Trustless System

DeFi & Other Applications in the fields of Finance & Governance

Subhojit Shome | Management Trainee | Vinod Kothari Consultants

Date: 04th August 2022

Kolkata:
1006-1009, Krishna
224 AJC Bose Road
Kolkata – 700 017
Phone: 033 2281 3742
Email: info@vinodkothari.com

New Delhi:
A-467, First Floor,
Defence Colony,
New Delhi-110024
Phone: 011 6551 5340
Email: delhi@vinodkothari.com

Mumbai:
403-406, Shreyas Chambers
175, D N Road, Fort
Mumbai
Phone: 022 2261 4021/ 3044 7498
Email: mumbai@vinodkothari.com

Website: www.vinodkothari.com

Image Courtesy: Kanchanara | Unsplash.com | Free License

Table of Contents

Trustless System

Repository of News & Information	Social Media	@FinMinIndia @RBI @MCA21India
Marketplace between buyers/ sellers	Transport Networks	Uber InDriver Ola
Authenticated Goods/ Services	Membership/ Artist Platform	Spotify Patreon

Legacy?

Newspaper Publication

Taxi/ Tour Operator

Record Labels

Business Models are changing. There is a transition from Product to Platforms

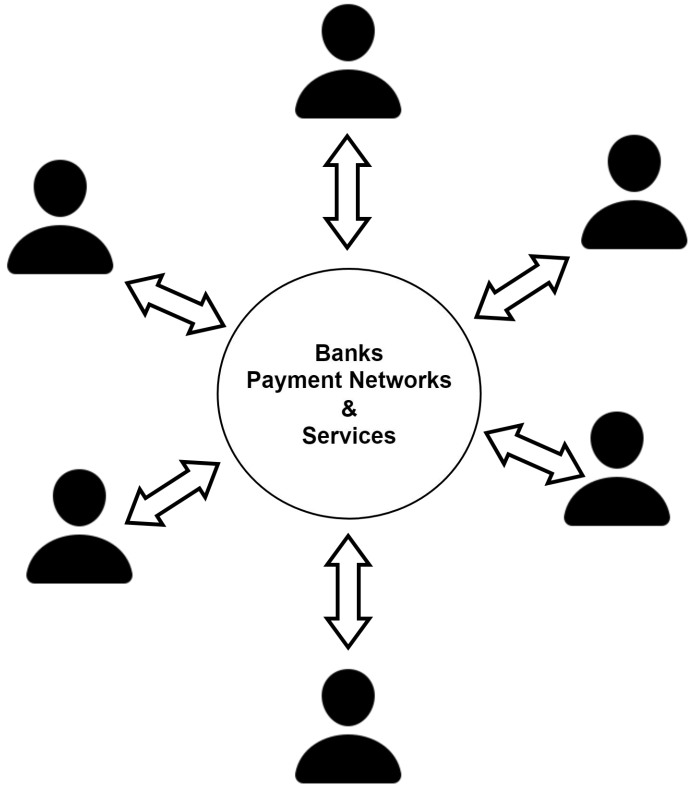
From: Companies providing products/ services directly to consumers

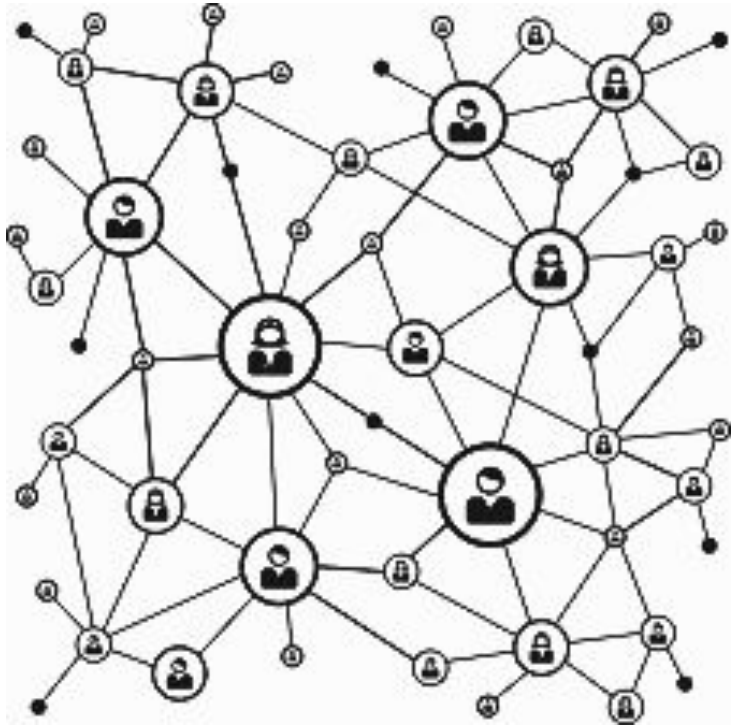
To: Companies (usually Big Tech) providing platforms for creators, service providers, gig workers and users to connect to each other

This has broadened the playing field but users still need to rely on these platform providers (few large corporates) to act as trusted middlemen. Such platform providers enjoy a large share of the revenue pie produced in the system, which is often disproportionate to their cost of developing and maintaining the underlying infrastructure

Trustless System

- Underlying idea is that it is possible to delegate to a technological artefact (system) the trust that we have thus far granted to existing corporate, social or political institutions.
- As such, the technology has been often referred to as "trustless technology" or "trust machine"because it eliminates the need to rely on trusted intermediaries, as long as one can trust the underlying technology"
- Trust in institutions/ people is replaced by trust in the underlying technological framework



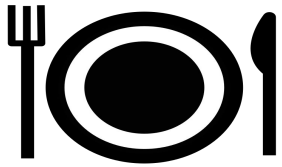


From Central Authority/ Intermediary Driven to a Distributed System

Trusted Party (1/3)

- Trusted (3rd) party is an entity which facilitates interactions between two (or more) parties where both trust the third party
- A Trusted Party may also facilitate interaction between a person and such person's assets/ liabilities
- E.g. banks, certifying authorities, trustees, brokers, etc.
- 'Trusted' means that the entity/ institution/ person needs to be trusted to act in your interests
- There is no way to adequately verify if such entity is actually acting in your interests
- If it could be verified to act in your interests, it would not need your trust
- If it can be demonstrated to operate against your interests you would not use it

Trusted Party (2/3)



You have a meal and a beverage at a restaurant.
How many trusted parties are needed for this transaction to be possible?

1. FSSAI License
2. Eating House License
3. Shops & Establishment License
4. Liquor License
5. Health Trade License
6. Fire Safety License/ NoC from Fire Department
7. Music License (IPRS.org)
8. Environmental clearance License
9. Signage License
10. Weights & Measures/ ISO
11. UIDAI, Passport Authority, RTO

13. RBI
14. Bank
15. Digital payment Service provider (Mastercard, Visa, Rupay, gpay, phone pe, …)

and others.

Trusted Party (3/3)

Secured NCD issue of ₹500 crores by a listed company on private placement basis.

How many trusted parties are necessary for this transaction?

