UNDERSTANDING BLOCKCHAIN TECHNOLOGY FOR MODERN BUSINESSES

Mr. Simon Sywak

A-STARS Advisors

Personal Introduction

Simon is a sophisticated financial services executive with over 25 years experience in electronic trading and digital transformation in equities, fixed income, FX, and commodities. With broad expertise in both leading sell and buy-side organizations he recently led the JP Morgan Asian e-trading platform strategy, spearheading JPM from 5th electronic platform to Number 1 in Asia. Simon has held senior leadership positions of multiple, geographically dispersed high-performance teams across trading, sales, operations and technology for FICC and equities markets.

AGENDA

VAULTEX

Algorand

- The basics of Blockchain technology
- How Blockchain transactions & mechanisms function
- Digital Capital Markets
- Consensus & Trust Mechanisms
- Tokenisation 1o1
- Practical use cases of Blockchain Technology

Questions and
Discussion Time

READING & ACKNOWLEDGMENTS

- Assets on Blockchain Security Token Offerings and the tokenization of securities Max Kops Copyright © 2019 Max Kops All rights reserved
- https://www.coindesk.com/markets/2017/05/09/the-blockchain-immutability-myth/Digital Capital Markets
- https://www.coindesk.com/markets/2017/03/04/a-short-guide-to-blockchain-consensus-protocols/

Algorand

VAULTEX

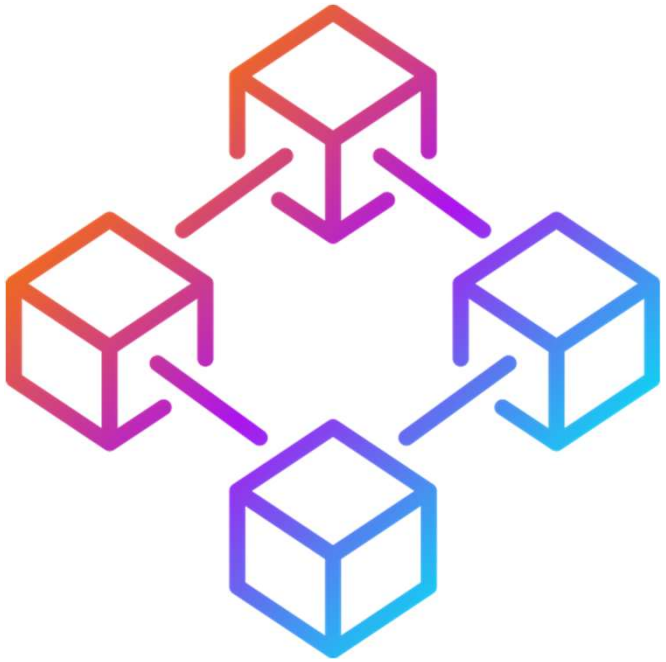
A-STARS Advisors

BLOCKCHAIN BASICS

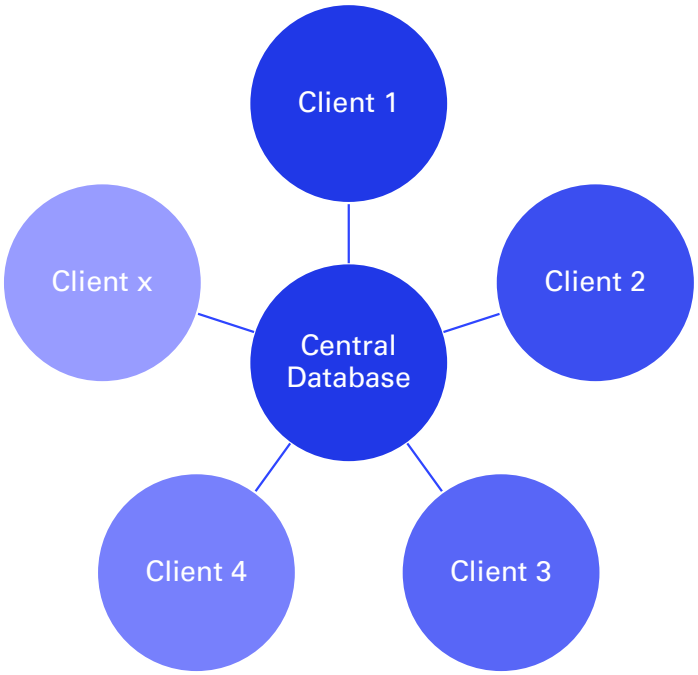
A-STARS Advisors

What is a Blockchain

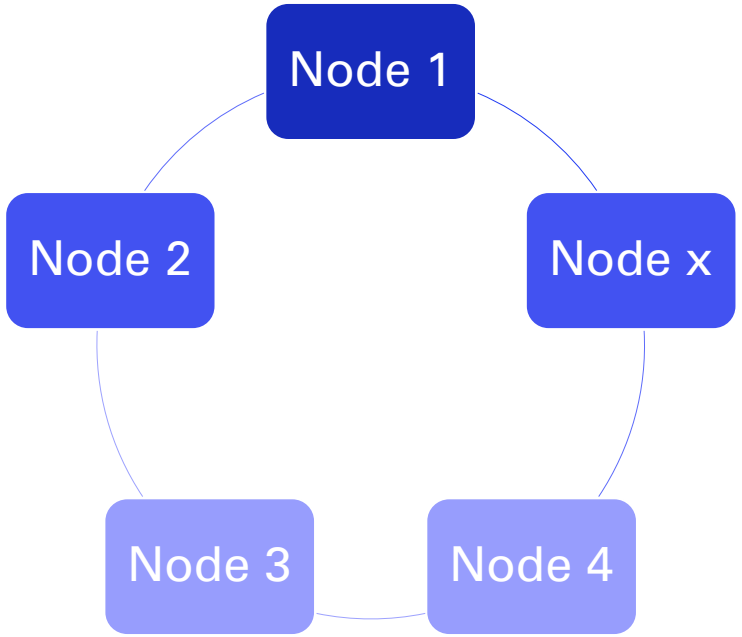
- A distributed database existing on many computers at a single point in time.
- Decentralized ledger recording digital assets over Peer-to-Peer networks.
- General examples of Blockchain use:
  - Transfer of money (no intermediary)
  - Transfer of medical data
  - Blockcerts
  - Tokenization of real assets



Distributed vs Centralized ledger

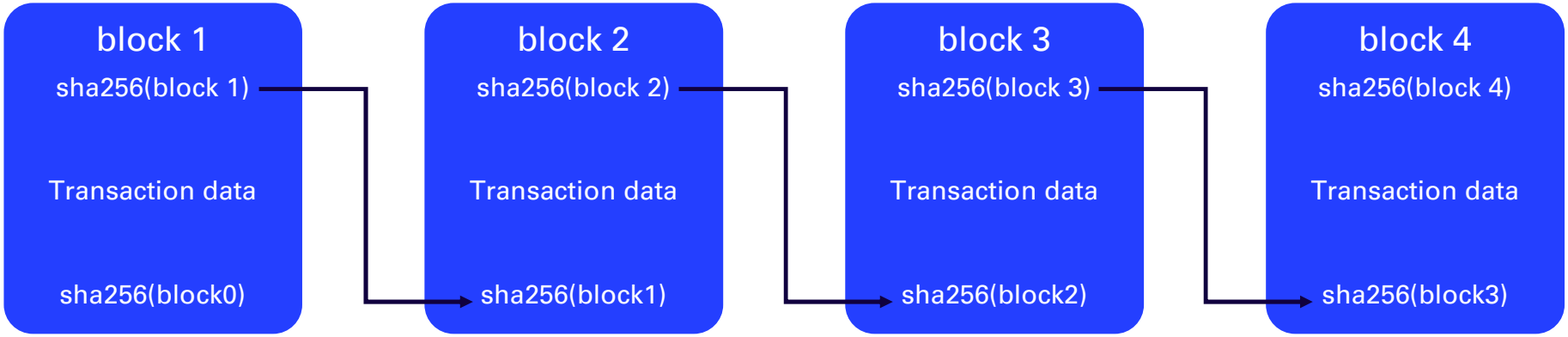


- Central database holds central ledger.
- Client x must reconcile their ledger with the central database if discrepancies arise.



