Sterling

Blockchain Assets and the Distributed Economy

Presented By: Brandon Caruana
Prepared On: 10/22/2017
Updated On: 1/24/2018

What is a Blockchain Asset?

[redacted] [redacted] [redacted] [redacted]

More specifically

A **blockchain asset** is a **digital store of value** that is designed to be used as a **medium of exchange**:

Blockchain Protocol	Blockchain Asset
• Protocol: set of **governing rules** • Blockchain Protocol: a set of rules that govern a **peer to peer transactions** without prejudice on a global scale • To **prove ownership** of an asset • Key aspects • Trustless • Immutable • Decentralized • Public **The Protocol is the real innovation.**	• A unit within the network • A store of value • Used to incentivize integrity within the network

The **first blockchain asset** to capture the public imagination was **Bitcoin**

It is important to note that

At this point in time, blockchain assets are **not issued by any central authority and have a fixed supply** theoretically limiting any third parties ability to directly influence or manipulate it

The Technology:
Cryptography, Hashes and **The Blockchain**

Cryptography

cryp·tog·ra·phy - the art of writing or solving codes.

Simply put, cryptography is a method to store and transmit data in a particular form so that only those for whom it was intended can read and process it.

Hash Function

A hash function is a one-way cryptographic algorithm that takes an input and returns a unique, random, fixed-size alphanumeric string

Bitcoin uses SHA-256 hash algorithm. A few examples are below:

Input	Output, Signature, ID, Address
Brandon Caruana	9b298f39d06298d39ef1d5f3e7ccc514c815a8f159d0dd37828183cfedd18ad9
Brando Caruana	E1bdf2d774ea911568814b2a14d2980b35cbc132c31db1f7a4738d70039b28e6
Send: 1BTC To: 9b298f39d06298d39ef1d5f3e7ccc514c815a8f159d0dd37828183cfedd18ad9 From: E1bdf2d774ea911568814b2a14d2980b35cbc132c31db1f7a4738d70039b28e6	De566e186ede727d77ced26366784d66f48b9fcc3f9cc4d12ccc7408d8ee5f6d

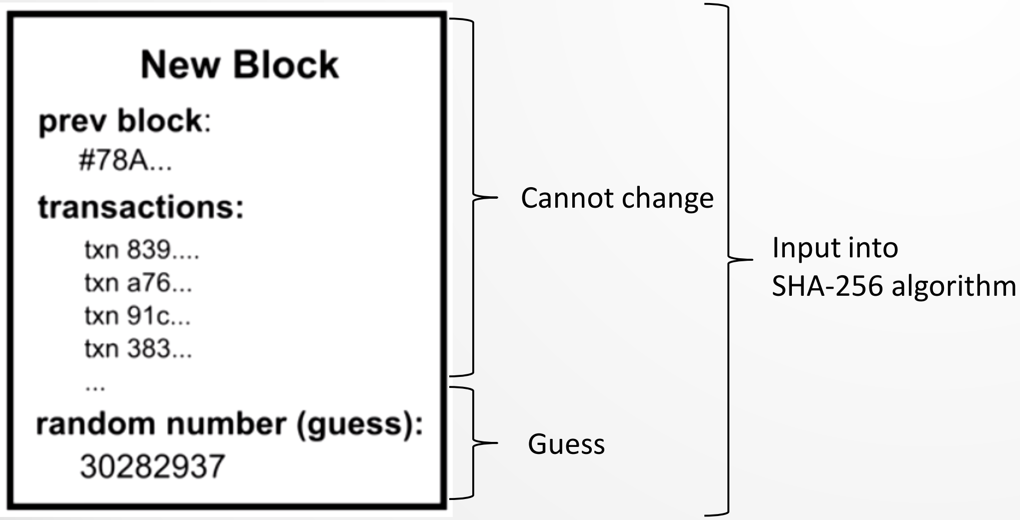
The BLOCKCHAIN

Simply put, a blockchain is a decentralized public ledger of peer to peer transactions that transfer and validate authority over an asset.

Blockchain

A transaction gets broadcasted to the network

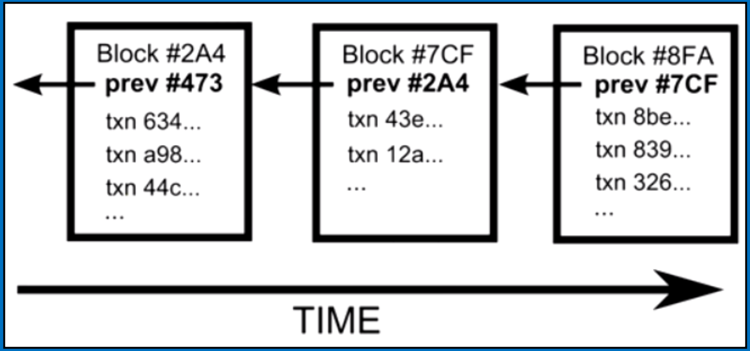
In Bitcoin, computers **compete to find an input** – through guessing a random number – that results in a hash that starts 18 zeroes – **this is known as mining**



