Blockchain and Cryptoassets

Alan Wunsche, MBA, CPA, CA, CBP
Toronto, Canada
November 15, 2018

Ivey
Business School
WESTERN UNIVERSITY · CANADA

TokenFunder

OUR OBJECTIVE

1. Know Key Terms and Concepts
2. Understand Cryptoassets, Tokens
3. Highlight Regulatory Concerns

Alan Wunsche
CEO, TokenFunder

AGENDA

1. Blockchain Primer

2. Tokens & CryptoAssets

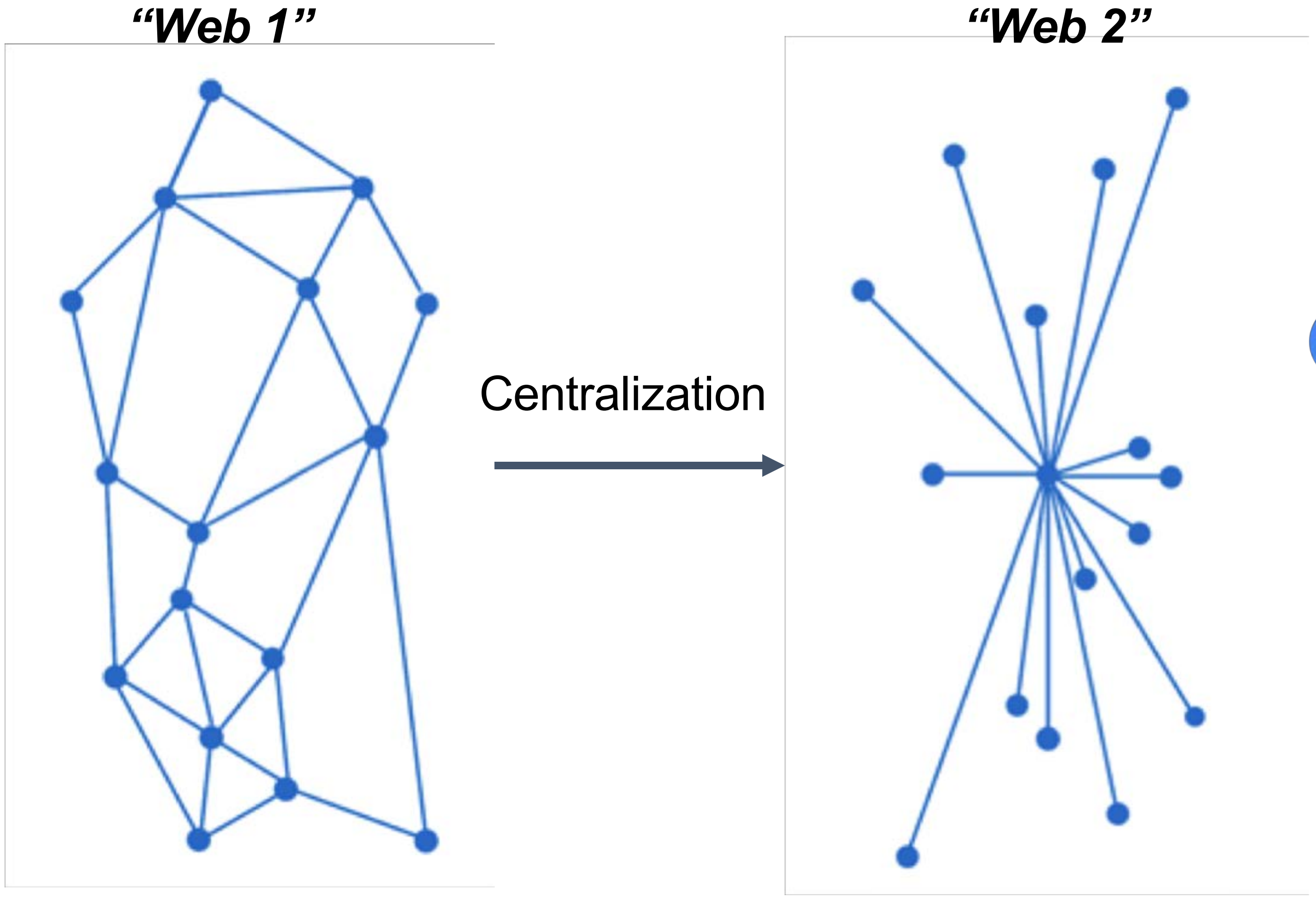
3. TokenFunder & Regulations

TokenFunder

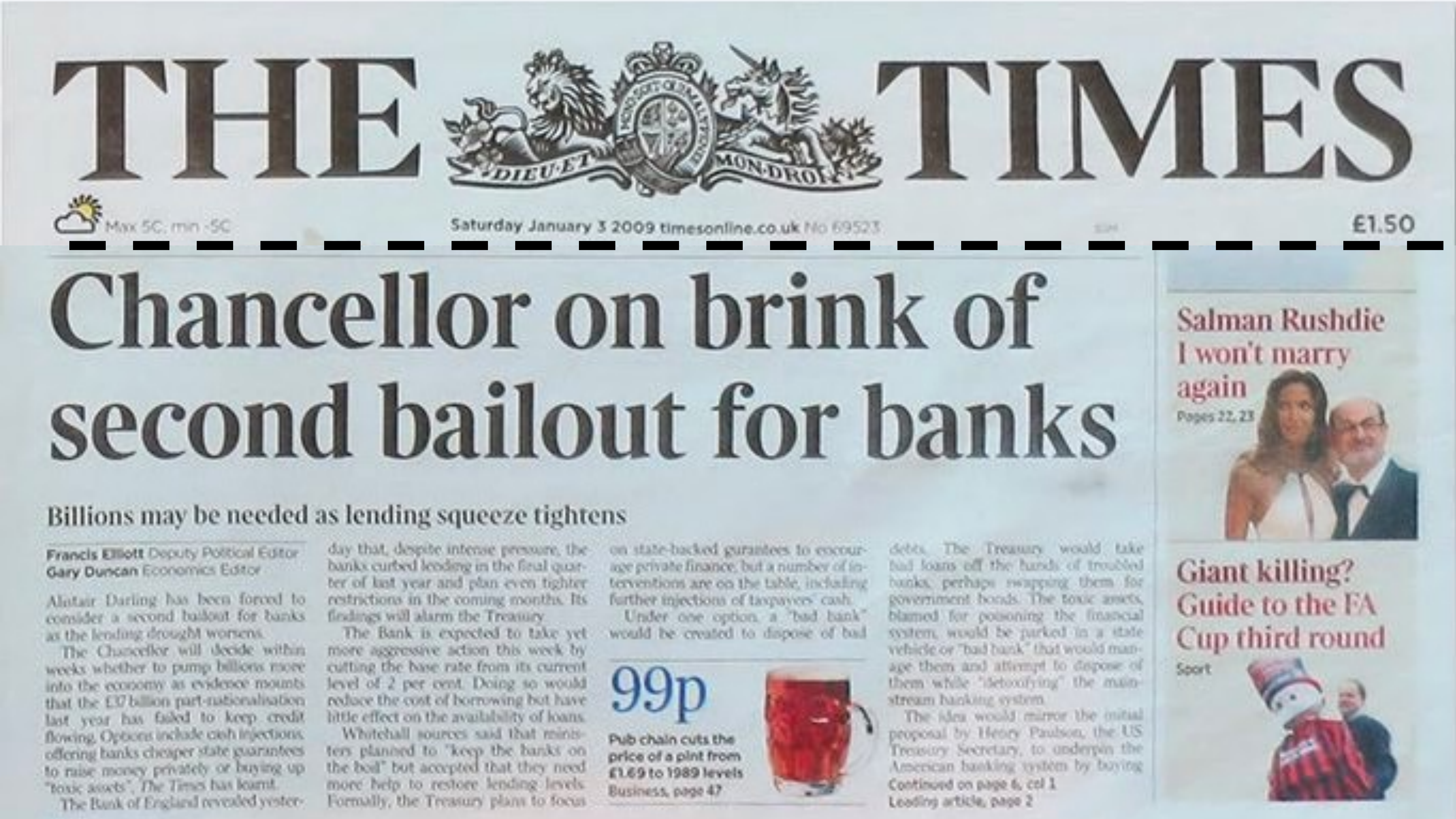
1. BLOCKCHAIN PRIMER

TokenFunder

Evolution of the Internet, Knowledge, Commerce



f	Social Network +
Google	Knowledge Network +
amazon	Commercial Network +
	Mobile. Apps +
UBER	“Sharing” Network



THE TIMES

DIEU ET MON DROIT

Max 5C, min -5C   Saturday January 3 2009 timesonline.co.uk No 69523   £1.50

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", *The Times* has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed gurantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

Business, page 47

Salman Rushdie I won't marry again

Pages 22, 23

Giant killing? Guide to the FA Cup third round

Sport

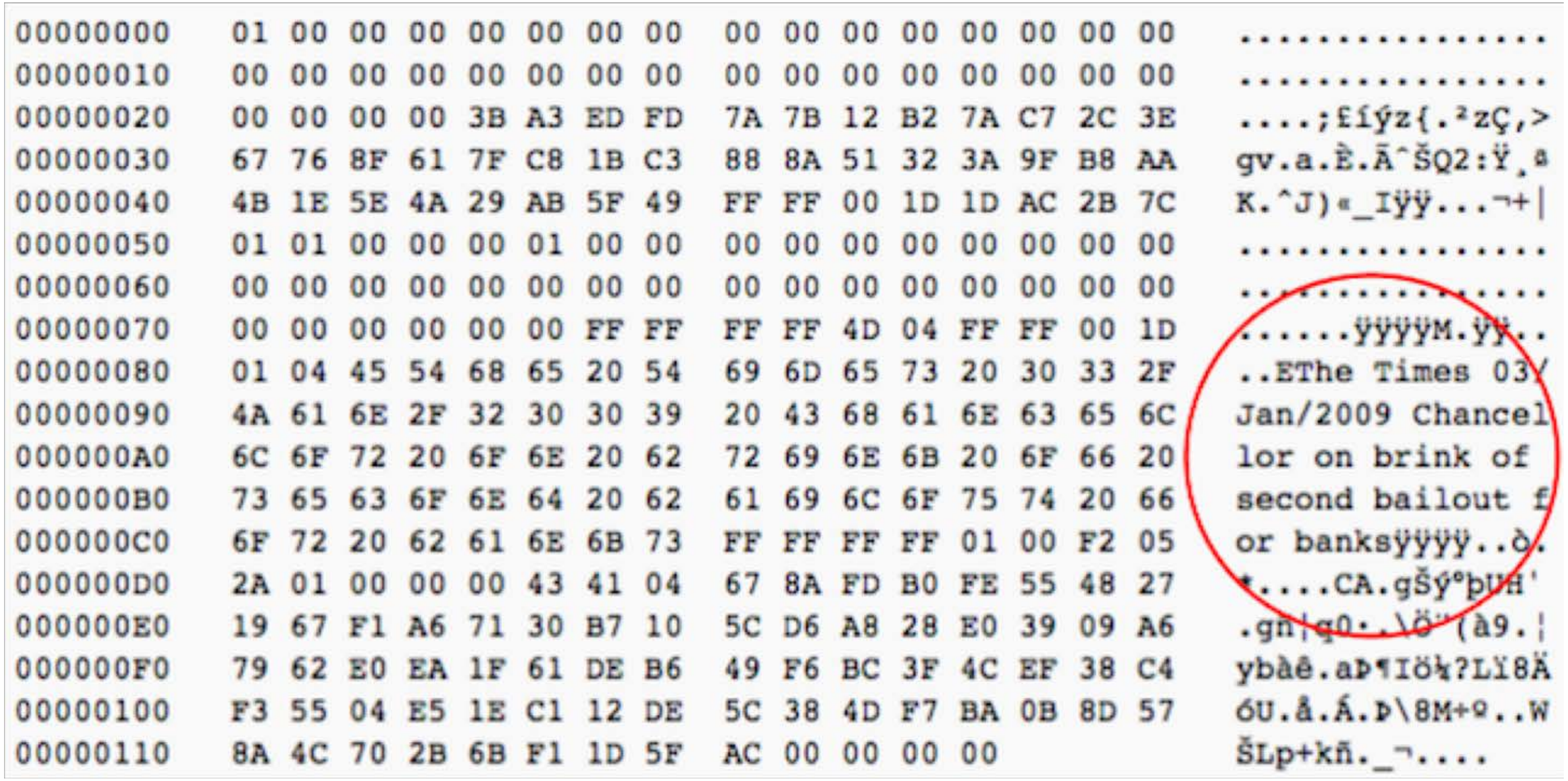
2008

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent ***directly from one party to another without going through a financial institution***. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a ***solution to the double-spending proble***m using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and ***nodes can leave and rejoin the network at will***, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin Genesis Block