- Only one ledger, all nodes have equal access to it.
- All nodes have agreed to a protocol that determines the true state of the ledger.

Bitcoin: How does Blockchain work



- A secure hashing algorithm 256 (sha256) is a function that converts any data into a string of numbers and letters of length 256 characters.
- sha256(block x) is typically used as the transaction ID of a given block.
- Each block is linked or “chained” to the previous block by the Transaction ID of the previous block.

Hash Functions and blockchain

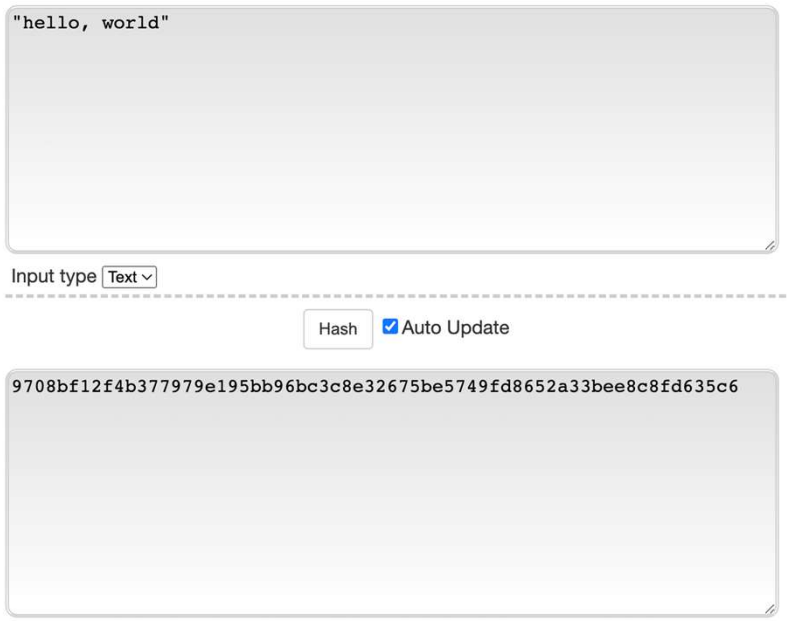
- secure hashing algorithm 256 (sha256) is an example of a cryptographic hash function.

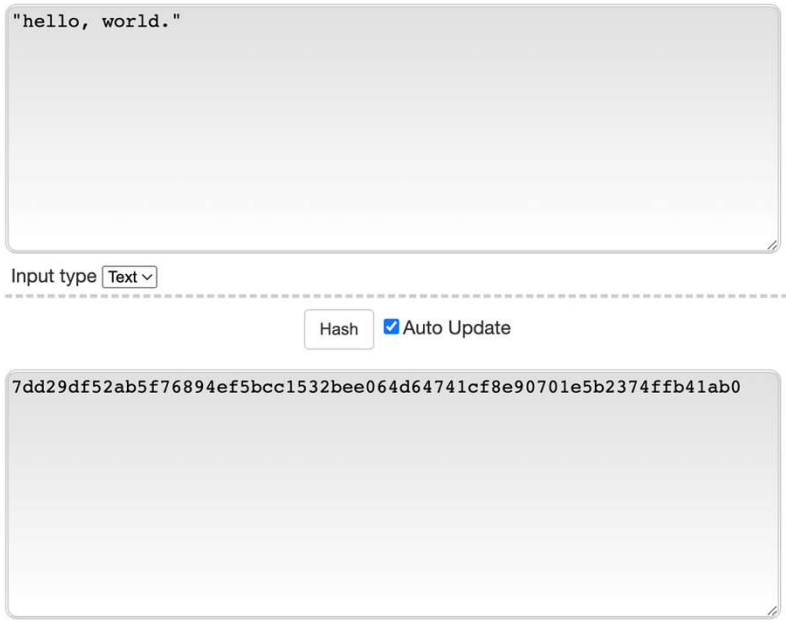
- Cryptographic hash functions have the following properties:
  - Deterministic
  - Quick Computation
  - Pre-Image resistant
  - Small change in input → large change in output
  - Collision resistant

Secure Hashing algorithm examples

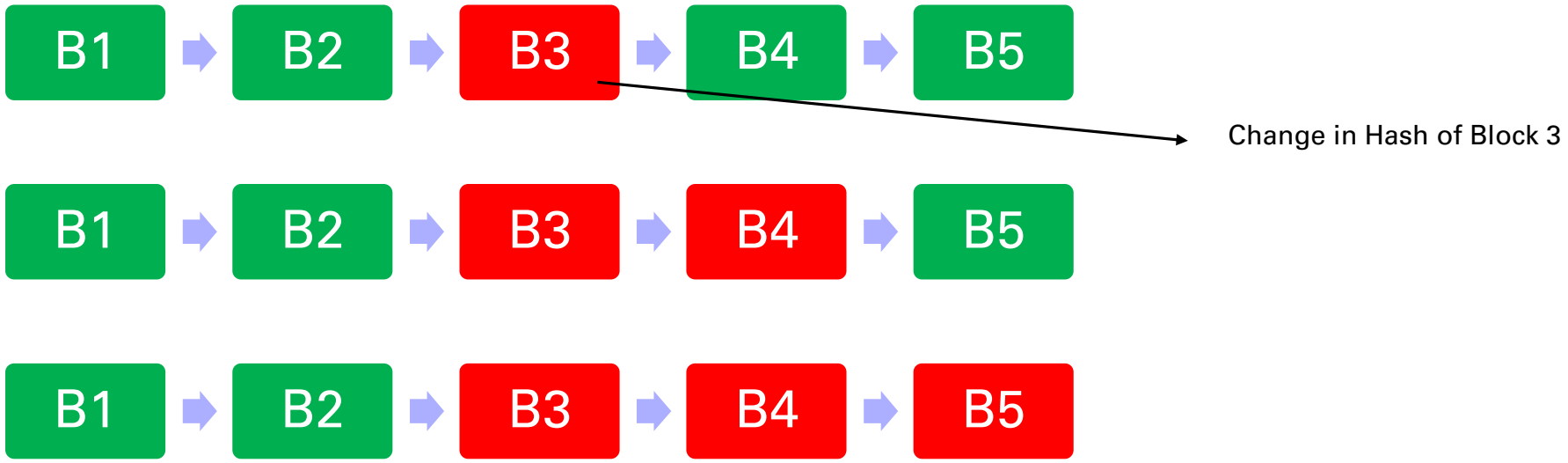
- Example sha256 generator: https://emn178.github.io/online-tools/sha256.html
- sha256 for data: “hello, world”
  - 9708bf12f4b377979e195bb96bc3c8e32675be5749fd8652a33bee8c8fd635c6
- Even Small changes in the input data completely changes the output sha256:
- sha256 for data: “hello, world.”
  - 7dd29df52ab5f76894ef5bcc1532bee064d64741cf8e90701e5b2374ffb41ab0
- The difference of only a “.” completely changes the output string.
- This means that it is impossible to find the input data based on a given sha256 value.

Example Continued



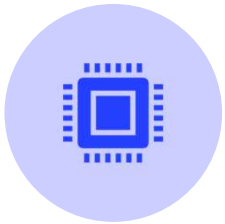


Immutability and resilience



- An attempt to change the input data in one block of a blockchain will alter the hash value of the block.
- This changes the hash value of the proceeding block, and so on.
- This is how blockchains attain immutability and resilience.

Key takeaways of Blockchains



BLOCKCHAIN IS A DISTRIBUTED, LEDGER OF TRANSACTIONS.

DECENTRALIZED → ALL PARTIES HAVE EQUAL ACCESS TO INFORMATION.

