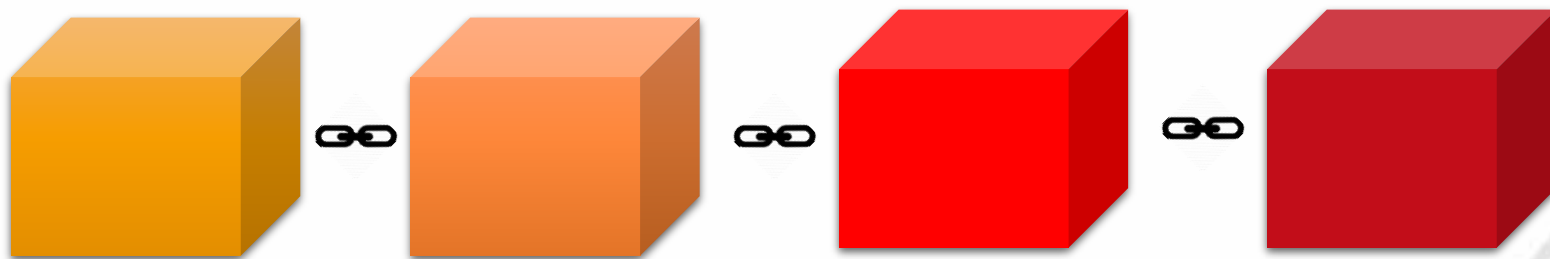




Live more,  
Bank less

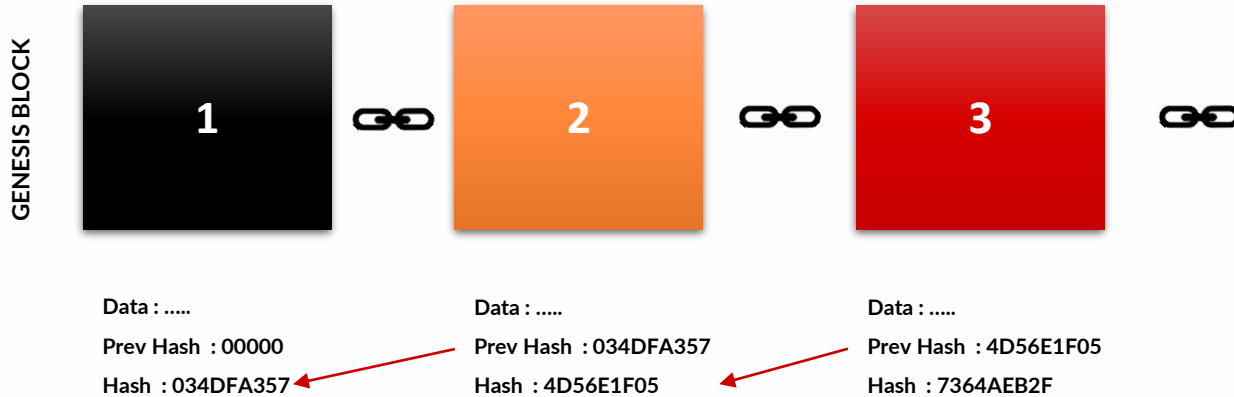
# Introduction to Blockchain



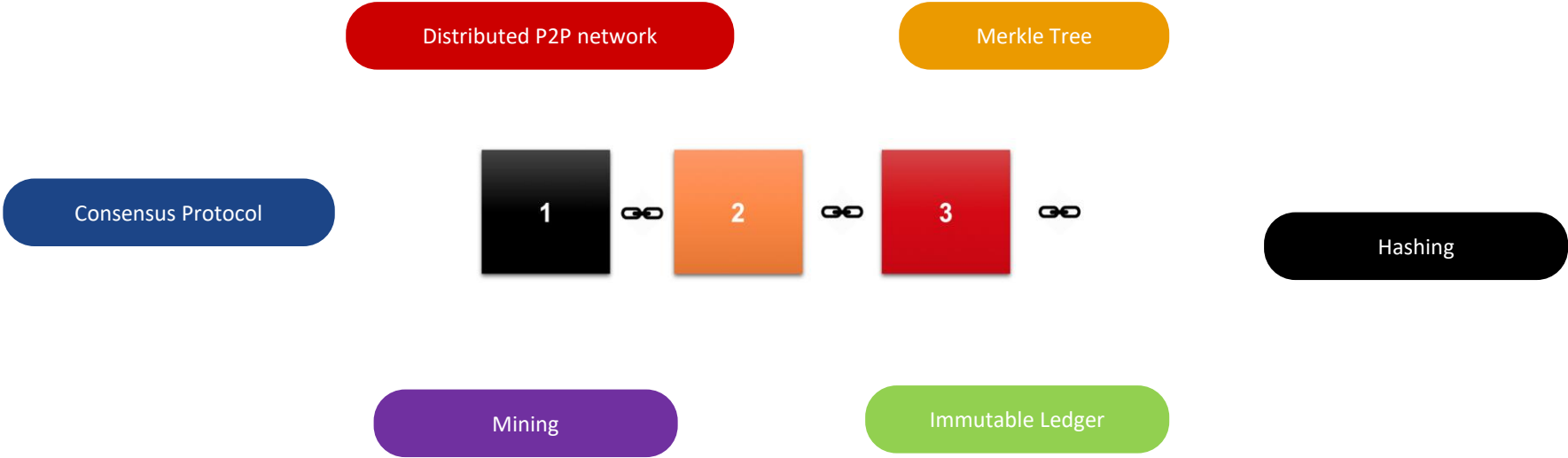
Target Audience : Novice | Beginner

# What is Blockchain ?

- **Blockchain** is a growing list of records, called *blocks*, that are linked using cryptography.