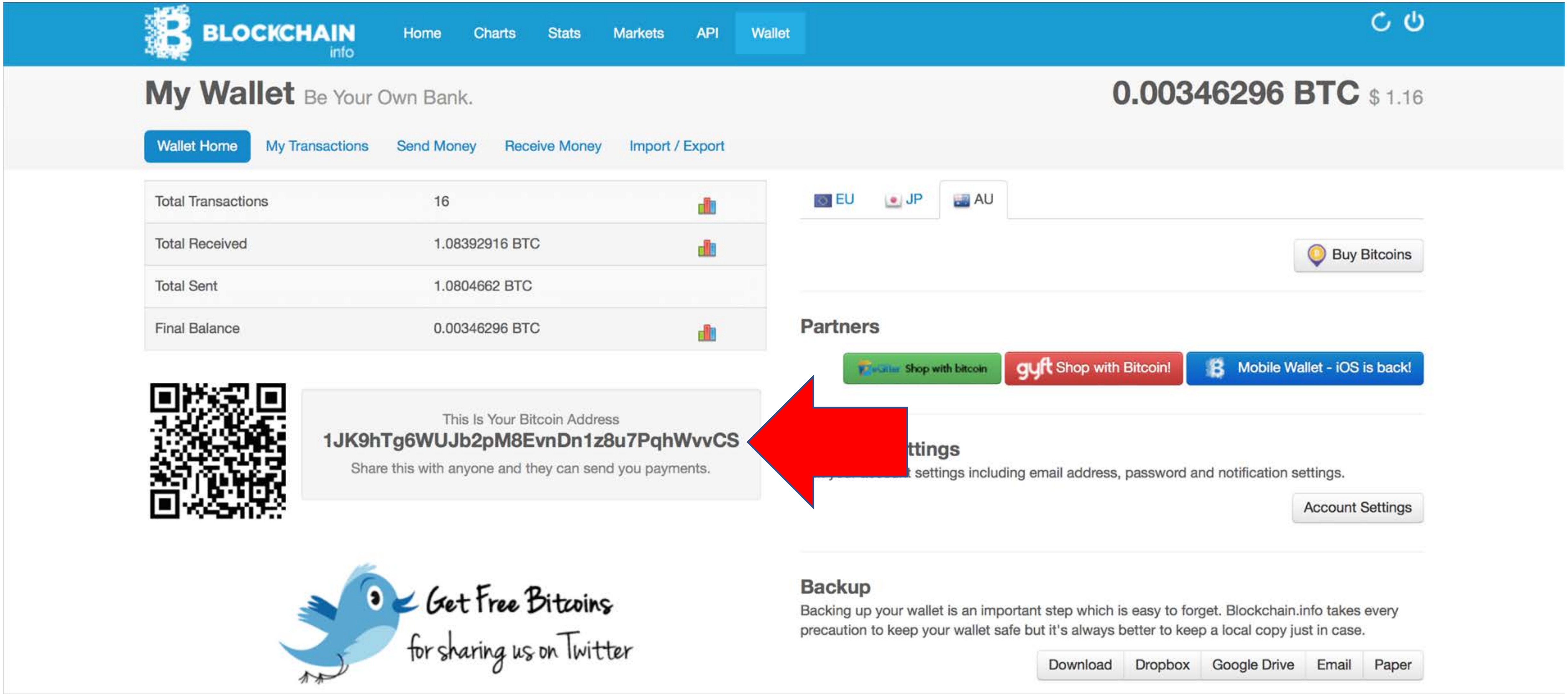


```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.ÃˆŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

Bitcoin was the first open source blockchain technology.

‘bitcoin’ (BTC) is the digital currency transferrable amongst users via Bitcoin.

Bitcoin Address == “Public Key” String



My Wallet Be Your Own Bank.

0.00346296 BTC $ 1.16

Total Transactions	16
Total Received	1.08392916 BTC
Total Sent	1.0804662 BTC
Final Balance	0.00346296 BTC

This Is Your Bitcoin Address

1JK9hTg6WUJb2pM8EvnDn1z8u7PqhWvvCS

Share this with anyone and they can send you payments.

Partners

ttings

t settings including email address, password and notification settings.

Backup

Backing up your wallet is an important step which is easy to forget. Blockchain.info takes every precaution to keep your wallet safe but it's always better to keep a local copy just in case.

Bitcoin Blocks (packages of transactions) – are “created” and secured by miners (computers running the Bitcoin software) every 10 minutes. Mining is Proof-of-Work and consensus.

TokenFunder

Next Generation Blockchains are Programmable

Canadian Startup
(2014)

Now in Switzerland

Next Generation
Decentralized
Applications

TokenFunder

Ethereum is open source blockchain technology.

Ethereum also refers to the public, permissionless blockchain (mainnet).

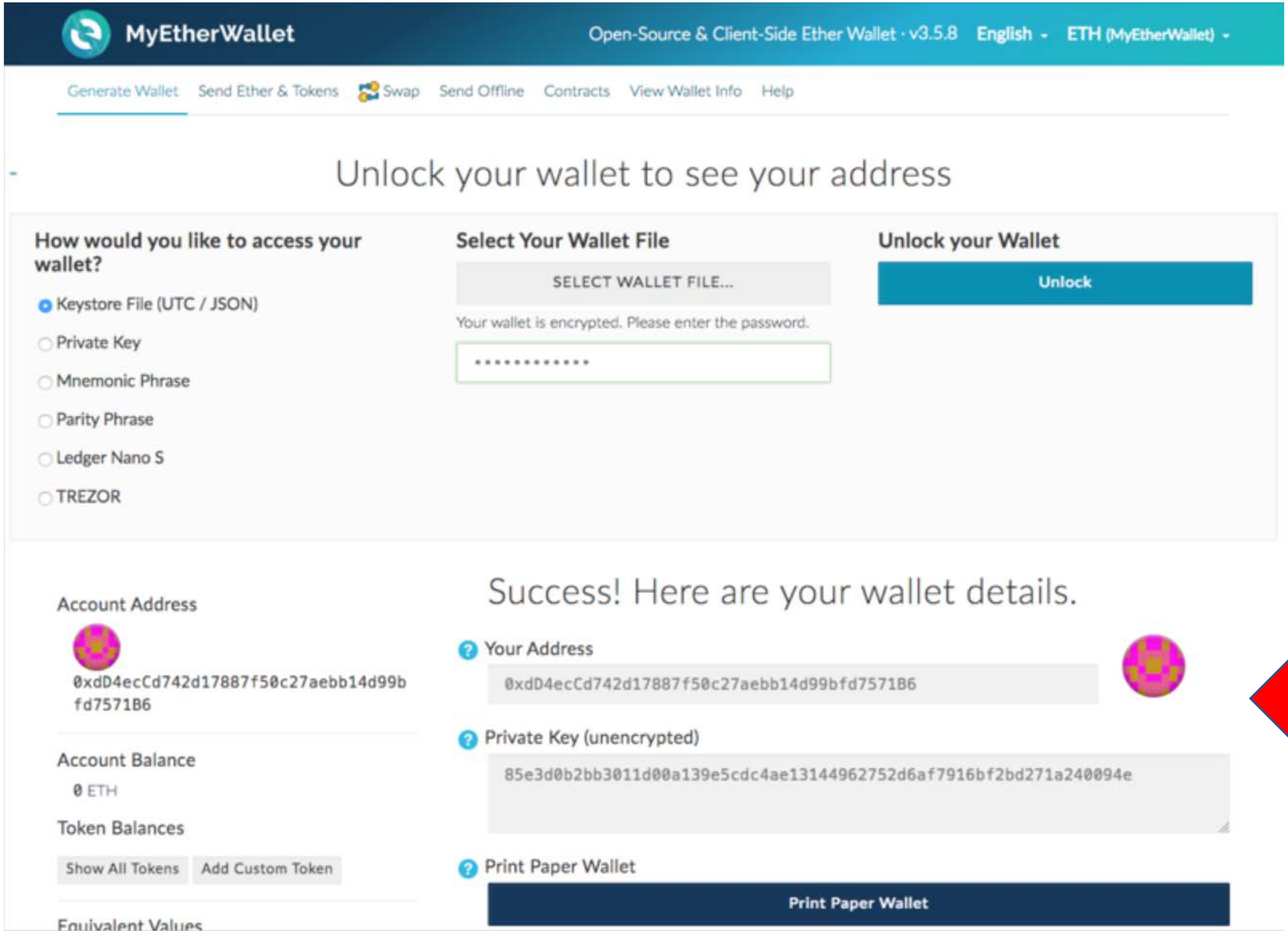
Ethereum is available as a world computer used for decentralized applications.

Users pay for the Ethereum blockchain's computation with Ether (ETH), Ethereum's native digital currency.

TokenFunder