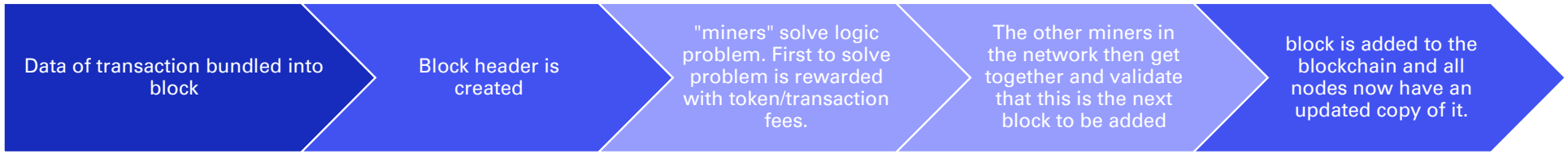
RESILIENT → NO SINGLE POINT OF FAILURE.

IMMUTABLE → HIGHLY TAMPER-PROOF.

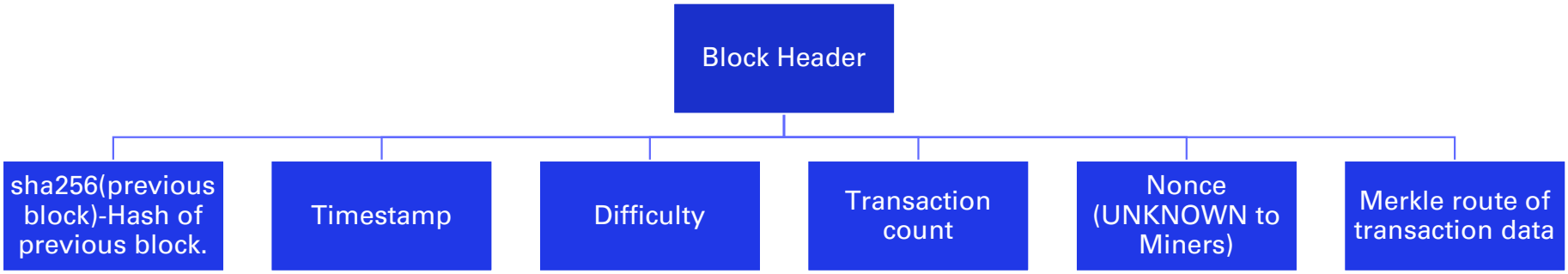
HOW BLOCKCHAIN MECHANISMS & TRANSACTIONS FUNCTION

A-STARS Advisors

How Transactions work



Block Verification: “Mining”



- Merkle root: the hash of all the hashes of all the transactions that are part of a block in a blockchain network.
- Nonce: a number added to a hashed—or encrypted—block in a blockchain that, when rehashed, meets the difficulty level restrictions.
- Miners are trying to find a number that, when added to the block header, the hash of the block starts with the specified number of zeros. (specified by the difficulty)

Continued: “Mining”

Block 732409

USD BTC

This block was mined on April 18, 2022 at 6:35 PM GMT+8 by SlushPool. It currently has 1 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 6.25000000 BTC ($243,787.63). The reward consisted of a base reward of 6.25000000 BTC ($243,787.63) with an additional 0.13267100 BTC ($5,174.97) reward paid as fees of the 3471 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this address.

- Hash of all transactions in this block:

Merkle root	8f593d8a9ec2f9f9ef48b9e863c949c3ed3aea0667243395d7cdb5c2317167c7

- Hash of block with correct number of starting zeros as specified by the difficulty:

Hash	00000000000000000001d684bd86207285138ca8e20a2190fa0e34ddb4f811fd

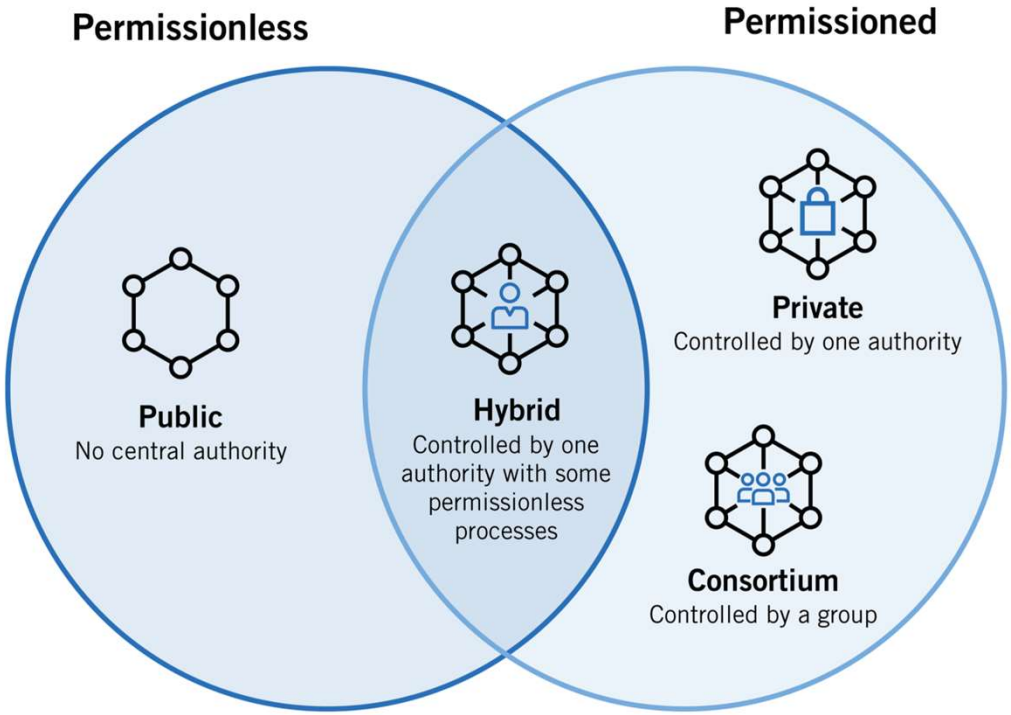
- Number when added to the block head will produce the hash:

Nonce	3,509,389,170

- How much bitcoin has been transacted on this block (6 billion USD):

Transaction Volume	154468.61801112 BTC

Types of Blockchain



- The type of blockchain network you want to utilize will depend on your use case and other requirements (mainly privacy and liquidity). Currently, public blockchains are the most popular form of blockchain being utilized by institutions.

Types of Blockchain: Continued

Public

- This is a blockchain that is open and accessible to anyone and everyone. The most popular examples of these are the Bitcoin and Ethereum blockchains.

Private

- This is a blockchain that is for members only (only members of the network can access, read and mine transactions). Examples include business-to-business virtual currency exchange network Ripple and Hyperledger.

Consortium

- Consortium blockchains are permissioned blockchains governed by a group of organizations. enjoy more decentralization than private blockchains, resulting in higher levels of security. Examples include CargoSmart, used in Global Shipping.

Hybrid

- Blockchains that are controlled by a single entity, but with oversight performed by the public blockchain, which is required to perform certain transaction validations. Examples include IBM Food Trust, which was developed to improve efficiency throughout the whole food supply chain.