- Each block contains a **data**, **Hash** value and **Hash of previous** block.

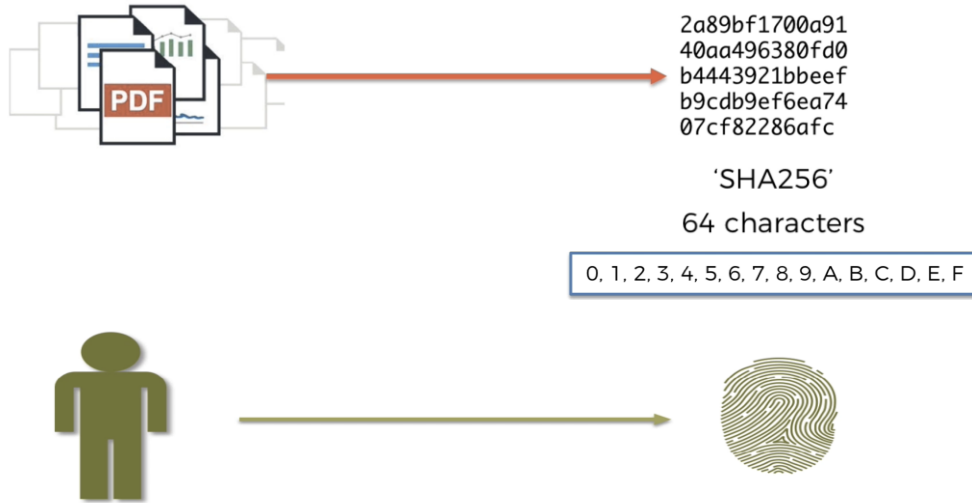


# Getting our feet wet



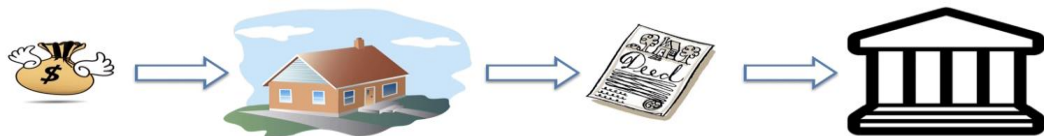
# Hashing function

- Hashing function takes in arbitrary length/size of data and outputs a fixed length of data.
- Output is unique. Exception cases are called **Collisions**.
- Algorithms – Message Digest , SHA
- One way