Cannot change

Guess

Input into
SHA-256 algorithm



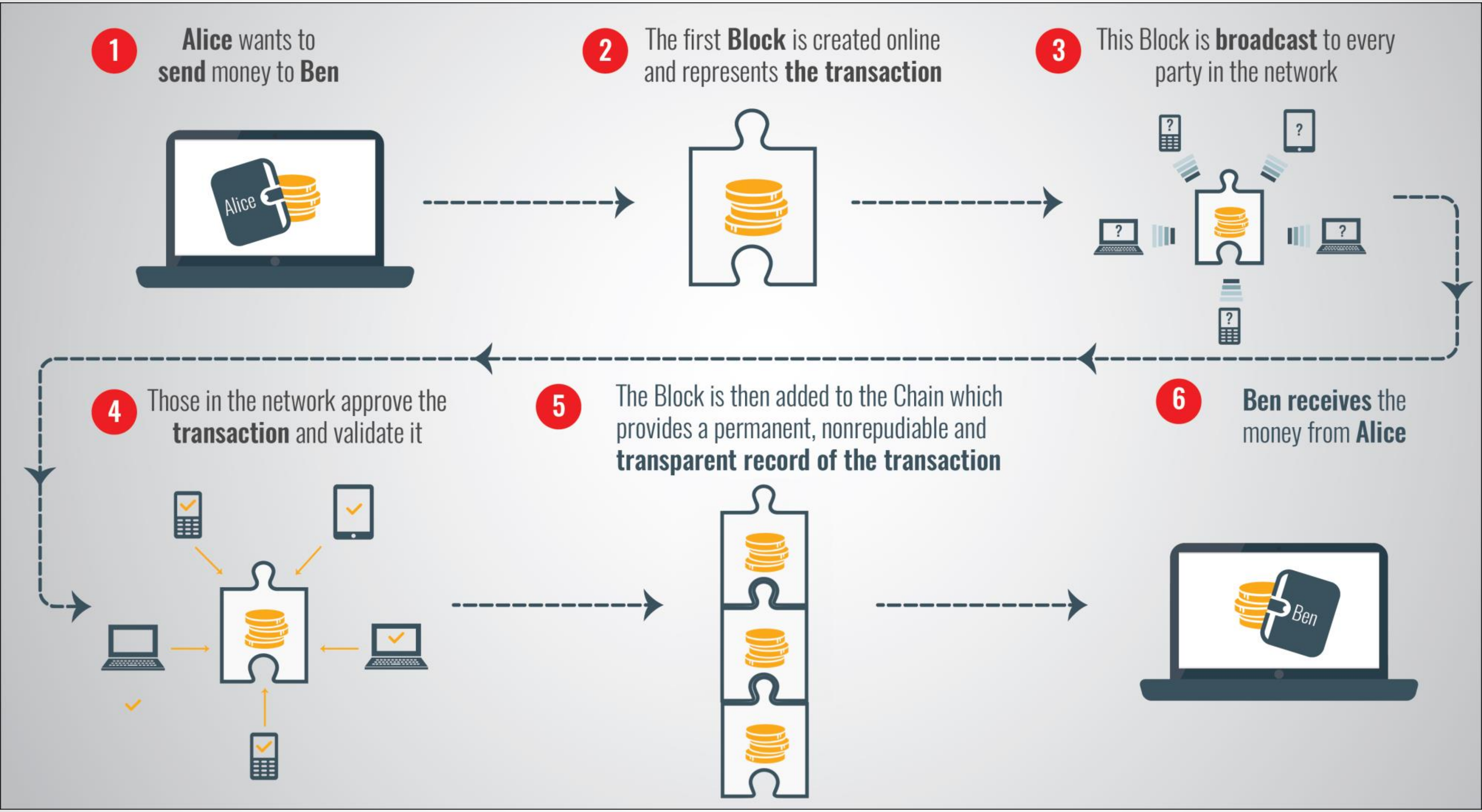
Trustless: Individuals confirm each other's transactions without reliance on a single authority

Immutable: If you change a historical transaction, you change the hash of that block and all subsequent blocks (prev #473 ← prev #2A4 ← prev #7CF)

Decentralized: Any individual can download software to begin confirming transactions

Public: Any individual can view all historical transactions

A Simplified Transaction



1 **Alice** wants to **send** money to **Ben**

2 The first **Block** is created online and represents **the transaction**

3 This Block is **broadcast** to every party in the network

4 Those in the network approve the **transaction** and validate it

5 The Block is then added to the Chain which provides a permanent, nonrepudiable and **transparent record of the transaction**

6 **Ben receives** the money from **Alice**

In Short

- Central to the genius of cryptocurrencies is the **block chain**
- The **blockchain** is a continuously growing **decentralized ledger of all the records, called blocks.**
- Each Block has a **hierarchal and immutable relationship with each other** through a cryptographic algorithm known as a **hash**
- Transactions are facilitated through the use of cryptography by using **public and private keys**
    - Public keys allow anyone to **verify proof of ownership**
    - Private keys allow the user to **execute a transaction**

Blockchain Asset Gateways

An gateway is an online platform that acts as an intermediary between buyers and sellers of the different pairs of blockchain assets or fiat currency.

Types of Gateways:

- Fiat to Blockchain (and vice versa)
- Blockchain A (eg. BitCoin) to Blockchain B (eg. Ethereum)
- Blockchain A Token to Blockchain A Token
- Centralized
- Decentralized
- High Risk Gateway
- Low Risk Gateway

Smart Contracts and Distributed Applications

Smart Contracts

- A smart contract is when blockchain is coupled with an internal scripting language to run logic-based programs
- Smart contracts are self-executing contracts with the terms of the agreement being directly written into lines of publicly verifiable code.
- There are a number of possible uses to which smart contracts could be put in the finance context, eg: proxy voting, the settlement of securities, payments under a derivatives contract and the recording of financial data
- Such a contracts can exist and be fully enforceable without the need for a securities exchange, a clearing house, a broker or even a legal system

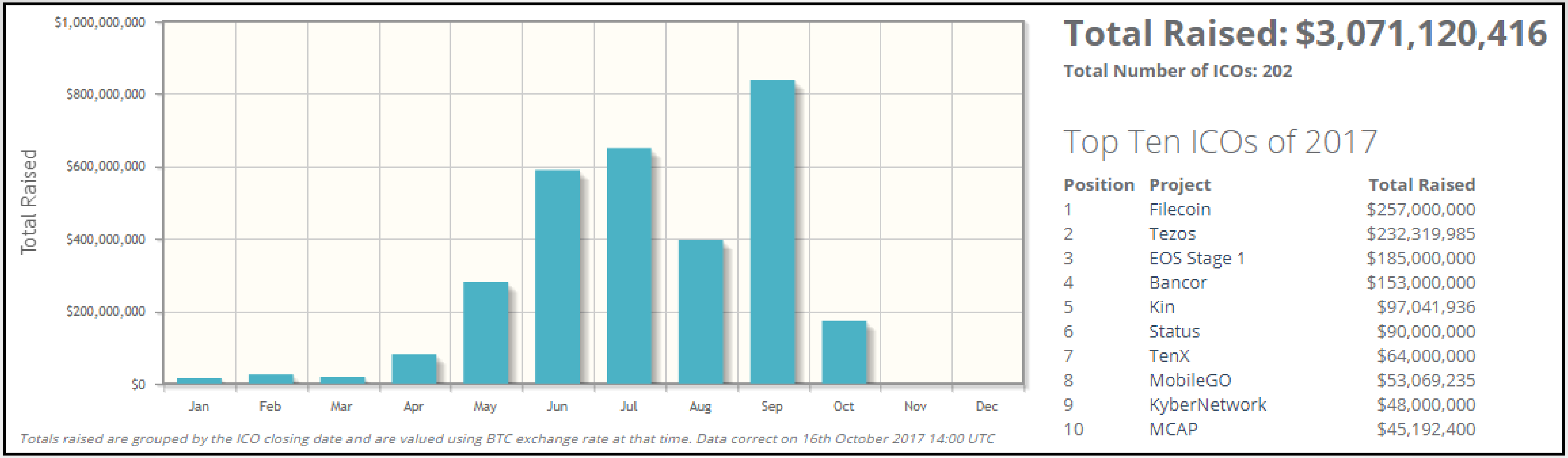
Distributed Applications (DApp)

In the emerging smart economy, a DApp can be thought of as a collection of smart contracts that are combined to form a complete application that is distributed across an entire blockchain network.