1. SEBI (Role as Trusted Party)
2. Debenture Trustee
3. Stock Exchange
4. MCA/ RoC (Role as Trusted Party)
5. Financial Auditor
6. Compliance Certification Authority
7. Valuer
8. Depository
9. Depository Participant
10. Credit Rating Agency
11. Registrar & Transfer Agent
12. Issuer's Bank/ Investors' Banks
13. RBI (Role as Trusted Party)
14. Notary Public

Mid-Sized IPO

1. SEBI (Role as Trusted Party)
2. MCA/ RoC (Role as Trusted Party)
3. Stock Exchange
4. Depository
5. Depository participant
6. Merchant Bankers
7. Underwriter
8. Financial Auditor
9. Compliance Certification Authority
10. Credit Rating Agency (IPO Grading)
11. SCSB
12. UPI (NCPI)
13. Valuer

Ref: *Checklist for issuance of listed debt securities on private placement basis*

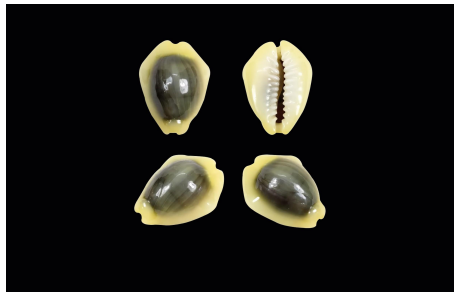
The Need for Trustless Systems

- **Reduce/ Eliminate reliance on a central authority figure**
  - The central authority figure need not be the Government/ Regulator, it can be anyone who can change the rules of the game without (necessarily) receiving consent of its players
  - Single Point of Failure
- **Reduce/ Eliminate the reliance on certifying authorities**
  - Current financial systems require the involvement of 3rd party certifying authorities to shore up trust of the users of the system. This is like having a referee for the game who himself does not participate in the game.
  - Complexity of financial systems make it often necessary to have multiple referees for a single game.
  - Referees are sometimes not entirely disinterested in the result of the game
- **Reduce/ Eliminate Inefficiencies**
  - Multiple parties need to keep their own records of a transaction, such as in the case of a syndicated loan where you have (say) 10 major banks contributing to a big ticket infrastructural project., There is a substantial expense in overhead, duplication, delay, as well as risk of error
- **Increase equity in the system**
  - Every member of the trustless system is simultaneously a contributor and an actual shareholder in the system .
  - As a result, the value produced within these networks can—at least theoretically—be redistributed in a much more equitable manner with participants consenting on such distribution.

Ref: *The Blockchain and the New Architecture of Trust, Kevin Werbach (2018, The MIT Press Cambridge, London)*

The Double Spending Problem

What is Money?

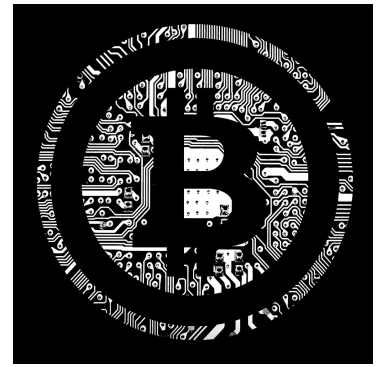


Scarce & Desirable

Control Supply

Counterfeiters will be beheaded

IN GOD WE TRUST



In Code we trust?

The Use Case

We need a Currency System which serves all traditional functions that money serves without the need of a Central Intermediary/ Authority

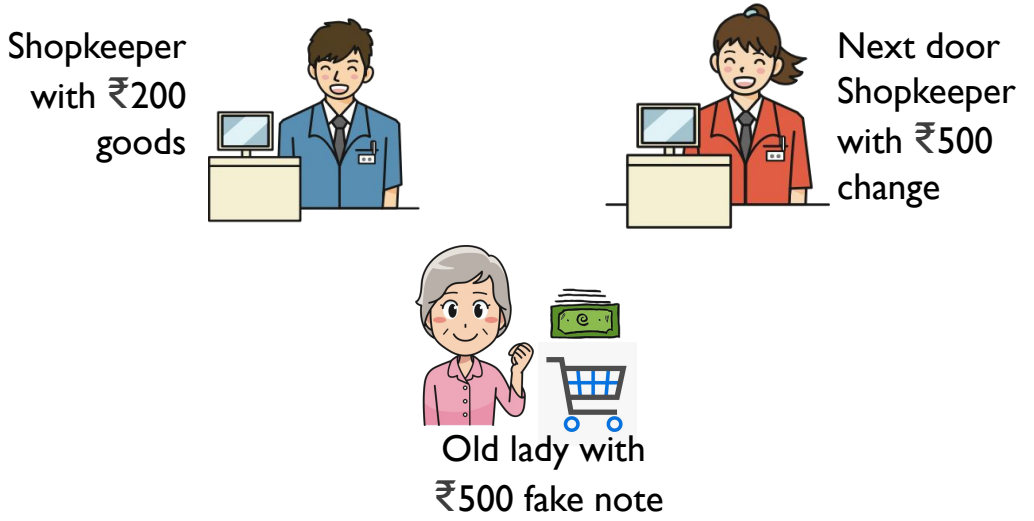
The Problem Statement

Removing the Central Intermediary/ Authority gives rise to the Double Spending Problem -

The double spending problem is a phenomenon in which a single unit of currency is spent simultaneously more than once creating a disparity between the spending record and the amount of that currency available.

Double Spending - The Lady, The Shopkeeper & The Fake Note

- An old lady buys goods worth ₹200 from a shop
- The lady gives the shopkeeper a ₹500 note
- The shopkeeper doesn't have change so he gets change of ₹500 from the next shop
- The shopkeeper returns the lady ₹300 and keeps ₹200 for himself
- Next day, the next door shopkeeper says the ₹500 note is a fake and takes her money back from the original shopkeeper



Assuming that the original shopkeeper had sold the good on a no-profit/ no-loss basis, how much profit/ loss does he incur as a result of this transaction?

Spending money that you don't own

- **Double spending** becomes a more serious issue when it comes to digital currency (token). - simpler to *'counterfeit'* at scale
- To prevent double spending payment systems use a central trusted third party that can verify whether a currency/ token has already been spent by a user/ participant of that system.
- Without relying on a central party, is it possible to ensure
  - [Currency Supply] Prevent individuals from devaluing the currency by generating additional unauthorized funds
  - [Non-repudiability] Secure and non-repudiable record of transactions
  - [Ownership Record] Who owned what amounts at any given point in time

