Blockchains, Smart Contracts (DApps), and Regulation

A briefing from Coin Center

Peter Van Valkenburgh

Intro:
What is Coin Center and what do we do?

DECENTRALIZE ALL THE THINGS

THE TEAM

Jerry Brito
Executive Director

Robin Wesiman
Senior Policy Counsel

Peter Van Valkenburgh
Research Director

Neeraj Agrawal
Communications Director

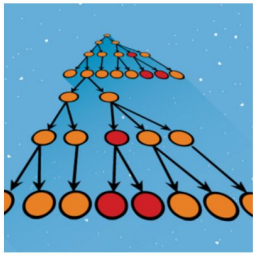
Antonie Hodge
Operations Director

OUR SUPPORTERS




What we do:
Education
Policy Research
Advocacy

Backgrounders



How can law enforcement leverage the blockchain in investigations?

Jason Weinstein • *May 12, 2015*

Former federal prosecutor Jason Weinstein explains how the nature of Bitcoin's underlying blockchain can be good news for law enforcement, and how law enforcement can ultimately be good news for Bitcoin.

Read More

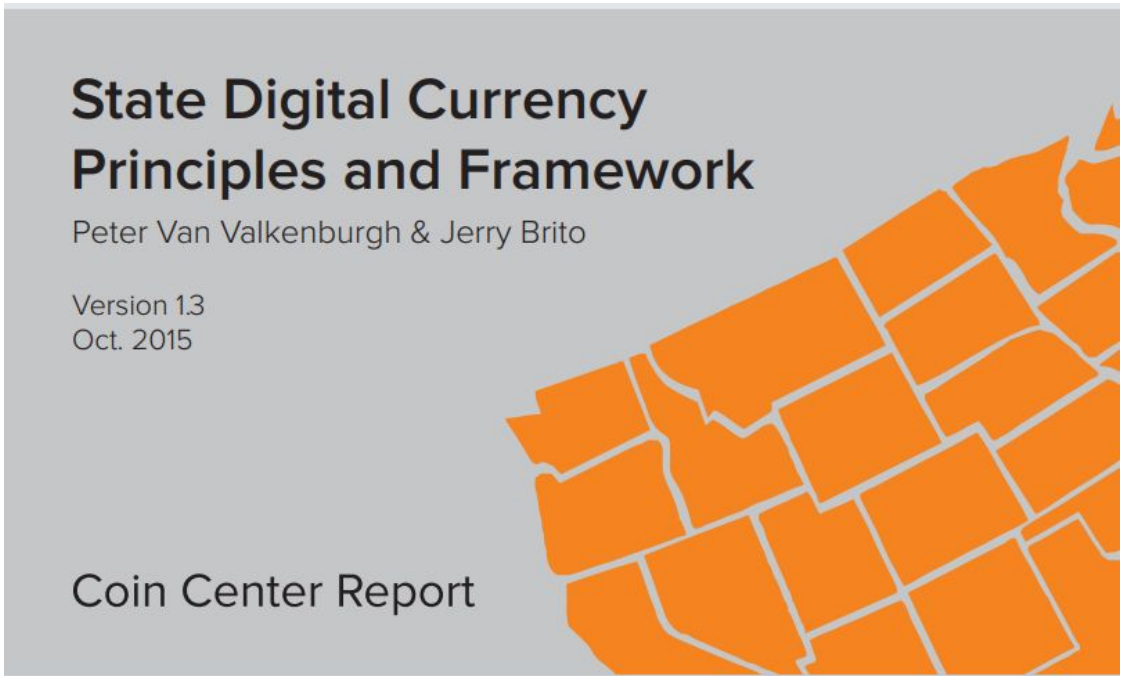
What is OFAC and how does it apply to Bitcoin?

Joshua Garcia • *May 5, 2015*

Attorney Joshua Garcia explains what OFAC is, how it can interact with cryptocurrency businesses, and why it "always applies."

Read More

Reports

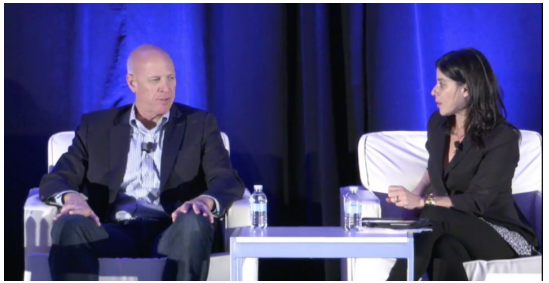

State Digital Currency
Principles and Framework
Peter Van Valkenburgh & Jerry Brito
Version 1.3
Oct. 2015
Coin Center Report

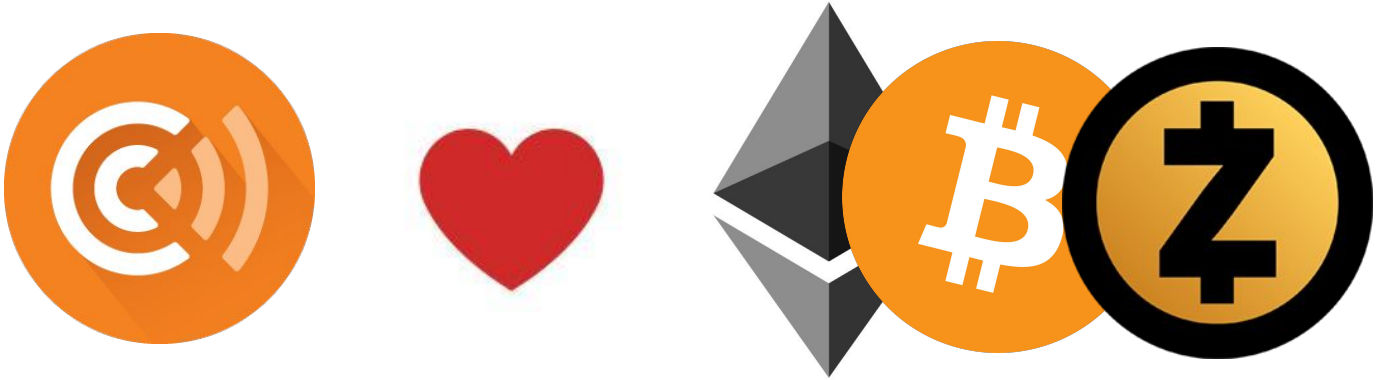
Regulatory Filings

Comments to the European Securities and Markets Authority on its Consultation on Distributed Ledger Technology Applied to Securities Markets

Our comments on ESMA's conclusion that "open" or "permissionless" blockchains may be inappropriate for financial services in its discussion paper entitled, "The Distributed Ledger Technology Applied to

Testimony and Briefings





Part I:
What is “Blockchain” !?

