101 Blockchains Think Tank Webinar Series

LIVE WEBINAR

101 Blockchains

Approaches to Overcome Scalability, Confidentiality and Data Privacy Issues For Enterprise Blockchains

Presented by:

Krishnan Mohan
Head, Distributed Ledger Technology CoE,
Bosch Engineering and Business Solutions

101 Blockchains

MISSION

101 Blockchains is the world's leading online independent global network for Enterprise Blockchain Practitioners

We don't sell blockchain. We help corporate executives understand and decide

How the technology fulfills their business needs and objectives.

Trusted

Strategic

Practical

101 Blockchains

MISSION

We are a professional and trusted provider of enterprise blockchain research and training

Our core mission is to train leading enterprise professionals to become global blockchain experts by providing them practical up to date knowledge and upskilling.

101 BLOCKCHAINS ACADEMY

VIRTUAL CONFERENCES

THINK TANK WEBINARS

Trusted by 11,000+ professionals!

101 BLOCKCHAINS ACADEMY

Trusted by 11,000+ professionals

101 Blockchains

BECOME A WORLD-CLASS BLOCKCHAIN PROFESSIONAL

All Courses, Blockchain Certifications

Certified Enterprise Blockchain Professional (CEBP)

★★★★★ (43)

30 Lessons

All Courses, Blockchain Certifications

Certified Enterprise Blockchain Architect (CEBA)

★★★★★ (19)

66 Lessons

All Courses, Blockchain Certifications

Certified Blockchain Security Expert (CBSE)

★★★★★ (23)

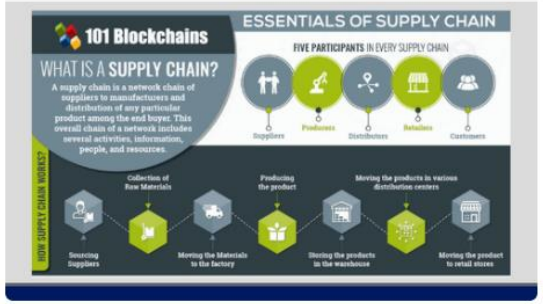
67 Lessons

All Courses, Blockchain Training

Enterprise Blockchains and Supply Chain Management

★★★★★ (27)

20 Lessons

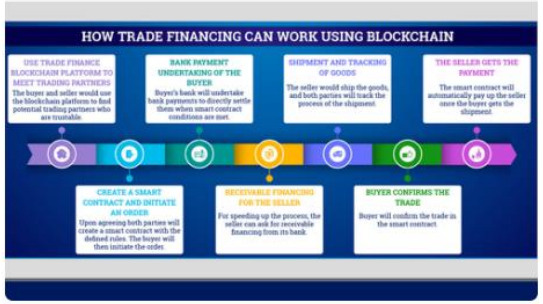


All Courses, Blockchain Training

Enterprise Blockchains and Trade Finance

★★★★★ (23)

20 Lessons



All Courses, Blockchain Training

Enterprise Blockchains Actionable Templates & Tools

★★★★★ (18)

17 Lessons

101 Blockchains Think Tank Webinar Series

LIVE WEBINAR

101 Blockchains

Approaches to Overcome Scalability, Confidentiality and Data Privacy Issues For Enterprise Blockchains

- Common Myths on Blockchain Security
- Need for addressing Security, Confidentiality and Privacy in Enterprise Blockchain Implementations
- Right Approach to adopt the technologies / techniques to address Security, Confidentiality and Privacy

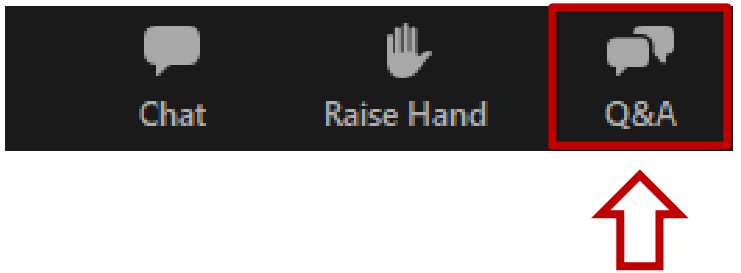
Presented by:

Krishnan Mohan
Head, Distributed Ledger Technology CoE,
Bosch Engineering and Business Solutions