Initial Coin Offering (ICO)

Initial coin offering (ICO) is a currently unregulated and controversial means of crowdfunding via use of cryptocurrency, which can be a source of capital for startup companies. In an ICO a percentage of the newly issued cryptocurrency is sold to investors in exchange for tokens or other cryptocurrencies such as Bitcoin.

- An Initial Coin Offering (ICO) is used by startups to bypass the rigorous and regulated capital-raising process required by venture capitalists or banks.
- An ICO campaign, is based on smart contracts and creates a proprietary token based off a parent cryptocurrency.
- A percentage of the tokens are sold to early backers of the project
- Tokens provide owners with access to the startups services as well as a potentially appreciating asset.



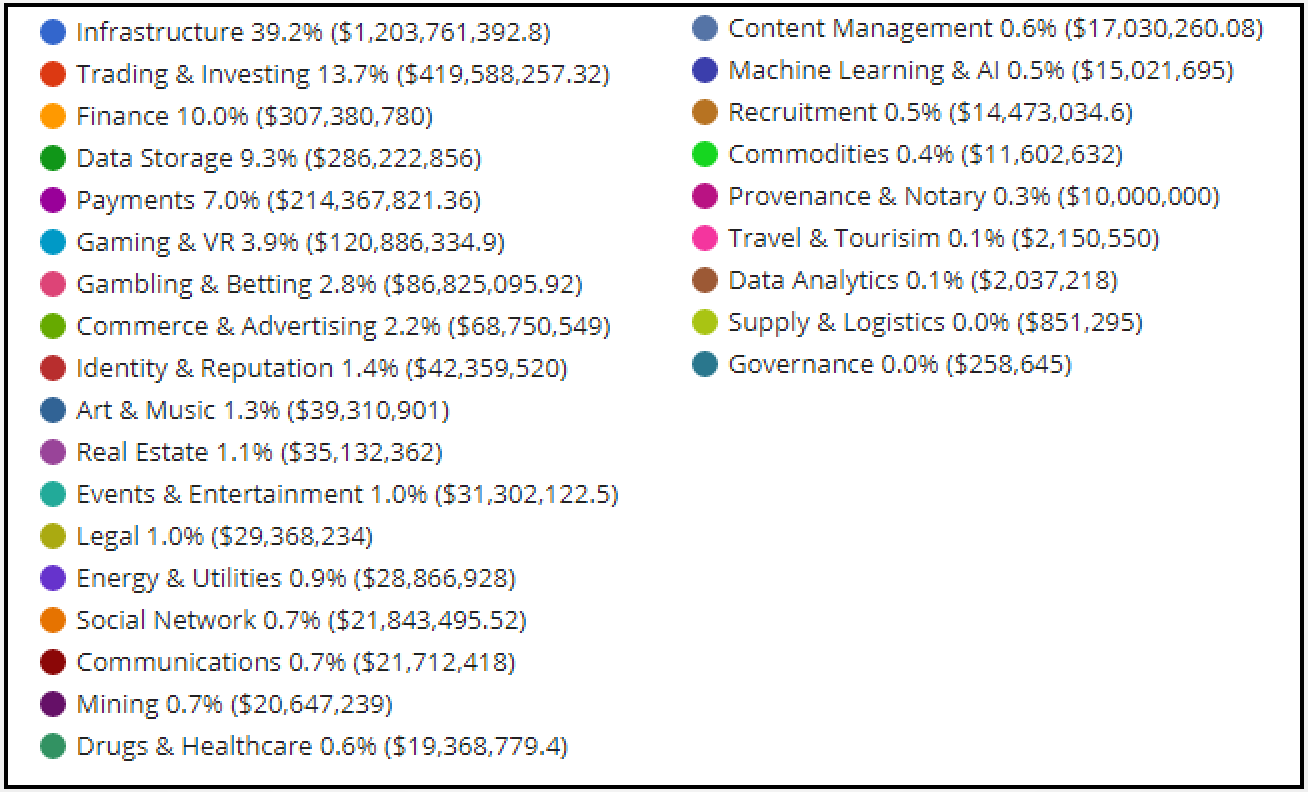
Totals raised are grouped by the ICO closing date and are valued using BTC exchange rate at that time. Data correct on 16th October 2017 14:00 UTC

Total Raised: $3,071,120,416

Total Number of ICOs: 202

Top Ten ICOs of 2017

Position	Project	Total Raised
1	Filecoin	$257,000,000
2	Tezos	$232,319,985
3	EOS Stage 1	$185,000,000
4	Bancor	$153,000,000
5	Kin	$97,041,936
6	Status	$90,000,000
7	TenX	$64,000,000
8	MobileGO	$53,069,235
9	KyberNetwork	$48,000,000
10	MCAP	$45,192,400



- ● Infrastructure 39.2% ($1,203,761,392.8)
- ● Trading & Investing 13.7% ($419,588,257.32)
- ● Finance 10.0% ($307,380,780)
- ● Data Storage 9.3% ($286,222,856)
- ● Payments 7.0% ($214,367,821.36)
- ● Gaming & VR 3.9% ($120,886,334.9)
- ● Gambling & Betting 2.8% ($86,825,095.92)
- ● Commerce & Advertising 2.2% ($68,750,549)
- ● Identity & Reputation 1.4% ($42,359,520)
- ● Art & Music 1.3% ($39,310,901)
- ● Real Estate 1.1% ($35,132,362)
- ● Events & Entertainment 1.0% ($31,302,122.5)
- ● Legal 1.0% ($29,368,234)
- ● Energy & Utilities 0.9% ($28,866,928)
- ● Social Network 0.7% ($21,843,495.52)
- ● Communications 0.7% ($21,712,418)
- ● Mining 0.7% ($20,647,239)
- ● Drugs & Healthcare 0.6% ($19,368,779.4)
- ● Content Management 0.6% ($17,030,260.08)
- ● Machine Learning & AI 0.5% ($15,021,695)
- ● Recruitment 0.5% ($14,473,034.6)
- ● Commodities 0.4% ($11,602,632)
- ● Provenance & Notary 0.3% ($10,000,000)
- ● Travel & Tourisim 0.1% ($2,150,550)
- ● Data Analytics 0.1% ($2,037,218)
- ● Supply & Logistics 0.0% ($851,295)
- ● Governance 0.0% ($258,645)

Decentralized Autonomous Organization (DAO)

- Corporations are, if you strip everything away to the bare bones, a complex set of contracts and agreements.

