www.pwc.com

Blockchain Technologies

Risks, Challenges, Opportunities

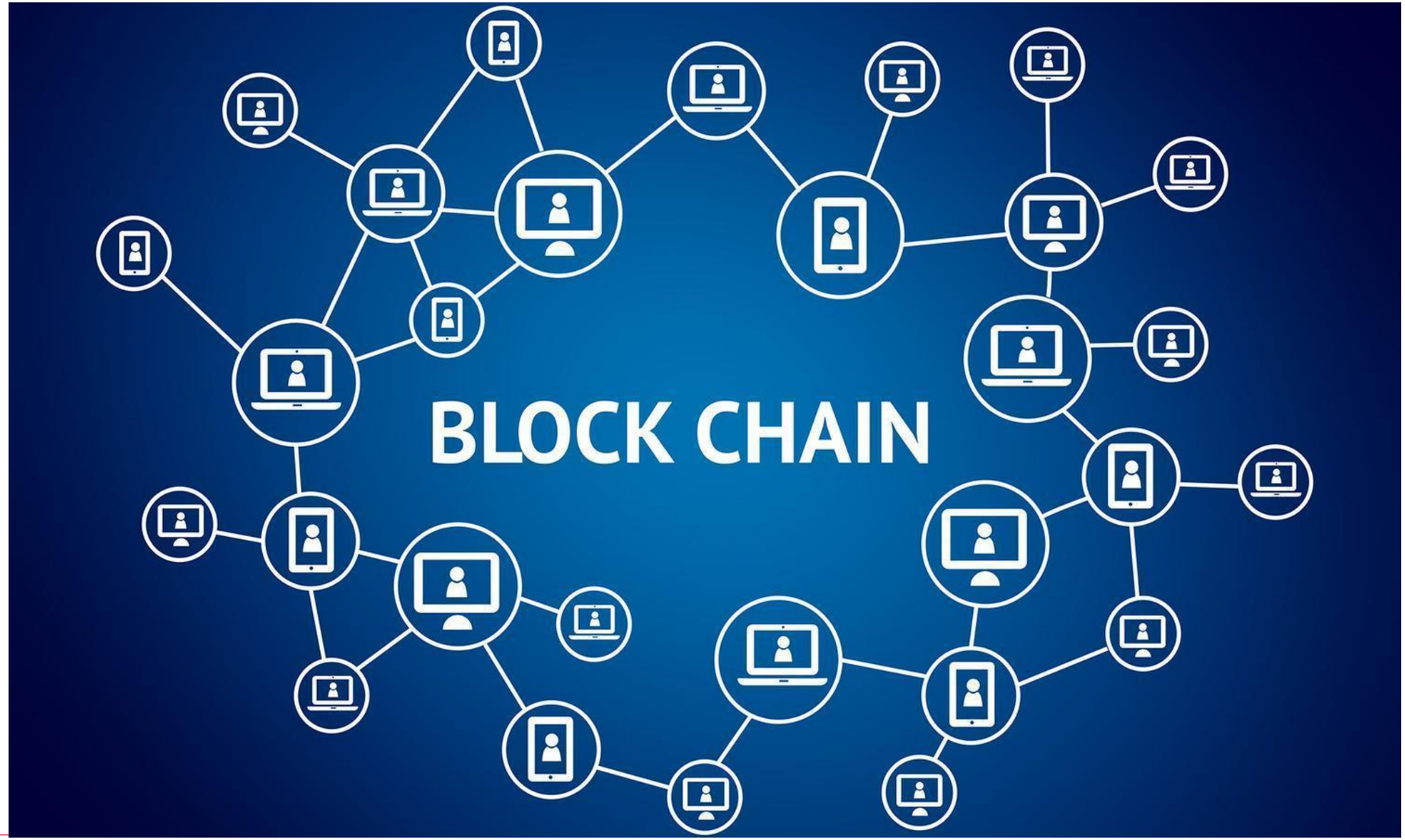
Strictly private and confidential

3 November 2017

pwc

Agenda

Blockchain Overview



Quick show of hands…

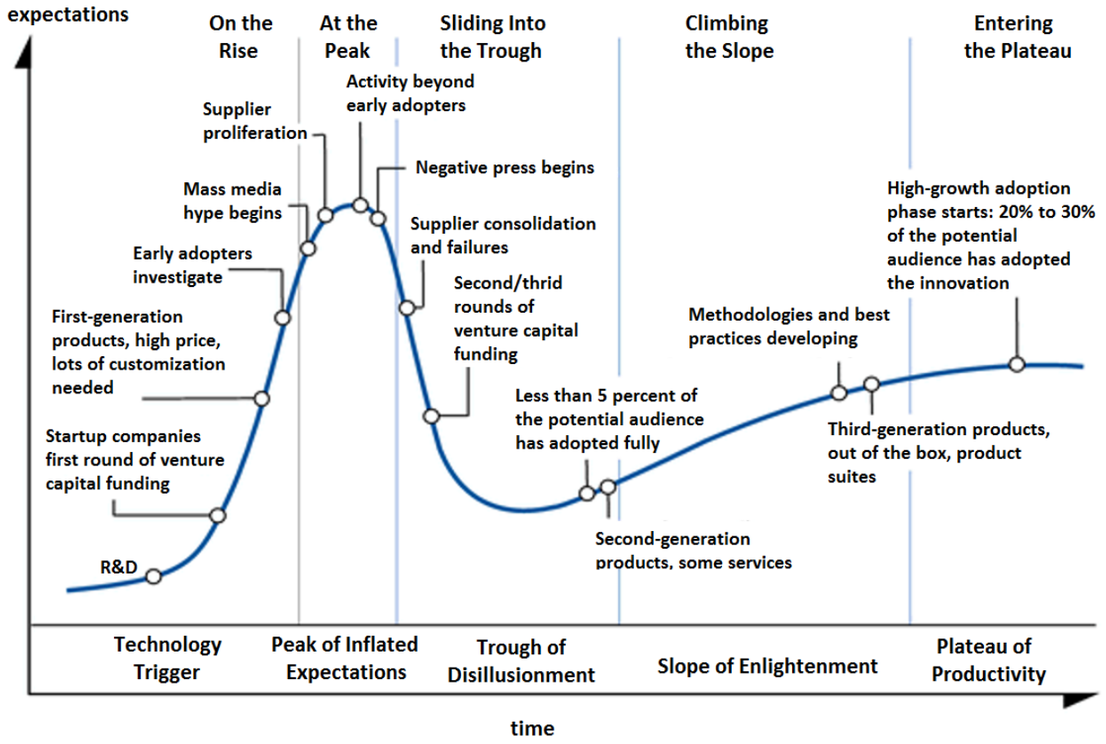
Raise your hands if:

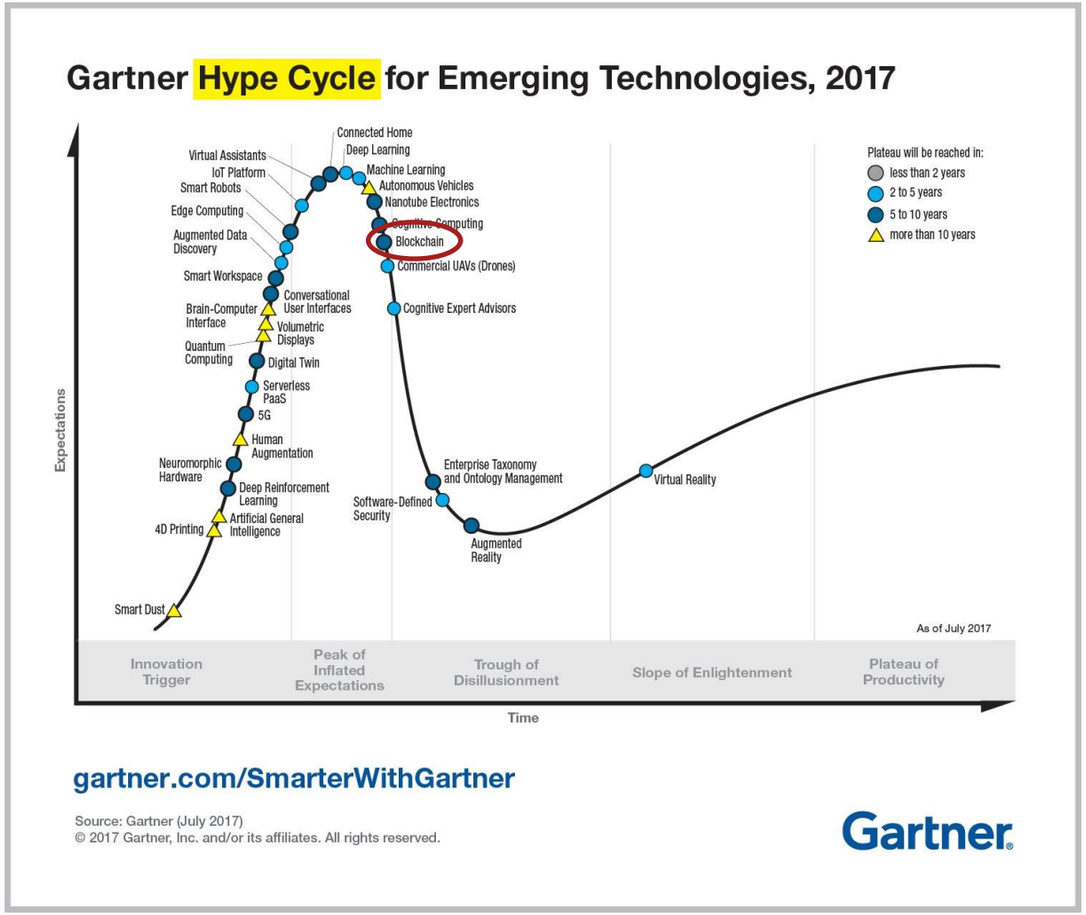
- You have heard of Blockchain technologies ?

Keep your hands raised if:

- You have heard of bitcoin ?
- You can explain the difference between bitcoin and Blockchain ?
- You can understand the benefits that is attracting various businesses towards Blockchain technologies ?
- You can appreciate the risks of the technology to design audit techniques ?

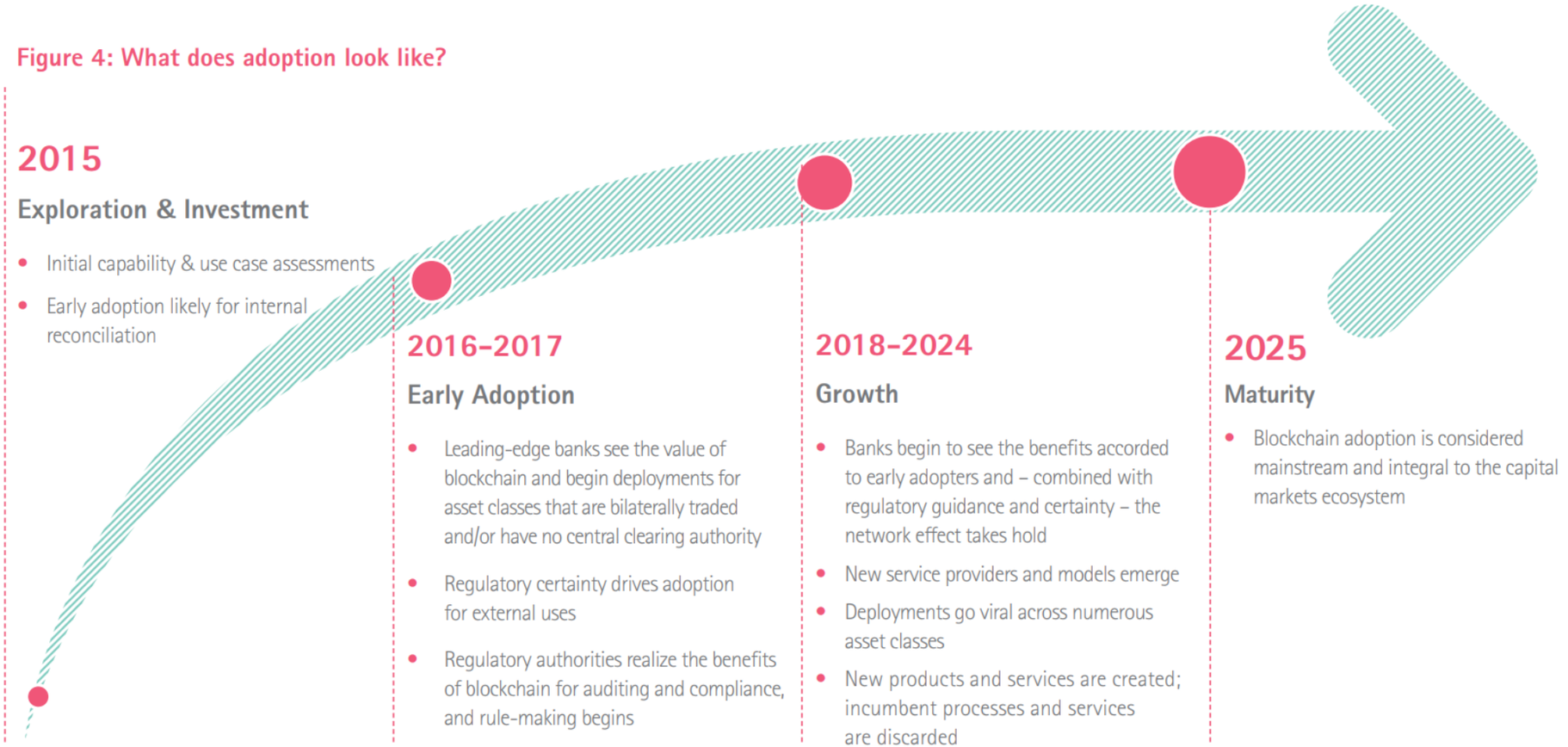
Gartner hype cycles – (source Gartner)





Accenture – source (Accenture - Blockchain adoption (2016))

Figure 4: What does adoption look like?