A few housekeeping tips

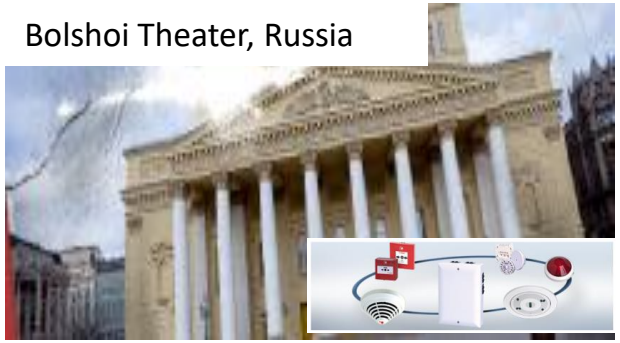
101 Blockchains

Use the **Q&A** tab to ask your questions



Bosch
Technology to enhance quality of life

Bosch Technologies..



BOSCH

Robert Bosch Engineering and Business Solutions Pvt Ltd

Digital - Bosch's stated position in shaping the new world

"The connected world is not some distant dream. It's already here.

We want to connect the virtual and the physical world."

Sensor

Software

Services

We connect everyThing & everyThing becomes a service

BOSCH

Robert Bosch Engineering and Business Solutions Pvt Ltd

Finding intersections and amplify vertical solutions

Healthcare

Agriculture

Retail

Energy

Smart Living (Smart Cities, Campus)

AI
(Including Computer Vision, Machine Learning, NLP, etc.)

DISTRIBUTED LEDGER TECHNOLOGIES

EDGE, FOG, CLOUD COMPUTING

IoT

New age technologies such AI, Blockchain(DLT), NLP, Edge Computing have the potential to disrupt multiple verticals acting as horizontal enablers

With these horizontal technologies at play; disruptions across verticals, by new comers displacing incumbents, is becoming a recurring phenomenon

Applying Bosch's IoT philosophy of Sensor, Software, Services, allows us to find intersection points within existing verticals and act as amplifiers. Also allowing to explore and apply innovative business models.

BOSCH

Enterprise Blockchains

BOSCH

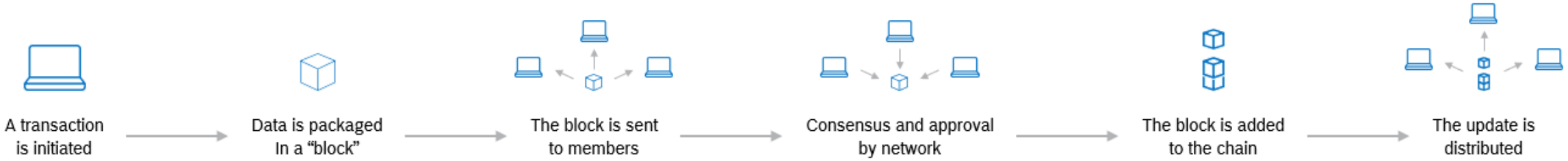
Robert Bosch Engineering and Business Solutions Pvt Ltd

Introduction to the Distributed Ledger Technology (DLT)

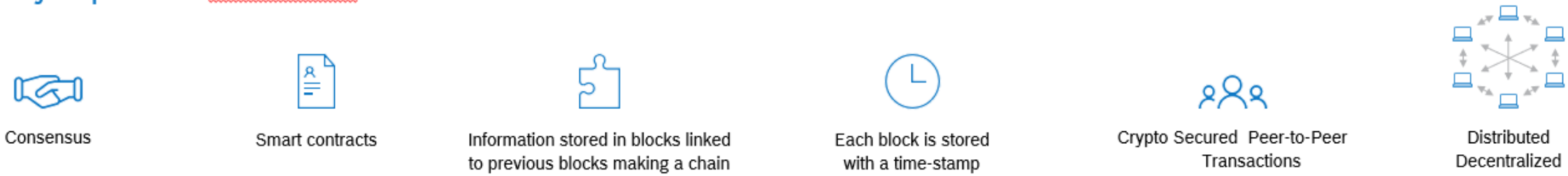
A **Distributed ledger** is a consensus of digitized, decentralized & replicated append only digital data geographically spread across multiple locations

Blockchain is one type of a distributed ledger. Blockchain organizes data into blocks, which are chained together in an append only mode.