A briefing from Coin Center

Peter Van Valkenburgh

The word

“Blockchain”

is like the word

“Vehicle”


No one says,
“how do you feel
about vehicle?”


Or,
“We can fix this problem with vehicle!”

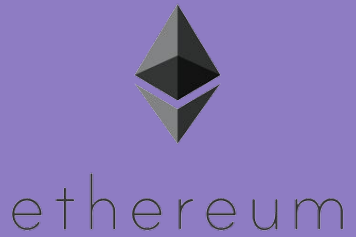

We might talk about
“vehicle technology”
but even that is strangely
abstract.

And “blockchain”
is the same...

There is no “the blockchain”
Any more than there is “the vehicle”

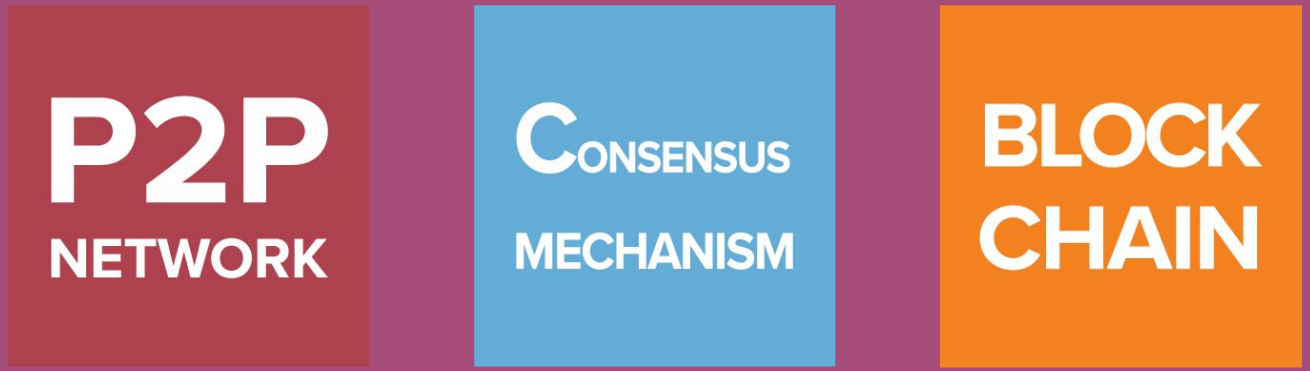
and “Blockchain Technology”
is a broad category.

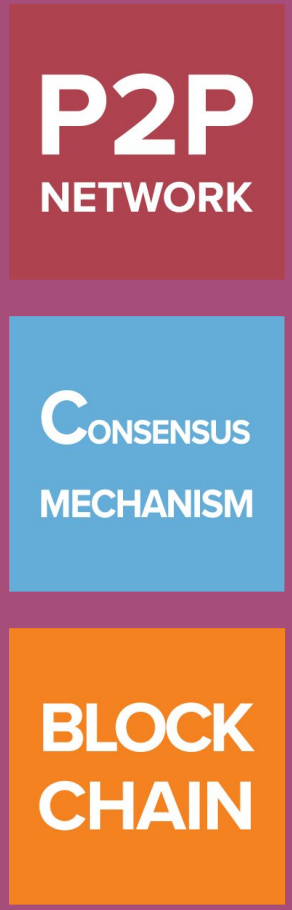
Blockchain technology.



Blockchain technology?

All blockchain technologies have three essential components:

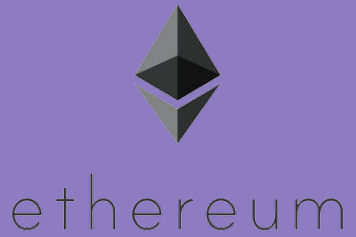




Connected computers...

...reach agreement over...

...shared data.



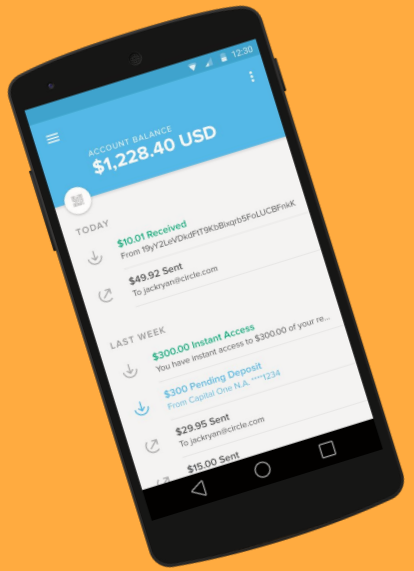
Blockchain technology.

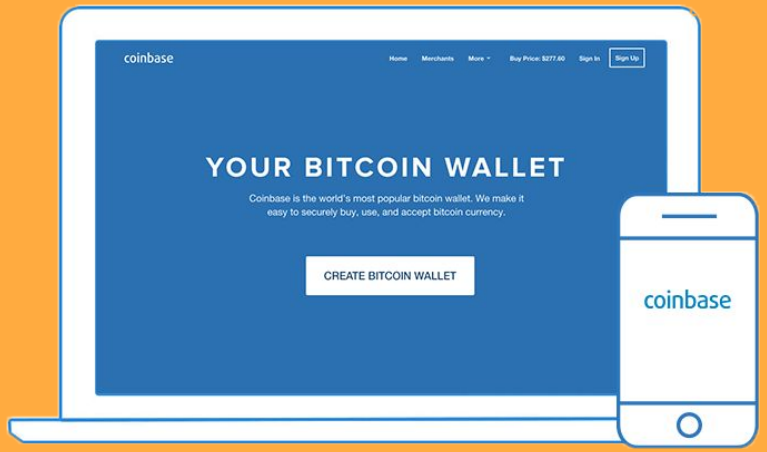
Blockchain technology.

bitcoin

Connected computers reach agreement over shared data.