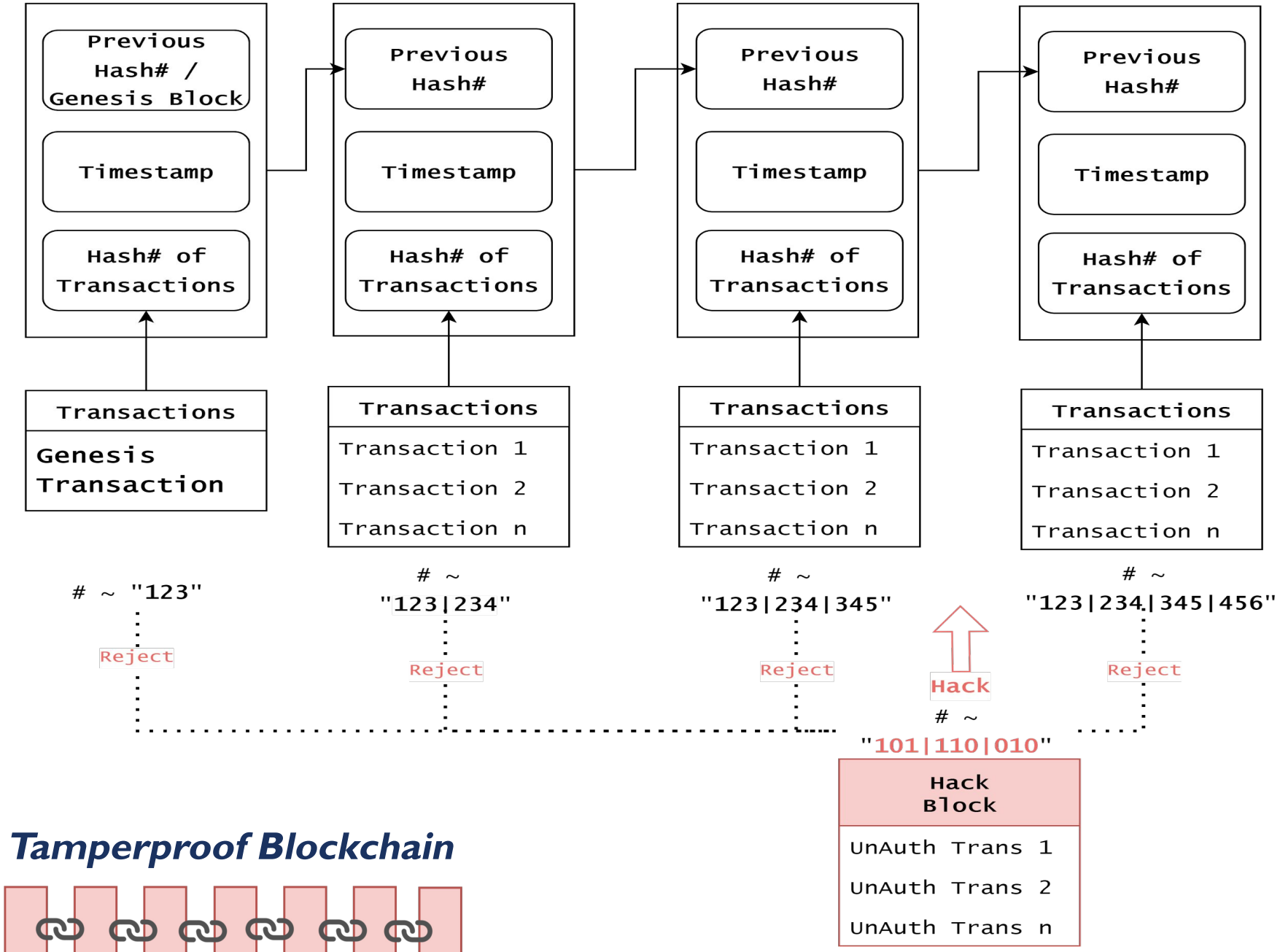
Distributed Ledger Technology (DLT) - Blockchain

What makes a Blockchain a Blockchain?

- Peer-to-peer network comprised of computers (known as "peers" or "nodes"), often scattered across the globe.
- These peers store exact or nearly exact copies of a blockchain
- The store is resistant against network failure/ corruption. A single live instance of the blockchain can regenerate the blockchain for all peers
- Peers coordinate by using a software protocol that precisely dictates how network participants store information, engage in transactions, and execute applications on top of the chain
- Data once written is immutable/ tamper-resistant
- Data is stored in a transparent and non-repudiable manner although parties/ peers writing the date are anonymous/ pseudonymous

Necessary Features

- A peer-to-peer (P2P) global network
- A failure resilient store of information
- A tamper resistant book of accounts/ ledger
- A consensus mechanism
- An anonymous/ pseudonymous network but with non-repudiable transactions



Tamperproof Blockchain

- Transactions records are grouped into a block and have a hash value generated though cryptographic means
- Same transactions records will have the same hash value. A change in the record will change the hash value value
- As more transactions enter the network they are again grouped into a block, the hash of the previous block is stored in the current block and is assigned its own hash value
- The block hash value prevents tampering of records of that specific block
- While "chaining" the previous hashes across blocks prevents unauthorised insertion of blocks
- Addition of a new block takes place based on a consensus mechanism defined by the network - Proof of Stake, Proof of Work, other incentivisation method

Pseudonymous But Non-Repudiable

Purpose	Address/ Key	Sample
Account	**Public/ Wallet Address (WK)**	1nspZFH47xMPKD1Txnmrecvu7i6hmK8BP
Password to Account	**Private Key (PK)**	9241938e3e1bf2b6def24a85d89dbc8f812428e8c5b185d85bb651d577e727df
Publicly Verify Access to Account	**Public Key (PBK)**	0371c28f32d3aa2c7d04eb329e257436c5717a4f26527fe2140553ce8fa05bed0e

*It is possible to **verify** the public address from public key without knowing the private key*

*The public address is generated uses a Base58 Check Encoding which allows systems to **validate** the public address - similar to the checksum process*

Access with the private key, Verify with a public key

This address has transacted 898 times on the Bitcoin blockchain. It has received a total of 144,342.34655065 BTC ($3,300,133,711.35) and has sent a total of 144,342.31210254 BTC ($3,300,132,923.76). The current value of this address is 0.03444811 BTC ($787.60).

Account Summary of of a Peer

Public/ Wallet Address of Peer

Address	1FfmbHfnpaZjKFvyi1okTjJJusN455paPH
Format	BASE58 (P2PKH)
Transactions	898
Total Received	144342.34655065 BTC
Total Sent	144342.31210254 BTC
Final Balance	0.03444811 BTC

Fee 0.00004234 BTC (18.735 sat/B - 7.376 sat/WU - 226 bytes) (29.403 sat/vByte - 144 virtual bytes) +0.00009566 BTC

Hash# of the Transaction Records

Hash b8e9a4dd30696d60513a5078abe4d471c60a318706f53b1eb9efb0... 2022-07-10 23:01

bc1qppgd4s2tza28nwueznet3wu7uwlqn5xpr5... 0.00064828 BTC

Public/ Wallet Address of Peer

bc1qppgd4s2tza28nwueznet3wu7uwlqn5xpr5p... 0.00051028 BTC
1FfmbHfnpaZjKFvyi1okTjJJusN455paPH 0.00009566 BTC

Fee 0.00021298 BTC (2.974 sat/B - 0.752 sat/WU - 7162 bytes) (3.008 sat/vByte - 7081 virtual bytes) +0.00270527 BTC

Hash 6af12b241ecdf6640b1231a8246b847f1a5a6bb93d19368c41e9840f... 2022-06-26 01:48

bc1qywef9uee5encshu2s9qm4w85fprc4e9d0fj... 3.05342728 BTC

3Lk1o76dmWqmnvBu3FxCAQMotBwWr1UwFn 0.00259714 BTC
3MCGoPX17GUbooVjjMv2i9VUbU6HA1U4k6 0.01619837 BTC
1LNniGt3Ho6r3iJq6jDTSwhMHhTYWoYtrw 0.00085246 BTC
36LsLqyZJzonfKZTJC1BWyH1TEpPfS8haJ 0.00944400 BTC
bc1qk84nryrr22mkmv2tdhyawzs9xyqmmzkhq8... 0.00209687 BTC
3JdNaC4CSNNAzRnjpo1JnvZw9NktzvWYjH 0.00433465 BTC
1P2axXJJoNn4P5yce6VK9yMWMXWpsa6ic4 0.00179383 BTC
34Hn9trTNKUxFBPKxmBX1oqM7kWh7Ec9SB 0.00271510 BTC
33yyk28aJyQTGRxzeyVC3T5g2oVapsHodY 0.0018888
3GHn8yS8hSfcdPhEkdYmXxufNYfDJgC7Dk 0.000212

Load more outputs... (203 remaining)

Transactions with/ by the Peer

This transaction was first broadcast to the Bitcoin network on July 10, 2022 at 11:01 PM GMT+5:30. The transaction currently has 3,409 confirmations on the network. At the time of this transaction, 0.00060594 BTC was sent with a value of $12.66. The current value of this transaction is now $13.98. Learn more about how transactions work.