How Blockchain works



Key aspects of Blockchain

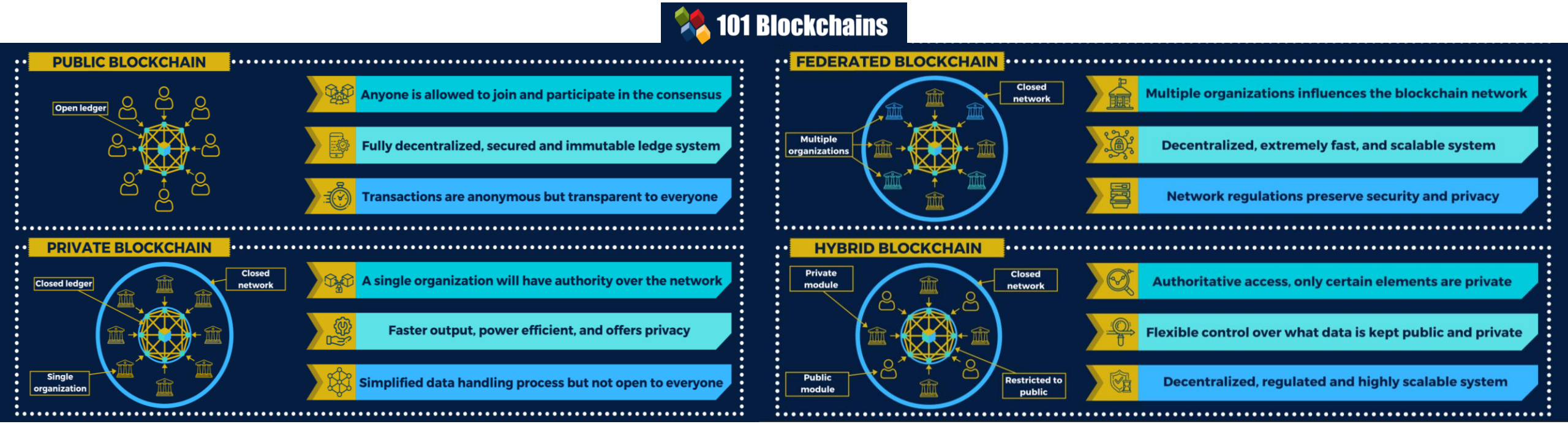


© Robert Bosch Engineering and Business Solutions Private Limited 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

BOSCH

Robert Bosch Engineering and Business Solutions Pvt Ltd

Types of Blockchains



- Each of the Blockchain Types have it's own pros / cons
- Many of them have to deal with Data privacy, confidentiality and security
- Scalability is one of the bigger technical problem as well

© Robert Bosch Engineering and Business Solutions Private Limited 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

BOSCH

Robert Bosch Engineering and Business Solutions Pvt Ltd

Distributed Ledgers as Enterprise backbone

DIGITAL CURRENCY

DLT / Blockchain blended with Enterprise systems acts as the backbone of nano and micro payments between humans and machines.

✓ Connected car eWallet, Consensus as a service

DLT

DIGITAL IDENTITY

Secure and efficient management and tracking of digital identities on the basis of Blockchain

✓ Seamless sign-on, cross-party identity

DIGITAL NOTARY

Blockchain as the basis for registering immutable, certain and indisputable information records

✓ Supply chain track and trace, odometer fraud prevention , Spurious parts detection

SMART CONTRACTS

Shared business rules and automatic business execution among different stakeholders

✓ Peer-to-peer microgrids, supply chain finance, clinical trials

ECONOMIC THINGS

Autonomous IoT devices enter into binding agreements and act as own legal entities