P2P NETWORK





Connected computers reach agreement over shared data.

CONSENSUS MECHANISM

Rules for Agreement:

1. Nobody can send bitcoins that they have not first received from someone else.

2. Every 10 minutes or so one of the connected computers will be selected to choose the order of valid transactions for that period.

bitcoin

Connected computers reach agreement over shared data.

Shared Data:

TX 230: Mark sent Reuben 1 Bitcoin

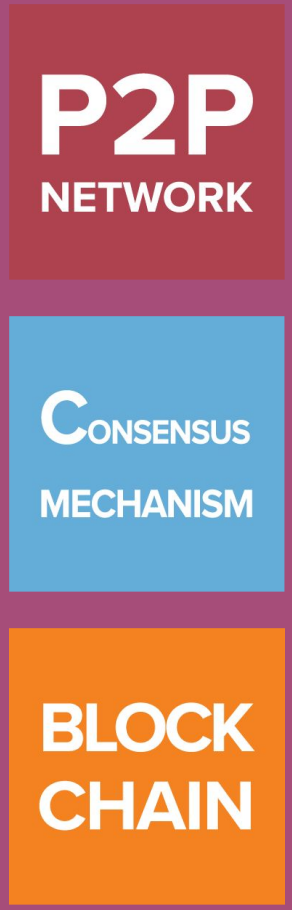
TX 229: Mark sent Robin 1 Bitcoin

TX 228: Peter sent Mark 2 Bitcoin

TX 227: Robin sent Peter 2 Bitcoin

BLOCK CHAIN

What about other blockchain technologies?



Connected computers...

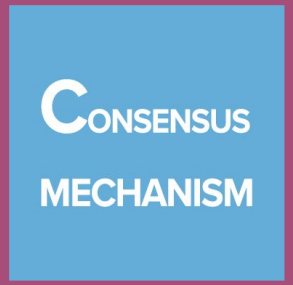
...reach agreement over...

...shared data.

BLOCK CHAIN

What data?

Identity Credentials
Votes
IOT (permissions to open smart locks / turn on smart bulbs)
Records of Securities Transactions
Property Records
Interbank Settlement Records
Provision of digital goods (cloud storage, network infrastructure)



What rules and design choices?

Open network (like Internet) or closed (like a company intranet)?

Data privacy or data transparency / auditability?

Security at the edge (immutable) or security at the center (mutable)?

When *Open* Consensus is Critical

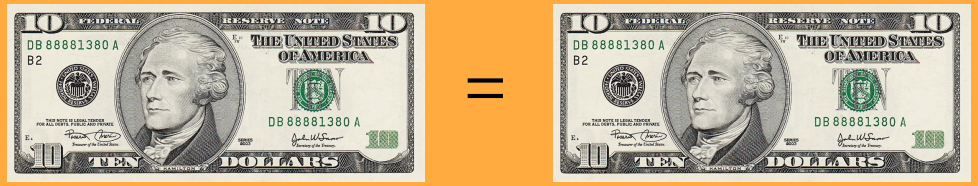
e-cash

identity

IOT

E-Cash

If a centralized authority can claim that a particular token is no longer as valuable as the others, or block certain participants from transacting, then the currency is not fungible, it is not cash. The efficiency of cash is that is ***does not require the user to consistently re-appraise the value of each note that they hold***. All $10 notes are worth the same and if someone gives it to you, then you have it.



Identity

Identity is a many-faceted concept. Your identity is a bundle of qualities that you exhibit, and attestations that others make about you. If a centralized authority can see as well as revoke ***any and all*** of your credentials this presents privacy and human rights issues.

Attestations:

US Gov: Peter is a citizen, he has this passport.

Bank of America: Peter is an account holder, he has $X

Transunion: Peter's credit score is XXX

Internet of Things

As devices further proliferate the power inherent in being the centralized control point on the network grows. This has ramifications for **privacy** as well as **competition policy**. Additionally, **interoperability is critical** and rival centralized systems may not cooperate.

Alexa! Find the best priced cat litter on the **WHOLE INTERNET!**

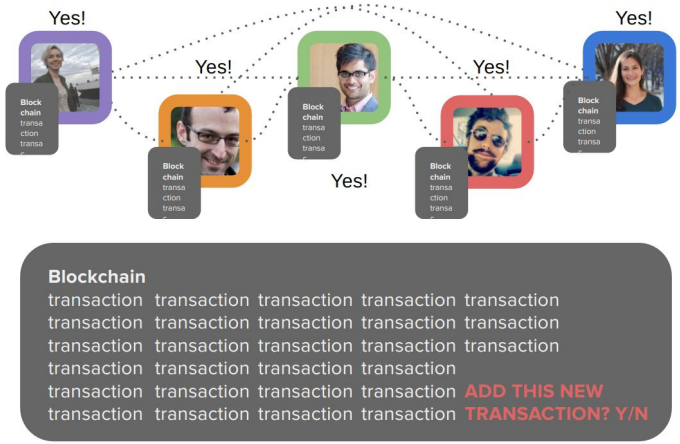
Alexa! Are you always listening to me?

Alexa! Play the music I bought on itunes!

Part II:
What is a
“Smart Contract” !?

Ethereum

- Connected computers come to agreement over state of a global computer, not just a ledger.
- It’s a platform for blockchain apps.



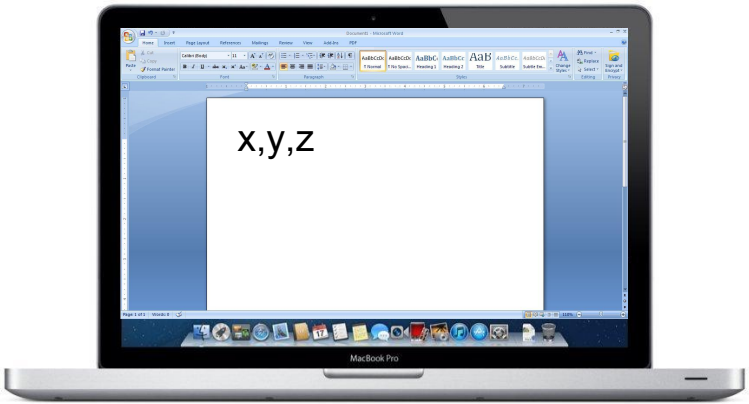
I understand agreement over a ledger of transactions, but what do you mean agreement over the *state* of a computer???