ETH and BTC are cryptoassets, ‘crypto’ because they deploy private and public key cryptography to secure transactions and the blockchain.

Ethereum Account == “Public Key” String



Unlock your wallet to see your address

How would you like to access your wallet?

- ● Keystore File (UTC / JSON)
- ○ Private Key
- ○ Mnemonic Phrase
- ○ Parity Phrase
- ○ Ledger Nano S
- ○ TREZOR

Select Your Wallet File

Your wallet is encrypted. Please enter the password.

•••••••••••••

Unlock your Wallet

Account Address

0xdD4ecCd742d17887f50c27aebb14d99bfd7571B6

Account Balance

0 ETH

Token Balances

Equivalent Values

Success! Here are your wallet details.

Your Address

0xdD4ecCd742d17887f50c27aebb14d99bfd7571B6

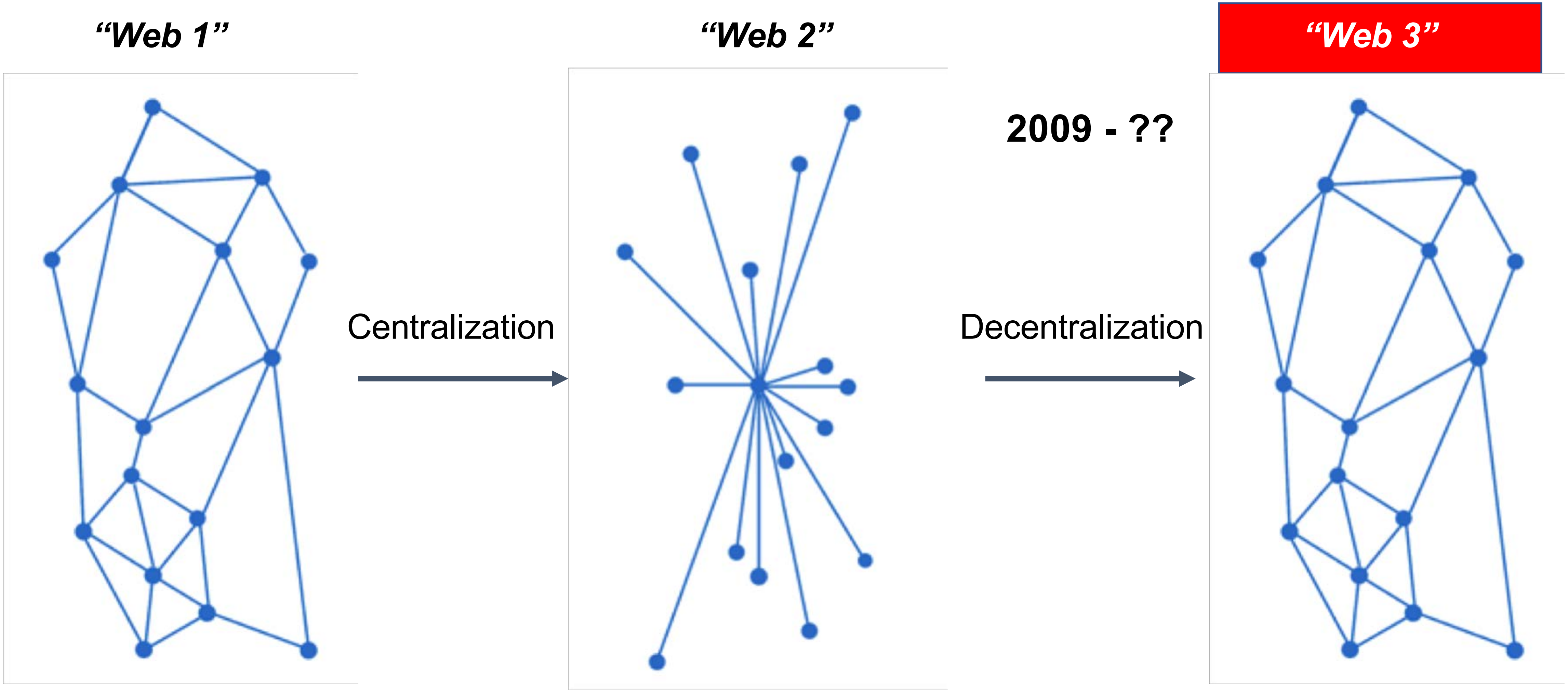
Private Key (unencrypted)

85e3d0b2bb3011d00a139e5cdc4ae13144962752d6af7916bf2bd271a240094e

Print Paper Wallet

TokenFunder

Public Blockchains => “Web 3”



“Web 1”

Centralization

“Web 2”

Decentralization

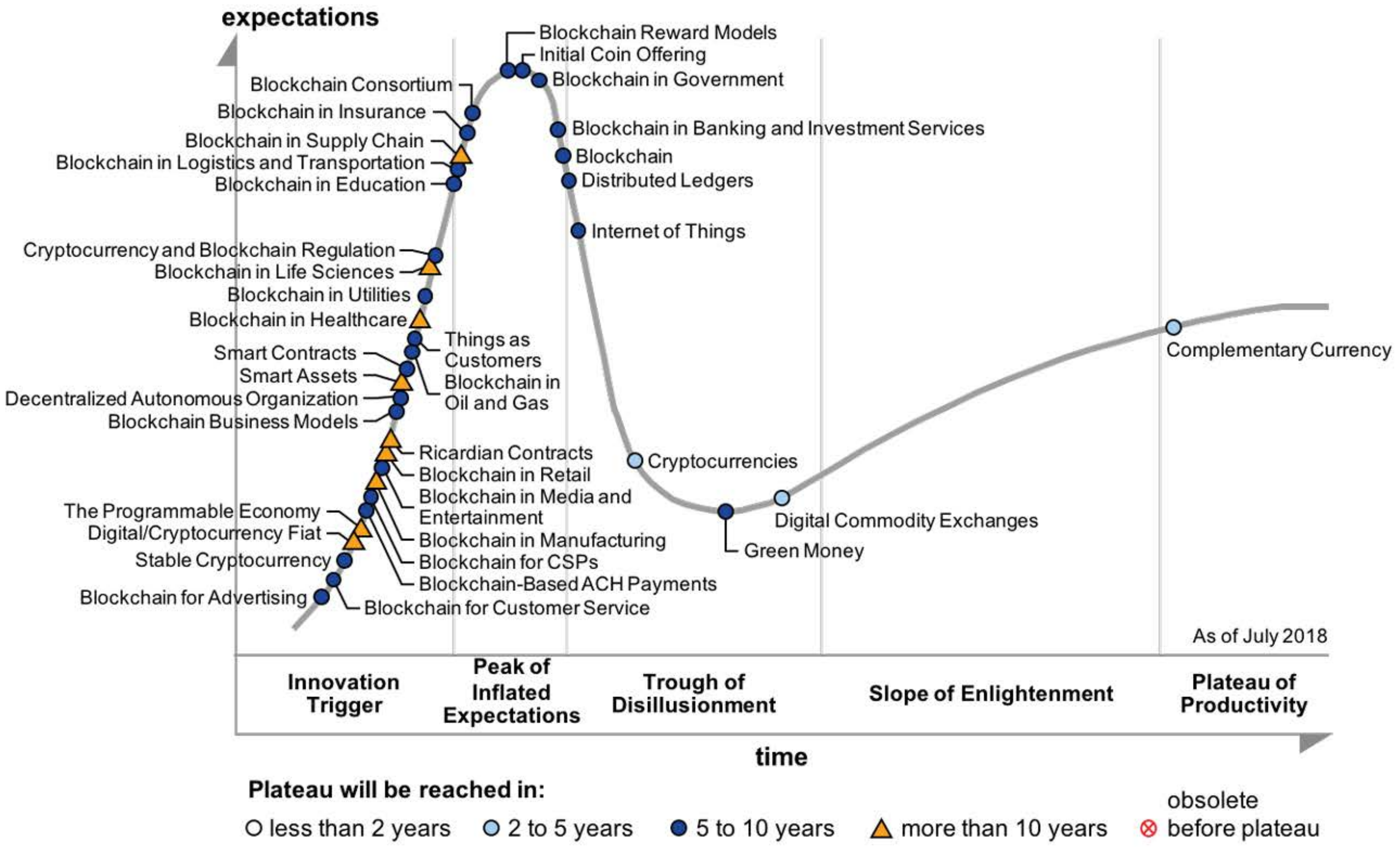
2009 - ??

“Web 3”

TokenFunder

Hyperledger – contributed by IBM to Linux – is another blockchain technology, used for private, permissioned blockchains.

Blockchain Technology “Hype Cycle”



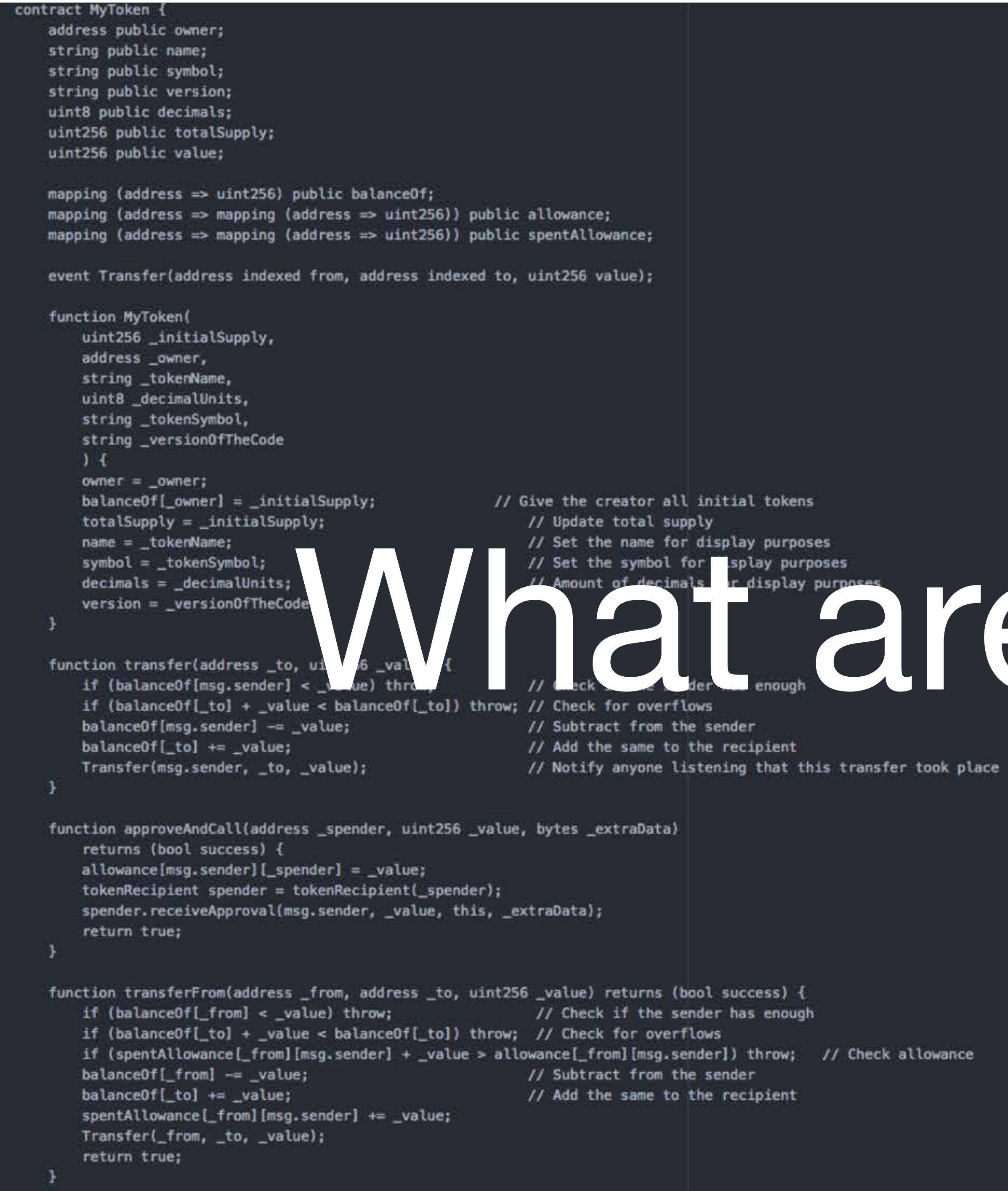
Gartner, July 2018.

TokenFunder

The largest hurdles to mass adoption of public blockchains: scalability of the blockchain software & user experience.

2. TOKENS & CRYPTOASSETS

What are Tokens?



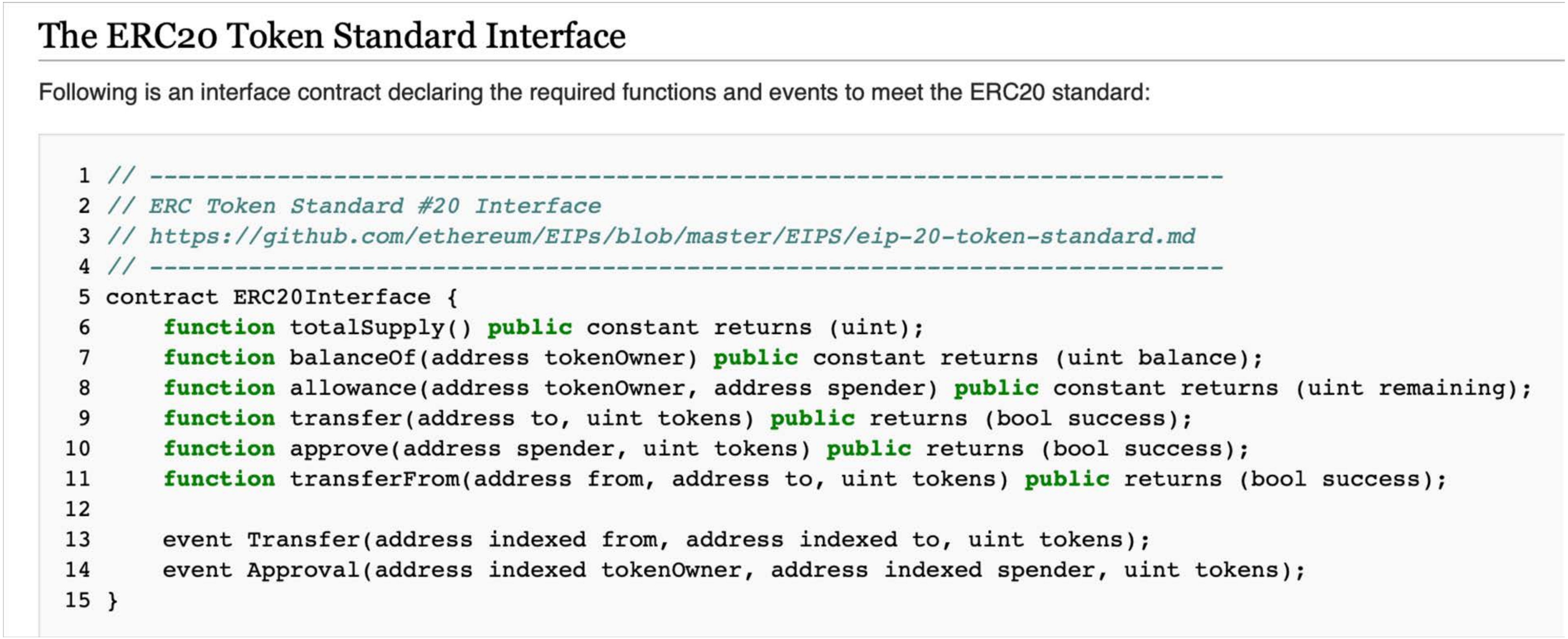
```
contract MyToken {
    address public owner;
    string public name;
    string public symbol;
    string public version;
    uint8 public decimals;
    uint256 public totalSupply;
    uint256 public value;