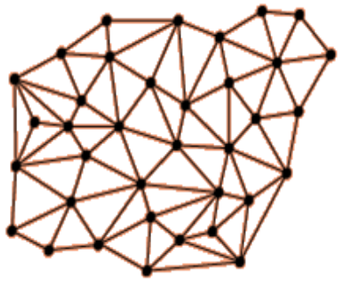


Blockchain – Disruption or hype ?

Perception	Blockchain technology, which first emerged as the backbone of Bitcoin in 2009, is being heralded as the most important innovation since the Internet itself.
Promising potential	Despite the underwhelming success of Bitcoin, there has been a flurry of advancements, new use cases, and applications of blockchain technology.
Rapid adoption	Blockchain technology has been steadily gaining traction. This is evident with the R3 Consortium in which over 100 banks, regulators, trade associations, etc have come together to implement a blockchain based financial system.

Let’s discover what blockchain technology really has to offer

To level set, Blockchain is NOT Bitcoin



Blockchain

≠

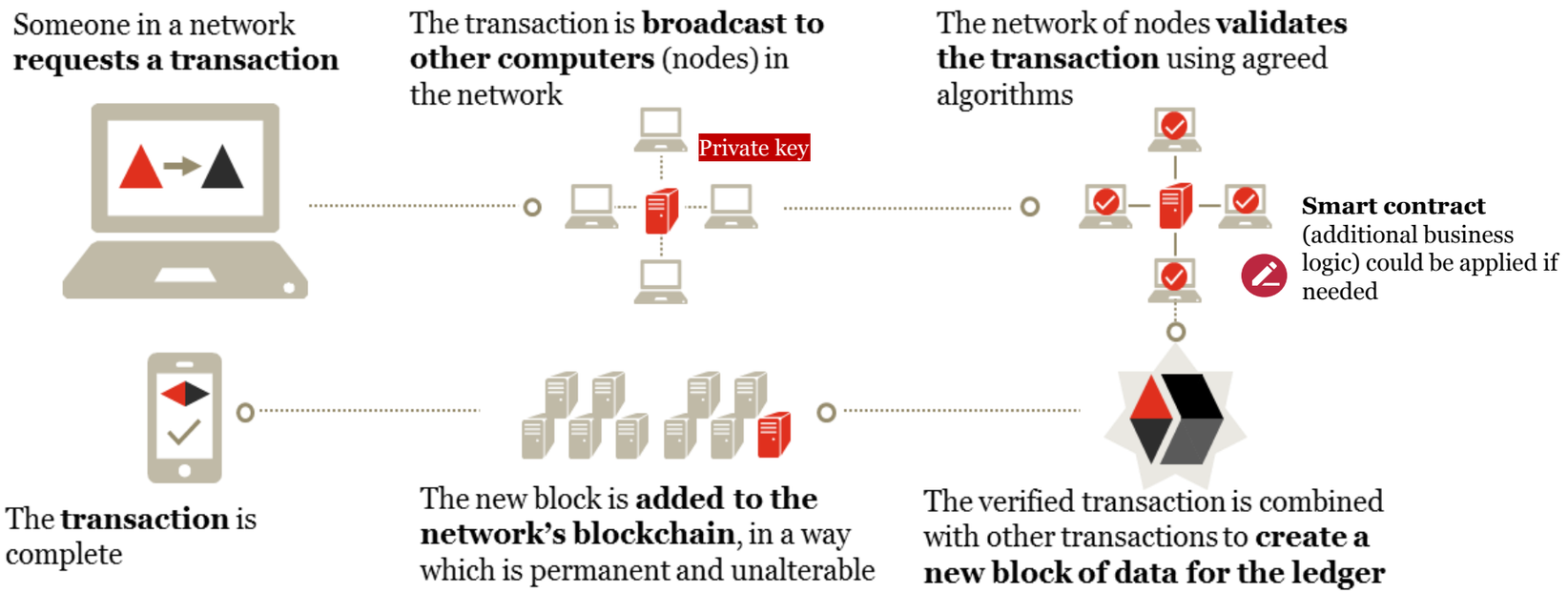
Crypto-Currency

1. Blockchain, ***does not*** require crypto-currency.
2. The platform can be constructed to handle a varying set of rules and configurations.
3. Related technology, such as smart contracts, can greatly improve process efficiency, transparency, reliability and reduce risk.

1. A crypto-currency is merely ***one application of*** crypto-technology, allowing the transfer of value via transactions recorded on a Blockchain.
2. There are many existing crypto-currencies, most notably Bitcoin.
3. Specific to crypto-currencies a key benefit include preventing double spending.

The Technology that can enable transformation

A blockchain is a decentralized ledger of all transactions in a network. Using blockchain technology, participants in the network can confirm transactions without the need for a trusted third party intermediary.



The Blockchain ecosystem

Distributed ledger

Every participant in the network has simultaneous access to a view of the information

Cryptography

Integrity and security of the information on the blockchain are ensured with cryptographic functions

Consensus

Verification is achieved by participants confirming changes with one another, replacing the need for a third party to authorise transactions

Smart contracts

The ability to run additional business logic means that agreement on the expected behaviour of financial instruments can be embedded in the blockchain

What does this mean for your organization?

Near real-time data availability and transparency that can eliminate the need for reconciliation	*Prevents unwanted intrusion on the network from non-authenticated participants*	*Facility for peers in the network to validate updated information ensuring validity and integrity of the data on the chain*	*Facilitates the ability to design and implement shared workflow and enhance automation*

Evolution of Blockchain Technologies

"A blockchain is a cryptographic, or encoded ledger comprising a digital log of transactions shared across a public or private network"

Blockchain 1.0 Currency

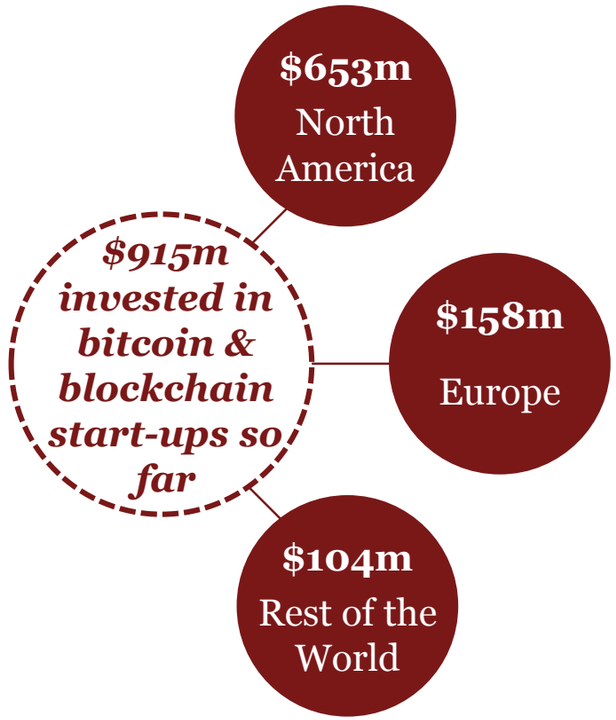
Using cryptocurrencies in cash related applications e.g. currency transfer, remittance, digital payment systems

Blockchain 2.0 Contracts

Deploying blockchains in economic, market and financial applications e.g. bonds, stocks, loans mortgages, titles, smart property

Blockchain 3.0 Applications

Employing blockchains in broader industry applications e.g. supply chain, transportation, health, cloud storage, etc.