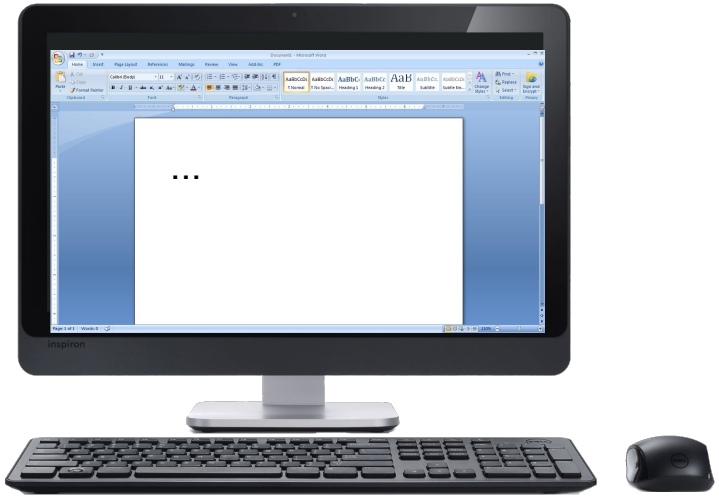
Example: Word Processing
MS Word

Where does the application code run?

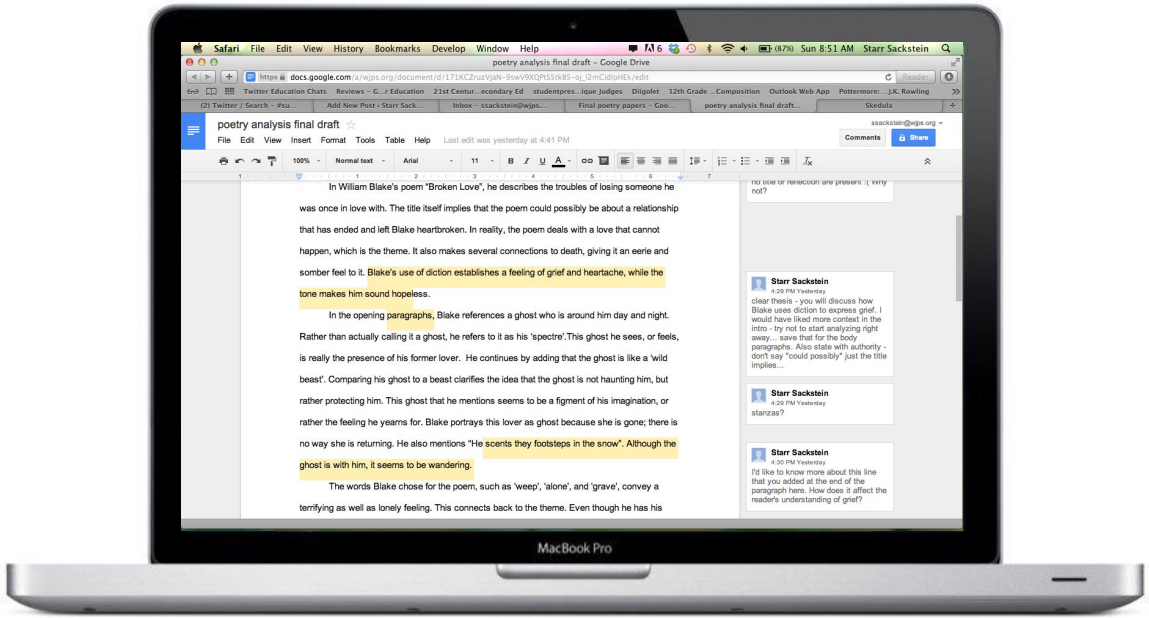
On your computer.

But collaboration is hard when the code runs locally.





Example: Word Processing
Google Docs

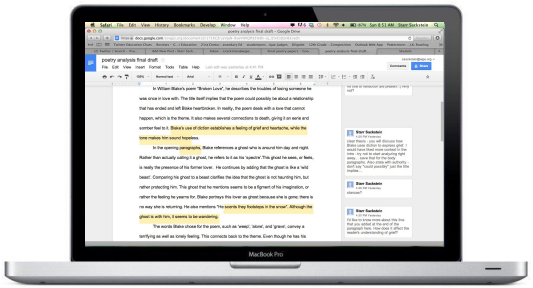


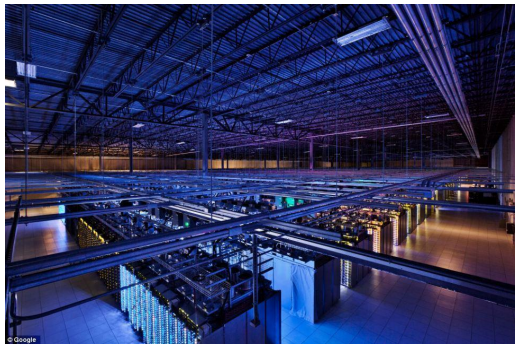
Where does the application code run?