Details of the Transaction

Hash# of the Transaction Records

Hash	b8e9a4dd30696d60513a5078abe4d471c60a318706f53b1eb9efb091ca6f5430
Status	Confirmed
Received Time	2022-07-10 23:01
Size	226 bytes
Weight	574
Included in Block	744462
Confirmations	3,409
Total Input	0.00064828 BTC
Total Output	0.00060594 BTC
Fees	0.00004234 BTC

Block in which transaction recorded

Block 744462

USD | BTC

This block was mined on July 10, 2022 at 11:05 PM GMT+5:30 by F2Pool. It currently has 3,409 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 6.25000000 BTC ($144,761.38). The reward consisted of a base reward of 6.25000000 BTC ($144,761.38) with an additional 0.28958332 BTC ($6,707.28) reward paid as fees of the 2813 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

A total of 104,721.25707427 BTC ($2,425,534,906.53) were sent in the block with the average transaction being 37.22760650 BTC ($862,259.12). Learn more about how blocks work.

Hash# of the Block

Hash	00000000000000000013e073beab1cfbfe9d9162f43e3b57e5bdac8ee3476bc
Confirmations	3,409
Timestamp	2022-07-10 23:05
Height	744462
Miner	F2Pool
Number of Transactions	2,813
Difficulty	29,152,798,808,271.88
Merkle root	cef7eae3973e0519ec138d6060e73b92cb73056078398c00249d497bfcdfbc8d

No. of Peers confirming validity

Peer who received incentive/mining fee

Details of the Block containing the Transaction

Issues Emerge - The Bitcoin Distributed Network

- With Transaction volumes and the network growing, the Bitcoin network became sluggish — it could only reach consensus and validate transactions roughly every ten minutes — and latency continued to rise
- Decentralised structure made its protocol hard to update and improve, and the network lacked formal governance, relying on the efforts of a small group of developers who slowly revised and fix bugs and made performance improvements to the underlying software
- It was becoming apparent that it was prohibitively expensive to maintain decentralised systems. Cost of computational resources required to validate transactions in a block started exceeding the incentive (in the form of Bitcoin) received from performing such function.
- In response to the above issue, validators ('miners') started pooling their computational resources resulting in the consensus mechanism becoming concentrated in a few large pools.

Decentralised infrastructure ≠ Decentralisation of powers within the infrastructure

Ref: *Blockchain Technology and Decentralized Governance:The Pitfalls of a Trustless dream; Primavera de Filippi (January 2020)*

Distributed Apps & Decentralised Finance

Emergence of Decentralised Application ('dapps')

Response to issues

- New blockchain networks - better software performance and incentivisation systems - with application
- Application/ Application platforms were built over (overlay) the existing bitcoin network
- Platforms provided user ability to interact with an underlying blockchain and also to build their own applications that interacted with the platform to store information (distributed ledger)
- Interactions with the Blockchain were through small computer programs called Smart Contracts (Platform native)

Dapps

Users could also configure their own smart contracts and create applications by combining such programs for richer and more diverse usages

- A large portion of such applications provided for traditional finance (TradFi) activities to be performed "on-chain"
- Since these applications were usually owned and controlled by specific parties with the underlying distributed blockchain used as a ledger, these applications are also referred to as CeFi (Centralised Finance)
- **"Pure DeFi"** - the blockchain technology framework also gave rise to certain finance activity (which did not exist in the traditional world of finance)
  - Staking
  - Lending

  Both related to yield mining

There also arose the concept of Permissioned Blockchain, where participation is limited and requires authorisation from a central authority

DeFi Tokens

- Blockchain-based *Tokens* can be described as digitally scarce units of value the characteristics and circulation of which are prescribed via computer code

- Tokens can almost represent any and everything, as determined by the issuer of the token
- Tokens are created and distributed by firms and platforms with a variety of purposes.
  - They can grant users access/participation to online services (utility tokens)
  - They can serve as a means of payment or assure the right to purchase products (exchange/ payment/ currency tokens) or
  - they can represent a stake in the issuer's company/ revenues (security token)

- Coins vs Tokens
- Fungible vs Non-Fungible (NFT)
- ICO vs STO vs IEO
- As part of DeFi, security token - asset or investment tokens that issuers use to raise funding and investors invest in to earn returns - play a significant role. Security tokens are issued in a security token offering (STO).

Ref:
Understanding Initial Coin Offerings EPRS Briefing Paper; Angelos Delivorias [July 2021]
IOSCO Decentralized Finance Report; IOSCO [March 2022]
6th STO/ ICO Report - A Strategic Perspective; PwC (Spring, 2020)

NFT - What is Fungible…

Units of Fiat Currency (₹)

Units of Fiat Currency ($)

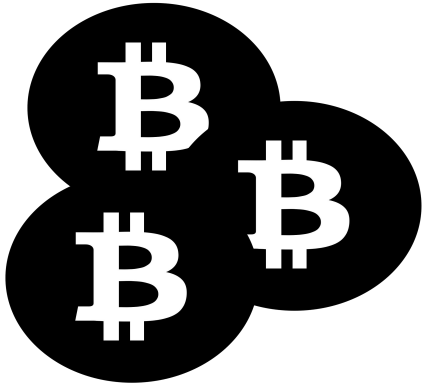
Reliance Industries Limited

TCS TATA CONSULTANCY SERVICES

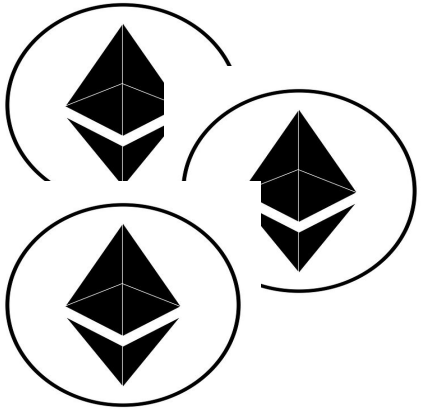
Securities of Companies (traditional demat)

Traditional Assets

Digitised Assets/ Tokens



Units of Bitcoin (BTC)



Units of ETH (Ξ)

THE WORLD BANK

Bond - i

Santander launches the first end-to-end blockchain bond

Securities issued and managed using Distributed Ledger Technology (Blockchain)

Ref:

https://www.worldbank.org/en/news/press-release/2018/08/23/world-bank-prices-first-global-blockchain-bond-raising-a110-million

https://www.santander.com/content/dam/santander-com/en/documentos/notas-de-prensa/2019/09/np-2019-09-12-santander-launches-the-first-end-to-end-blockchain-bond-en.pdf

NFT - What is NOT Fungible…

Mona Lisa
by
Leonardo Da Vinci

Sunflowers
by
Vincent Van Gogh

Sgt. Pepper's
Music Album
by
The Beatles

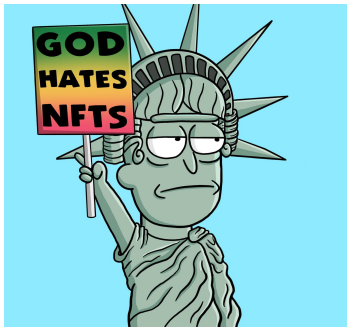
Malabar Hill Property,
Mumbai

Malad West Property,
Mumbai

Traditional Assets

Digitised Assets/ Tokens

Women Unite
by MissKaina



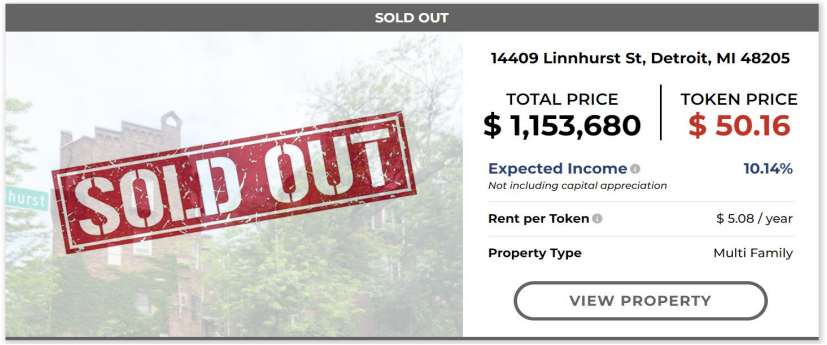
God Hates NFTees
by SrPetersETH

Digital Art Tokens

"This Bonus Track can be paired with your Player or Death Row Records node once the node network is activated to unlock earning potential on the Gala Music network! You can also use this instrumental to make your own beats, mashups, songs, and remixes!"