✓ Self-renting autonomous car, energy trading EV

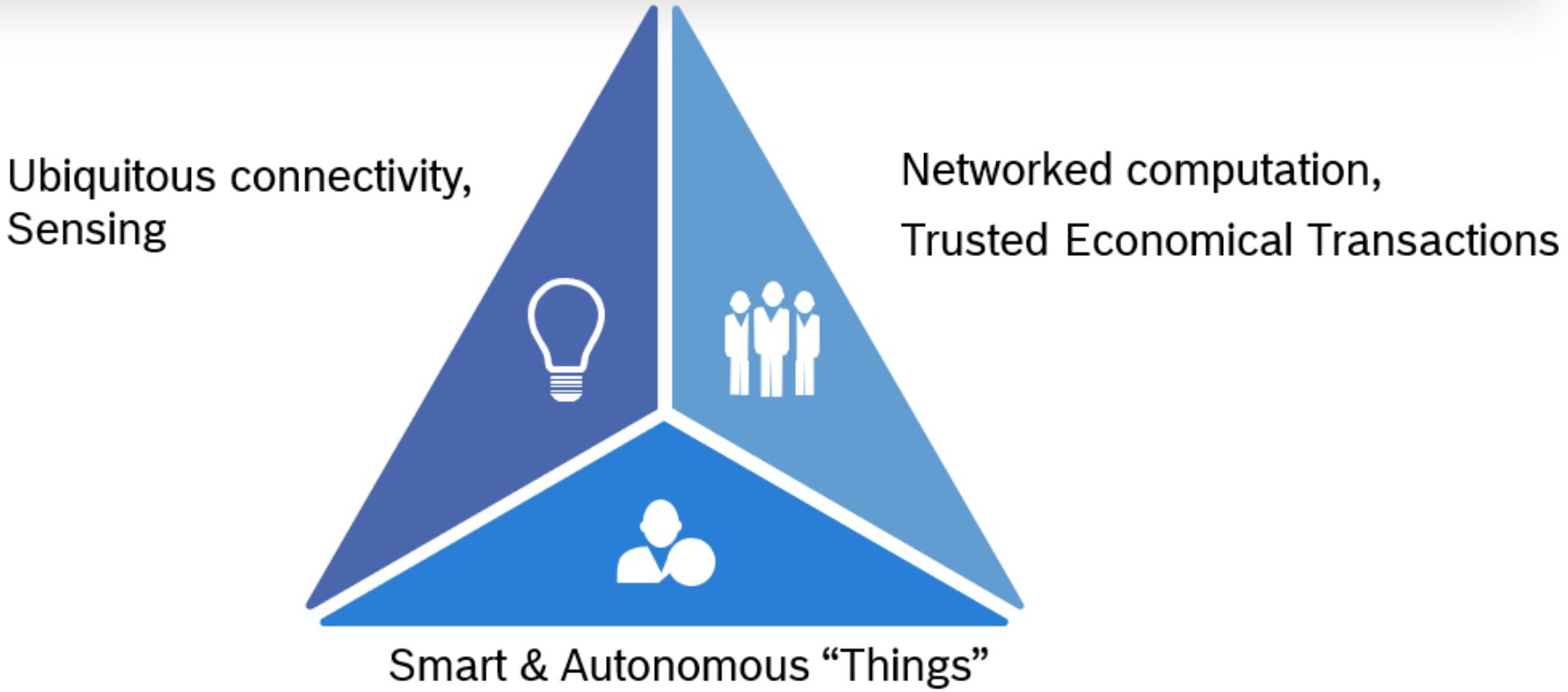
BOSCH

Bosch Vision – Economy Of Things

Robert Bosch Engineering and Business Solutions Pvt Ltd

Our Vision - Economy of Things

Economy of Things is one where the smart, autonomous, networked and economically independent machines act as the participants, carrying on the necessary activities with little to no human intervention.



BOSCH

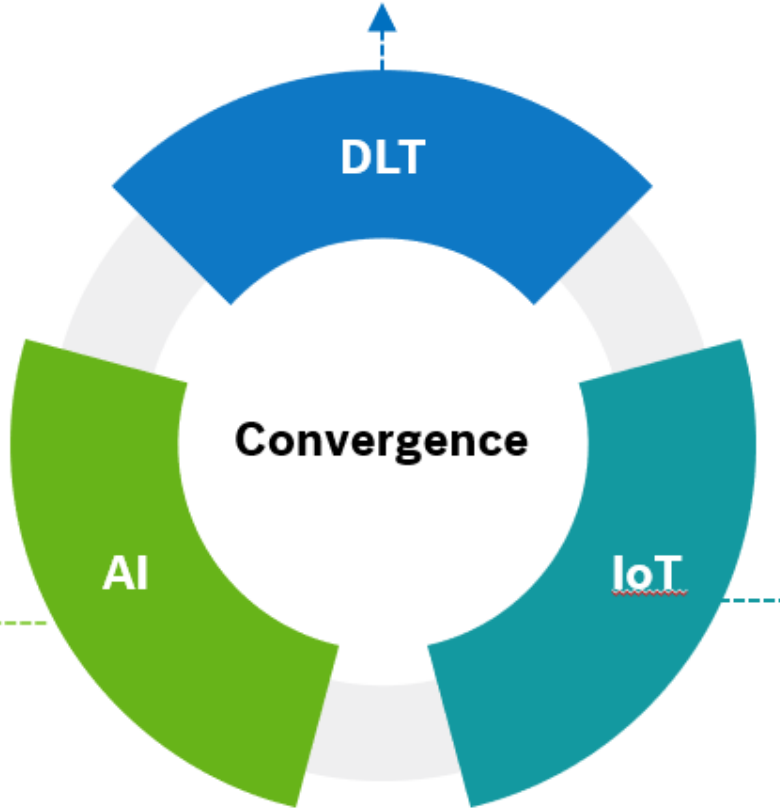
Robert Bosch Engineering and Business Solutions