Example: Word Processing
Google Docs

Internet

User Interface

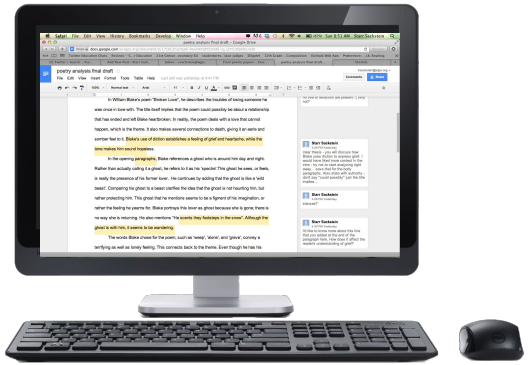




Actual Computing

Internet

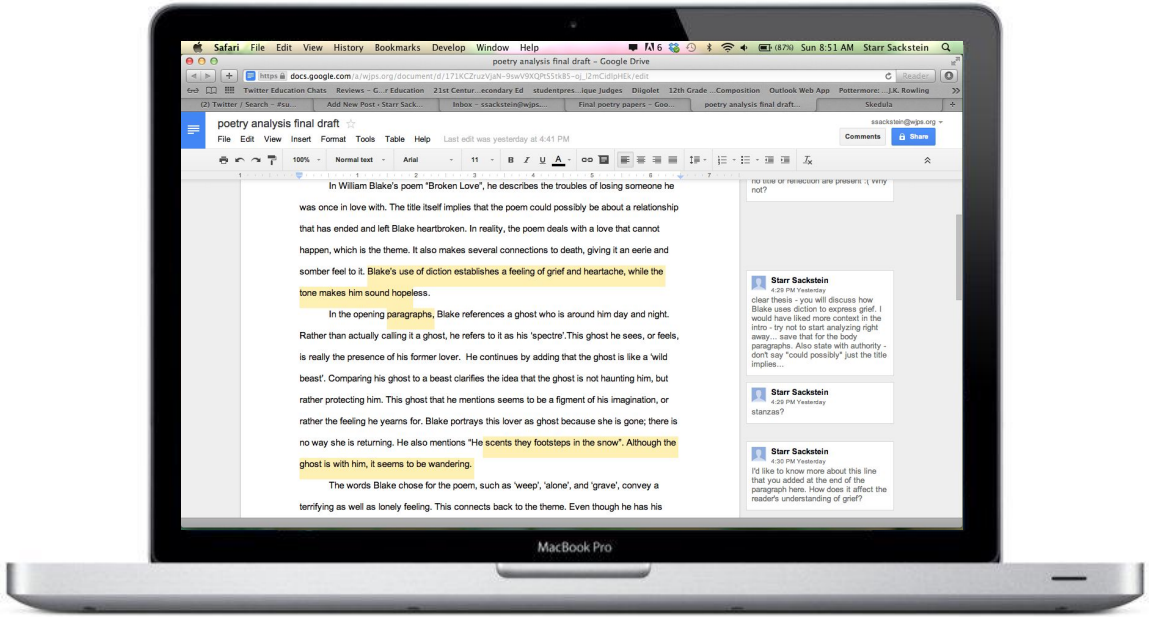
User Interface



Where does the application code run?
On a Google server in a warehouse.