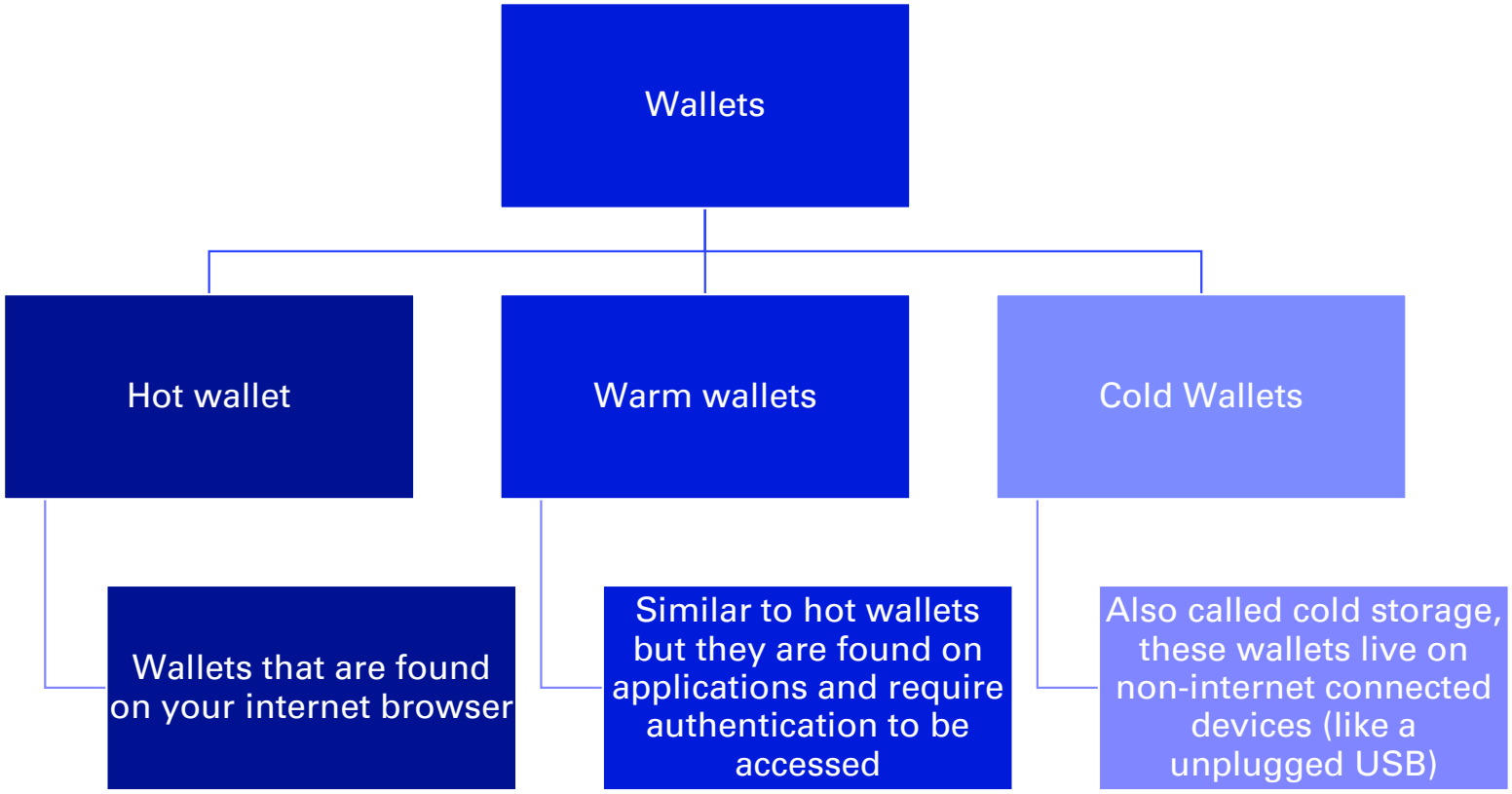
Keys

- In order to transact or interact with any digital asset, you will need three basic things:
  - Private key
  - Public key
  - Wallet
- Public and private keys: a string of characters that are randomly generated and nearly impossible to replicate.
  - Public key is the address people send transactions to – any transaction can be traced back to a public key.
  - Private keys allow you to initiate and authenticate transactions to access the digital assets you have stored on the blockchain in your wallet.

Wallets

- Digital wallets are similar to physical wallet that holds things of monetary value (cash, credit cards, debit cards, etc.)
- Your wallet contains both your public and private keys and has what's called a wallet address.
  - Wallet address is just a cryptographically hashed version of your public key that makes it easier to send digital assets to and from it (so your wallet address and your public key are mathematically related but not identical).
  - Same principle as sha256 (hash value) used in bitcoin blocks

Wallet: Hot vs warm vs cold



DIGITAL CAPITAL MARKETS

A-STARS Advisors

What are Digital Capital Markets

- Digital capital markets are made up of layers that provided services that are required for the function of the market. These layers as.
  - Ledger Layer
  - Transaction Execution Layer
  - Services Layer

Ledger Layer

Algorand

- Blockchain Protocols
  - These are the technology infrastructures used for logging transactions (e.g. Bitcoin, Ethereum, Solana, or Cardano).
- Blockchain Tokens (cryptocurrencies)
  - These are the tokens that are used as the medium of exchange for transactions on the blockchain protocols (e.g. BTC, ETH, SOL, or ADA).
- Miners and Validators
  - Institutions or people that mine the transactions and create new blocks on the blockchain.

Transaction Execution Layer

- Exchanges
  - Marketplaces that facilitate the buying and selling of digital assets.
- Lending Desks
  - Institutions that will lend to market participants taking digital assets as collateral.
- Liquidity Providers / Market Makers
  - Institutions providing liquidity to markets to facilitate trading (e.g. OTC desks).

Services Layer

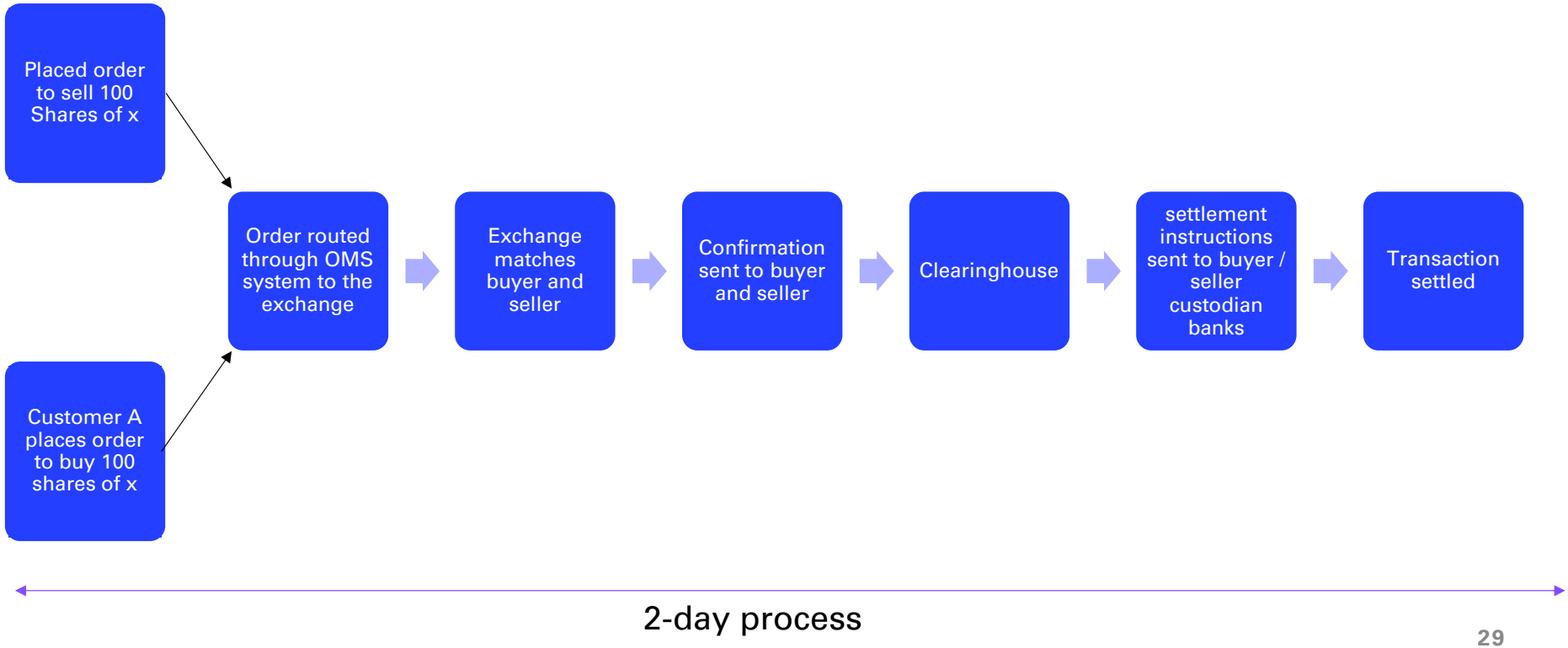
- Compliance
  - Blockchain compliance for anti-money laundering / know your transaction (KYT) and know your customer (KYC).
- Custodians
  - Institutions that will hold your private keys (these can be dedicated custodians or exchanges).
- Administrative and Tax Providers
  - Companies that provide crypto fund administrative and tax services.
- Infrastructure for Transfer and Settlement
  - Companies that help facilitate the transfer and settlement of digital asset transactions.
- Fiat on and off-ramp
  - Banks and Financial institutions that facilitate the exchange of fiat currency into digital assets.