Technology Convergence Stack – DLT, IOT, AI

Economy of Things

Networked computation, Trusted Economical Transactions

Collaboration of Things



Internet of Things

Smart & Autonomous “Things”

Ubiquitous connectivity, Sensing

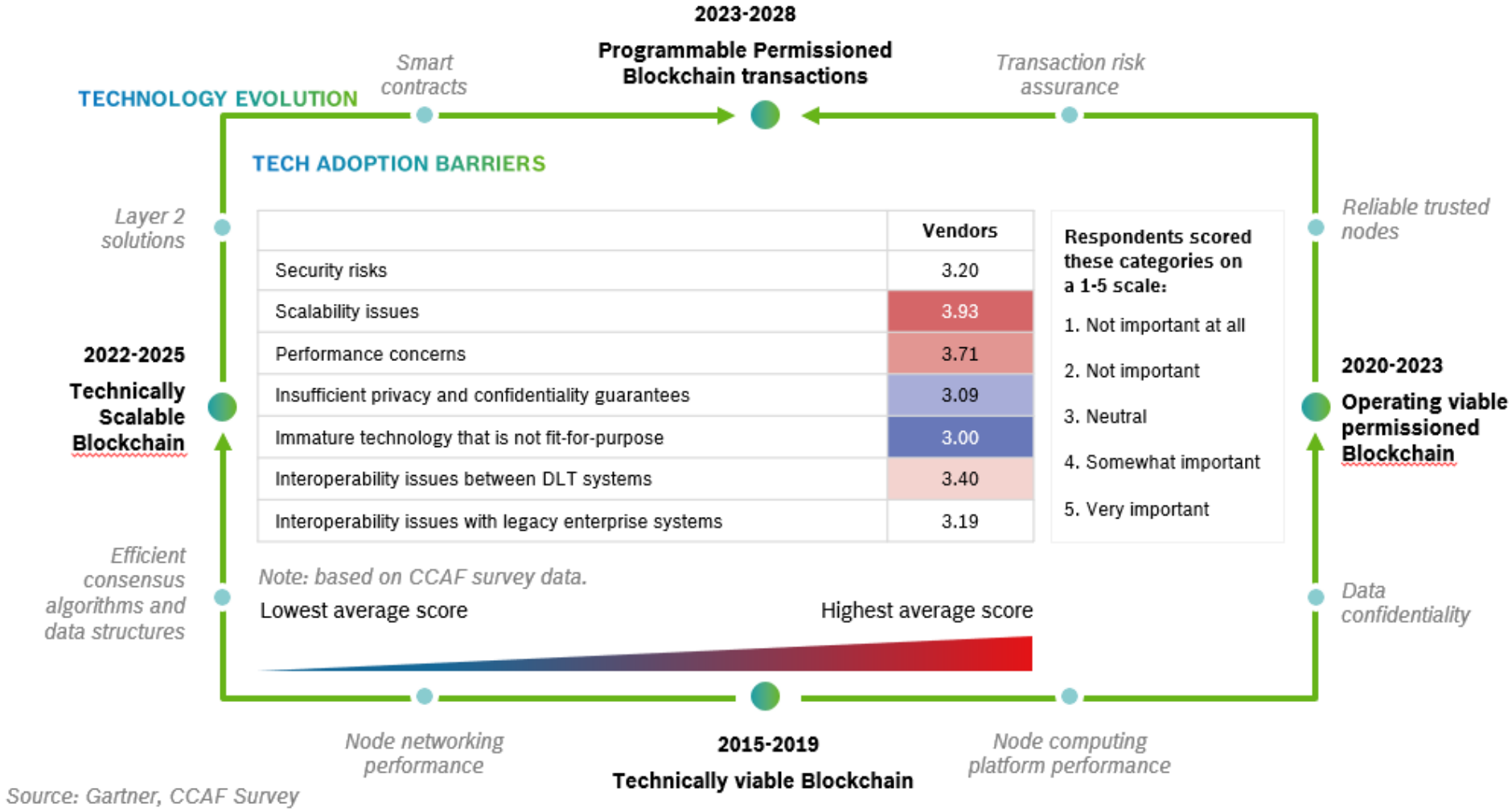
© Robert Bosch Engineering and Business Solutions Private Limited 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

