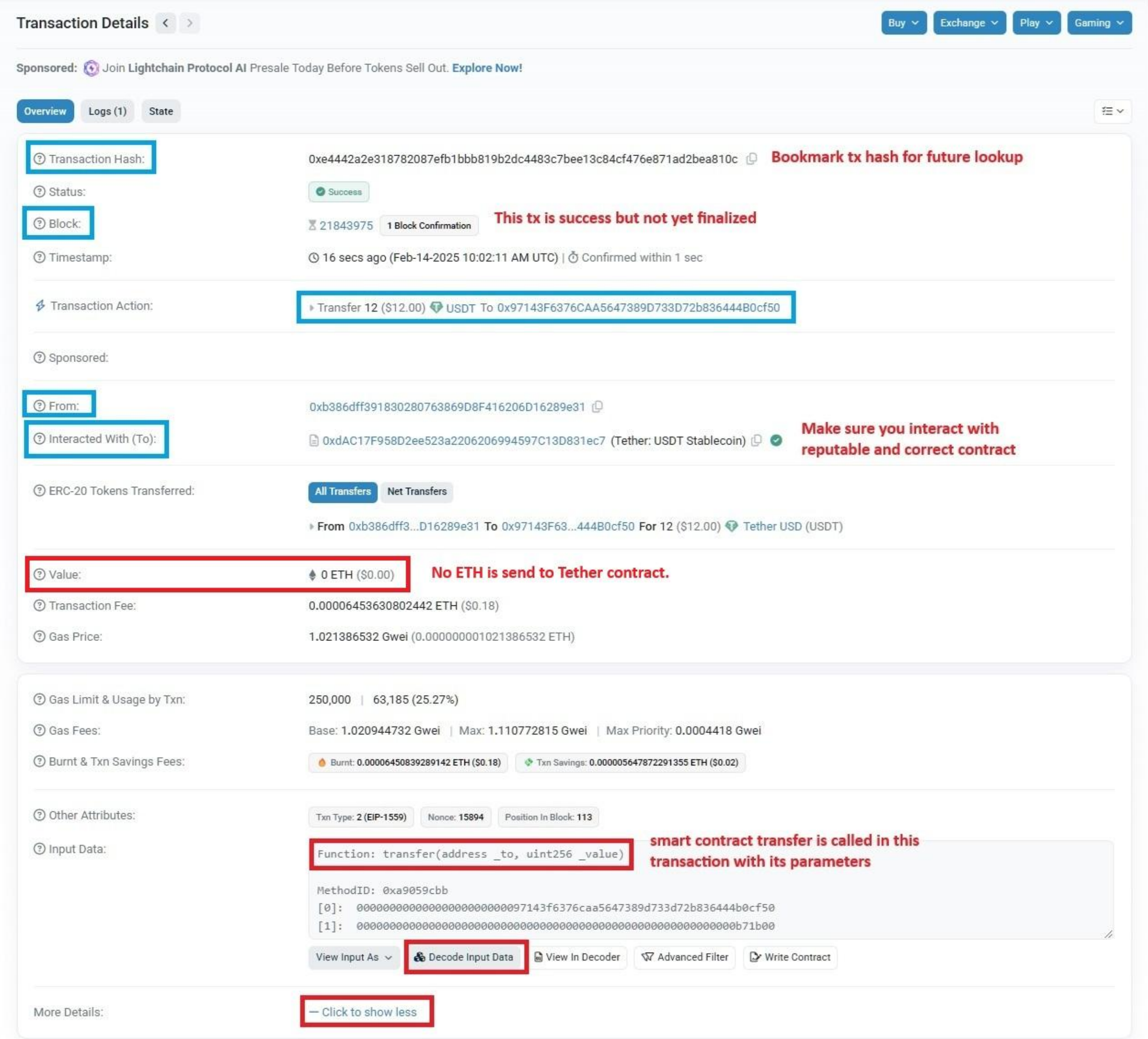
Sponsored: **Stake**: 200% Bonus, 75k Raffle, Best VIP Program, Instant Withdrawals - Provably Fair. **Claim Bonus**

A set of information that represents the current **state** is updated when a transaction takes place on the network. The below is a summary of those changes :

Address		Before	After	State Difference
0x95222290...5CC4BAfe5 Producer	beaverbuild	11.180417986354975032 Eth Nonce: 2023844	11.143494160577481768 Eth Nonce: 2023845	▾ 0.036923825777493264
0xD286b452...166a97cDd		4.507579026826437678 Eth	4.544479523425620989 Eth	▴ 0.036900496599183311

A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our Knowledge Base.

Transaction: Interact with Contract



Sponsored: Join Lightchain Protocol AI Presale Today Before Tokens Sell Out. Explore Now!

Transaction Hash: 0xe4442a2e318782087efb1bbb819b2dc4483c7bee13c84cf476e871ad2bea810c — Bookmark tx hash for future lookup

Status: Success

Block: 21843975 1 Block Confirmation — This tx is success but not yet finalized

Timestamp: 16 secs ago (Feb-14-2025 10:02:11 AM UTC) | Confirmed within 1 sec

Transaction Action: Transfer 12 ($12.00) USDT To 0x97143F6376CAA5647389D733D72b836444B0cf50

Sponsored:

From: 0xb386dff391830280763869D8F416206D16289e31

Interacted With (To): 0xdAC17F958D2ee523a2206206994597C13D831ec7 (Tether: USDT Stablecoin) — Make sure you interact with reputable and correct contract

ERC-20 Tokens Transferred: From 0xb386dff3...D16289e31 To 0x97143F63...444B0cf50 For 12 ($12.00) Tether USD (USDT)

Value: 0 ETH ($0.00) — No ETH is send to Tether contract.

Transaction Fee: 0.000064536308002442 ETH ($0.18)

Gas Price: 1.021386532 Gwei (0.000000001021386532 ETH)

Gas Limit & Usage by Txn: 250,000 | 63,185 (25.27%)

Gas Fees: Base: 1.020944732 Gwei | Max: 1.110772815 Gwei | Max Priority: 0.0004418 Gwei

Burnt & Txn Savings Fees: Burnt: 0.00006450839289142 ETH ($0.18) | Txn Savings: 0.000005647872291355 ETH ($0.02)

Other Attributes: Txn Type: 2 (EIP-1559) | Nonce: 15894 | Position In Block: 113

Input Data:

```
Function: transfer(address _to, uint256 _value)

MethodID: 0xa9059cbb
[0]:  00000000000000000000000097143f6376caa5647389d733d72b836444b0cf50
[1]:  0000000000000000000000000000000000000000000000000000000000b71b00
```

smart contract transfer is called in this transaction with its parameters

More Details: — Click to show less

Exercises: Blockchain Explorer

- How to find genesis transactions?
  - Genesis transaction is first transaction on blockchain
- Which address hold most of Tether USDT token?
  - Tether USDT is ERC-20 for stablecoin
  - Stable coin is token that value pegged to real asset, in USDT 1 token = $1.
- How to get first transaction of Tether USDT?

Refences

- https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/#transaction-execution-ethereum-pos
- https://ethereum.org/en/developers/docs/oracles/

Q&A

- Questions?