Additional Service Layer Decentralized finance ("DeFi") Layer

- These are the decentralized applications that are built on top of blockchain protocols. There are two major components to the DeFi layer:
  - DeFi Protocols
    - Similar to blockchain protocols in that they act as the "venue" for you to interact with various aspects of DeFi (borrowing, lending, staking, etc.).
  - DeFi Tokens
    - Tokens of DeFi protocols that allow for governance of the protocol.

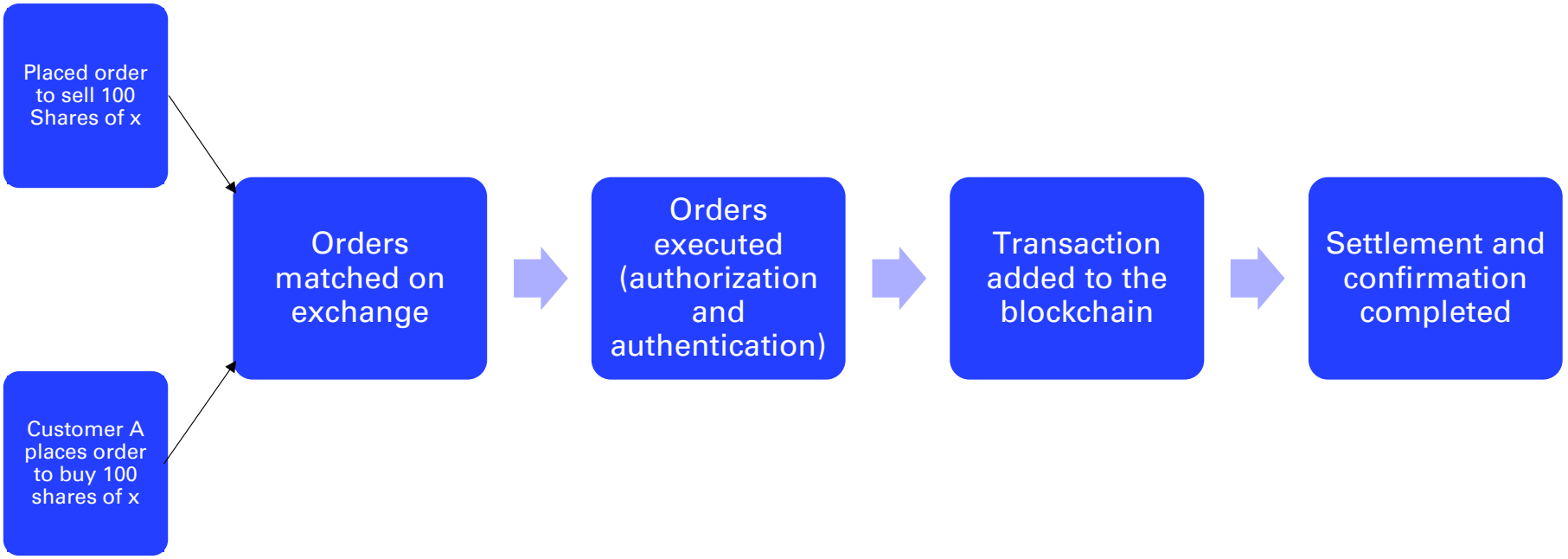
Example: Traditional Assets

Assume I want to purchase 100 Shares of Stock x:



Example: Digital Asset Transaction

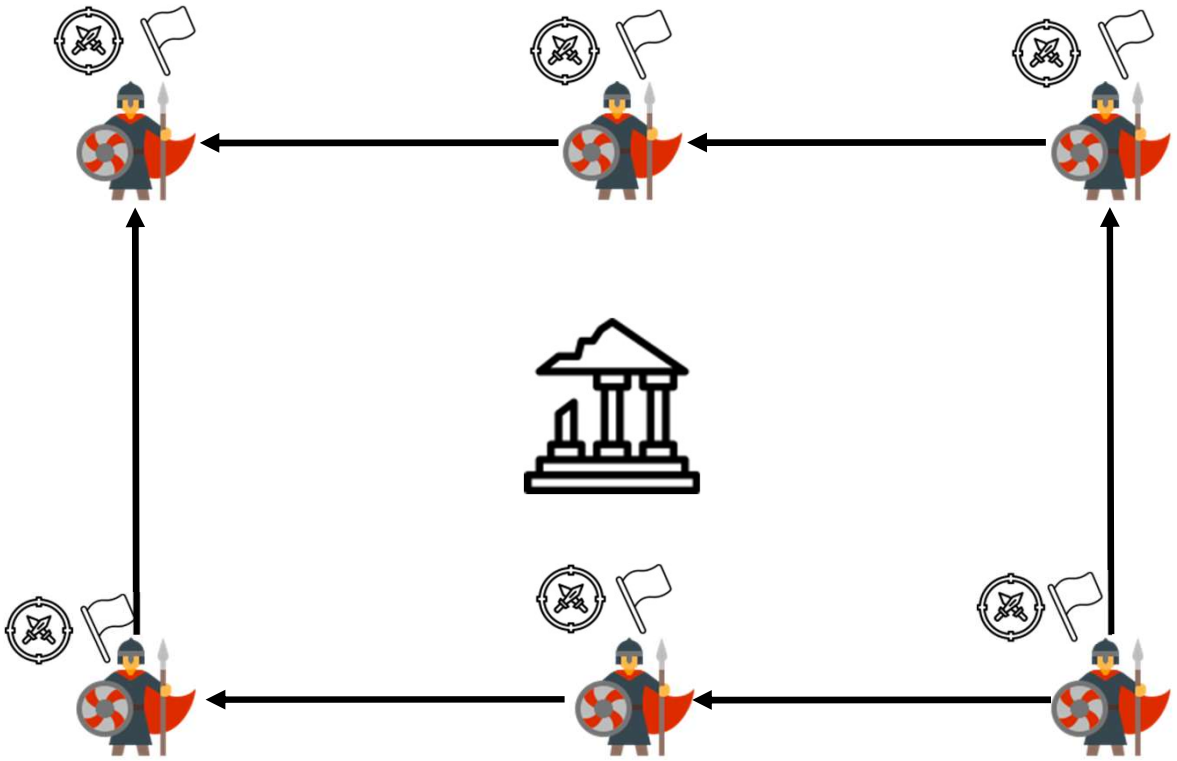
Assume I want to purchase 1 BTC:



CONSENSUS & TRUST MECHANISMS

A-STARS Advisors

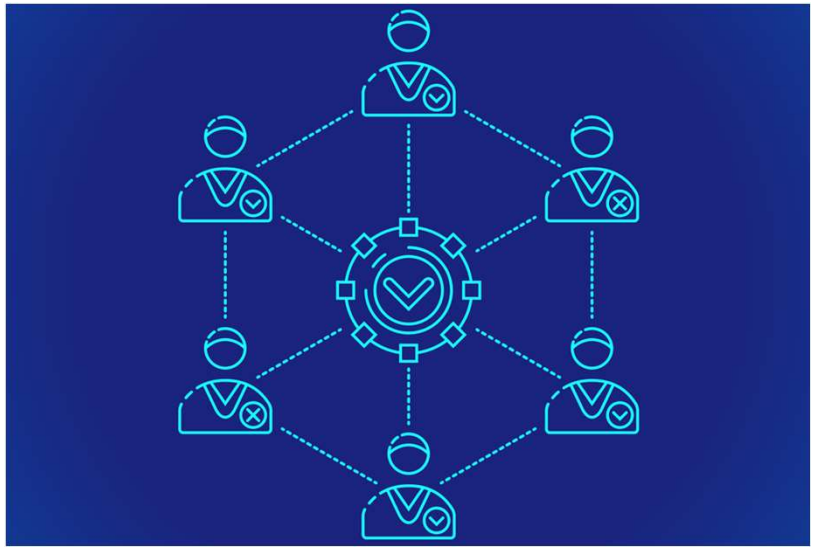
Byzantine fault



- Armies → represent nodes in a decentralized network.
- Byzantine general's problem→ refers to the potential for systems failure if nodes fail or act maliciously.