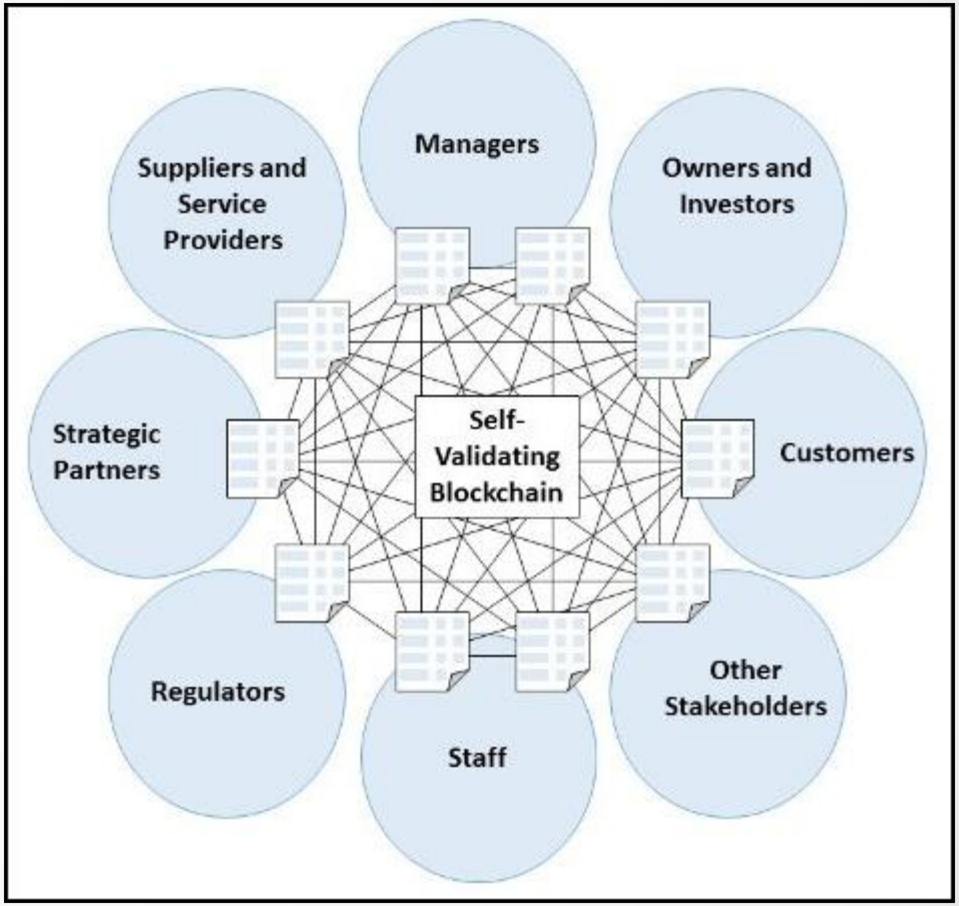
- Most simplistically, employment contracts set the terms for workers pay, duties and responsibilities. Contracts with vendors and customers ensure supply chains are established and maintained. Lease agreements cover office space, vehicles, large machinery and rights to intellectual property. Corporate debt are bond indentures, and equity shares give owners rights to vote and a share of profits.

- Smart contracts exist without the need for those institutional layers. An organization can be built where all of these agreements are replaced by such smart contracts, and in essence the corporation will exist entirely as an entity on a blockchain. As such it will be a decentralized organization, existing across all the nodes of the network.

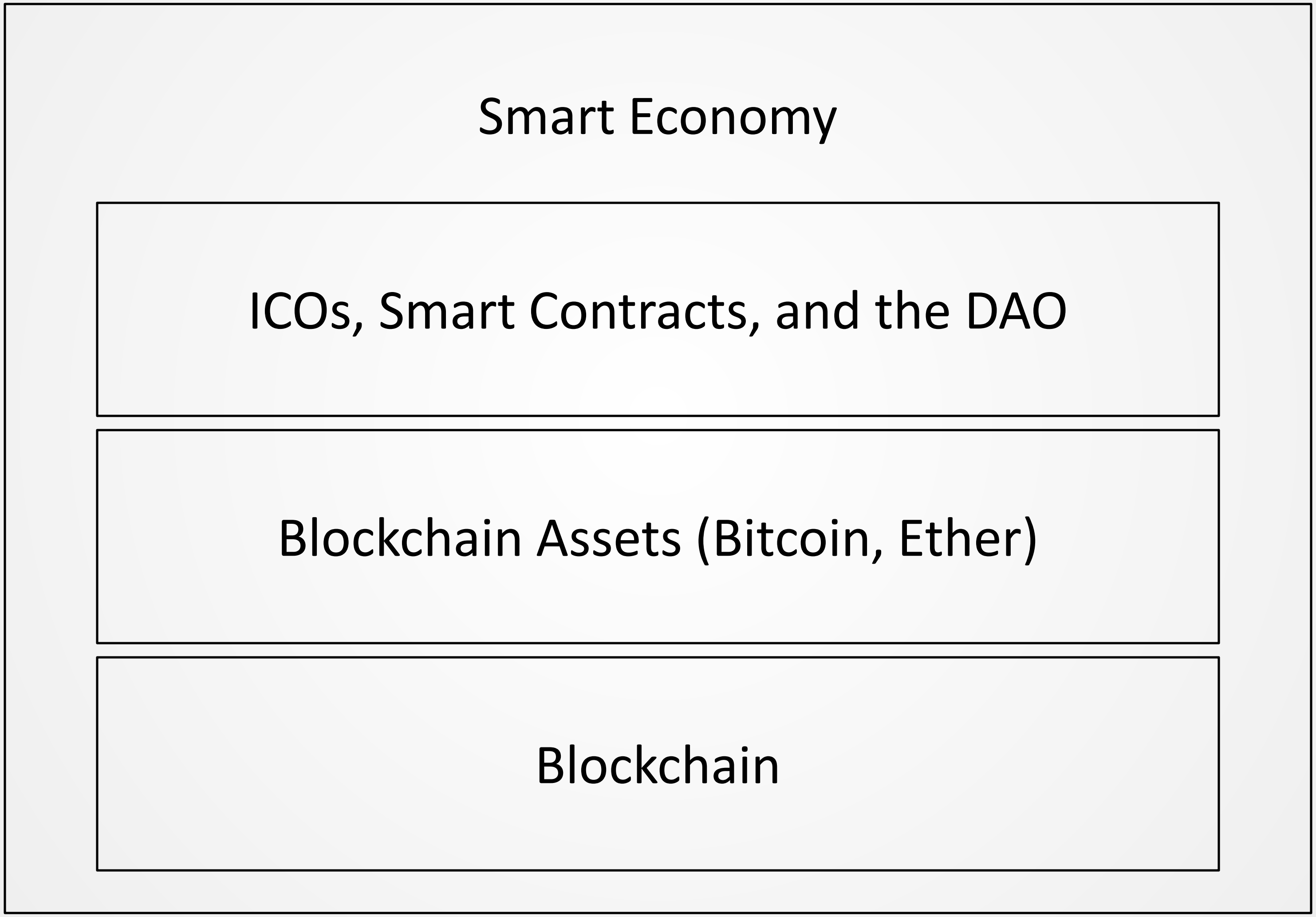
- A DAO would be in the business of generating economic profits if it were structured as a corporation (DAC), and it could raise capital through crowdsales of tokens directly to the blockchain, akin to shares in a public company. Tokenholders would be entitled to their share of profits in the form of dividends, and could vote on the direction of the company. Those tokens could also trade on a secondary market (also on the blockchain) for people to buy and sell them at will.