    mapping (address => uint256) public balanceOf;
    mapping (address => mapping (address => uint256)) public allowance;
    mapping (address => mapping (address => uint256)) public spentAllowance;

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

    function MyToken(
        uint256 _initialSupply,
        address _owner,
        string _tokenName,
        uint8 _decimalUnits,
        string _tokenSymbol,
        string _versionOfTheCode
        ) {
        owner = _owner;
        balanceOf[_owner] = _initialSupply;             // Give the creator all initial tokens
        totalSupply = _initialSupply;                       // Update total supply
        name = _tokenName;                                  // Set the name for display purposes
        symbol = _tokenSymbol;                              // Set the symbol for display purposes
        decimals = _decimalUnits;                           // Amount of decimals for display purposes
        version = _versionOfTheCode
    }

    function transfer(address _to, uint256 _value) {
        if (balanceOf[msg.sender] < _value) throw;          // Check if the sender has enough
        if (balanceOf[_to] + _value < balanceOf[_to]) throw; // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
        Transfer(msg.sender, _to, _value);                  // Notify anyone listening that this transfer took place
    }

    function approveAndCall(address _spender, uint256 _value, bytes _extraData)
        returns (bool success) {
        allowance[msg.sender][_spender] = _value;
        tokenRecipient spender = tokenRecipient(_spender);
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }

    function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
        if (balanceOf[_from] < _value) throw;                // Check if the sender has enough
        if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
        if (spentAllowance[_from][msg.sender] + _value > allowance[_from][msg.sender]) throw;   // Check allowance
        balanceOf[_from] -= _value;                         // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
        spentAllowance[_from][msg.sender] += _value;
        Transfer(_from, _to, _value);
        return true;
    }
```

FNDR

Tokens are programmed applications.

(aka “Smart Contracts”)

Ethereum’s ERC-20 Token Standard



The ERC20 Token Standard Interface

Following is an interface contract declaring the required functions and events to meet the ERC20 standard:

```
// ----------------------------------------------------------------------------
// ERC Token Standard #20 Interface
// https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md
// ----------------------------------------------------------------------------
contract ERC20Interface {
    function totalSupply() public constant returns (uint);
    function balanceOf(address tokenOwner) public constant returns (uint balance);
    function allowance(address tokenOwner, address spender) public constant returns (uint remaining);
    function transfer(address to, uint tokens) public returns (bool success);
    function approve(address spender, uint tokens) public returns (bool success);
    function transferFrom(address from, address to, uint tokens) public returns (bool success);