Consensus Mechanisms

- A consensus mechanism is defined as any number of methodologies used to achieve agreement across a decentralized network.
- In the context of blockchain, proof-of-work (PoW) and proof-of-stake (PoS) are two of the most common consensus mechanisms.
- There are many other consensus mechanisms, such as:
  - Proof-of-activity
  - Proof-of-capacity
  - Proof-of-burn
- However the 2 most prevalent are proof-of-work and proof-of-stake.



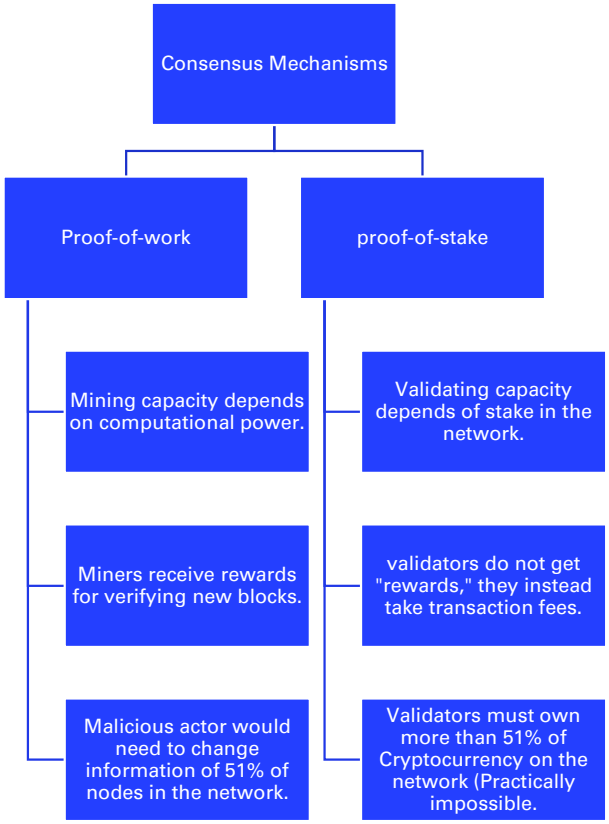
Proof-of-work

- Proof of Work requires the nodes in the network to solve a complex mathematical problem to be able to add a block to the chain. Solving the problem is known as mining, and 'miners' are usually rewarded for their work in cryptocurrency. (example explained in section above.)
- The mathematical problem can only be solved by trial and error and the odds of solving the problem are about 1 in 6 trillion. (depending on difficulty set)
- It requires substantial computing power which uses considerable amounts of energy.
- Rewards for mining must outweigh the cost of the electricity cost of running the computers required to solve the mathematical problem.

Proof-of-stake

- Later blockchain networks have adopted “Proof of Stake” validation consensus protocols, where participants must have a stake in the blockchain - usually by owning some of the cryptocurrency - to be in with a chance of selecting, verifying & validating transactions.
- This saves substantial computing power resources because no mining is required.
- In addition, blockchain technologies have evolved to include “Smart Contracts” which automatically execute transactions when certain conditions have been met.
- This process is used by blockchain protocols such as Algorand.