BOSCH

Enterprise Blockchain Problems

Robert Bosch Engineering and Business Solutions Pvt Ltd

Key barriers to adoption and our focus Areas

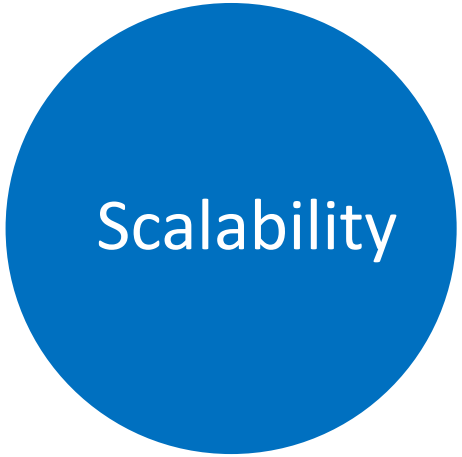


Source: Gartner, CCAF Survey

BOSCH

Scalability

Scalability – Different Approaches



Parameter Tweaks	Bigger Blocks, More Transactions
Layer 2	The second layer scalability solution or off-chain solution adds a second layer to the main blockchain network in order to facilitate faster transactions. The secondary protocols built on top of the main blockchain where transactions are 'off-loaded' from the main blockchain to save space and reduce network congestion
Alternate Consensus models	Reduces the computations cost and helps increase the privacy and the scalability of the blockchain by moving the state transition concepts to off chain.
Sharding	Sharding is a form of database partitioning, also known as horizontal partitioning. The process involves breaking up a very large database into smaller, more manageable segments, with the idea of improving performance and reducing the query response time.