    event Transfer(address indexed from, address indexed to, uint tokens);
    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
}
```

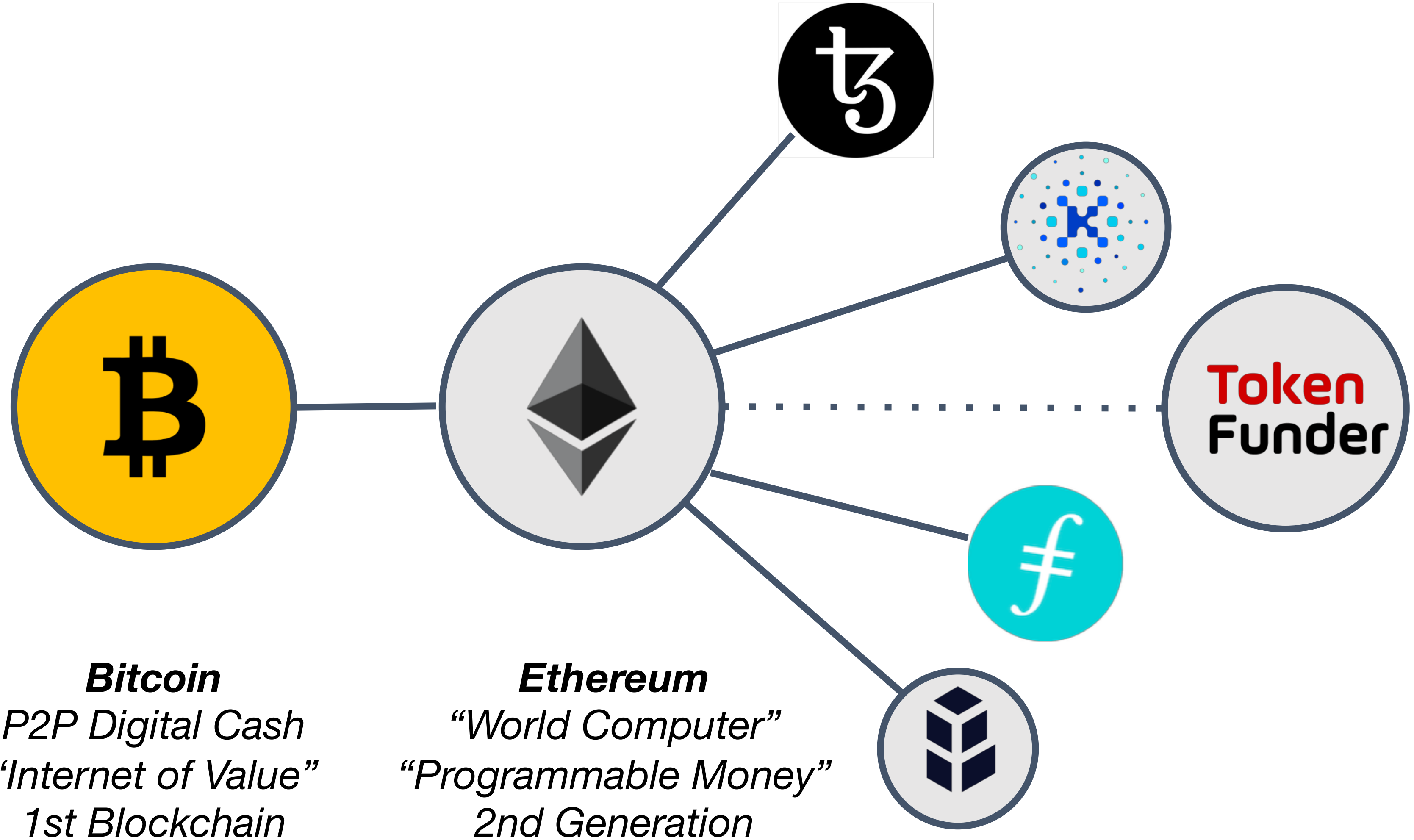
Ethereum's ERC-20 token standard smart contract was a catalyst for initial coin offerings (ICOs)

The ERC-20 **token standard** was easily integrated and rapidly accepted by **digital exchanges.** (e.g. Coinbase, Binance, Coinsquare)

Initial Coin Offerings (ICOs)

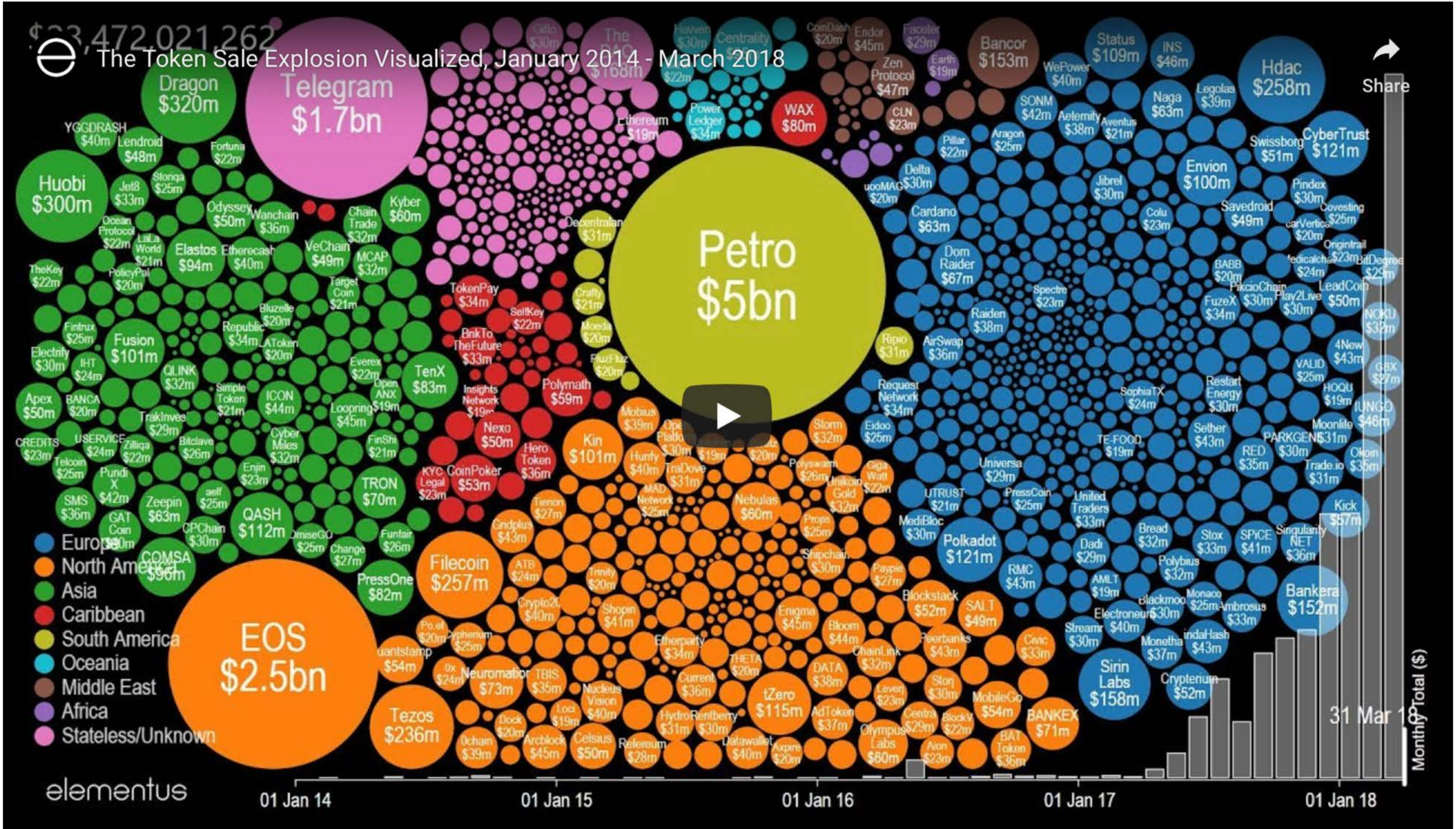
The dawn of cryptofinance…

Blockchain Token Evolution: 2009-2017



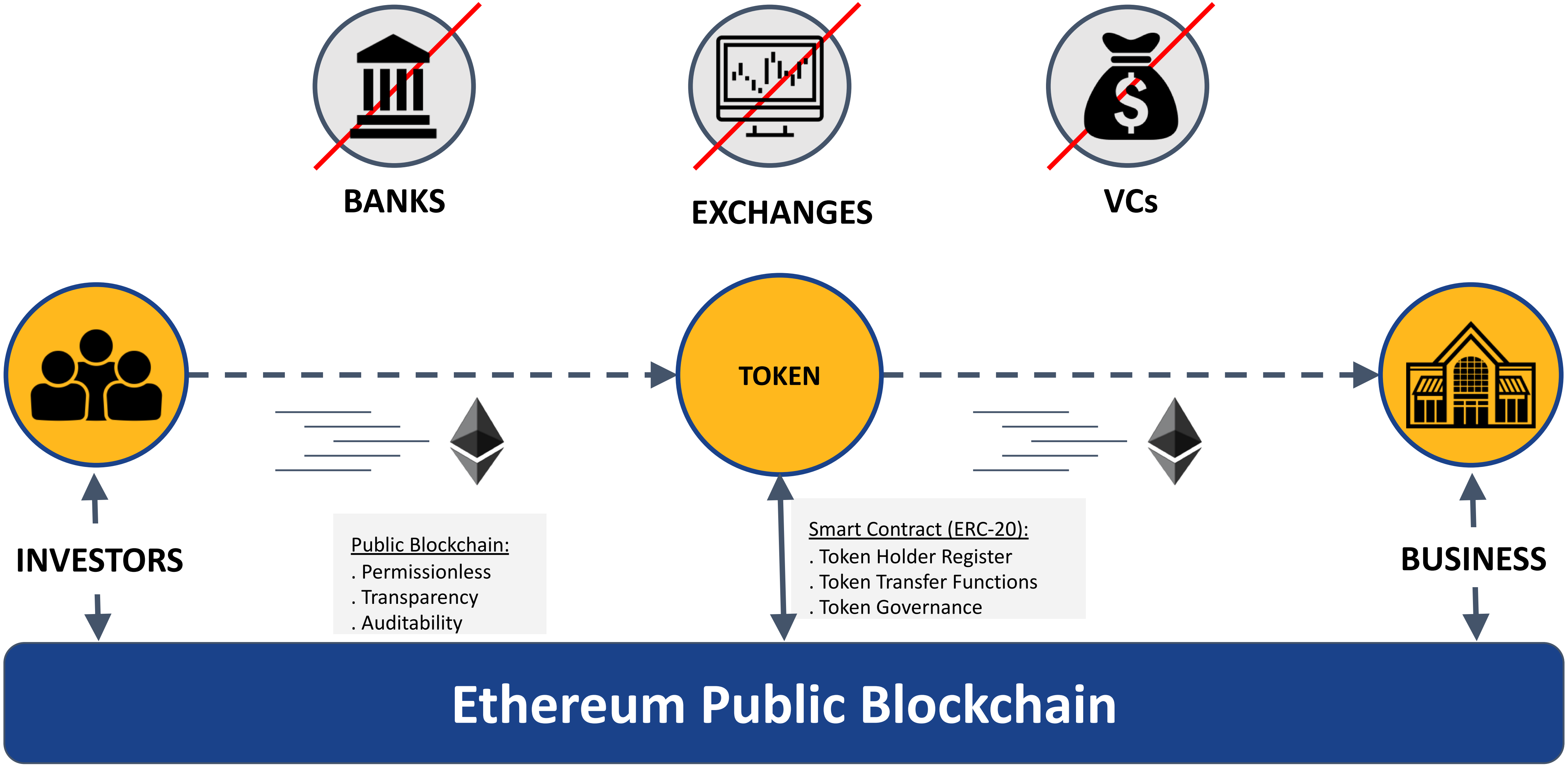
Bitcoin
P2P Digital Cash
"Internet of Value"
1st Blockchain

Ethereum
"World Computer"
"Programmable Money"
2nd Generation Blockchain



The Token Sale Explosion Visualized, January 2014 - March 2018

TokenFunder



BANKS

EXCHANGES

VCs

INVESTORS

TOKEN

BUSINESS

Public Blockchain:
. Permissionless
. Transparency
. Auditability

Smart Contract (ERC-20):
. Token Holder Register
. Token Transfer Functions
. Token Governance

Ethereum Public Blockchain

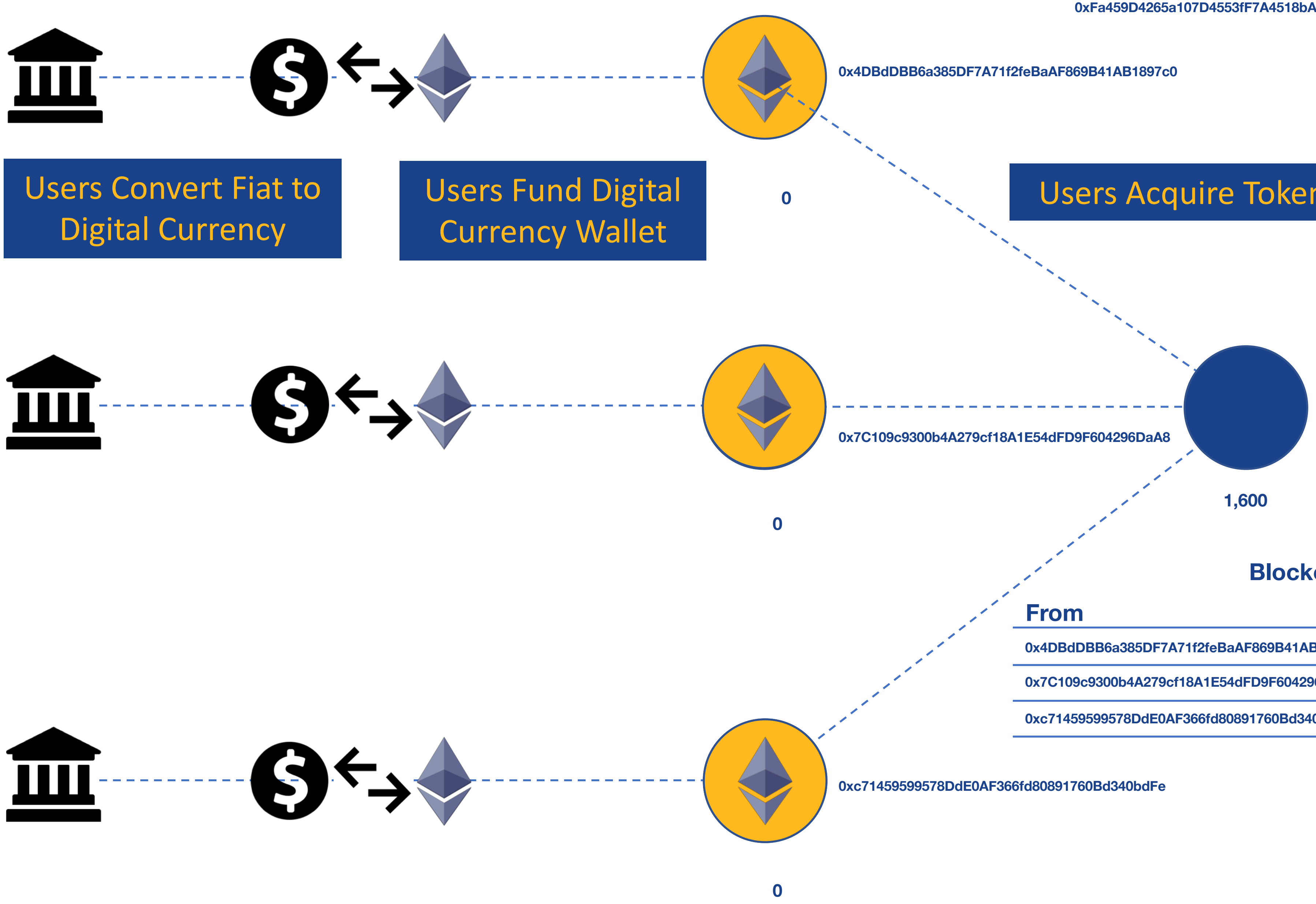
Bank

Digital Currency Exchange

Digital Currency Wallet

Smart Token

0xFa459D4265a107D4553fF7A4518bA7110FeF2C3c



0x4DBdDBB6a385DF7A71f2feBaAF869B41AB1897c0
0
0x7C109c9300b4A279cf18A1E54dFD9F604296DaA8
0
0xc71459599578DdE0AF366fd80891760Bd340bdFe
0
1,600

Users Convert Fiat to Digital Currency

Users Fund Digital Currency Wallet

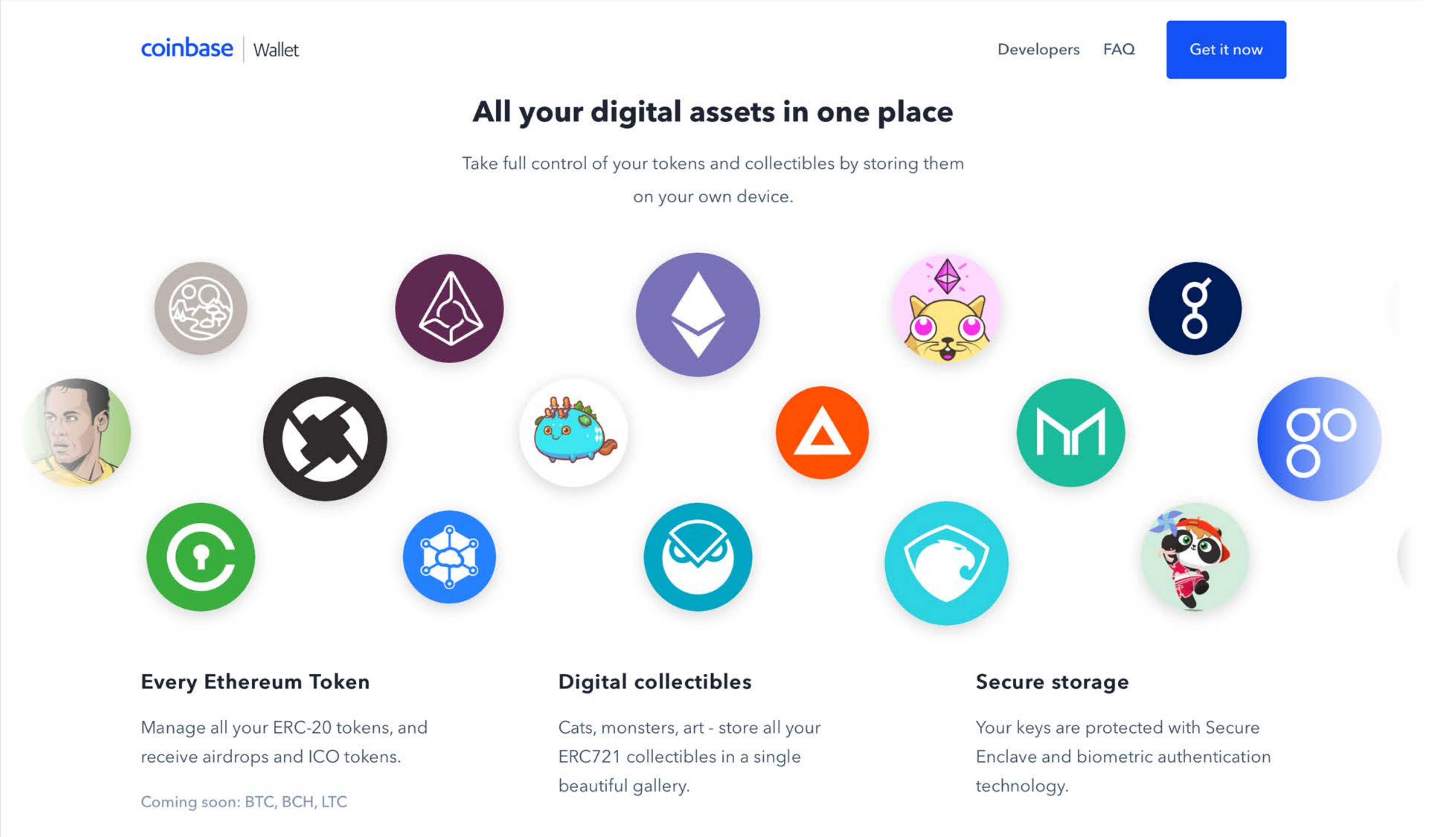
Users Acquire Tokens

Token Holders Registered

Token Holders	Balance
0x4DBdDBB6a385DF7A71f2feBaAF869B41AB1897c0	1,000
0x7C109c9300b4A279cf18A1E54dFD9F604296DaA8	500
0xc71459599578DdE0AF366fd80891760Bd340bdFe	100

Blockchain Transactions

From	To	Amt
0x4DBdDBB6a385DF7A71f2feBaAF869B41AB1897c0	0xFa459D4265a107D4553fF7A4518bA7110FeF2C3c	1,000