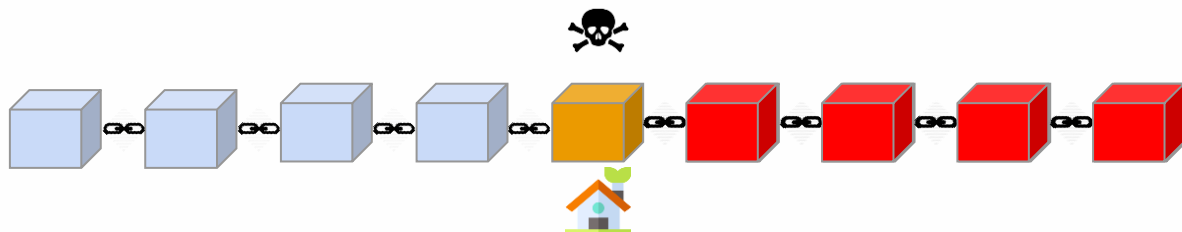


Bitcoin	SHA 256
	RIPEMD 160
Ethereum	Keccak-256

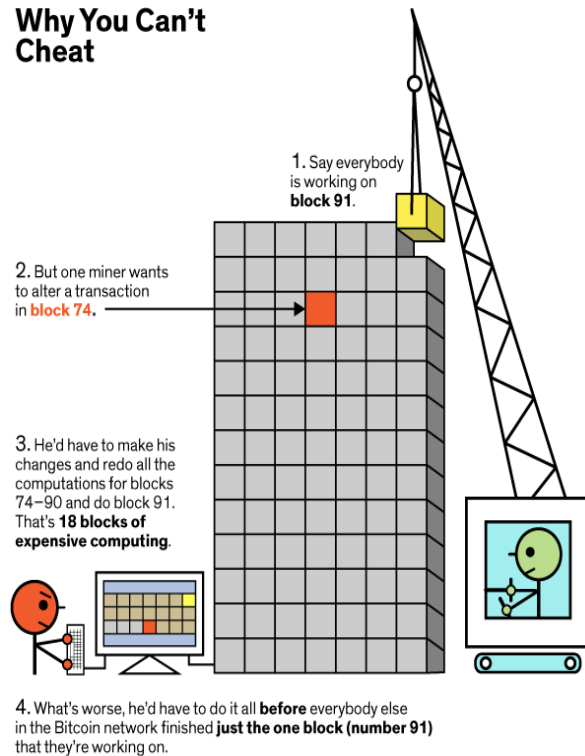
# Immutable Ledger



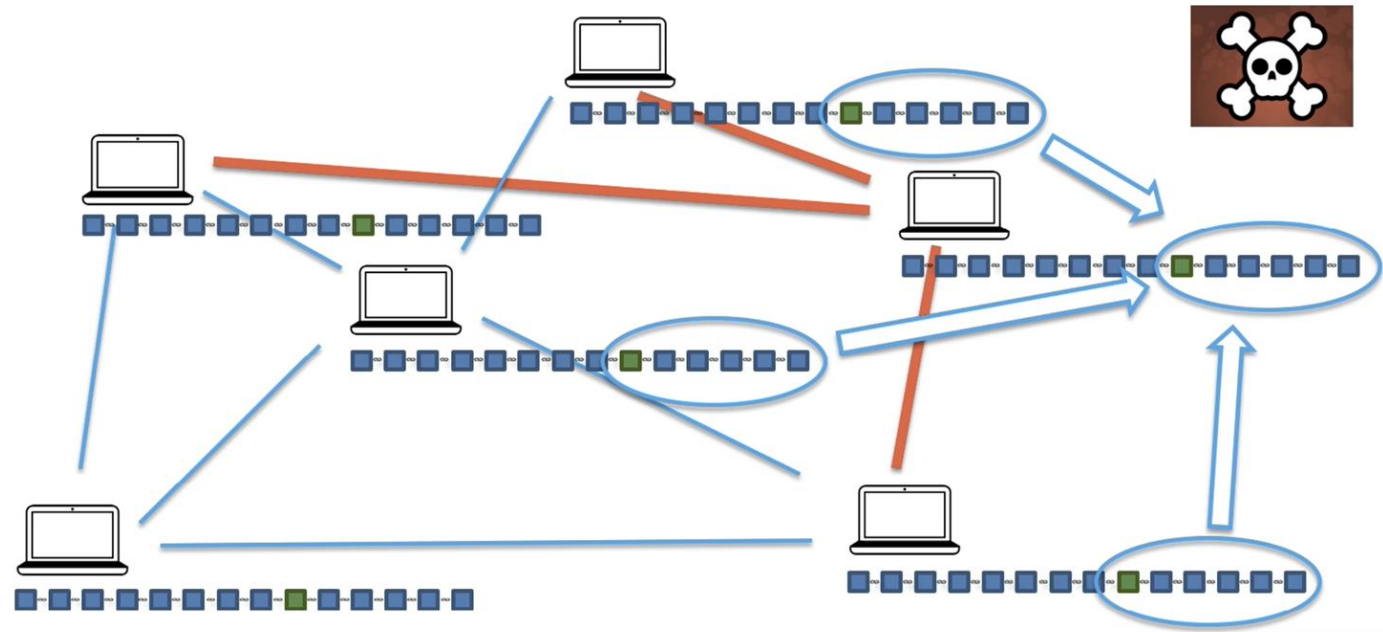
## Traditional Ledger



## Why You Can't Cheat

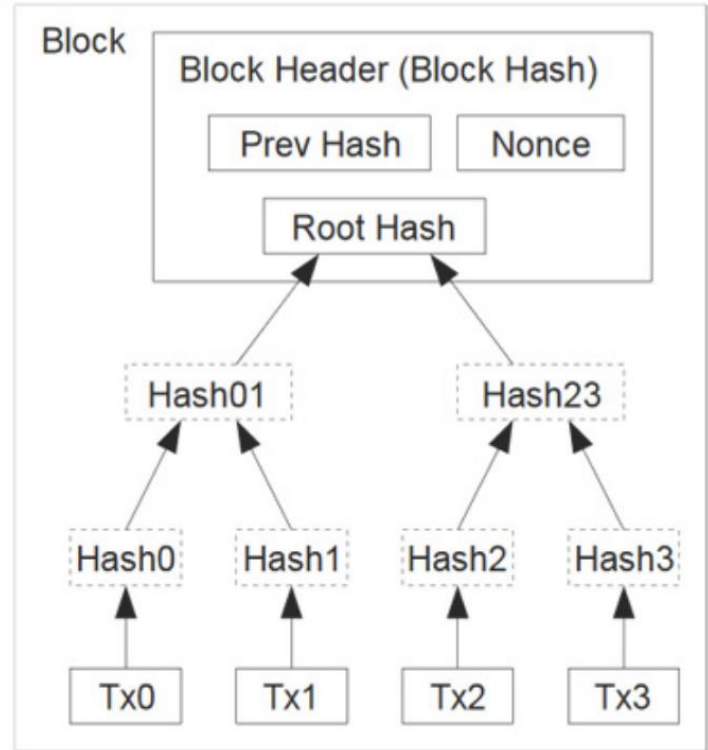


# Distributed P2P network



# Merkle Tree

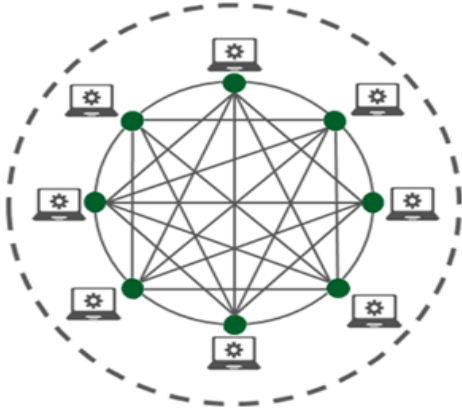
Merkle trees are an integral component of blockchains and effectively allow them to function with provable immutability and transaction integrity.