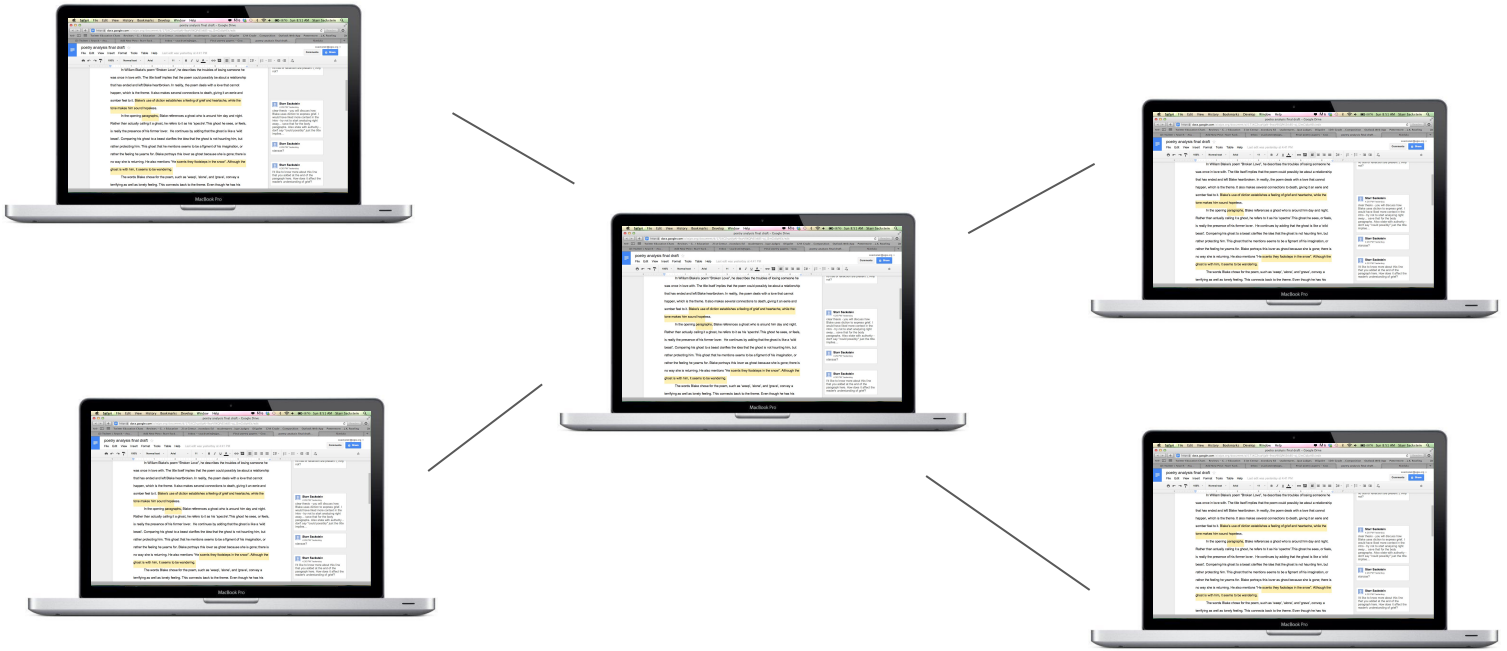

There is no cloud
it's just someone else's computer

Example: Word Processing
Ethereum

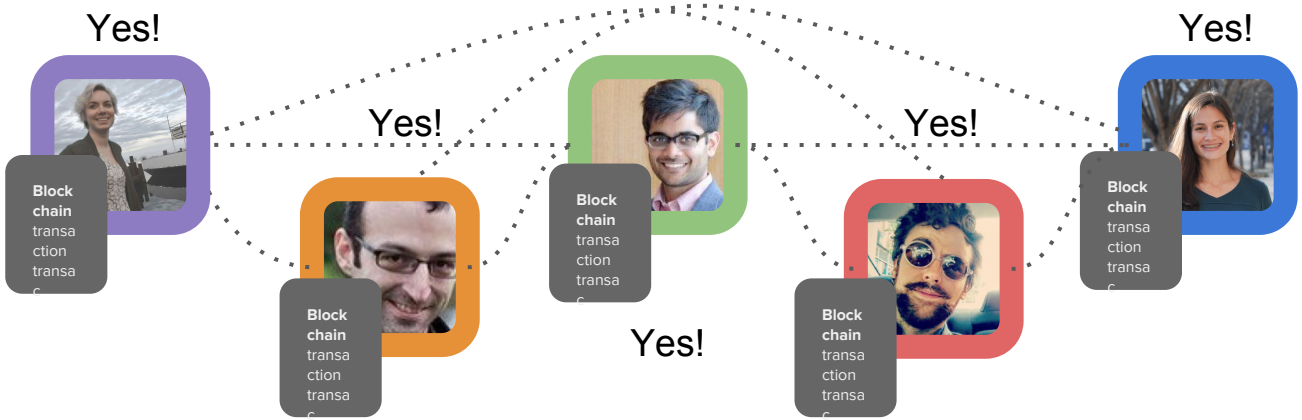


Where does the application code run?

Example: Word Processing
Ethereum

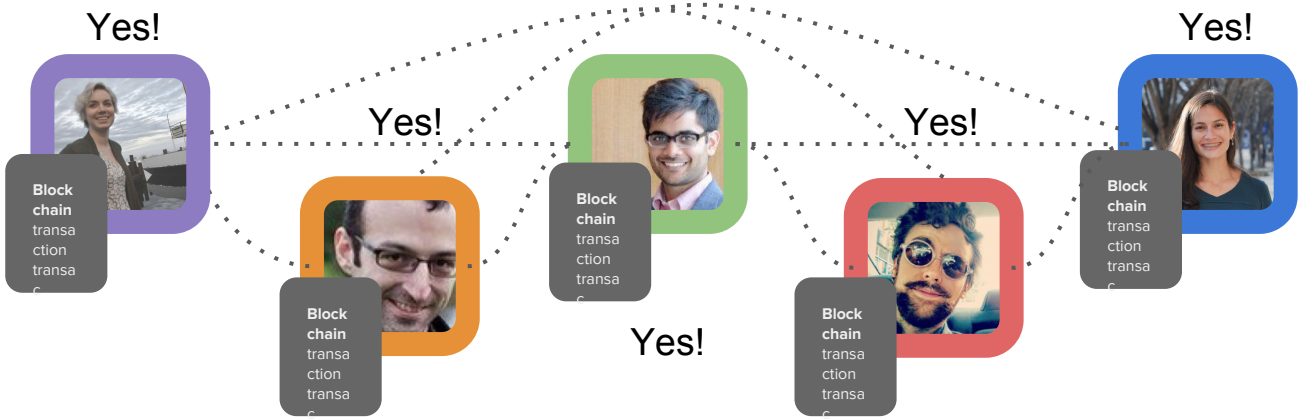


Where does the application code run?
Every computer on the network.



Blockchain

transaction transaction transaction transaction transaction
transaction transaction transaction transaction transaction
transaction transaction transaction transaction transaction
transaction transaction transaction transaction
transaction transaction transaction transaction **ADD THIS NEW**
transaction transaction transaction transaction **TRANSACTION? Y/N**



Blockchain

computing computing computing computing computing
computing computing computing computing computing
computing computing computing computing computing
computing computing computing computing
computing computing computing computing **Did User A type XYZ?**
computing computing computing computing

Ethereum is designed to be an open platform just like:

Personal Computers

The World Wide Web

Applications that run on the ethereum platform are called Decentralized Applications (or Dapps).

MIT
Work in Progress 2015-11-16

Working Prototype 2015-11-15

Live 2015-11-15

Concept 2015-11-14

Concept 2015-11-13

Live 2015-11-13

Shapeshift Bot

Alex Beregszaszi

Simple Ethereum contract to transfer Ether to Bitcoin

MIT

Working Prototype 2015-11-12

PublicVotes

Dominik Schiener

A publicly verifiable Voting System, powered by Smart Contracts

MIT

Working Prototype 2015-11-12

Oraclize

Thomas Bertani

Provable honest oracle service

Live 2015-11-10

Etheria

fivedogit

The first-ever decentralized virtual world

GPL

Live 2015-11-07

Project Mati

Harsh Patel

Decentralized KYC and Credit rating function on blockchain

Working Prototype 2015-11-06

Spore

Denis Erfurt

Simple package manager for dApp development based on ethereum and IPFS

MIT

Working Prototype 2015-10-29

Grove

Piper Merriam

Fast, efficient, queryable storage for ethereum contracts

MIT

Live 2015-10-07

LightWallet

ConsenSys / Chris Lundkvist

Lightweight JS Wallet for Node and the browser

MIT

Working Prototype 2015-10-07

ethereum-datetime

Piper Merriam

Ethereum Date and Time tools

MIT

Working Prototype 2015-10-07

Populus

Piper Merriam

Ethereum Contract Development Framework

MIT

Working Prototype 2015-10-07

slock.it

Christoph Jentzsch

If you can lock it, we will let you rent, sell or share it.

GPL

Working Prototype 2015-10-02

meteor-embark

Chris Hitchcott

Streamlined Ethereum Integration for Meteor

MIT

Working Prototype 2015-09-30

Colony

AttaAtta

Companies for the 21st Century

Working Prototype 2015-09-29

Dereo

Dereo

Decentralized over-the-air television streaming network

Concept 2015-09-28

Dynamis

Joshua Davis

Insurance Dapp

Work In Progress 2015-09-24

Ethereum Alarm Clock

Piper Merriam

Schedule contract calls

MIT

Live 2015-09-24

CryptoRPS

CryptoRPS

Rock-Paper-Scissor game with a twist

Live 2015-09-24

Project Basil

Harsh Patel

Decentralised Vulnerability feed management

MIT

Working Prototype 2015-09-15

AuditDog

Roman Plášil

SW audit repository

MIT

Working Prototype 2015-09-08

Universal ĐApp

d11e9

A Universal Interface for contracts on the Ethereum blockchain

MIT

Live 2015-09-03

Avatar

d11e9

distributed profile registry

MIT

Working Prototype 2015-08-28

EtherPot

Aakil Fernandes

Provably Fair Lottery

MIT

Working Prototype 2015-08-27

PirateChest

d11e9

p2p magnet discovery

MIT

Working Prototype 2015-08-26

Occams Run

d11e9

All things being equal (50/50) only The Brave will win

MIT

Working Prototype 2015-08-26

content

Ethos

HitFin

Raikoth

ChainGraph

EtherListen

When a decentralized application can also assume control over assets and mediate decisions over how those assets should be used, we sometimes call it a Smart Contract (atomistic/single use) or a DAO (larger system/repeated use)