Potential of Blockchain

Key Features

Identity Abstraction: Cryptographic security keys are required to gain access

Transaction Linkage: Every transaction is linked to previous transactions

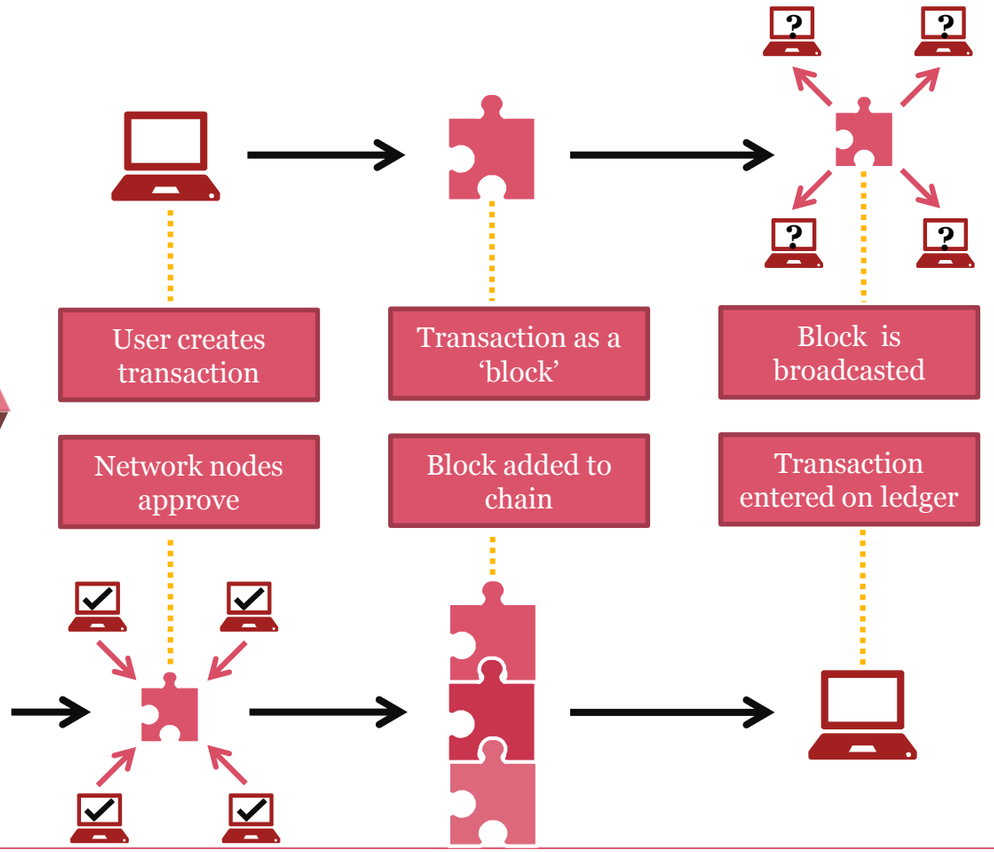
Transaction Scripts: Standardized rules are applied to a transaction at every node

Distributed Ledger: Standards for transaction storage on nodes

Decentralized Consensus: Mathematical rules for all nodes to agree on data integrity

Permissioned vs Not Permissioned: Ability to participate in a blockchain can be open or upon approval

Blockchain Functioning



Criteria that can help an organization determine whether a blockchain-enabled solution is appropriate

Multiple parties share data

multiple participants need views of common information

Multiple parties update data

multiple participants take actions that need to be recorded and change the data

Requirement for verification

participants need to trust that the actions that are recorded are valid

Intermediaries add complexity

removal of intermediaries can reduce cost and complexity

Time sensitive interactions

reducing delay has business benefits

Transactions interact

transactions created by different participants depend on each other

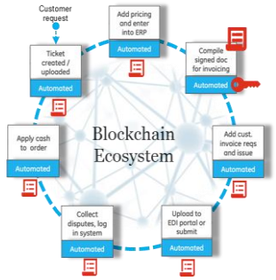
Blockchain-enabled transformation poses a few key challenges

Participant Trust

- **Safety:** Re-assuring participants that their transactions are secure
- **Public vs. Private:** What are key differences and criteria for private and public blockchains?
- **Information Accessibility:** Are participants willing to expose more information to participate in a network

Legal, Regulatory & Audit Framework

- **Regulatory Body:** Currently there is no global regulatory body to set standards on blockchain transactions
- **Auditing Challenge:** How do you audit this technology ?



Blockchain Maturity

- **Young Technology:** May not operate at scale without compromising on security, speed or cost
- **Cost:** Hard to estimate true cost of total conversion

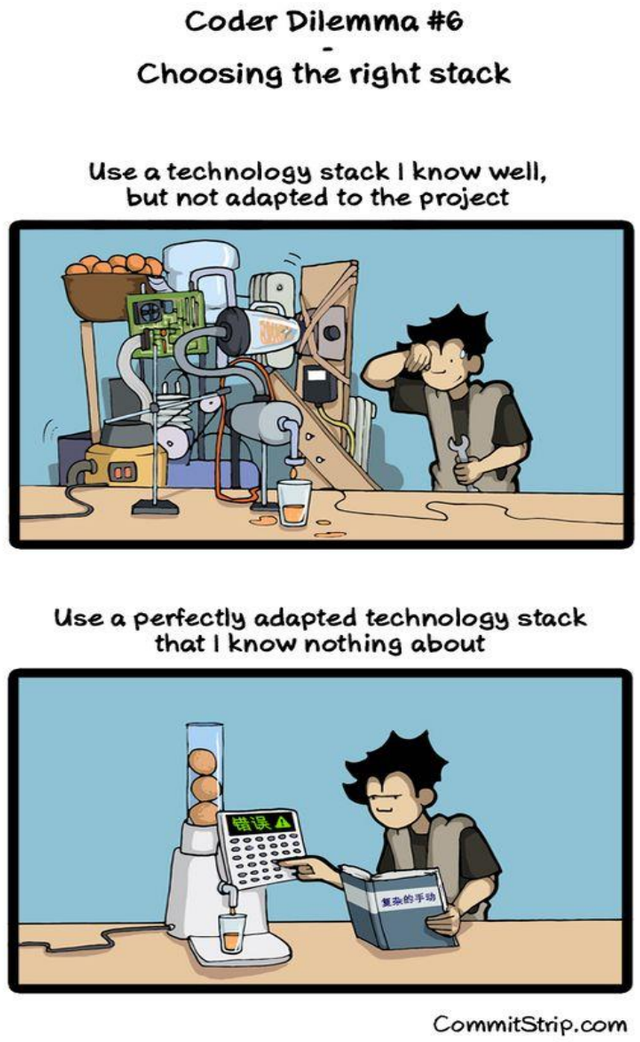
Adoption

- **Proper Incentives:** Potential participants will need to be sold on the value of the platform
- **Consensus Needed:** Participants must come to group agreement on platform and standards acceptable to all