© Robert Bosch GmbH 2020. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

BOSCH

Web3 Stack & State Channels

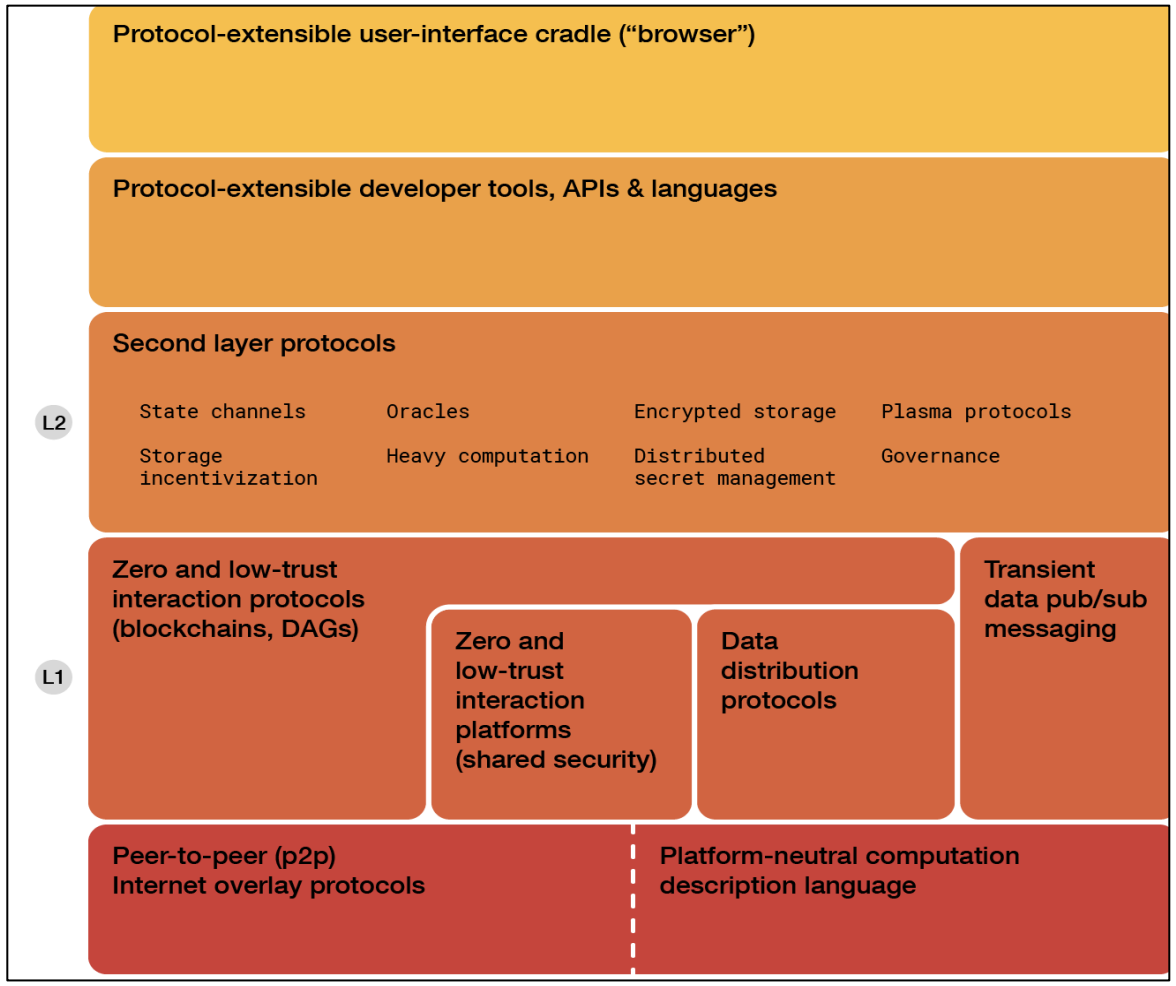


Image Source

Categories of Layer-2

- **State channels**
  - Payment channels
  - General state channels
- **Sidechain**
  - An independent blockchain which runs parallel to it’s parent blockchain.
  - Optimistic Rollups
- **Off-chain computation**
  - Reduces the computations cost and helps increase the privacy and the scalability of the blockchain by moving the state transition concepts to off chain.