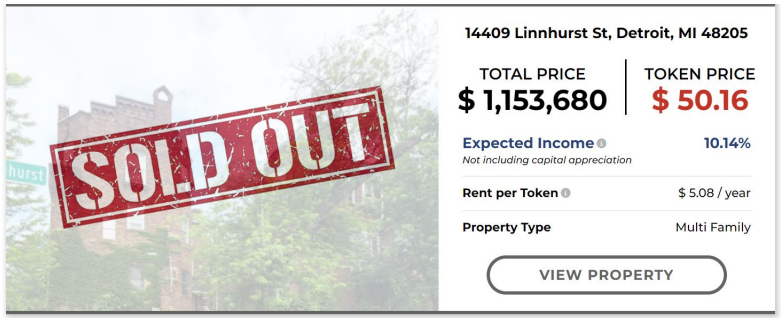
B.O.D.R by Snoop Dogg

Copyrighted Music Tokens



Property Rights Token

NFT - Not Fungible But Fractional



PROPERTY HIGHLIGHTS

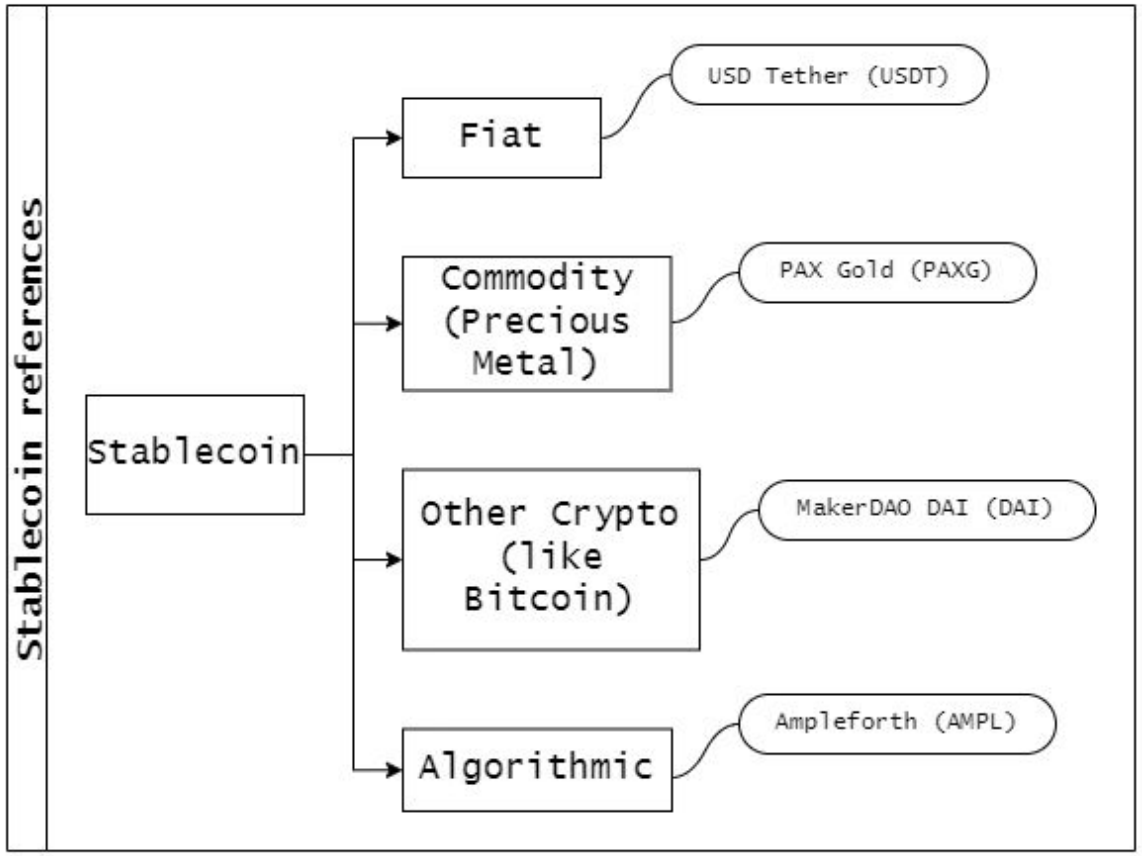
Expected Income *Not including capital appreciation*	**10.14%**
Rent Start Date	July 15, 2022
Rent per Token	$ 5.08 / year
Token Price	$ 50.16
Total Tokens	23,000

PROPERTY HIGHLIGHTS

Expected Income *Not including capital appreciation*	**10.13%**
Rent Start Date	July 4, 2022
Rent per Token	$ 5.03 / year
Token Price	$ 49.59
Total Tokens	2,500

- Further fractionalisation may be possible depending on token implementation
- Users may be able to exchange a fractional value of the token itself, similar to how a single unit of Bitcoin can be fractionalised (e.g. 0.001 BTC)

Stablecoins – volatility neutral tokens



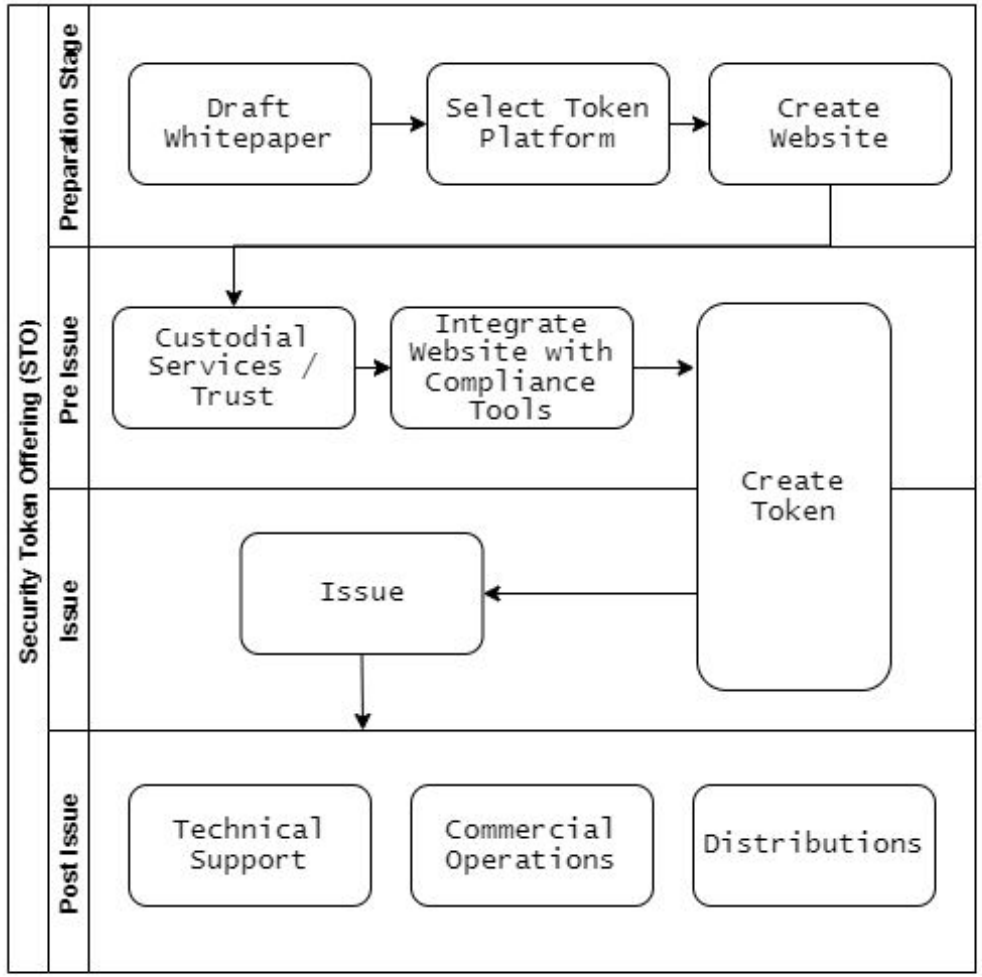
- Stablecoins are tokens that seek to achieve a particular characteristic (ie, price stability). They act as a low volatility store of value and means of exchange that is global, efficient and accessible.
- Stablecoins attempt to achieve price stability by being pegged to one or more of fiat currencies, other real-world assets, other crypto-assets or have their values being algorithmically maintained by adjusting token supply to fluctuations in demand
- The fiat currencies, or assets with equivalent fair value, may or may not be safeguarded by a custodian
- Although an essential part of DeFi, the stablecoin itself may reside and be managed on a centralized network under the control of a specific promoter instead of a public blockchain