Features of a DAO

- No central control
- Administered entirely on the web
- Relationships regulated with smart contracts thereby replacing traditional contracts
- Highly transparent
- Ability to scale decision making to thousands of globally distributed entities
- Impartial



The Distributed Economy



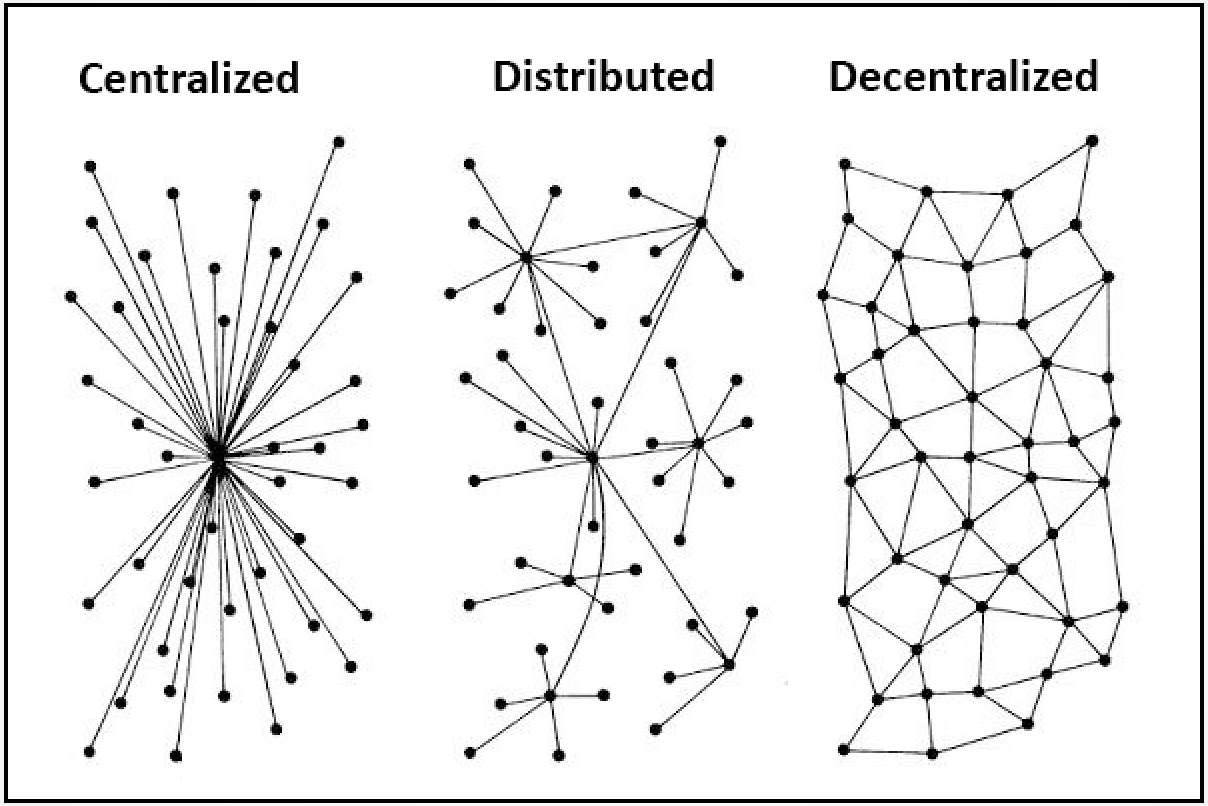
Smart Economy

ICOs, Smart Contracts, and the DAO

Blockchain Assets (Bitcoin, Ether)