0x7C109c9300b4A279cf18A1E54dFD9F604296DaA8	0xFa459D4265a107D4553fF7A4518bA7110FeF2C3c	500
0xc71459599578DdE0AF366fd80891760Bd340bdFe	0xFa459D4265a107D4553fF7A4518bA7110FeF2C3c	100



All your digital assets in one place

Take full control of your tokens and collectibles by storing them on your own device.

Every Ethereum Token

Manage all your ERC-20 tokens, and receive airdrops and ICO tokens.

Coming soon: BTC, BCH, LTC

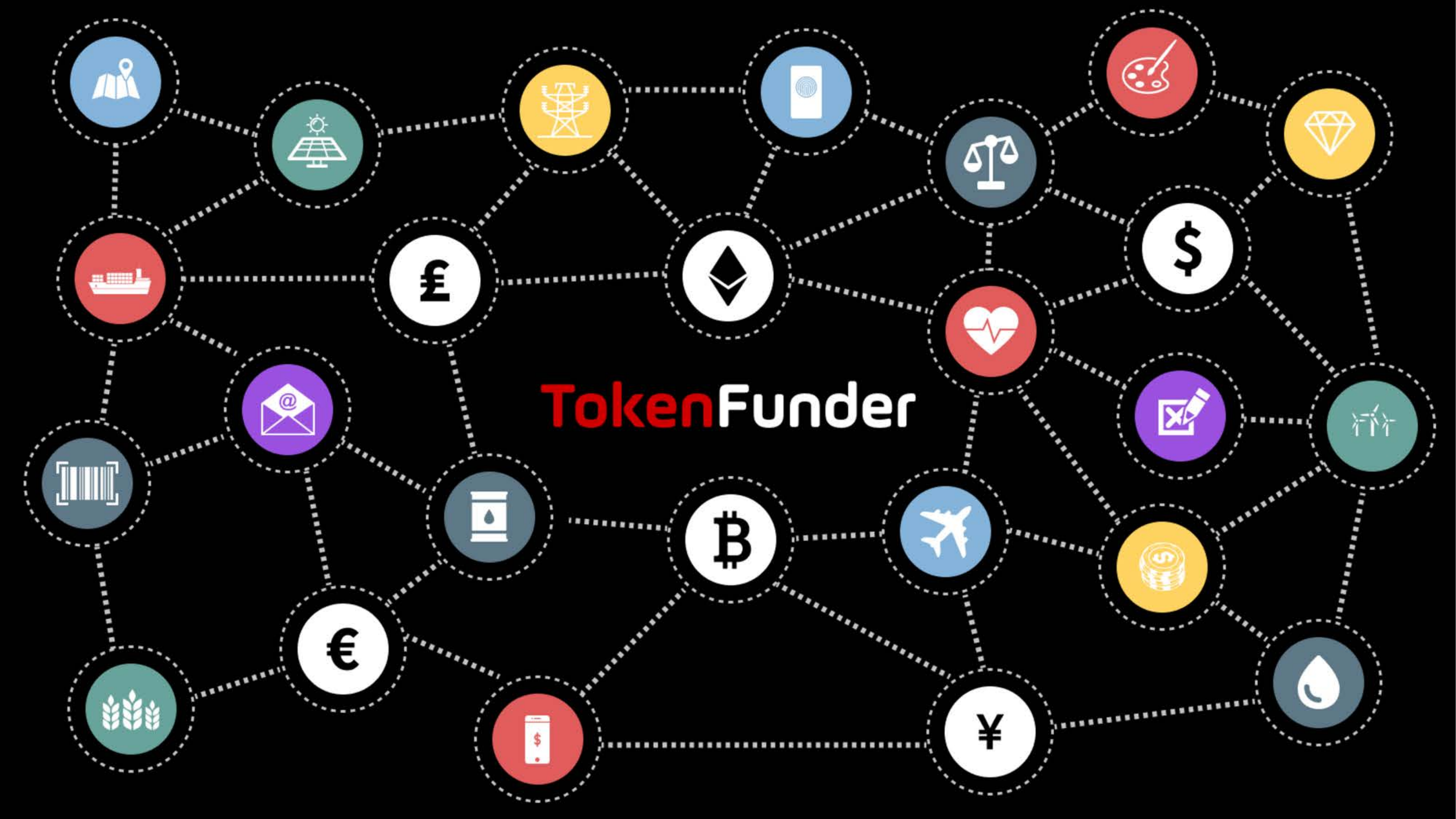
Digital collectibles

Cats, monsters, art - store all your ERC721 collectibles in a single beautiful gallery.

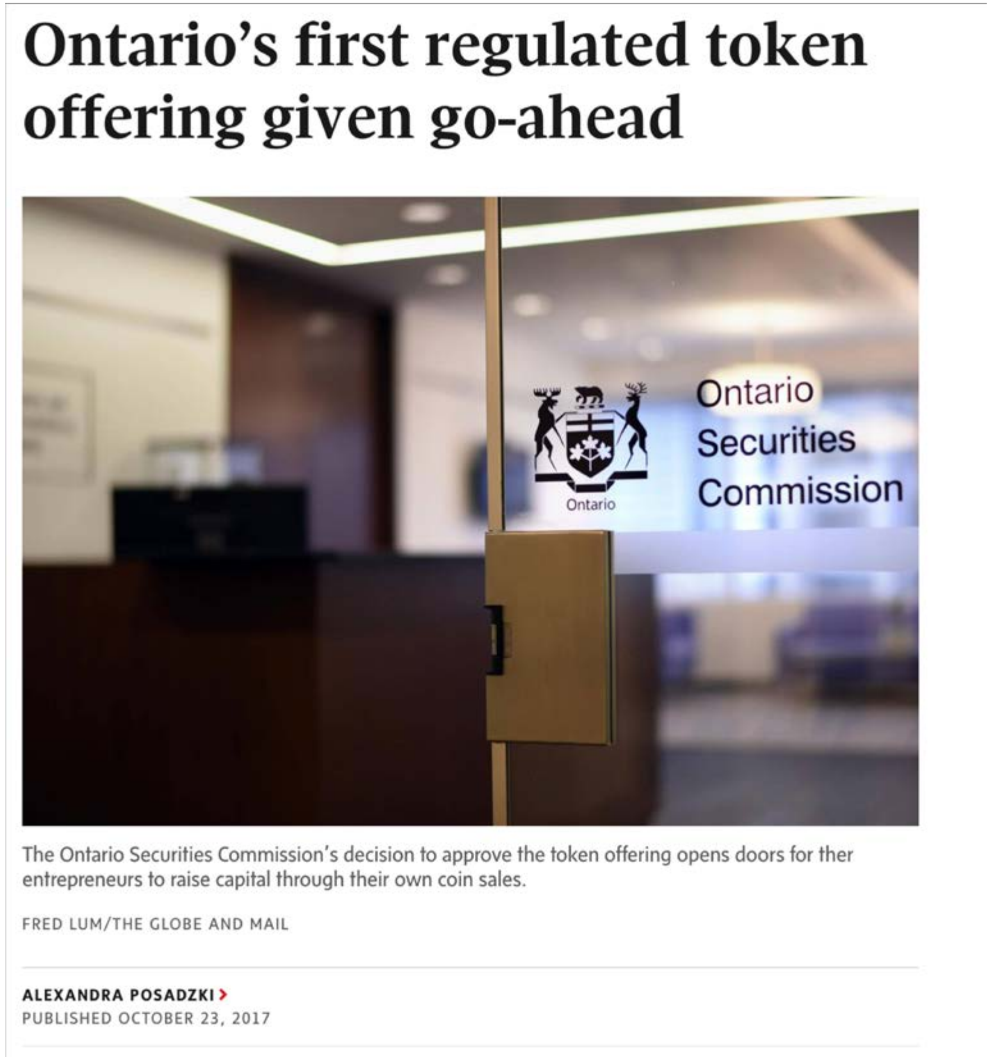
Secure storage

Your keys are protected with Secure Enclave and biometric authentication technology.

3. TOKENFUNDER & REGULATIONS


TokenFunder

TokenFunder Regulatory Leadership



Ontario's first regulated token offering given go-ahead

The Ontario Securities Commission's decision to approve the token offering opens doors for ther entrepreneurs to raise capital through their own coin sales.

FRED LUM/THE GLOBE AND MAIL

ALEXANDRA POSADZKI ›
PUBLISHED OCTOBER 23, 2017

- *The* ***Ontario Securities Commission*** *has,* ***for the first time ever****, given the green light to an "****initial token offering****", as regulators around the world grapple with the emerging online fundraising method.*
- *The regulator's decision means Toronto-based* ***TokenFunder*** *will be permitted to sell digital tokens to retail investors in order to fund the creation of its platform, which will allow other entrepreneurs to raise capital through their own coin sales.*

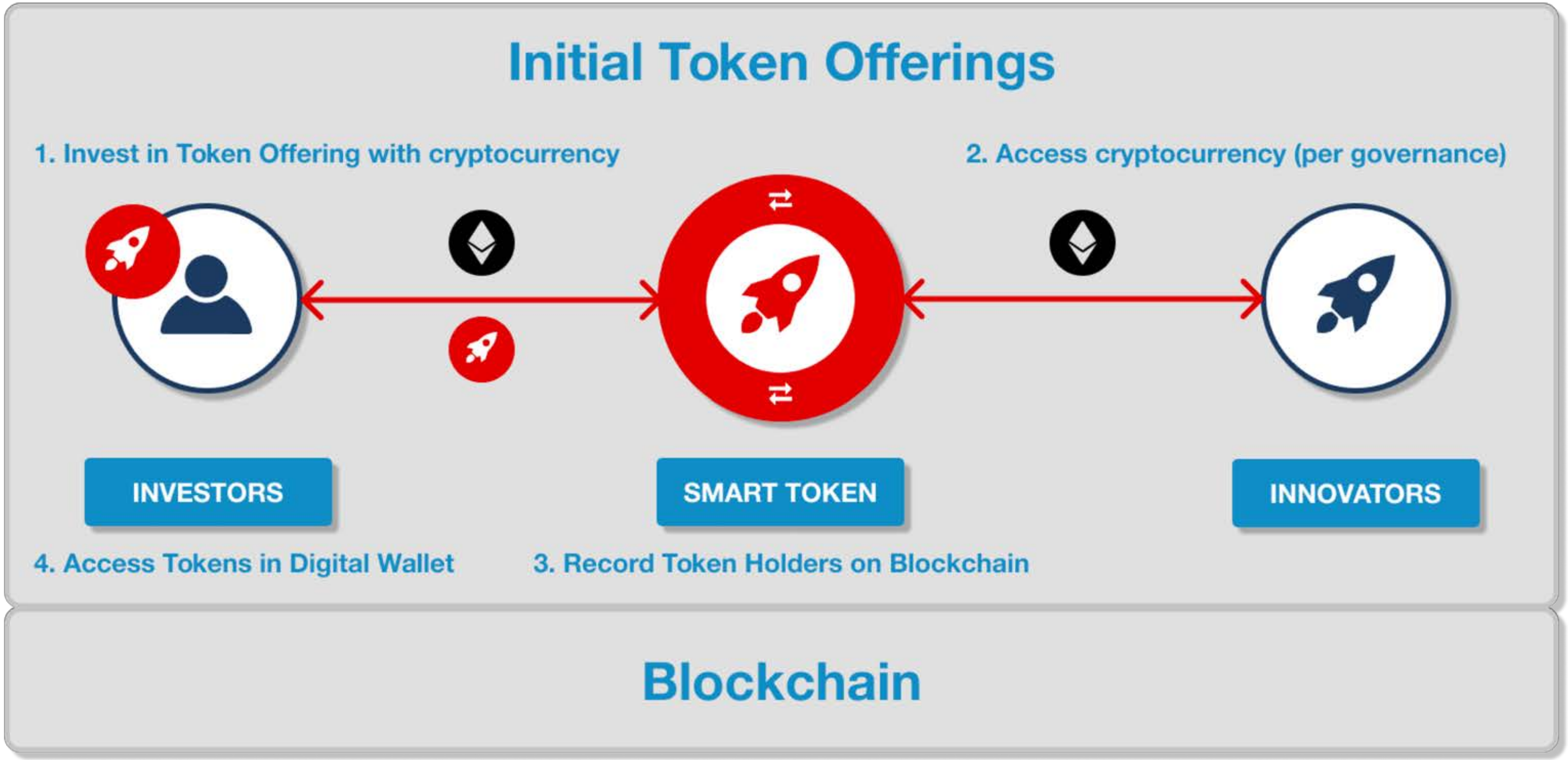
Regulatory Mandates

OSC ONTARIO SECURITIES COMMISSION

"To provide protection to investors from unfair, improper or fraudulent practices and to foster fair and efficient capital markets and confidence in capital markets."