Transactions Hashed in a Merkle Tree

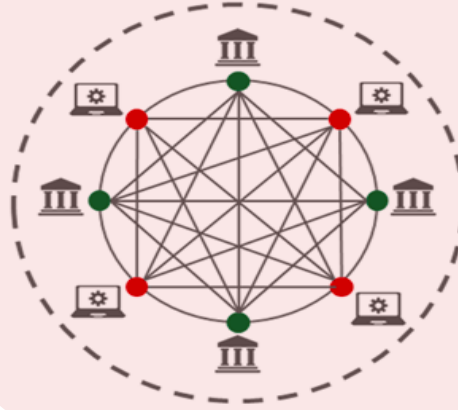
# Types of Blockchain

## Public



- Many, unknown participants
- Writes by all participants
- Reads by all participants
- Consensus by PoW / PoS

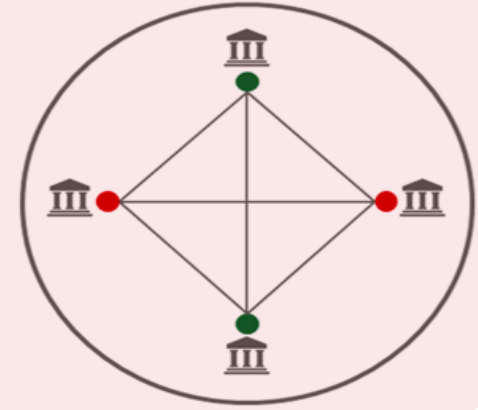
## Hybrid



- Known participants from multiple organizations
- Writes requires consensus of several participants
- Reads may be public / restricted
- Consensus by multiple algorithms

## Enterprise

## Private

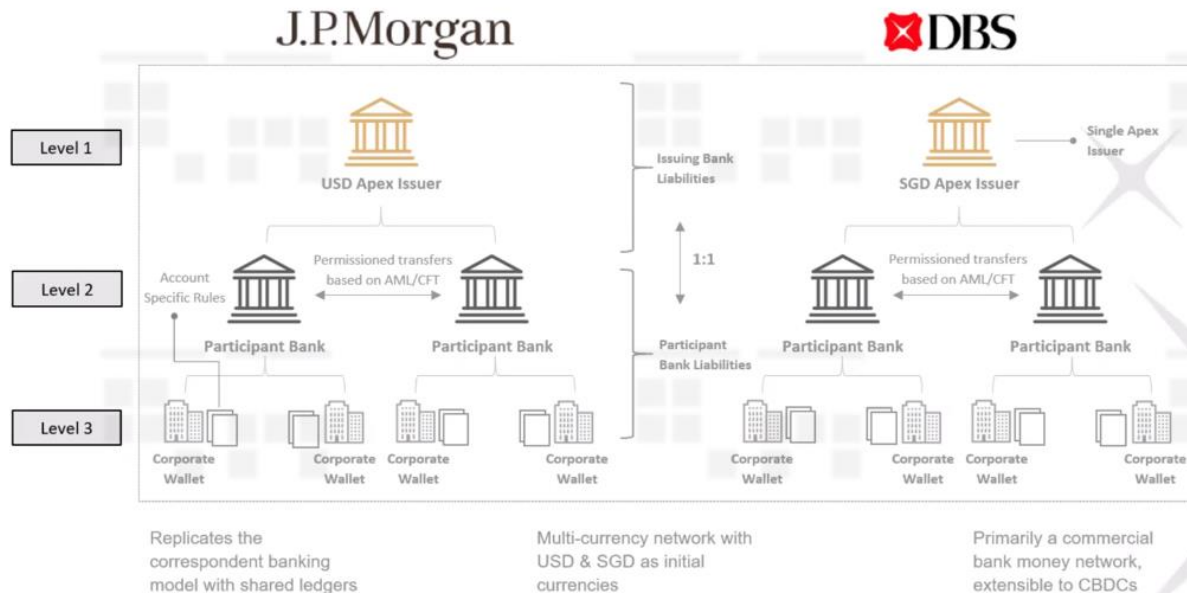


- Known participants from one organization
- Writes permissions centralized
- Reads may be public / restricted
- Consensus by multiple algorithms