Blockchain

Distribution Spectrums

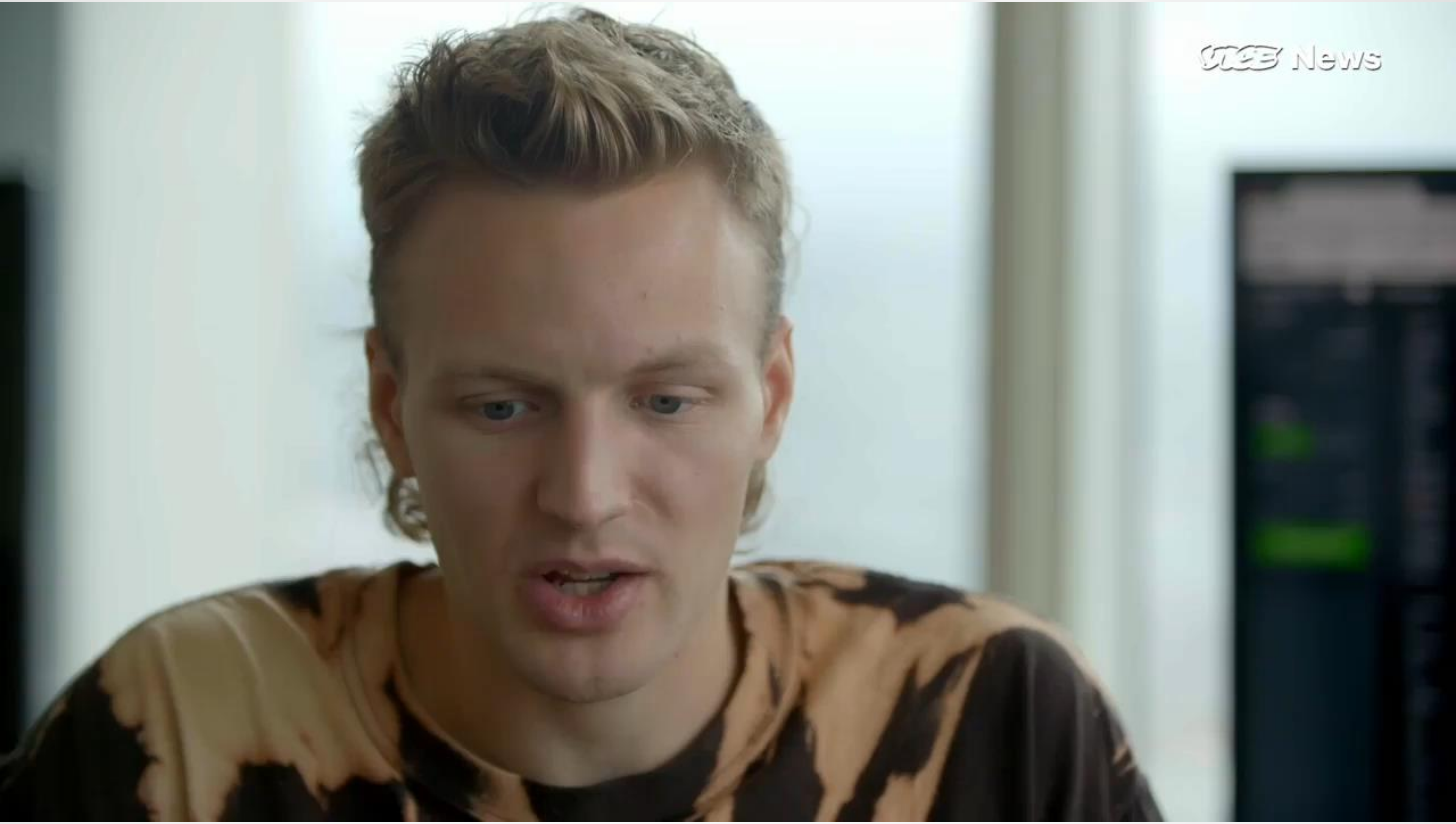


VICE News

- Driverless cars will pick up passengers (who pay it in digital currency) and then the car goes and fills up gas spending digital currency from its own wallet. The car can hire a person to change its oil or fix a flat tire, and could even hire a developer to improve its software code.

- The question becomes: who owns the car? In this scenario, the car owns itself; it is effectively a DAO. Because it uses a digital currency like Bitcoin, it can open a 'bank account' without a social security number, drivers license or any other credential that a person is required to today

- When this happens, machines (hardware and software) become peers in the economy rather than mere tools. Imagine a world where drones that own themselves make deliveries, where autonomous software applications engage in virtual business such as buying and selling server time, or even buying and selling stocks and bonds


VICE News

Where to Start? Compliance & Custody

Digital Custody

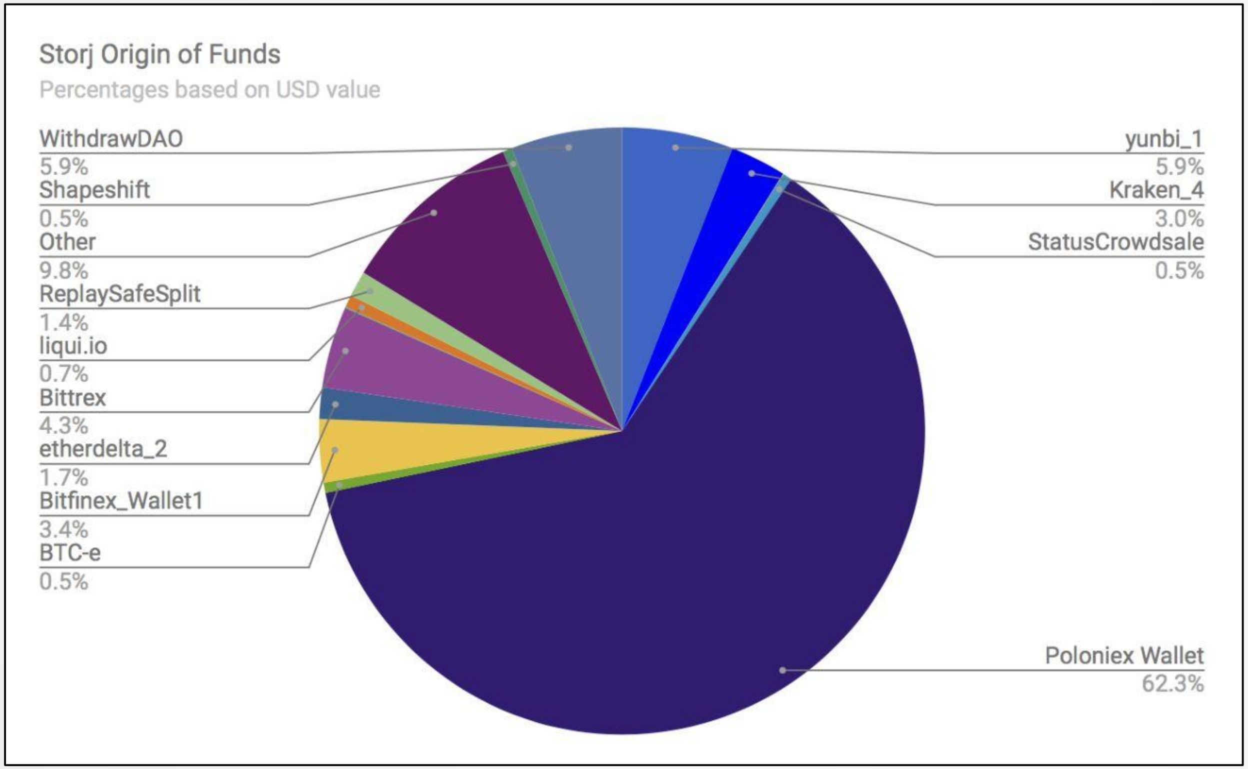
Digital Cold Storage Custody physically located in an offline environment provides investment vehicles a secure **Physical jurisdictional management and reporting framework** to securely maintain the safety and oversight of their digital assets.