TokenFunder

Initial Token Offerings



Initial Token Offerings

1. Invest in Token Offering with cryptocurrency

2. Access cryptocurrency (per governance)

INVESTORS

SMART TOKEN

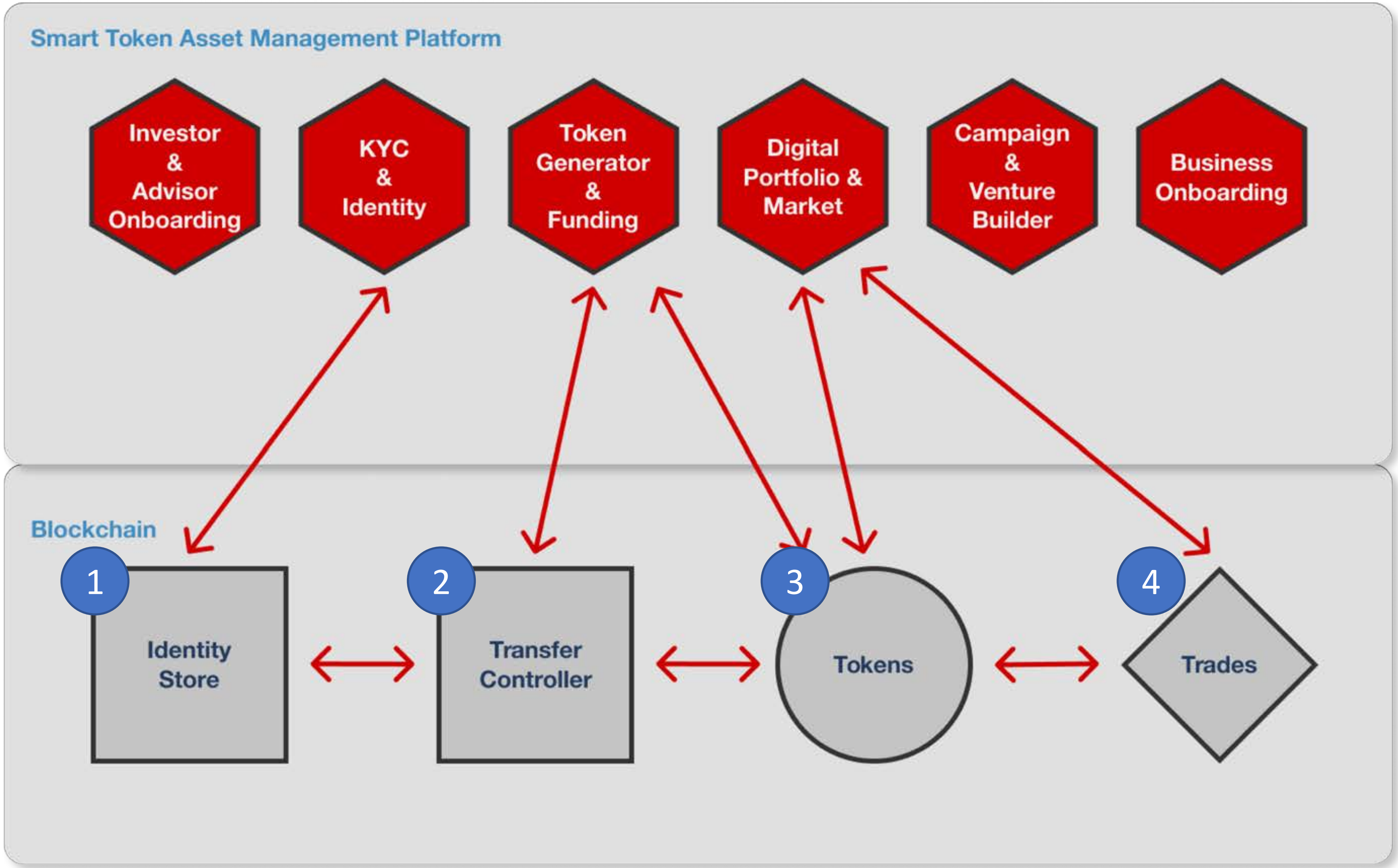
INNOVATORS

4. Access Tokens in Digital Wallet

3. Record Token Holders on Blockchain

Blockchain

TokenFunder Model



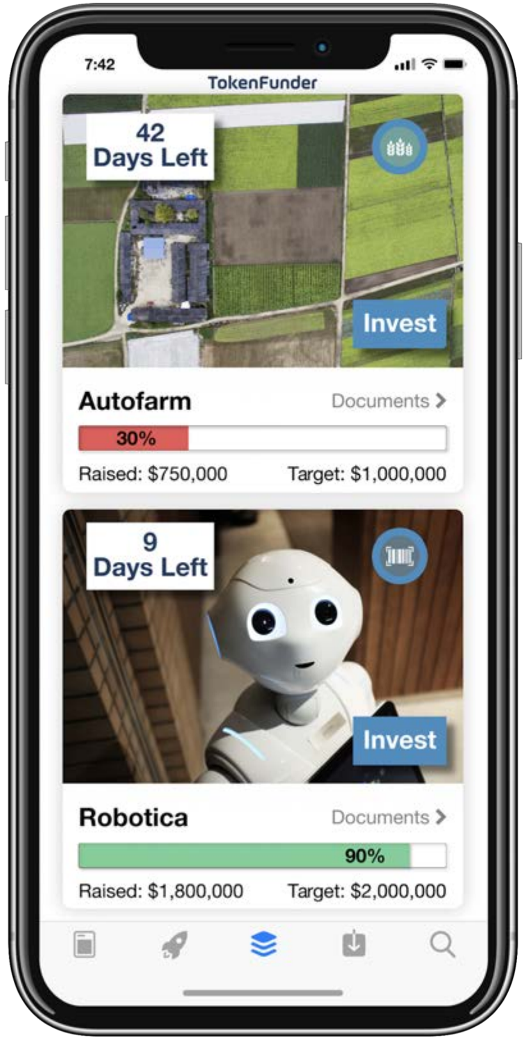
Smart Token Asset Management Platform
Investor & Advisor Onboarding
KYC & Identity
Token Generator & Funding
Digital Portfolio & Market
Campaign & Venture Builder
Business Onboarding
Blockchain
1
Identity Store
2
Transfer Controller
3
Tokens
4
Trades

Key Onchain Elements

1. **Identity Store**
   - Investor Identity
   - Investor category (AI, R)
2. **Transfer Controller**
   - Approves transfers within set rules
3. **Tokens**
   - Smart contract token holder register, governed by Transfer Controller
4. **Trades**
   - Transfer transactions

TokenFunder

Vision for a Decentralized Investment Experience



7:42

TokenFunder

42 Days Left — Invest

Autofarm — Documents >

30%

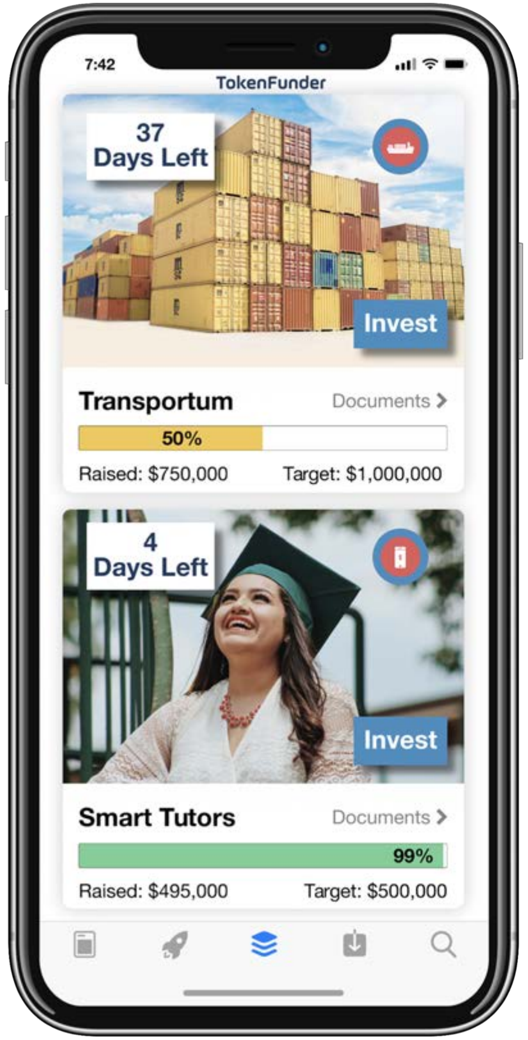
Raised: $750,000 Target: $1,000,000

9 Days Left — Invest

Robotica — Documents >

90%

Raised: $1,800,000 Target: $2,000,000



7:42

TokenFunder

37 Days Left — Invest

Transportum — Documents >

50%

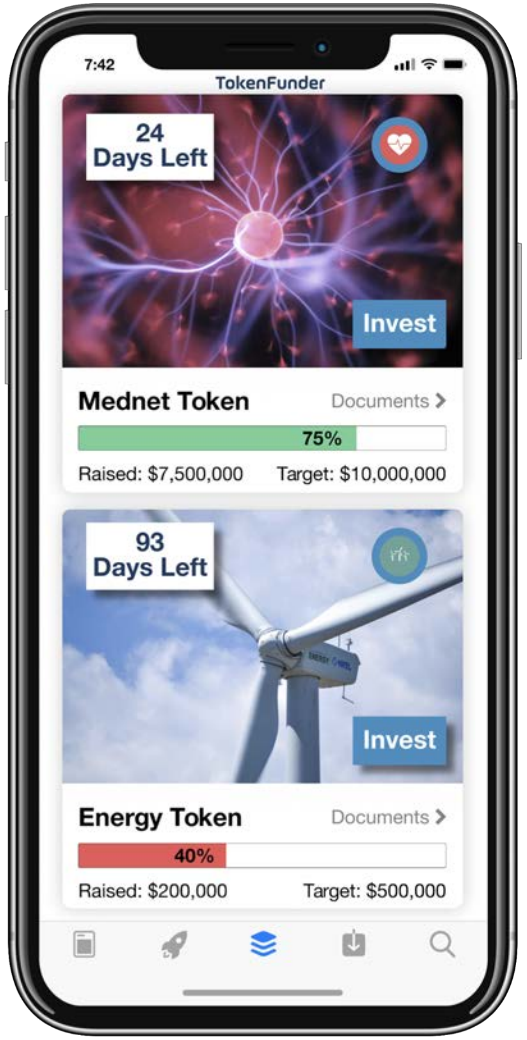
Raised: $750,000 Target: $1,000,000

4 Days Left — Invest

Smart Tutors — Documents >

99%

Raised: $495,000 Target: $500,000



7:42

TokenFunder

24 Days Left — Invest

Mednet Token — Documents >

75%

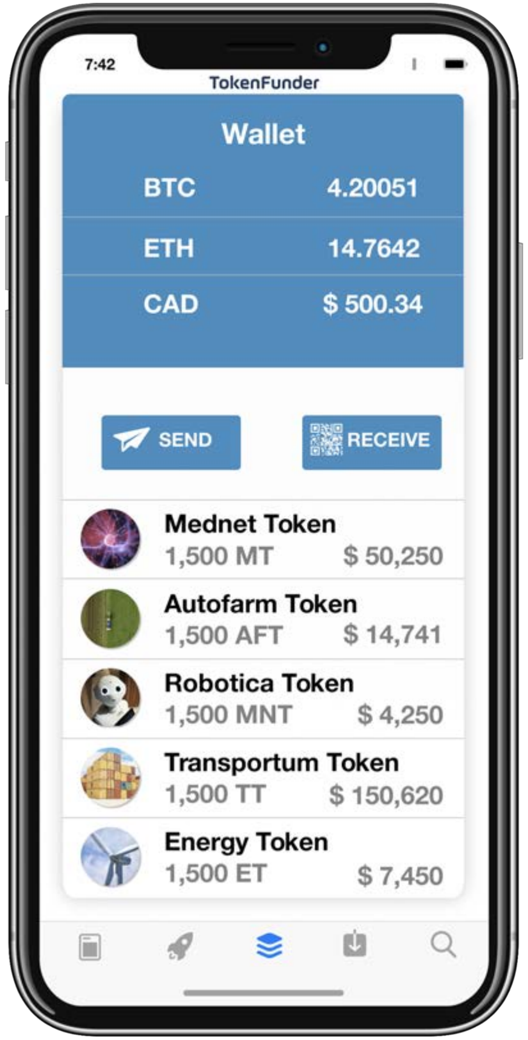
Raised: $7,500,000 Target: $10,000,000

93 Days Left — Invest

Energy Token — Documents >

40%

Raised: $200,000 Target: $500,000



7:42

TokenFunder

Wallet

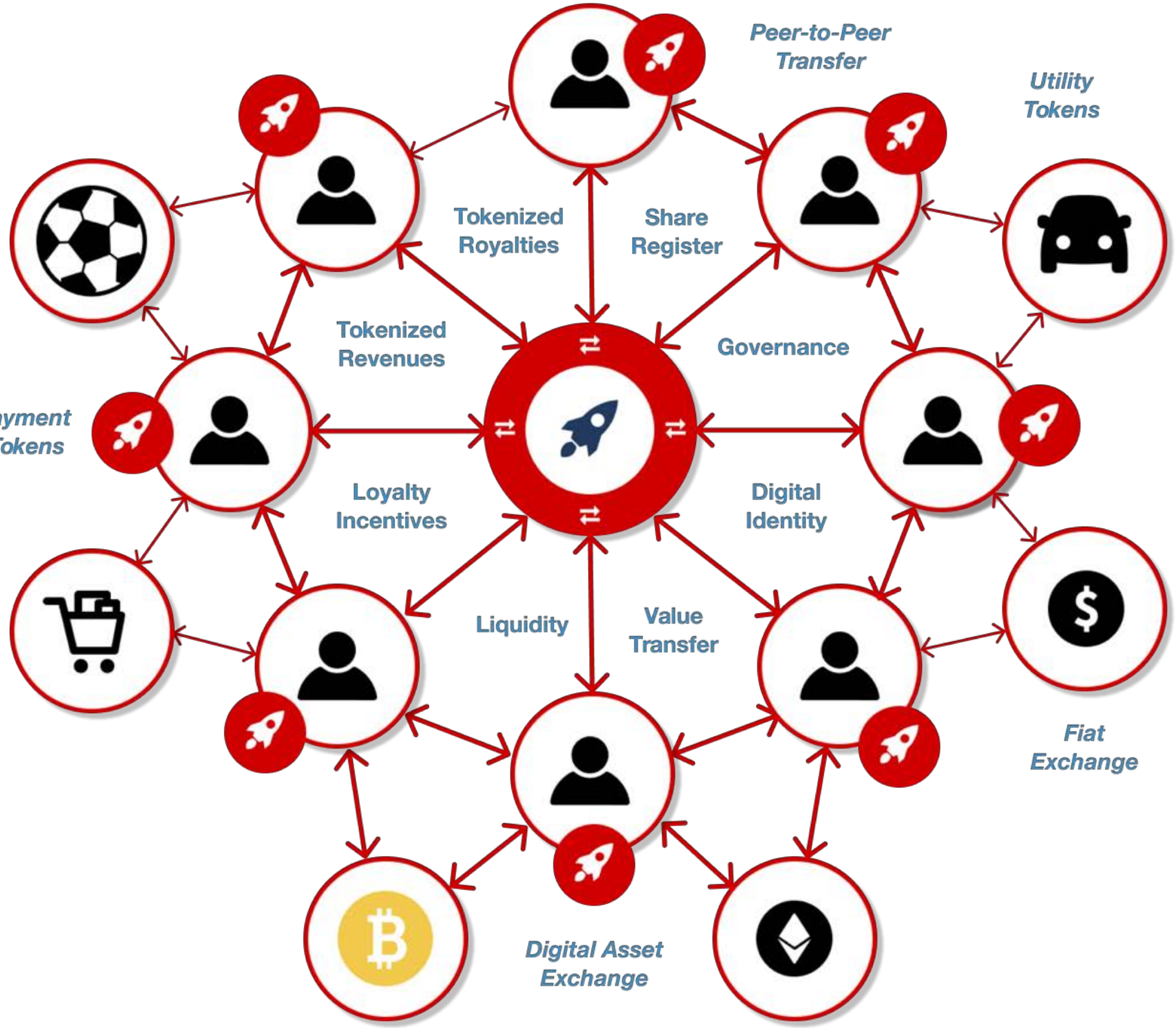