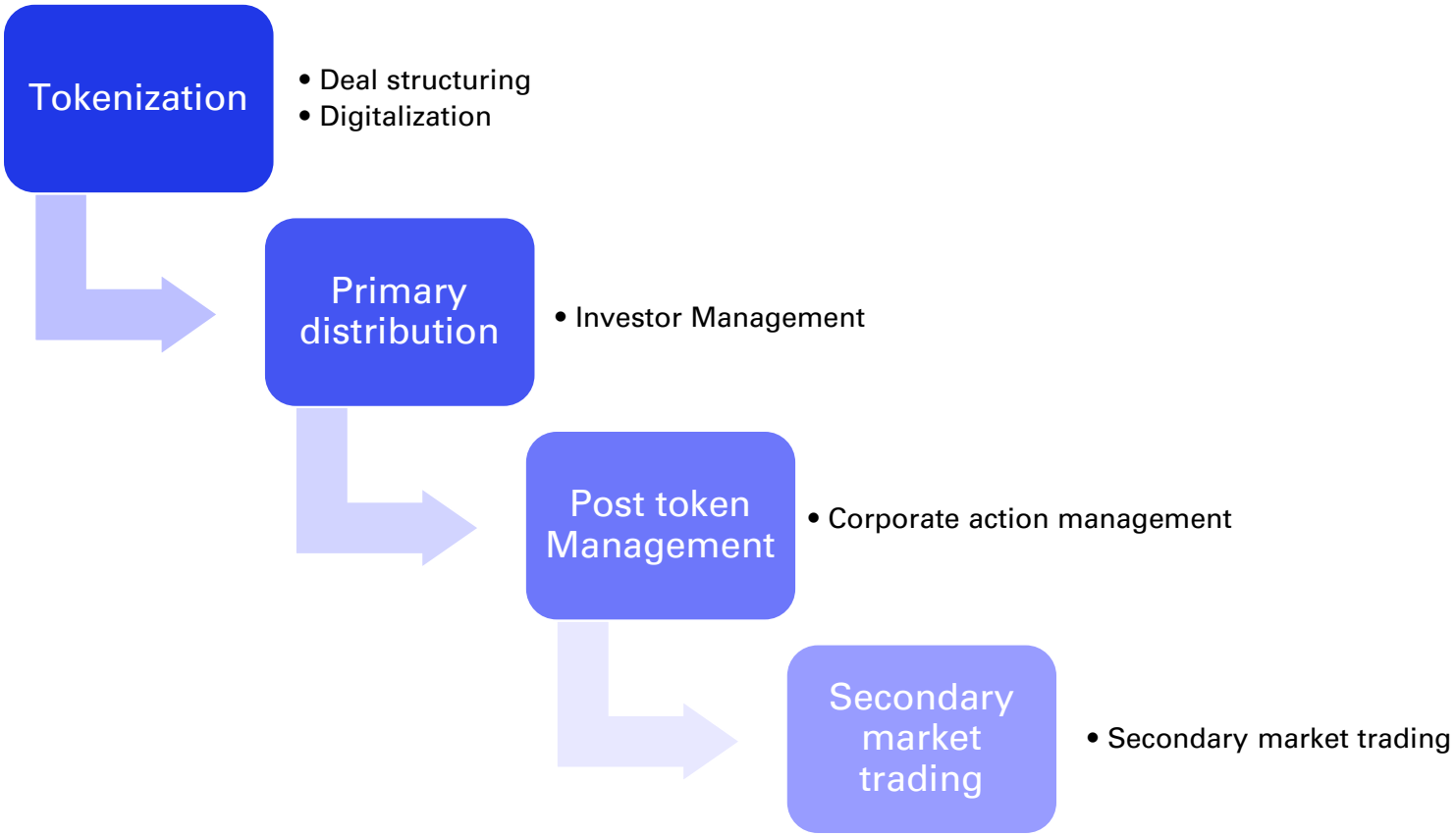
Problem vs Solution



TOKENISATION 101

A-STARS Advisors

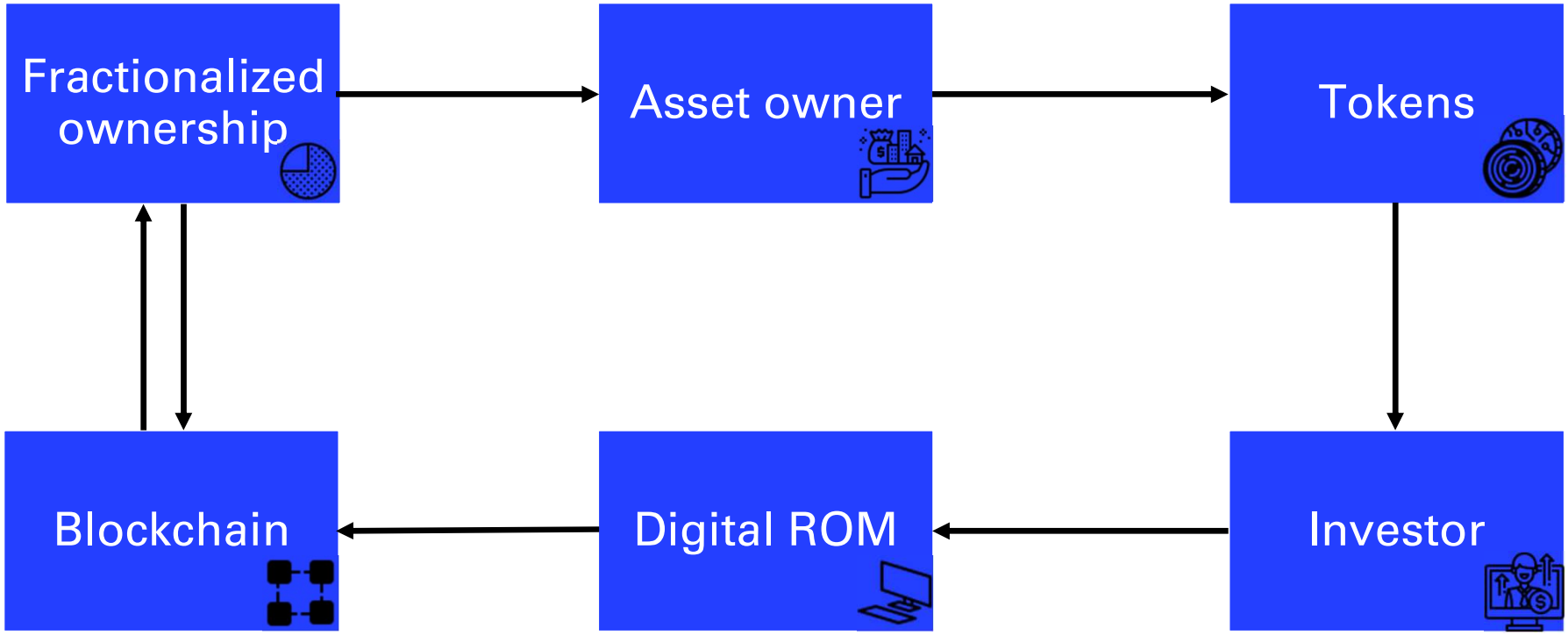
The Tokenization Process



Tokenization

- Deal Structuring:
  - Tokenized assets are treated as a traditional security. They are subject to the same governance and regulatory frameworks of normal securities, such as:
    - legal ownership
    - investor know-your-client (KYC) detailing
    - compliance, accounting and investment due diligence.
  - They are subject to a regime that governs the token's:
    - Offer
    - Issuance
    - Marketing
    - Distribution
    - investment management
    - the operation of a platform for its secondary trading.
- Digitalization:
  - Once the deal structure is finalised, the underlying asset can be tokenised using blockchain technology, and sold/issued by the asset's owner. Each transaction will be recorded, updated and managed on a digital record of members ('ROM').
  - The issuance of a digital tokenisation can:
    - greatly increase liquidity by increasing fractional ownership.
    - Increase efficiencies with automated digital transaction settlement.
    - Asset owners unlock liquidity in previously illiquid assets.

Tokenization: Continued



Post Tokenization Phases

- Primary distribution:
  - After relevant checks for investors are carried out and passed, investors can be “whitelisted” and tokens can be issued. This is then recorded on the ROM. Token issuers retain authority to finalise the transaction throughout the process, whether this is after compliance protocols are run, while screening is conducted, or before smart contracts are executed.
- Post token Management:
  - Smart contracts save time and money as the allow the following actions to be carried out more efficiently: (List not exhaustive but shows potential)
    - real time alerts
    - issuing shareholder updates and communication, initiating and completing voting activities.
    - distributing dividends / interest / principal.
    - issuing new tokens.
    - freezing and reversal
- Secondary Market Trading:
  - Secondary markets will increase the liquidity of an asset
  - positively affect the valuation of the asset itself.
  - Currently, secondary digital markets suffer from incomplete/unclear regulations but the development and clarification of global regulatory frameworks in response to asset tokenisation will support a thriving secondary market where tokens can be traded, with transactions recorded near instantaneously.

PRACTICAL USE CASES OF BLOCKCHAIN TECHNOLOGY

A-STARS Advisors

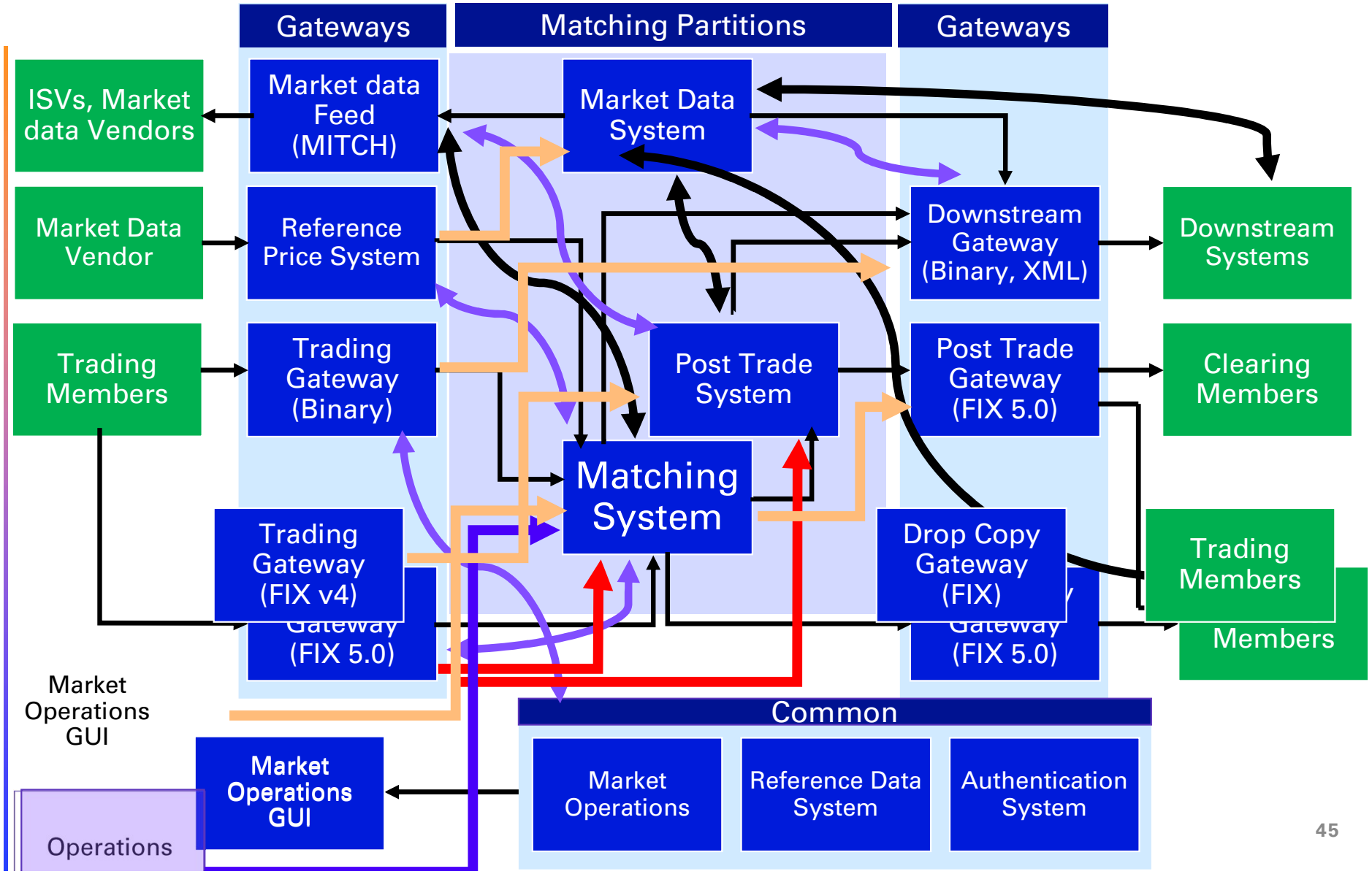
Vaultex: Tokenization of Gold

- Through blockchain technology, any asset that bears value can be tokenized.
- Tokenizing assets opens up the potential investor base to a broader market, increases liquidity compared to traditional securities, and reduces the time required to trade.
- Vaultex in an example of an exchange platform for real assets such as gold.