Cold Storage

- Intermediaries can transfer digital assets holdings to an **offline segregated account** outside the reach of external digital threats.
- Sterling has developed a proprietary cold storage system to **secure the private keys of digital assets**.
- Through the user interface, custody clients can instruct **deposit and withdrawal transactions** through a multi-factor authentication system.
- All external **source and destination addresses will be evaluated and risk rated** before any transaction are approved for execution.
- Risk rating external addresses allows Sterling to **authenticate the likely hood that digital assets have interacted with nefarious activities**

STORJ DIGITAL ASSET SOURCE ANALYSIS EXAMPLE

3,147 addresses contributed to the ICO on Ethereum. The top 33% of the total ICO funds were contributed by 27 investors who each invested between $30,000 - $457,000. This is approximately $2,500,000 of the $11,000,000.



Category	Percentage	ETH Value	USD Value
82.4%	204,404	2,060,000	
9.8%	16,044	245,000	
7.8%	109.618	195,000	
100.0%	330,067	2,500,000	

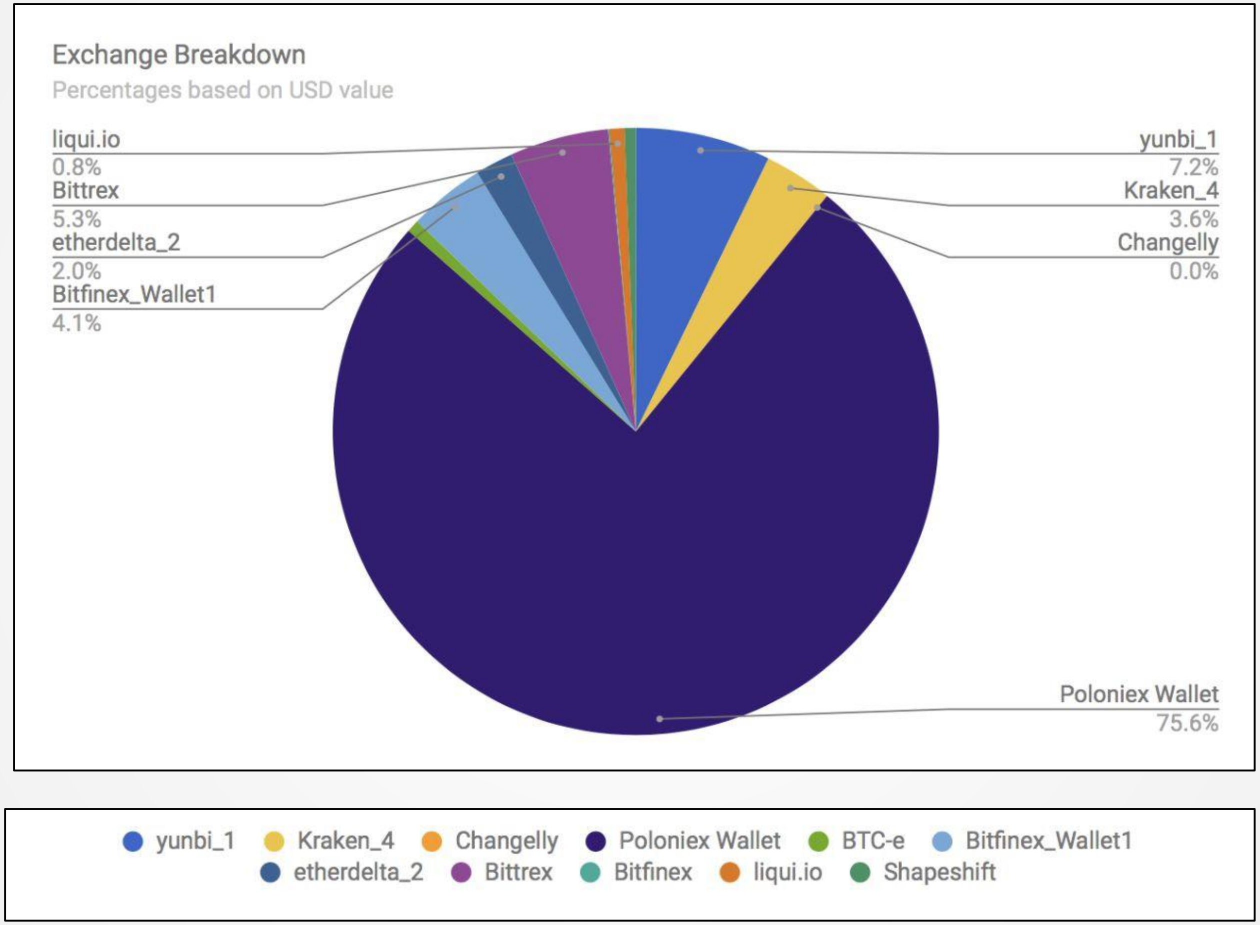
STORJ DIGITAL ASSET SOURCE ANALYSIS EXAMPLE

The vast majority, **82.4%, of funds are sourced from Exchanges**. Within the category of Exchanges, 75.6% came from Poloniex, 7.2% from Yunbi. 5.4% from Bittrex, 4.1% from Bitfinex, and 3.6% from Kraken. These **exchanges follow AML/KYC procedures** and thus perceived as low risk.

Additionally within the category, 2.0% from Etherdelta, 0.8 % from liqui.io, 0.7% came from BTC-e, and 0.6% from Shapeshift.

- These **exchanges are riskier because they are decentralized or are not fully regulated**.
- Shapeshift and Etherdelta are decentralized exchanges.
- BTC-e and Liqui.io are high risk exchanges given that they do not meet all regulatory requirements.