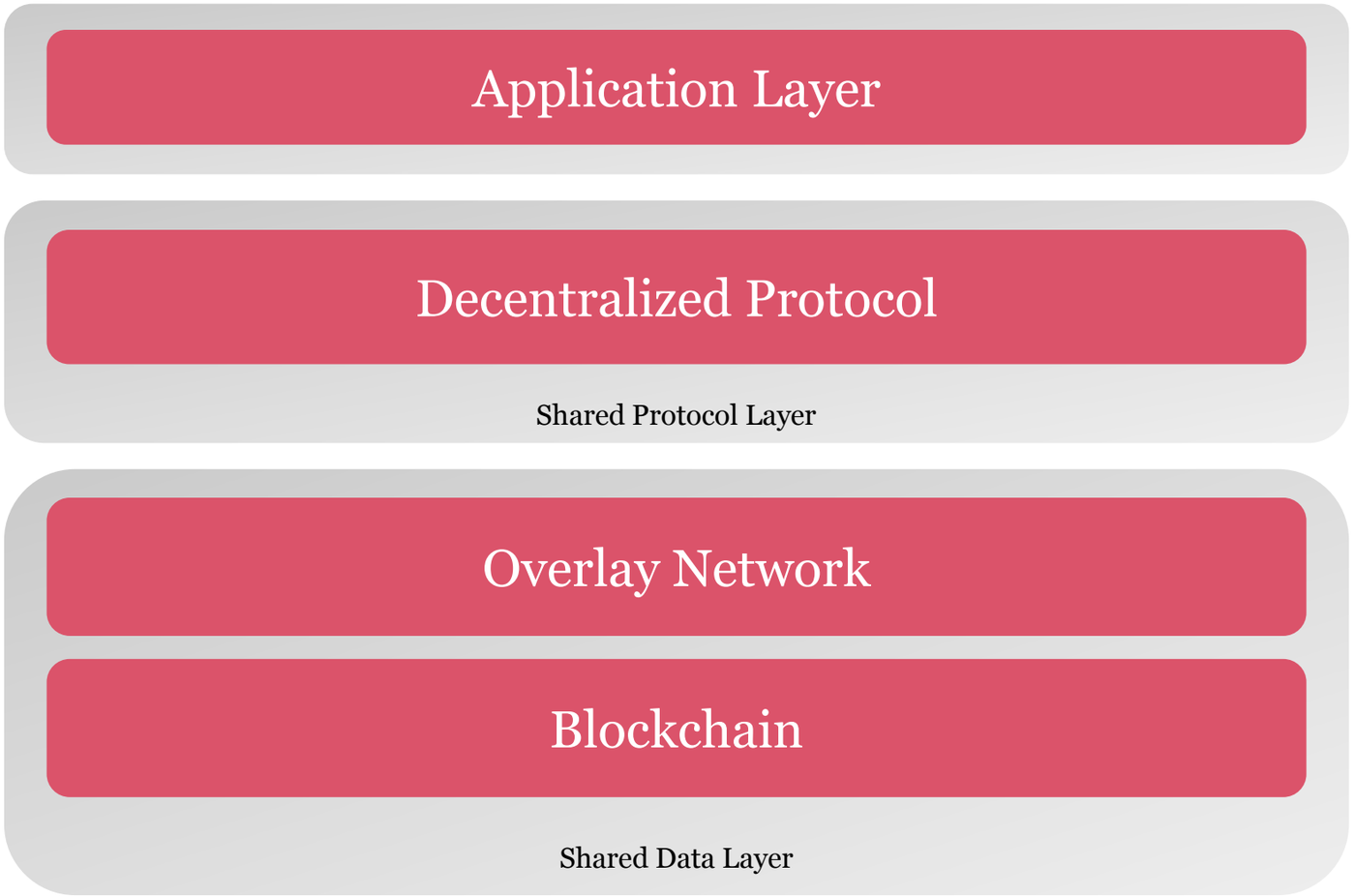
Interoperability/ Integration

- **Interoperability:** Ability to integrate with participant existing client systems and processes
- **Architectural Role:** How will blockchain eliminate, replace, or work with current technological platforms

Blockchain Technology Stack



Generic Technology Stack



Build consumer facing applications using API's

Define specialized business rules at a higher level of abstraction

Complement the blockchain with additional functionality

Plug applications into a shared data ledger

Blockchain layer

Description

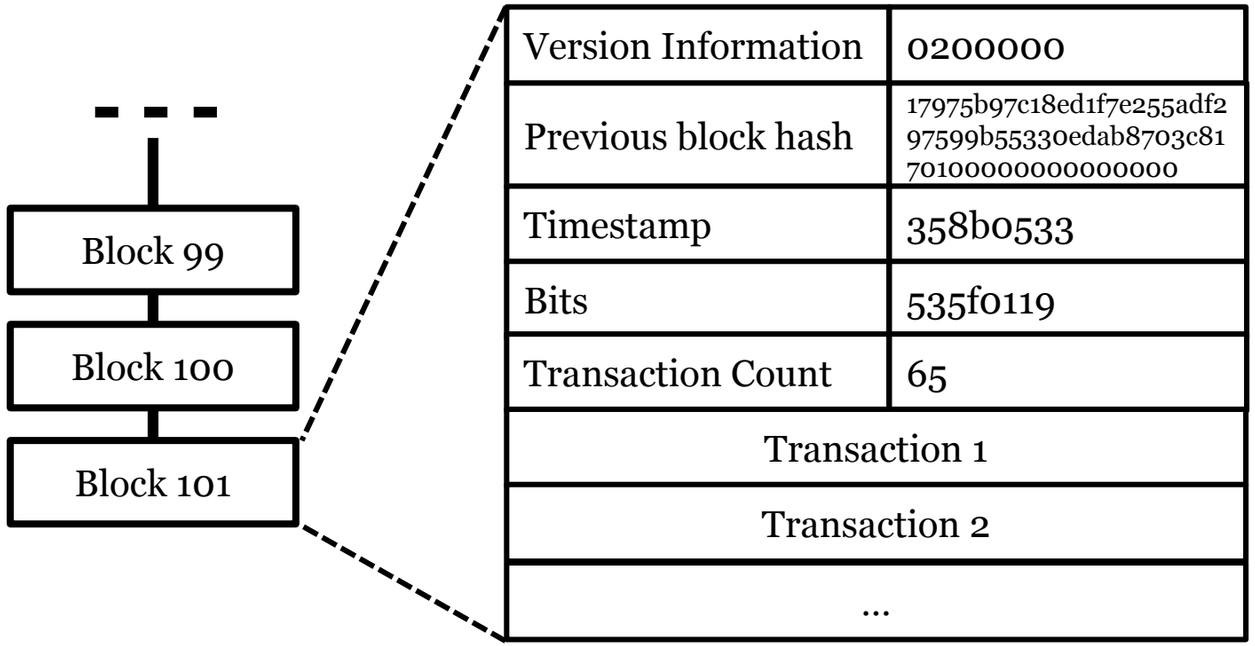
This layer holds a permanent record of all blockchain transactions which resides in a network of specialized validation nodes (miners).