How does Vaultex Function?

- Basic function of Vaultex:
  - Gold is approved by LBMA/ SBMA.
  - A token deployed on the public blockchain (Algorand protocol).
  - Vaultex retains the gold securely.
  - Investors can buy/sell gold without any difficulties.
  - Fully backed by gold bullion, traceable through an Atomic Smart Contract.
  - Fully redeemable for gold or cash at any point.

- The Vaultex Exchange operates similarly to a traditional securities exchange.
- Gold is offered by Vaultex through the tokenization process and the sale of security tokens representing such assets on a security token exchange.
- Vaultex is in the secondary market for the tokenization businesses. The technology behind Vaultex is very modular and scalable allowing expansion into other assets classes in the future.

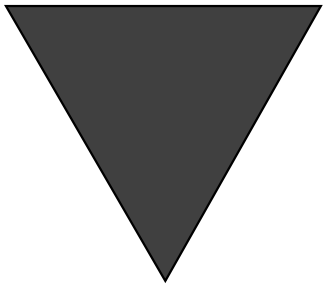

Gateways
Matching Partitions
Gateways
ISVs, Market data Vendors
Market data Feed (MITCH)
Market Data System
Market Data Vendor
Reference Price System
Downstream Gateway (Binary, XML)
Downstream Systems
Trading Members
Trading Gateway (Binary)
Post Trade System
Post Trade Gateway (FIX 5.0)
Clearing Members
Matching System
Trading Gateway (FIX v4)
Drop Copy Gateway (FIX)
Trading Members
(FIX 5.0)
(FIX 5.0)
Members
Market Operations GUI
Common
Market Operations GUI
Market Operations
Reference Data System
Authentication System
Operations

How Blockchain works for with Vaultex

- Ledger Layer:
  - Digitalization of real assets (gold), which is owned and verified by Vaultex.
  - This digitalization is carried out by the same procedure laid out above.

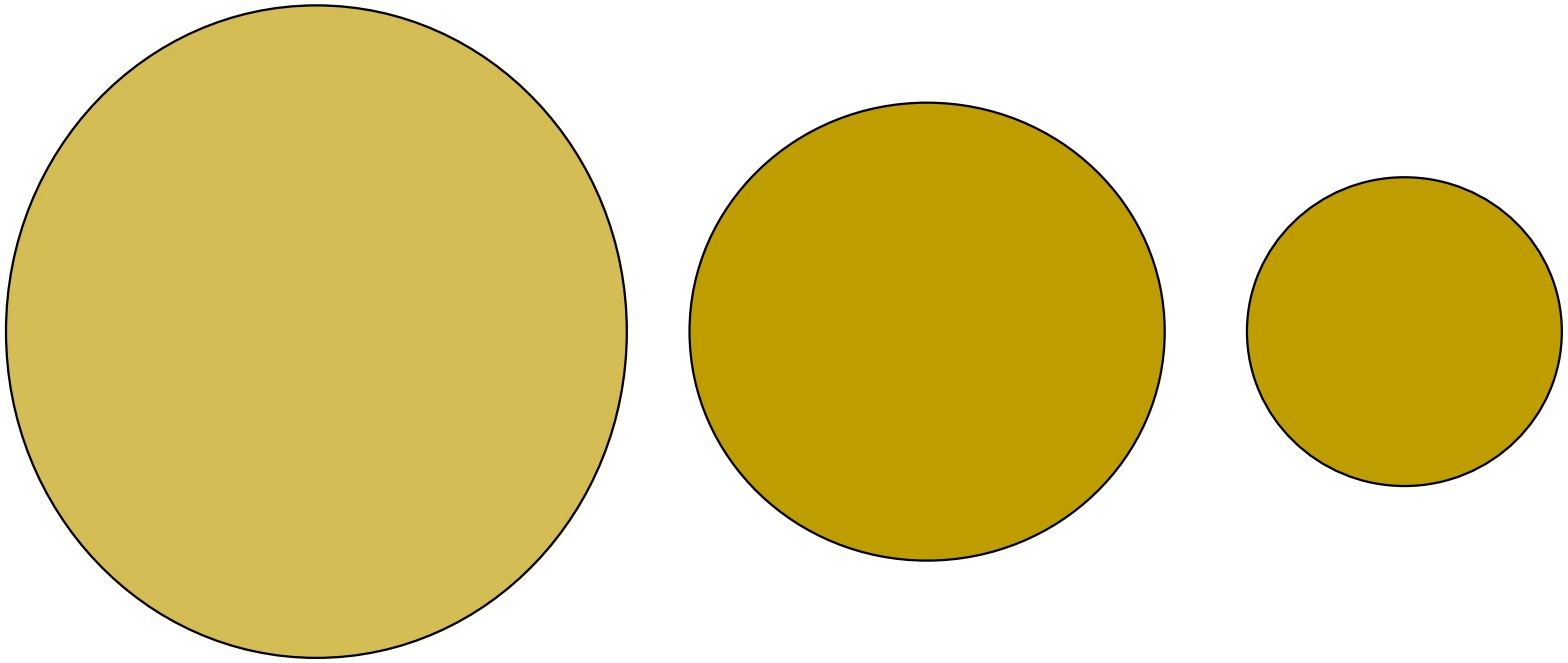
How Blockchain works for with Vaultex

- Transaction layer:
  - Vaultex then functions as a secondary market for the tokenized gold.
  - The technology behind Vaultex is very modular and scalable allowing expansion into other assets classes in the future.



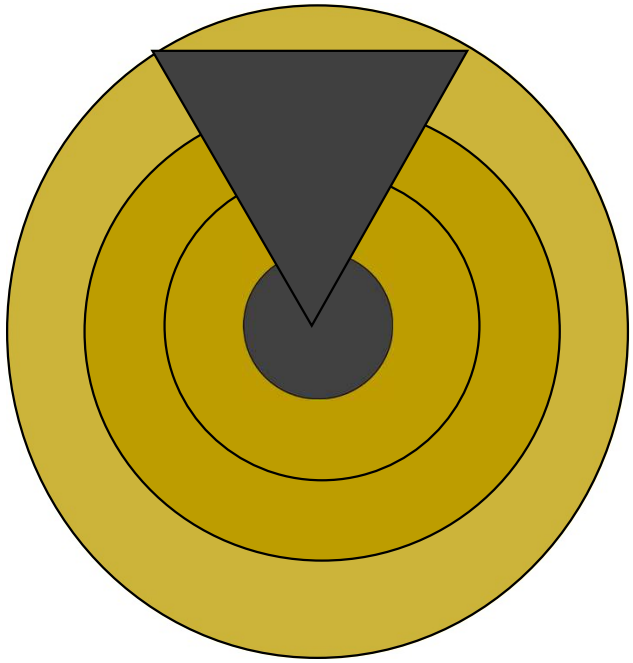
How Blockchain works for with Vaultex

- Services Layer – built out of core information fro, transactional and ledger layers



Vaultex

- Complete Vaultex: Future Exchange Infrastructure



Algorand

- Algorand is a pure proof of stake blockchain cryptocurrency protocol with a consensus mechanism chosen for scalability.
- Algorand attempts to solve the Byzantine fault through proof of stake to ensure reliability:
  - In a Byzantine fault, a component such as a server can inconsistently appear both failed and functioning to failure-detection systems, presenting different symptoms to different observers.
  - It is difficult for the other components to declare it failed and shut it out of the network, because they need to first reach a consensus regarding which component has failed in the first place.

THANK YOU FOR LISTENING
FINAL Q&A

A-STARS Advisors