CADE METZ BUSINESS 06.06.16 7:00 AM

THE BIGGEST CROWDFUNDING PROJECT EVER—THE DAO—IS KIND OF A MESS

Part III: Regulation


Regulatory Considerations for Token-Creating Smart Contracts

Why *Securities Laws* and Tokens?

Securities Laws are *Heavy Duty* Regulation.

Crowdsales and Presales may subject developers to securities regulation.

Several Scams have drawn attention to this area.

Several vocal pundits have already suggested that *all* appcoin/crypto crowdsales qualify as unregistered securities issuance.

Why *Securities Laws* and Tokens?

MINIMUM VIABLE TOKEN

The token contract is quite complex. But in essence a very basic token boils down to this:

```
contract MyToken {
    /* 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 MyToken(
        uint256 initialSupply
        ) {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    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
    }
}
```

Why *US* Securities Laws?

If you have any US purchasers you are subject to US Securities Regulations

US Securities Law are the Most Broadly applied.

In other jurisdictions, there is generally an enumerated list of what arrangements constitute a “security,” in the US there is a flexible and court-adjudicated test.

The US Securities and Exchange Commission is already investigating Paycoin. The DAO got the attention of some staff.

Why are US Securities Laws Broadly Applied?

Definition of Security includes an undefined term: “investment contract”

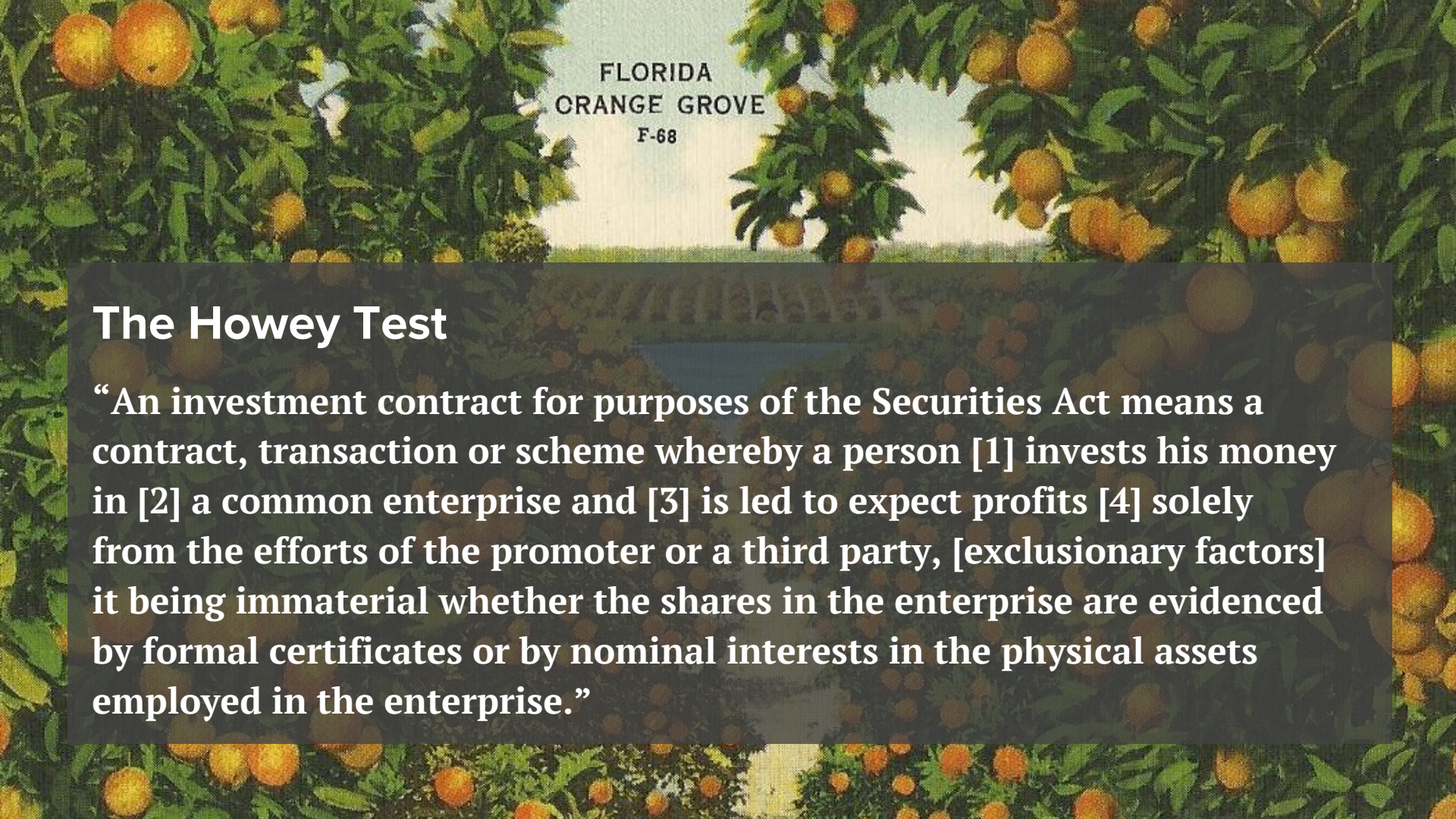
Term has been defined by Federal Courts

Courts have sought to ensure that definition is inclusive in order to reach:

> *“the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits”*

Primary Case is *SEC v. W. J. Howey Co.*

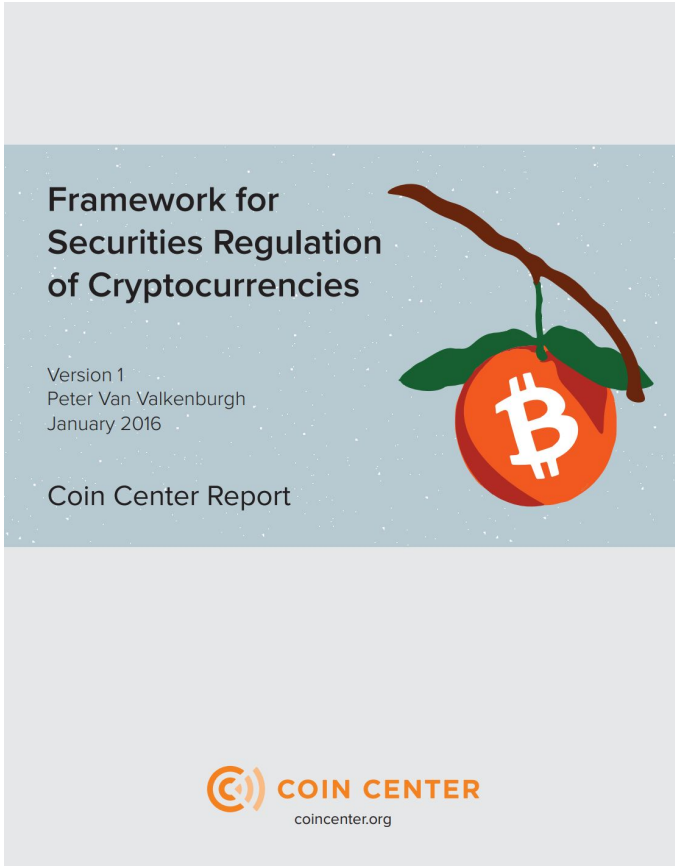
From that case we get the Howey Test for a Security



The Howey Test

“An investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person [1] invests his money in [2] a common enterprise and [3] is led to expect profits [4] solely from the efforts of the promoter or a third party, [exclusionary factors] it being immaterial whether the shares in the enterprise are evidenced by formal certificates or by nominal interests in the physical assets employed in the enterprise.”


What Is PayCoin™?
PayCoin™ is a global currency that lets you send money to anyone, anywhere, anytime.
Sending and accepting money is totally free, lightning fast and insanely easy
- whether you're a person or a business.
Purchase PayCoin
Buy Now

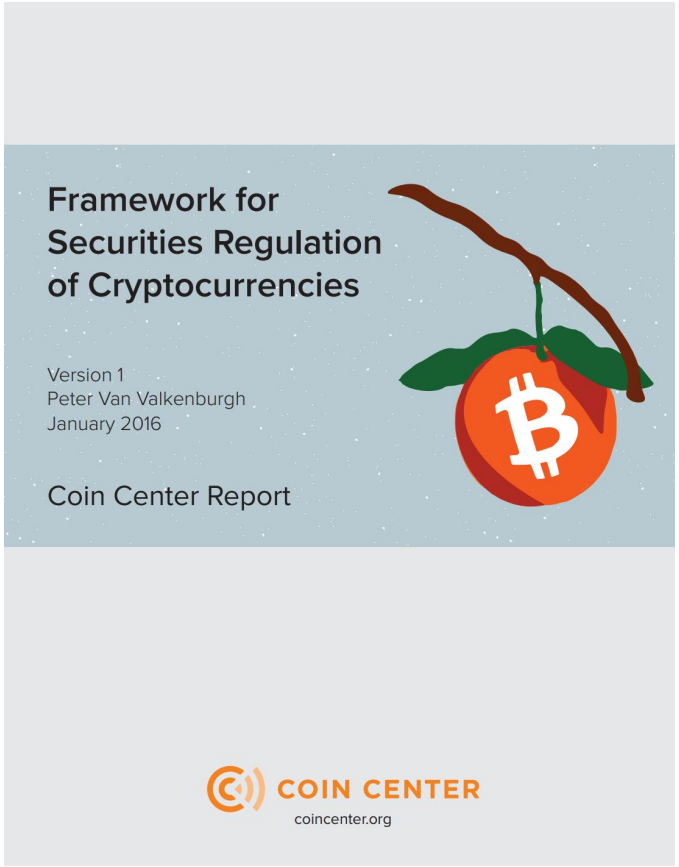


Likely to qualify as securities:

Closed-source or **low-transparency** cryptocurrencies because without visibility into the operation of the technology there is no reason to believe that profits come from anything other than a promoter's hype.

Open but heavily marketed **pre-sales** or sales of **pre-mined cryptocurrencies** with a **small and non-diverse mining and developer community** when the facts indicate that profits come primarily from the efforts of this discrete and profit-motivated group.

Cryptocurrencies with **permissioned ledgers** or a **highly centralized community of transaction validators**.



Less likely to qualify as securities:

Highly decentralized cryptocurrencies (e.g. Bitcoin, Litecoin) because of a lack of vertical commonality or a discernible third party or promoter upon whose efforts investors rely.

Sidechained Cryptocurrencies/Blockchains because there is no expectation of profits if value pegged to their existing bitcoin holdings.

Cryptocurrencies where initial distribution is made through **open competitive mining or proof-of-burn** because there is no investment of money.

App-Coins or **Distributed Computing Platforms** (e.g. Ethereum) because participants seek access to these tokens for their use-value rather than an expectation of profits.

Key findings for Appcoins or Dapp Tokens

The following are less likely to be treated as securities:

Token was purchased for *use-value* rather than profit expectation.
(Condominium cases: *Goldberg v. North Wabash Venture*, *United Housing*)

Token was purchased after application is already up and running.
(Country Club cases: *Silver Hills Country Club v. Sobieski*, *All Seasons Resorts*)

Token's value is dependent on the purchaser's own efforts and/or the efforts of a large number of other unaffiliated investors/users/developers.

Some things to avoid.

Language that suggests securities issuance:

- **Initial (coin) Offering**
- **Profit Sharing**

Endorsing risky ventures or claiming endorsements:

- **Severe penalties can await anyone who is deemed a “promoter” of an unregistered security.**
- **The definition of “promoter” is vague.**


Please don’t hesitate to contact us.
peter@coincenter.org