The Infamous Bitcoin Pizza

In 2010, Laszlo Hanyecz spent 10,000 Bitcoins (BTC) at a local pizza restaurant to buy himself two pizzas. Back then, it was worth only $40.
Today, 10,000 BTCs can be redeemed for over ₹35 billion. Stablecoins are designed to guard against such price volatility.

Source:
Global Stablecoin Initiatives Public Report, IOSCO [March 2020]
Ethereum.org

Security Token Offering (STO) - Bird's Eye View



In the way it is currently used an STO can be considered the DeFi alternative to traditional sources of start-up funding such as venture capital (VC), private equity or angel finance rather than an alternative to a full blown traditional finance IPO

- An STO usually starts with creating a *white paper/ offer memorandum that* contains a details of the business model, project team and management, the risk factors of the project and rights and restrictions built into the token being issued.
- Then follows selecting the platform to issue and manage the tokens, plugging in the offer details, compliance tools (KYC/AML) and the issue interface with the project's website or app (often the token platform itself provides such services or user interface).
- The actual issue taken place by registering the token on the platform and configuring and executing a smart contract which mints and issues the token against receipt of investor funds and writes the transactions to the underlying distributed digital ledger (blockchain).
- Post issue 'distributions' (such as dividend, interest payments) continue to be managed by the smart contract through the issue of additional token to investors and writing the transactions to the underlying blockchain.

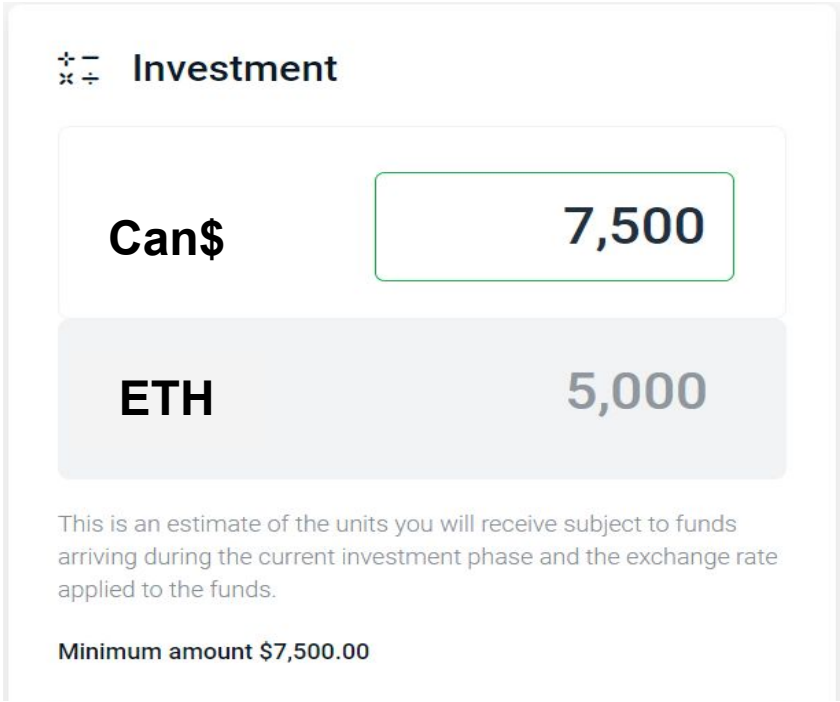
The STO Smart Contract

- The STO smart contract ('Launch STO') in the adjoining diagram provides an illustrative list of the parameters that an issuer may configure to launch and manage a tiered STO.
- Such parameters include the specifications regarding
  - when the STO should launch or close
  - the minimum investment increment
  - the maximum investment permitted from *non-accredited investors*
  - the currencies (native platform currency, other cryptocurrencies, stablecoin or fiat that the investor may invest in)
  - the wallet (electronic) to which issue proceeds should be credited,
  - the price of tokens and discounts available in each tier of the STO, etc.

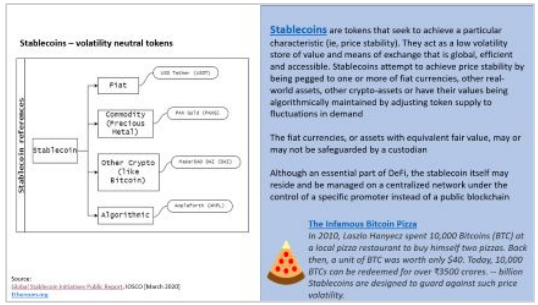
```
await (
  await token.issuance.offerings.launchTieredSto({
    startDate: new Date(2020, 5, 6),
    endDate: new Date(2020, 7, 8),
    nonAccreditedInvestmentLimit: new BigNumber(10),
    minimumInvestment: new BigNumber(5),
    currencies: [Currency.ETH],
    raisedFundsWallet: userAddress,
    unsoldTokensWallet: userAddress,
    allowPreIssuance: true,
    tiers: [
      {
        tokensOnSale: new BigNumber(1000),
        price: new BigNumber(89),
        tokensOnSale: new BigNumber(100),
        price: new BigNumber(45),
      },
    ],
  })
).run()
```