Key Features

- **Decentralized** – The blockchain data ledger is stored fully or partially in a network of nodes
- **System Requirements** – These nodes need to have an adequate memory space, sufficient computing power and a functioning network connection to verify transactions
- **Cryptographic Encryption** – All data blocks stored in the ledger are encrypted and linked to the previous blocks, restricting data modification

Example

The illustration of the data block below showcases a mock-up of what kinds of encrypted information is stored in a typical block



Data blocks in blockchain

Overlay networks Layer

Description

Overlay Networks extend blockchain's existing functionality while managing the peer-to-peer communications.

Key Features

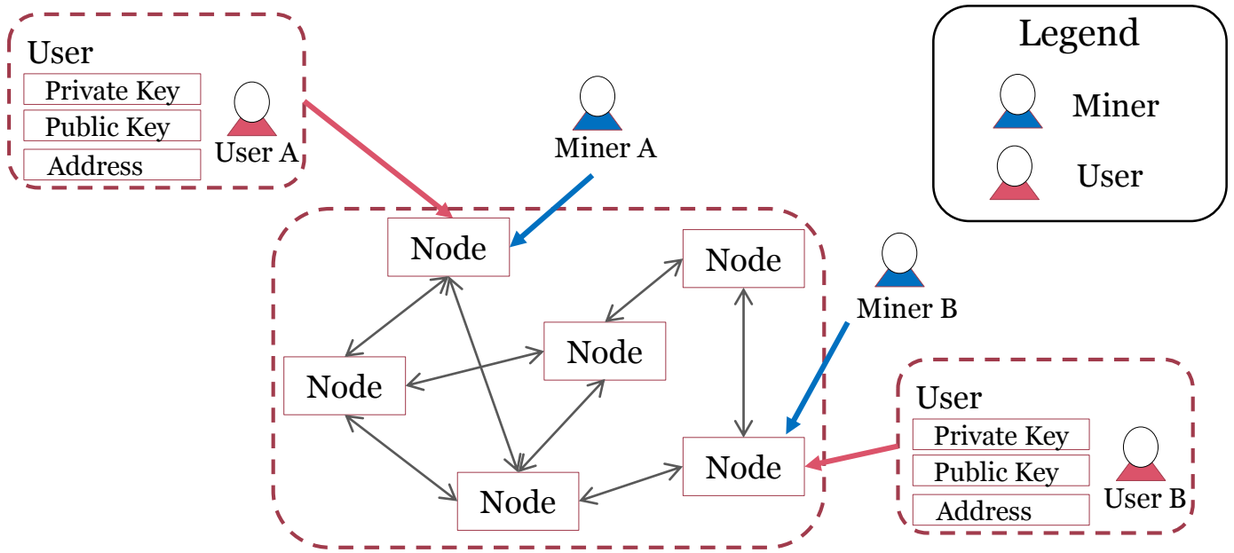
- **Communication** – Network protocols in this layer enable the following:
  1. Publishing – Validation nodes disseminate a block to other nodes in the network
  2. Conflict Resolution – The network prescribes the valid blockchain in case of forks
  3. Synchronization – Network parameters to enable periodic ledger synchronization

- **Functionality** – Additional capabilities such as storing different file formats and sizes can be incorporated via network protocols

Example

Overlay networks for auditing services could include protocols for -

1. Proof of Existence: Document existed in s certain format
2. Proof of Process: If the document is linked to an updated document
3. Proof of Audit: Verifying that the document was validated



Peer-to-peer network of nodes in a blockchain

Decentralized protocols

Description

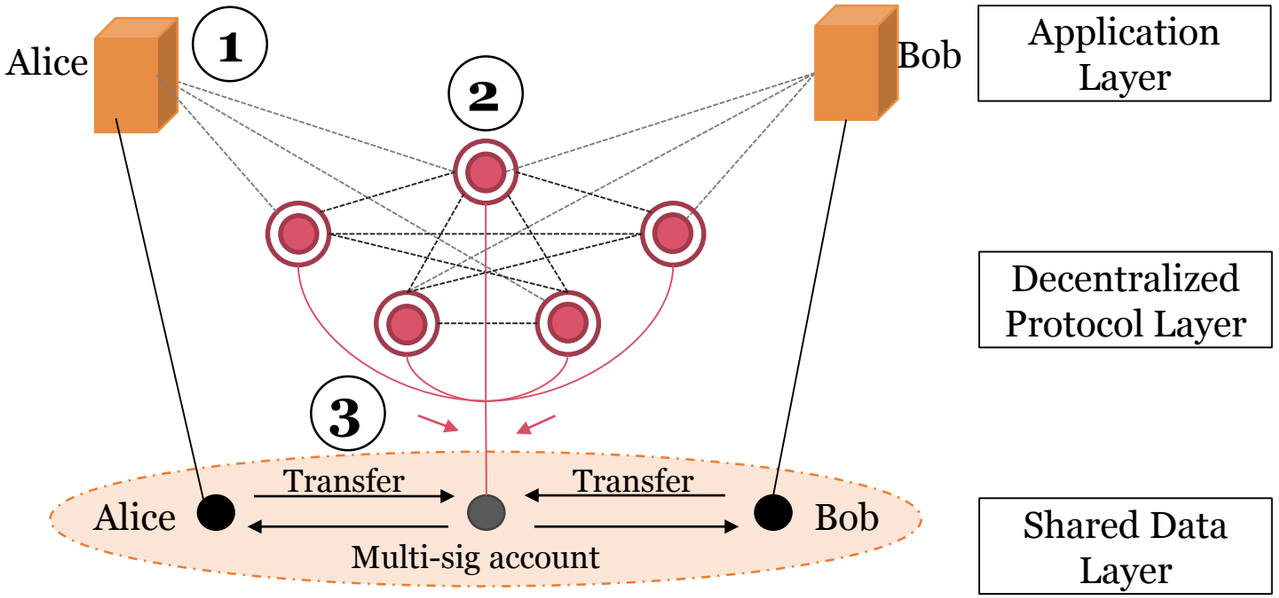
Decentralized protocol layer helps incorporate programmable business rules in the application.

Key Features

- **Programmability** – Rules and associated consequences related to every potential scenario are implemented as programmable software code
- **External Interaction** – The protocol layer can be configured to interact with external services that accept cryptographically signed commands
- **Hand-off** – After enforcing business rules embedded in protocols, the transaction is circulated to the shared data ledger for execution

Example

1. Alice broadcasts request with asset details
2. Nodes in decentralized layer verify details such as asset existence, Alice's ownership and Bob's balance to pay for asset
3. After approval, data layer nodes add the transaction to ledger



Functioning of decentralized protocol layer

Application layer

Description

This layer consists of APIs (Application Programmable Interfaces) to facilitate the use of blockchain functions and user interfaces to enable consumer interaction.