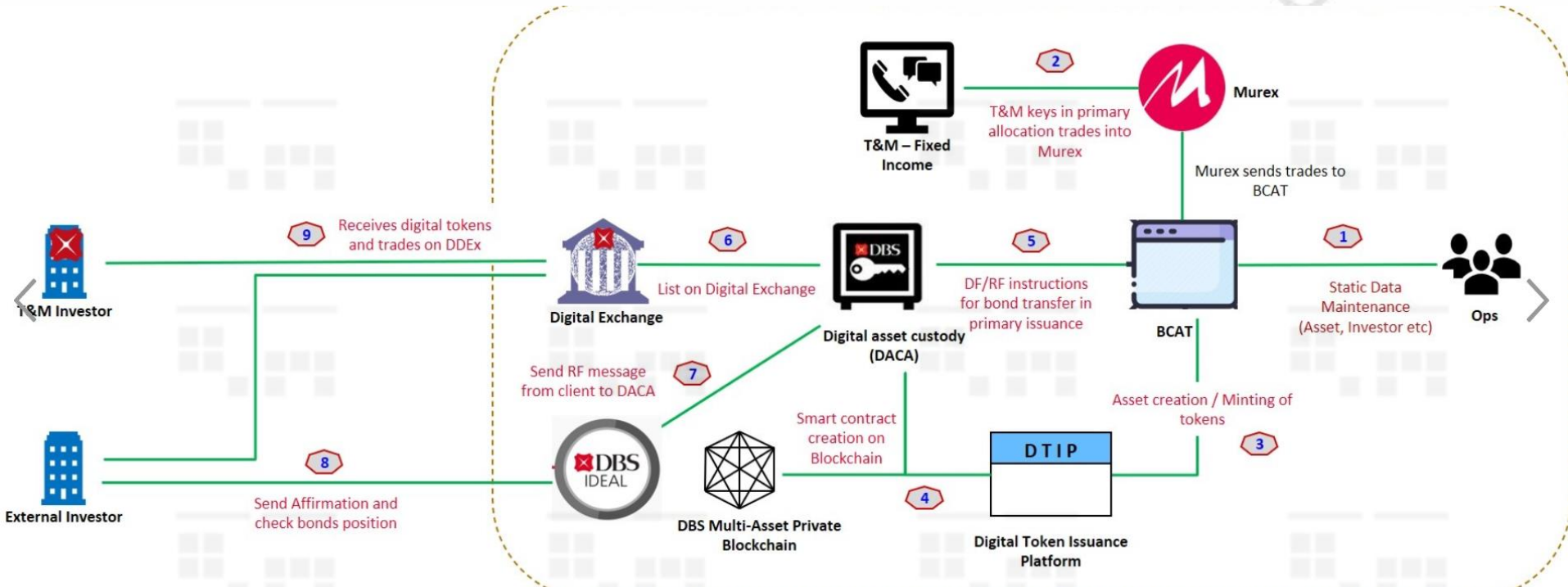
## Partior

- DBS together with **Temasek** and **JPMorgan** set up an technology company, **Partior**, which works on cross-border payments and settlements work using blockchain technology.
- Current cross-border payments and settlements are constrained by a T+2 problem and Hub and Spoke Model.
- Partior aims to provide infrastructure support for not just money transfers but also for use cases like delivery-versus-payment and payment-versus-payment, the assets market, the securities market



# BCAT (Block-Chain Asset Tokenization Open System)

- BCAT is a blockchain platform for Fixed Income (Bonds) trading, inter-entity trading, processing & other Treasury-related blockchain use-cases.
- BCAT is used by TMO, to monitor tokenized deals from murex and settlement status that is being effected by IBGT systems.



END