Source: code snippet from the Polymath SDK – Launching a non-USD STO

Currency of investments

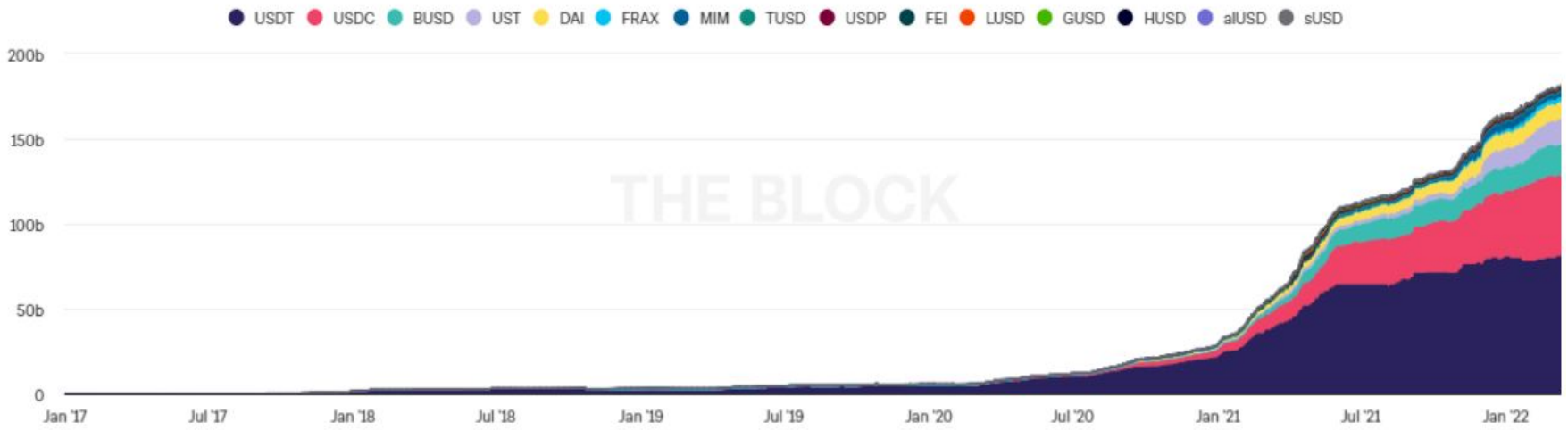



```
await (
 await token.issuance.offerings.launchTieredSto({
  ...
  currencies: [Currency.ETH, Currency.StableCoin],
  stableCoinAddresses: [
   '0xStableCoinAddress' // stable coin address
  ],
  customCurrency: {
   currencySymbol: 'CAD',
   ethOracleAddress: '0xOracleAddress' // address of the oracle that
states the price of ETH in the chosen currency
  },
  tiers: [...],
 })
).run()
```



Source: code snippet from the Polymath SDK – Launching a non-USD STO

- Smart contracts allows investments to be denominated in a number of crypto or fiat currencies. In the case of fiat currency the issuer needs to the indicate the stablecoin pegged to such currencies.
- The smart contract uses an interface (open source data feeds called an *Oracle*) to convert the value of a specified currency.
- In the illustrative snippet, the code converts Canadian dollars (CAD) to ETH (native currency of the Ethereum blockchain platform).
- This is an illustration of why stablecoins are significant to DeFi adoption. It becomes difficult to incorporate into a DeFi application a fiat currency not having a corresponding stablecoin implementation.



Total stablecoin supply volumes saw significant rise during 2021. The rise is seen to be fueled by an increased need for liquidity by DeFi applications. Although USD pegged fiat-stablecoins account for the significant share of the liquidity

Total value of crypto-assets locked in DeFi applications is estimated to be over $230 billion. The IOSCO Report on DeFi identifies capital formation, development and deployment of DeFi platforms, investment and settlement to be the primary causes leading to the rise in crypto-assets

Source:
IOSCO Decentralized Finance Report, IOSCO [March 2022]
DeFi Dashboard - https://defillama.com/

DeFi - Global Regulatory Aspects

Case Study - Securities (1/2)

Scenario 1

- An owner of arable land divides it into parcels and offers the parcels for sale to interested parties

Scenario 2

- An owner of arable land divides it into parcels and offers the parcels for sale to interested parties.
- Said owner also adds a service agreement to develop and maintain a fruit orchard on such land for a fee

Scenario 3

- An owner of arable land divides it into parcels and offers the parcels for sale to interested parties.
- Said owner also adds a service agreement to develop and maintain a fruit orchard on such land for a fee
- As part of service agreement the said owner also has an obligation to harvest the fruit, sell them in the market and disburse the sale proceeds to the prospective parcel owners after recouping the fee and other related expenses

Can any of these scenarios be considered as a case of offer of Securities?

Case Study - Securities (2/2)

- ☑ Is there an investment of money/ money's worth?
- ☑ Is there a "Common Enterprise"?
- ☑ Is there an expectation of Profit/ Return? Is the Profit/ Return based on the Efforts of Others?

The Howie Test

- The US SEC applies the Howie Test to determine whether to hold tokens issued during ICOs as "Securities"
- Tokens that pass this test qualify as **"Security Tokens" and fall within the regulatory perimeter of the SEC**
- Other developed economic jurisdictions also apply similar test to gauge whether the tokens issued should be subsumed under the extant securities laws

Case Study - Offer/ Issue of Securities (1/2)

Scenario 1

- Tomahawk seeks to raise funds through an ICO to fund the cost of drilling oil wells
- For this purpose it intends to issue 200 million TOM tokens on a "decentralized exchange" based on a blockchain platform
- Half of the tokens (100 million TOM) would be available for purchase by potential investors at a cost of $.05 each.
- ICO Website includes a business plan that describes "a substantial investment opportunity" that is "capable of producing significant risk adjusted rates of return,"
- Tomahawk described the digital asset as a token "backed by profits generated by Tomahawk Exploration LLC an oil producing company."

Scenario 2

- Tomahawk seeks to raise funds through an ICO to fund the cost of drilling oil wells
- For this purpose it intends to issue 200 million TOM tokens on a "decentralized exchange" based on a blockchain platform
- Half of the tokens (100 million TOM) would be available for purchase by potential investors at a cost of **0.0005 BTC (Bitcoin)** each.
- ICO Website includes a business plan that describes "a substantial investment opportunity" that is "capable of producing significant risk adjusted rates of return,"
- Tomahawk described the digital asset as a token "backed by profits generated by Tomahawk Exploration LLC an oil producing company."

Case Study - Offer/ Issue of Securities (2/2)

Scenario 3

- Tomahawk seeks to raise funds through an ICO to fund the cost of drilling oil wells
- For this purpose it intends to issue 200 million TOM tokens on a "decentralized exchange" based on a blockchain platform
- Half of the tokens (100 million TOM) would be available for purchase by potential investors at a cost of 0.0005 BTC (Bitcoin) each
- Tomahawk initiated a **"Bounty Program"** - offering between 10 and 4,000 TOM for activities such as authoring posts about the TOM token on blogspots and other online forums like Twitter or Facebook, and creating Insta posts/ reels or YouTube shorts.
- Tomahawk **issued more than 80,000 TOM as bounties** to approximately 40 wallet holders on a decentralized platform

- Issuance of tokens under so-called "bounty programs" were held to constitute an offer and sale of securities because the issuer provided tokens to investors in exchange for services designed to advance the issuer's economic interests and foster a trading market for its securities. In Re. Tomahawk Exploration LLC, the SEC took the stand that -

> *…the lack of monetary consideration for "free" shares does not mean there was not a sale or offer for sale for purposes of [ ]. Rather, a "gift" of a security is a "sale" within the meaning of [ ] when the donor receives some real benefit*
>
> ***Further, the lack of monetary consideration for digital assets, such as those distributed via a so-called "air drop," does not mean that the investment of money prong is not satisfied;***
>
> *… In a so-called "airdrop," a digital asset is distributed to holders of another digital asset, typically to promote its circulation.*

Case Study - Utility Token (1/2)

- In 2013, Vitalik Buterin conceives the Ethereum Network/ Platform. The Platform allows anyone to deploy permanent and immutable decentralised (incl. DeFi) applications onto it, with which users can interact.
- Vitalik Buterin and other co-founders of the Platform start development of the platform in 2014 raising crowdsourced funds using the "Ethereum Foundation" as an SPV and the platform goes live on 30th July 2015.
- The platform can be used by its users to launch a wide variety of DeFi applications including crypto lending and crypto exchanges. Ethereum also allows users to create and exchange NFTs.
- To become an "User" of the platform one has to purchase ETH Token (Ξ) which are offered as "Bounties" or at a price of 0.005 BTC (Bitcoin)

- [ ] Are the fortune of the investors dependent on the fortunes of Vitalik Buterin, other co-founders of the Platform or the 'Ethereum Foundation'?