STORJ DIGITAL ASSET SOURCE ANALYSIS EXAMPLE

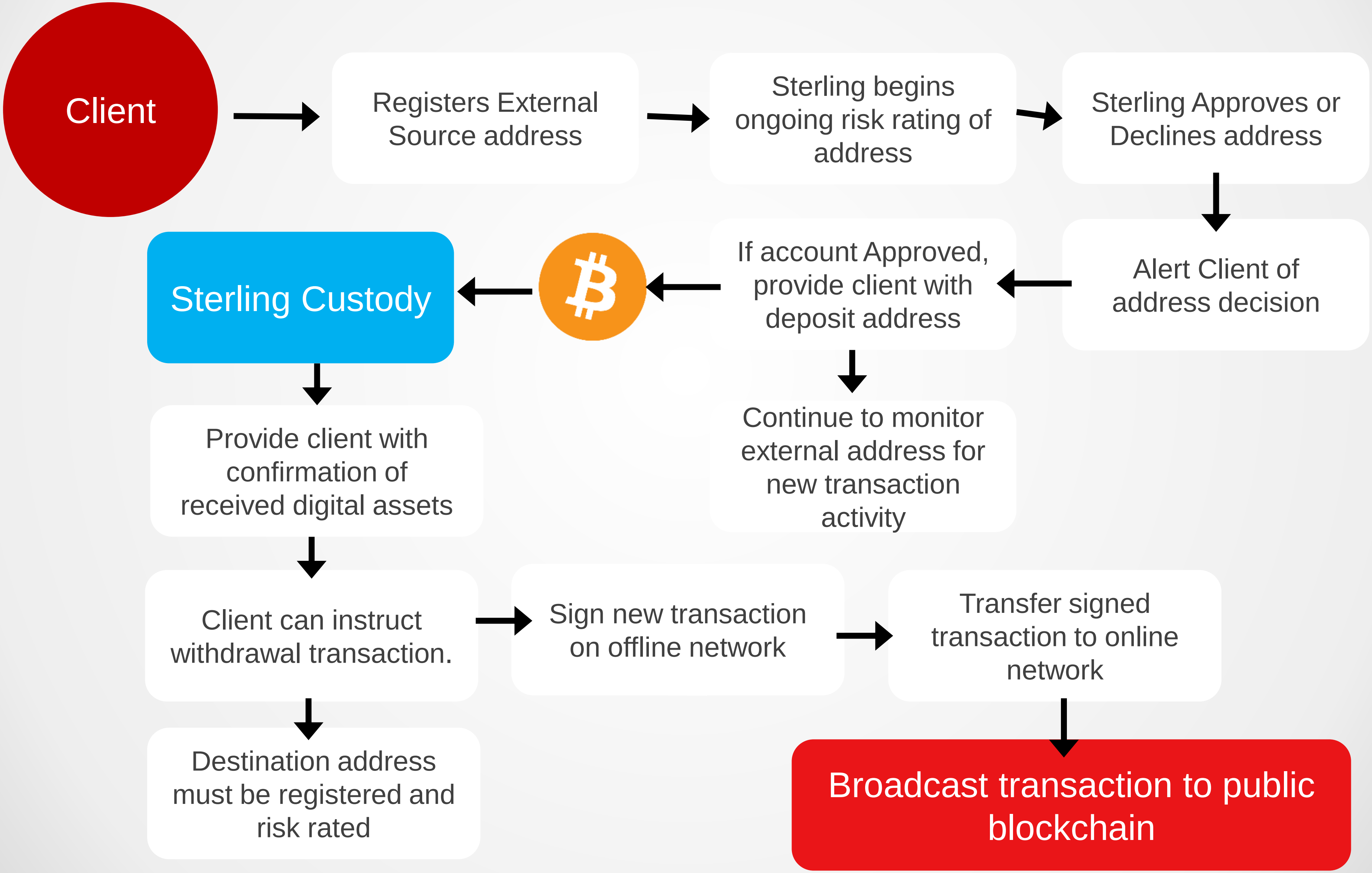


STORJ DIGITAL ASSET SOURCE ANALYSIS EXAMPLE

Table below is a list top 15 investors including ETH and USD and percentage of sources per investor.

#	Address (investors)	ETH Value	USD Value	Source %
1	0xfec1ddff4c93268f25d7cb3575e8f8e6606e3ef3	2800	457,044.00	0.7 % Kraken 93 % Poloniex
2	0x18ec06065afd93736470735e4f4a2855348ea7d4	2000	249,200.00	100 % Poloniex
3	0x5816c2687777b6d7d2a2432d59a41fa059e3a406	2000	247,620.00	10.8 % Poloniex
4	0xb418a48cafa238b6d579d55ed53ac6e57278f138	1500	171,735.00	N/ A
5	0xc287648d7493f67cc0b798ae37c2b2dfb562fb80	1000	191,160.00	N/ A
6	0x5884125bb2bbc3e8b02e94ebf1eacf97489ad3c3	900	124,254.00	99.9 % Poloniex
7	0xf49486831535cfebbefb5715321e7dbdb29752af	849	97,202.01	N/ A
8	0x69b556c8f06198f732118ec3ad810312e56d75bc	805	92,164.45	100 % Poloniex
9	0x68a54e5d0ef549e809eaf794886b936f30a07155	800	91,592.00	1.9 % Poloniex
10	0x0413f607ebce5fc58e3fdc8eb0bbfd7420df8835	510	57,681.00	0.1 % Yunbi 62.2 % Poloniex 0.2 % BTC-e
11	0xdaef46f89c264182cd87ce93b620b63c7afb14f7	500	61,990.00	53.5 % Yunbi 22.7 % Bitfinex
12	0x75b65657986c07aa457485d54bb85f9f8134f44b	500	66,330.00	75.8 % Kraken
13	0x8c81413b022da6fdae6b887e79b9316d271845b7	439	49,703.12	N/ A
14	0x96c94cc58a45b48fdb56c632218bb4b495dd7c99	421	48,313.76	69.1 % Kraken
15	0x8d02909a554d55bd08815619a0f0a791d7657cc2	400	45,240.00	0.7 % Poloniex 9.5 % Etherdelta 33.1 % Bittrex 11.4 % Liqui.io 4.7 % Shapeshift

Operations



Client

Registers External Source address

Sterling begins ongoing risk rating of address

Sterling Approves or Declines address

Alert Client of address decision

If account Approved, provide client with deposit address

Continue to monitor external address for new transaction activity

Sterling Custody

Provide client with confirmation of received digital assets

Client can instruct withdrawal transaction.

Destination address must be registered and risk rated

Sign new transaction on offline network

Transfer signed transaction to online network

Broadcast transaction to public blockchain

In Summary

Sterling has developed a digital asset custody solution to maintain the security and oversight of client digital assets within the jurisdiction of the Cayman Islands.

- All digital asset external source and destination addresses are risk rated and continually evaluated.
- Client digital assets are segregated and never commingled.
- All of these digital assets are stored and secured offline using unique digital asset addresses in our Cold Storage System, which are independently verifiable and auditable on their respective blockchains.
- This service is ideal for institutional customers like hedge funds, mutual funds, and exchange-traded funds, who may be *required by law* to store their digital assets with a licensed custodian in a segregated and non-commingled custody account.