Key Features

APIs resemble modular building blocks that enable different kinds of functionalities to be implemented into end-user applications. Some key features are:

- **Usability** – APIs are quick and easy to use, with consistent structure and business functionalities, enhancing developer productivity
- **Extensibility** – Modular API design can ease capability extension

User interfaces (Apps) utilize APIs and are capable of communicating with each other

Example

1. Alice uses a wallet to explore and execute various asset transfer functionalities
2. On hitting 'Send Asset' button, several underlying APIs are invoked
3. Alice can view her transaction log or be notified if balance changes

Sample Blockchain APIs

Wallet API

Get Balance
Get Address
Get Current Price
Get Transaction History

Notification API

Create Notification
Enable Notification
Display Notification
Disable Notification

Sample User Interface

Welcome Alice! Current Balance: 20 BTC

Send Asset **Market Price** **Transaction Log**

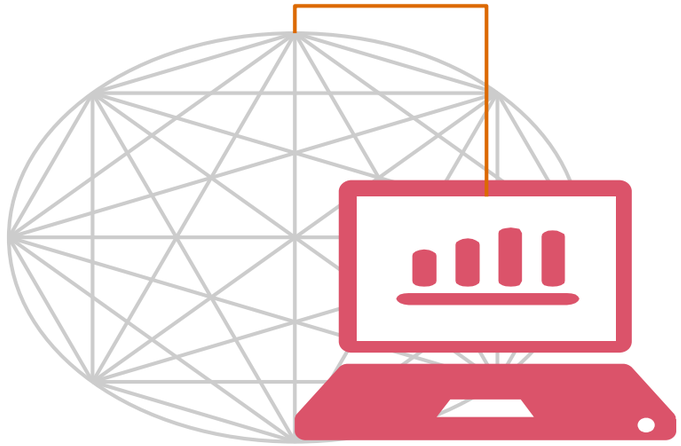
Why do we think about it in layers

- It helps break down complex technologies into *"bit"* size concepts to help with understanding the risks and controls.
- Doesn't help answer the question how to audit them but it will help in everyone "*speaking a recognizable language*".
- Examples:
  - Blockchain layer: is it a public Blockchain or a private one or a hybrid ? Once we know the answer to that we can think about what risks and controls might be relevant; ex: how will cryptographic keys be used in the transaction ? What's the strength and how will they be kept secure.
  - Network Layer: How are transactions verified and does that align with the agreed upon logic ? Who can verify the transactions ? Can there be limits placed on verifications ?
  - Decentralized Protocols: What other business logic has been built into the implementation ? How will the implemented logic have an impact on the transactions on the chain?
  - Application layer: Not too different from what we do now a days ?

One Possible Audit Approach

Enterprise Need and Challenges

Increases in transaction volume and rapidly evolving complex technologies are creating a critical need for business, technology and compliance functions to be prepared, adaptive and agile to emerging challenges.

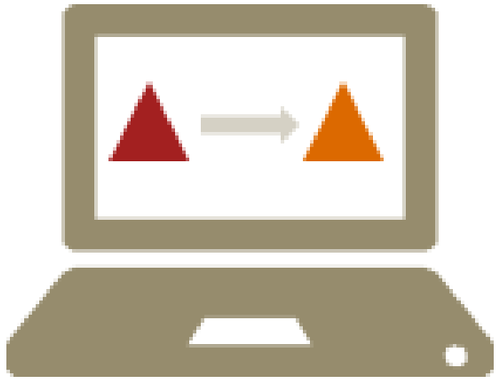


Transaction Volume

Due to increase in transaction volume current audit methodologies that are **manual**, **sample-based** and point in time do not provide the level needed level of confidence.

Traditional Audit Approach

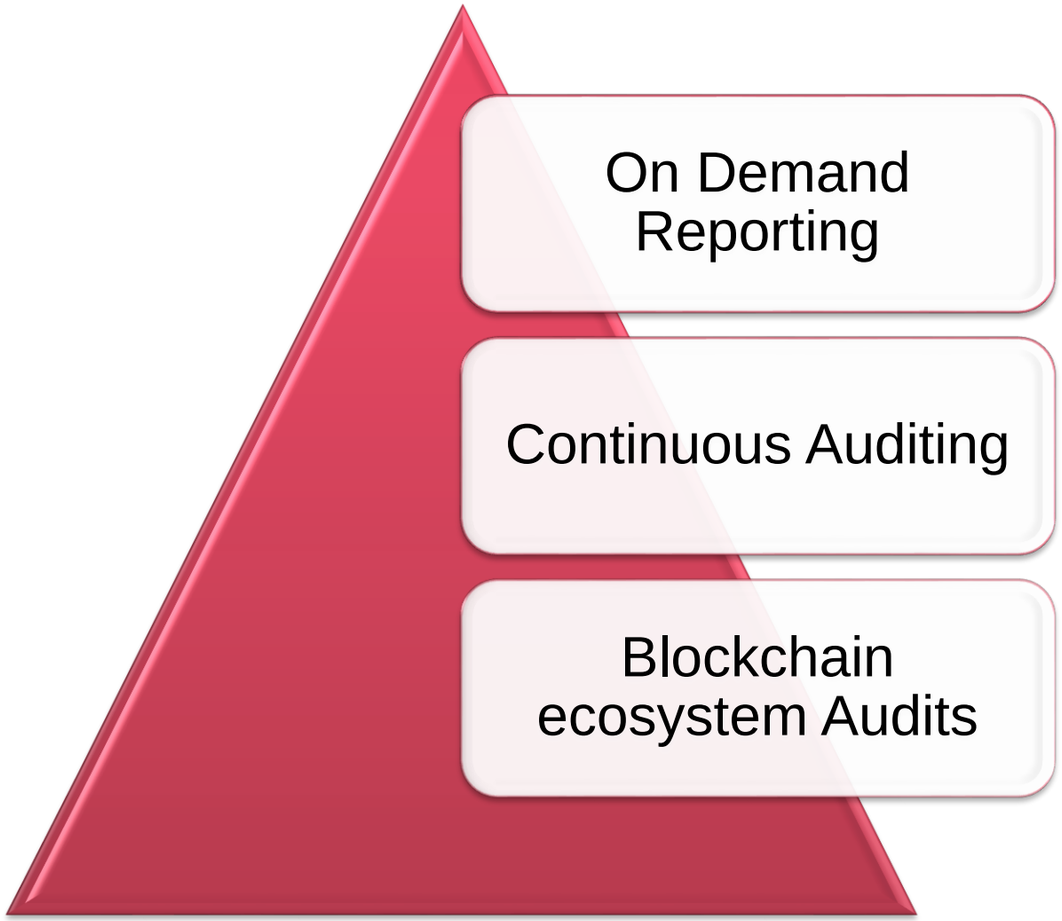
Methodologies will have to shift from a manual to an **automated and continuous approach to** address a significant increase in transaction volumes and new emerging complex technologies.



Technological Challenges

Current methodologies **cannot provide the necessary assurance** in areas when a blockchain is used.