BTC	4.20051
ETH	14.7642
CAD	$ 500.34

SEND RECEIVE

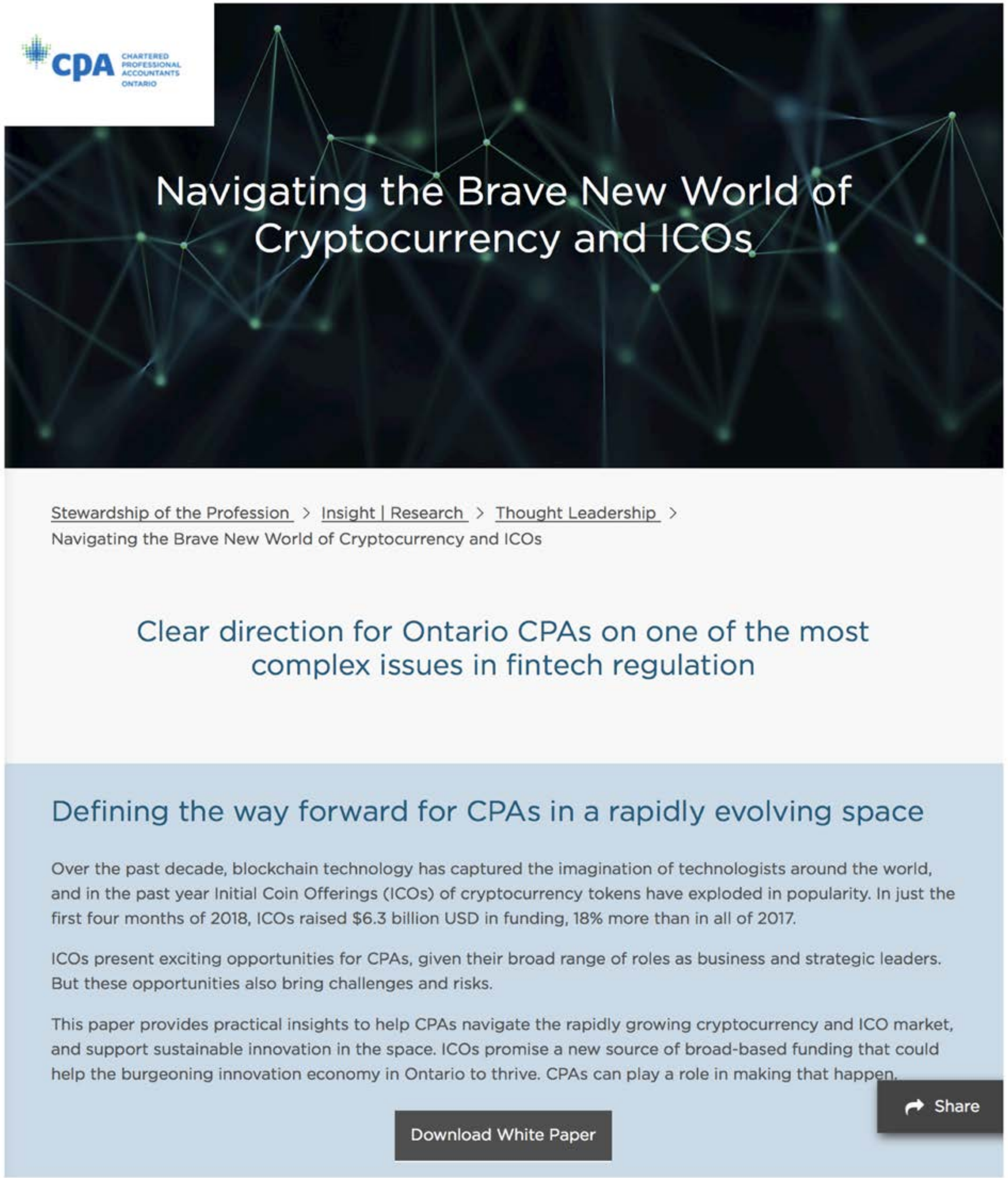
Mednet Token 1,500 MT	$ 50,250
Autofarm Token 1,500 AFT	$ 14,741
Robotica Token 1,500 MNT	$ 4,250
Transportum Token 1,500 TT	$ 150,620
Energy Token 1,500 ET	$ 7,450

TokenFunder

TokenFunder Future Token Economy



TokenFunder



Navigating the Brave New World of Cryptocurrency and ICOs

Stewardship of the Profession > Insight | Research > Thought Leadership >
Navigating the Brave New World of Cryptocurrency and ICOs

Clear direction for Ontario CPAs on one of the most complex issues in fintech regulation

Defining the way forward for CPAs in a rapidly evolving space

Over the past decade, blockchain technology has captured the imagination of technologists around the world, and in the past year Initial Coin Offerings (ICOs) of cryptocurrency tokens have exploded in popularity. In just the first four months of 2018, ICOs raised $6.3 billion USD in funding, 18% more than in all of 2017.

ICOs present exciting opportunities for CPAs, given their broad range of roles as business and strategic leaders. But these opportunities also bring challenges and risks.

This paper provides practical insights to help CPAs navigate the rapidly growing cryptocurrency and ICO market, and support sustainable innovation in the space. ICOs promise a new source of broad-based funding that could help the burgeoning innovation economy in Ontario to thrive. CPAs can play a role in making that happen.

UNDERSTANDING DIGITAL TOKENS:

Market Overviews and Proposed Guidelines for Policymakers and Practitioners

PREPARED BY - TOKEN ALLIANCE
AN INDUSTRY INITIATIVE OF THE CHAMBER OF DIGITAL COMMERCE

TokenFunder

Thank You!

Alan Wunsche
CEO, TokenFunder

alan@tokenfunder.com

@alanwunsche @TokenFunder

t.me/alanwunsche