- [ ] Do the returns that users' earn from their DeFi Apps deployed on the Platform depend on the actions and decisions of Vitalik Buterin, the other co-founders or Developers of the Platform or on the Management of the 'Ethereum Foundation'?

Case Study - Utility Token (2/2)

- ☑ Investment of money/ money's worth
- ☒ Is there a "Common Enterprise"?
- ☑ Is there an expectation of Profit/ Return?
- ☒ Is the Profit/ Return based on the Efforts of Others?

The Utility Token

- Utility Token are token which can be redeemed for access to a specific product or service that is typically provided using a DLT (Blockchain) platform.
- ICO whitepapers often describe the Coins offered as Utility Token. One must, however, inspect the rights and obligations that the token entail in order to determine whether it truly is an Utility Token

Case Study - "True" Utility Token

Scenario 1

- iCommunity Labs issues a token (iBST) that it describes in its whitepaper document as a 'pure utility token'.
- The token will allow the holder to access a technology platform, the iBS Platform, the firm is developing.
- The token also allows the holder a share in profits in line with their holdings, once the iBS Platform launches and more users subscribe to its services.
- The developers have been careful to make sure the token cannot be be traded on the capital markets.

Scenario 2

- iCommunity Labs issues a token (iBST) that it describes in its whitepaper document as a 'pure utility token'.
- The token allows the holder to access a technology platform, the iBS Platform, the firm is developing.
- Once the iBS Platform launches, more users are expected to subscribe to its services by obtaining iBST tokens.
- The developers have been careful to make sure the token cannot be be traded on the capital markets.

The Regulatory Mandate (1/2)

Investor Protection

- Subsumed under existing securities laws/ regulation (most developed economies)
- Outright Ban (PRC)
- Specific Regulations (Malta)

Innovation and Access to Capital Markets

- Safe Harbour Regulations
- Recognition of Blockchain/ DLT based securities market intermediaries (Registrar and Share Transfer Agent, Depository/ Depository Participant, etc.)
- Recognition of Blockchain/ DLT based securities exchanges/ marketplaces
- Technology Standard & Certification (instead of Trusted Party certification of transactions)

The Regulatory Mandate (2/2)

- **Digital Identity and Data Privacy**

Patrick Breyer v Bundesrepublik Deutschland (Federal Court, Germany)

Subject matter:

> *Dynamic IP address registered by an online media services provider when a person accesses a website that that provider makes accessible to the public constitutes, with regard to that service provider, personal data within the meaning of that provision, where, only a third party, in the present case the internet service provider, has the additional data necessary to identify him*

‘

Personal data’‘mean any information relating to an identified or identifiable natural person (“data subject”)’. Pursuant to that provision, an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity

> *…it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored*

Others Issues -

- AML/ CFT/ Sanction Avoidance
- Tax Avoidance

DeFi - India

Token Offerings by Indian Issuers

- There have been a few token offerings made by Indian companies pre-COVID starting from 2018
- Issuers were mostly cryptocurrency exchanges or fiat-to-bitcoin conversion service providers
- Purpose of the Issue were to create/ maintain applications (DeFi or CeFi) over existing blockchain platform
- Issuers released Whitepaper/ Litepaper providing details of the offering
- Social media was the primary means of promoting the offers
- Offers were launched on crypto exchanges and may be referred to as IEM
  - India has not recognised any cryptocurrency exchanges and does not have specific securities/ financial services laws that apply to them
- The Offers included extra-national entities,
- Investment could be made in foreign currency, currency backed stablecoin, other popular cryptocurrencies (BTC, ETH)
- A percentage of Tokens were also issued as 'Airdrops'
- Tokens issued were described as Utility Token or Currency Token
- Tokens were made available for trade on secondary markets (crypto exchanges)

Regulatory Aspects

Legislative/ Regulatory Aspects

- Investor protection based on general statutes like the Consumer Protection Act
- Prevention of Money Laundering Act (PMLA) applicable and enforcement actions have taken place from early 2020
- No sectoral regulations available yet
- Cryptocurrency Exchanges continue to be outside the regulatory ambit of the securities and financial markets Regulators

SEBI

- Representation submitted by SEBI to GoI, stating need for
  - "feature-based characterisation of the tokenised version of the assets, which may attract supervision of different sectoral regulators"

RBI

- 2018, ban on banks from holding or facilitating cryptocurrency transactions which substantially limited cryptoexchanges carrying on their business.
- The directive was set aside by the Hon'ble Supreme Court in March 2020
- There has not been any further regulatory action from the RBI
- Expect regulatory action if there is an INR stablecoin implementation

Taxation Aspects

GST

- Rates based on the nature of the token
  - Security Token - not covered under GST
  - Utility Token - akin to Vouchers/ Closed system PPI
- Other DeFi activities will also attract GST
  - Brokerage/ Commission Fee
  - Financial Services
- Certain NFTs covered under definition of OIDAR, etc

Enforcement Action

Spate of CBIC actions, during mid to late 2021, against crypto exchanges for GST evasion most related to (utility) token issues.
Enforcement actions led to recovery and imposition of penalties/ interest.

Income Tax

- The Union Budget 2022 introduced tax on virtual digital assets (VDA)
- Definition of VDA under section 2(47A) is comprehensive and covers all token types - security, utility or exchange

  The definition also includes NFTs without any "feature based characterisation"

  This may cause a dichotomy with the underlying asset transfer being taxed at a different rate to the NFT, essentially the taxation principle is not being technology agnostic
- Income from VDAs are taxed at a flat rate of 30%. No deduction allowed except cost of acquisition, no set off or carry forward of loss on transfer (per section 115BBH Income Tax Act)
- TDS applicable per @1%
- Per CBDT Circular no.13 of 2022,
  - person paying consideration ultimately responsible for deducting TDS
  - crypto to crypto trades - both legs should have tax deducted
  - As parties may be trading through Exchanges, the Exchange may perform the deduction

Recommended Reading

Articles/ Papers/ Reports & Regulatory Guidelines

- *European Parliament Briefing - Understanding Initial Coin Offerings, A new means of raising funds based on blockchains; Angelos Delivorias (July 2021)*
- *IOSCO Decentralized Finance Report, IOSCO (March, 2022)*
- Cryptoasset Taskforce - Final Report; HM Treasury, FCA, BoE (October 2018)
- FCA Consultation Paper (CP19/3) - Guidance on Cryptoassets, FCA (January 2019)
- FINMA ICO Guidelines, FINMA (February 2018)
- ESMA Advice - Initial Coin Offerings and Crypto-Assets, ESMA (January 2019)
- SEC Framework for "Investment Contract" Analysis of Digital Assets, SEC (April 2019)
- Blockchain Technology and Decentralized Governance: The Pitfalls of a Trustless dream. Primavera de Filippi (January 2020)

Books

- Blockchain and the Law - The Rule of Code; Primavera De Filippi and Aaron Wright (Harvard University Press, 2018)
- Great Chain of Numbers - A guide to smart contracts, smart property and trustless asset management; Tim Swanson (2014, CC (attribution) license)
- The Blockchain and the New Architecture of Trust, Kevin Werback (2018, The MIT Press Cambridge, London)
- Cryptocurrency Compliance and Operation - Digital Assets, Blockchain and DeFi; Jason Schaferman (2022, Palgrave Macmillan)
- Blockchain and Cryptocurrency: International Legal and Regulatory Challenges; Dean Armstrong (QC), Dan Hyde, Sam Thomas (2019 , Bloomsbury Professional Law)