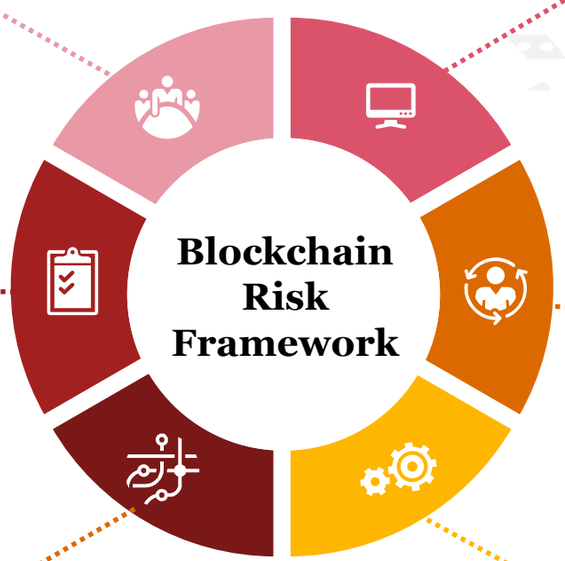
End to End Auditing approach



- Blockchain ecosystem audit aligns with the technology stack. Executed periodically on a rotational basis.
- Software based continuous auditing translates audit tests into programmable logic which is executed against every/set of transactions. Benefits include:
  - Improve Risk Coverage
  - Improve Testing Efficiency
  - Repeatable Process
  - Near real time results

One possible Audit Approach - PwC

A Proprietary Framework to evaluate the current state of a Blockchain use case against **6 different risk categories** and **across 100+ sub-categories** in order to **address assurance and compliance needs** of stakeholders.



Governance and Oversight

- Business Objectives
- Program Sponsorship
- Leadership Commitment
- Program Management
- Operational and Capital Expenditure Oversight
- Project Management

Overlay network layer

- Cloud Security
- Data Security
- Data Privacy
- Penetration Testing
- Network Security
- Patch and vulnerability
- Threat detection
- Threat response

Blockchain Layer

- Blockchain Platform & Protocol Configuration
- Hardware Security Modules
- Signature Management
- Cryptography
- Scalability
- Availability

Decentralized Protocol layer

- Smart Contacts
- Digital Assets
- Digital Currency
- Clearing and settlement
- Business Use Case Transactions

Blockchain ecosystem

- Permissioned network management
- Participant Onboarding and Off-boarding
- Application layer
- Blockchain consensus
- program management
- Integration with off-Blockchain systems and processes

Application Layer

- Servers and Databases Configuration
- ITGCs
- Business Continuity and Disaster Recovery
- IT Asset Management

Compliance with Applicable

- Internal Policies & Procedures
- External Standards & Regulations
- Business Oversight & Monitoring

Blockchain Continuous Auditing Risk Framework – Governance and Oversight

Governance is the combination of processes and structures implemented by the board to **inform, direct, manage, and monitor** the activities of the organization toward the achievement of its objectives. Governance consists of the **leadership**, **organizational structures**, **capital and operational expenditures**, and **processes** that ensure the **success of Blockchain program, strategy and objectives, and project management.**

Risk sub-categories

- Blockchain program management
- Blockchain use case business objectives and sponsorship
- Blockchain use case leadership Commitment
- Blockchain use case project Management
- Blockchain use case operational and capital expenditure oversight

Objectives

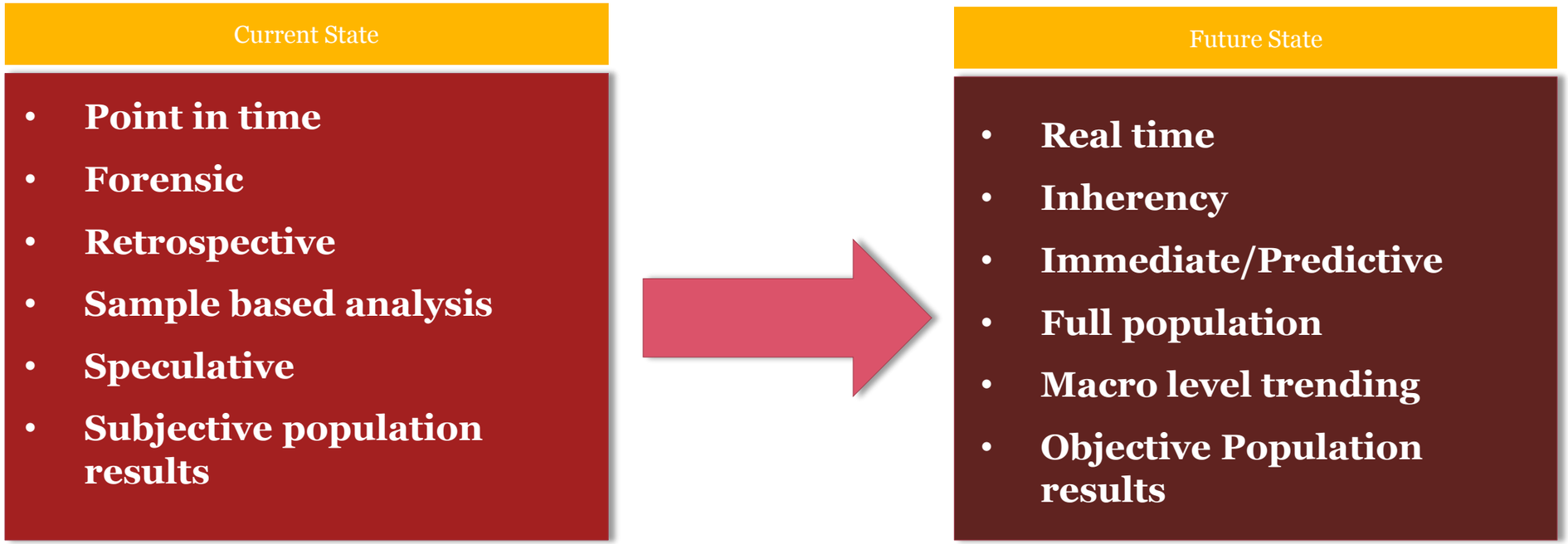
- Ensure strategic and operational decisions are in alignment for the Blockchain program and business use case projects
- Ensure project performance, risk management, and oversight to safeguard success of the Blockchain program and projects
- Ensure OPEX and CAPEX availability, priority, alignment, oversight to support blockchain use case
- Ensure KPIs and Metrics availability and usage for monitoring purposes

Scope

- Blockchain strategy and program
- Program sponsorship and leadership
- Economic model, OPEX and CAPEX commitment
- KPIs, Metrics and reporting
- Blockchain use case projects
- Project Management

Fundamental Shift in Audit Philosophy

Providing this transparency requires a fundamental shift in how we think about audit and control. It must go from retrospective, or forensic, point in time efforts to actual *real time* auditing where the underlying foundations of audit and control become part of the *nature* of each discrete transaction.



Questions ?

Vikram M Panjwani – Partner – Assurance

300 Madison Avenue, New York NY, 10017

Vikram.Panjwani@pwc.com

T: +1.646.471.0070
M: +1.415.238.7604