© Robert Bosch GmbH 2020. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

State Channel Introduction

How State Channel Works

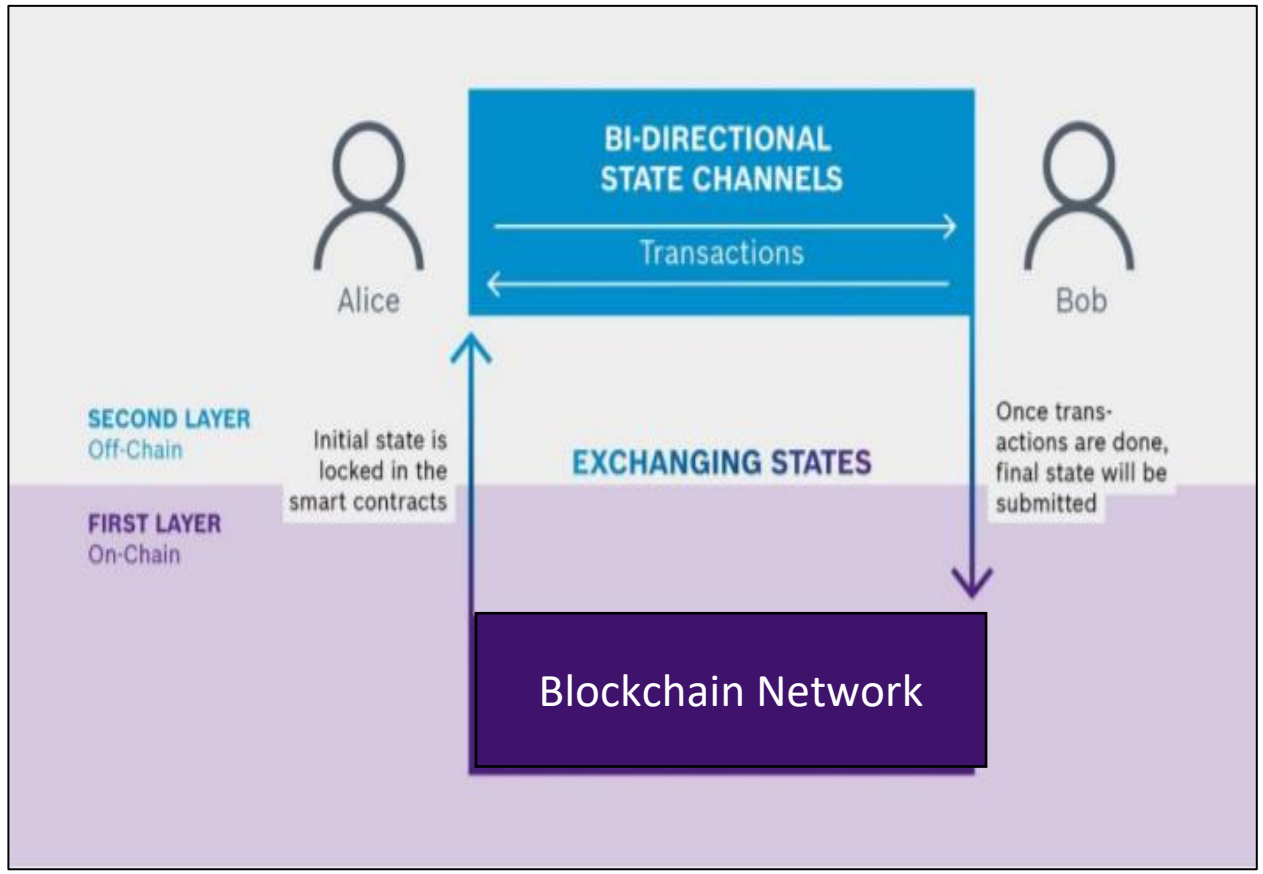


Image Source

State Channel protocols(Second Layer) enabled solutions to operate “on top” of existing blockchain (First Layer) promising big strides in scalability, interoperability and trusted computations.

Second Layer protocols involve minimal interaction with the blockchain network reducing the overhead of cost incurred in the network.

© Robert Bosch GmbH 2020. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

BOSCH

LITERATURE SURVEY

Various state channel protocols

General State Channel

Payment Specific

Counterfactual

- State channels let parties securely modify locked portions of blockchain state called state deposits.
- These deposits are typically held in multi-signature wallets, where the participants to the state channel are the signers to the multisig.

Funfair

- State channels work by allowing participants to engage in a rapid back-and-forth countersigning of updated "claims" on an escrowed amount of funds.

GeoProtocol

- Provides full atomicity for multi-ledger networks, allows to conduct complex transactions atomically with several assets and implements post-quantum cryptography for long-term sustainability.

Lightning Network

- Lightning is a decentralized n etwork using smart contract functionality in the blockchain to enable instant payments across a network of participants.

Raiden

- The goal of the network is to solve the scaling issues of Ethereum by creating a solution that allows agreeing participants to perform unlimited, bidirectional transfers without going through the blockchain for every transaction

Celer Network

- Layer-2 scaling platform that enables fast, easy and secure off-chain transactions for not only payment transactions, but also generalized off-chain smart contract.

Perun Network

- Introduces a technique called "virtual payment channels" that avoids involvement of intermediary for each individual payment.

IEEE - A Systematic Framework For State Channel Protocols Identification for Blockchain-based IoT Networks and Applications

Security, Confidentiality & Privacy

Robert Bosch Engineering and Business Solutions Pvt Ltd

Security, Confidentiality And Privacy (SCP)

Privacy & Confidentiality In Smart Contracts

Software Based Techniques

- Zero Knowledge Proofs
- Homomorphic Encryption

Hardware Based Techniques

- Trusted Enclaves
- Multi Party Computation

© Robert Bosch Engineering and Business Solutions Private Limited 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

BOSCH

Common Myths on Blockchain Security

Blockchains are the “Holy grail” for security problems… *Not True / Not Yet*

- ✓ Blockchains are secure by default
- ✓ Blockchains are not hackable
- ✓ Enterprise Blockchains doesn’t have security bottlenecks

Risk of Security, Confidentiality, Privacy

	Public	Private
Permissioned	Medium	Low
Permissionless	High	Medium

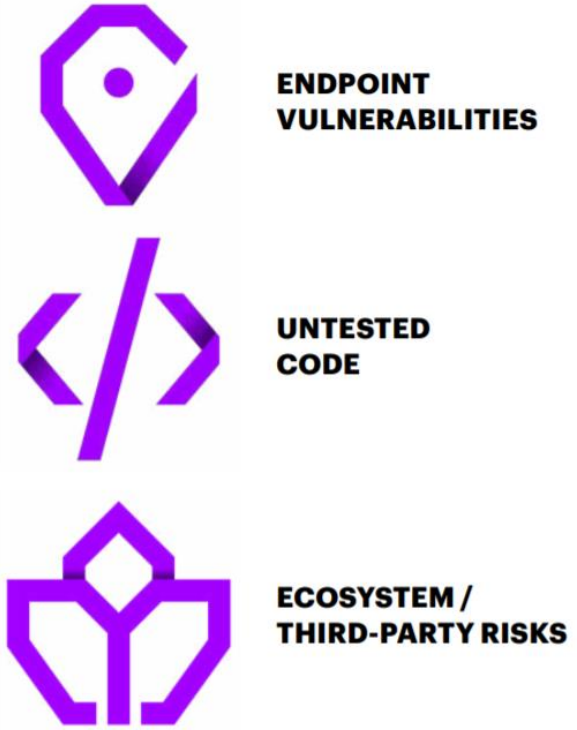


Image Source

© Robert Bosch Engineering and Business Solutions Private Limited 2018. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

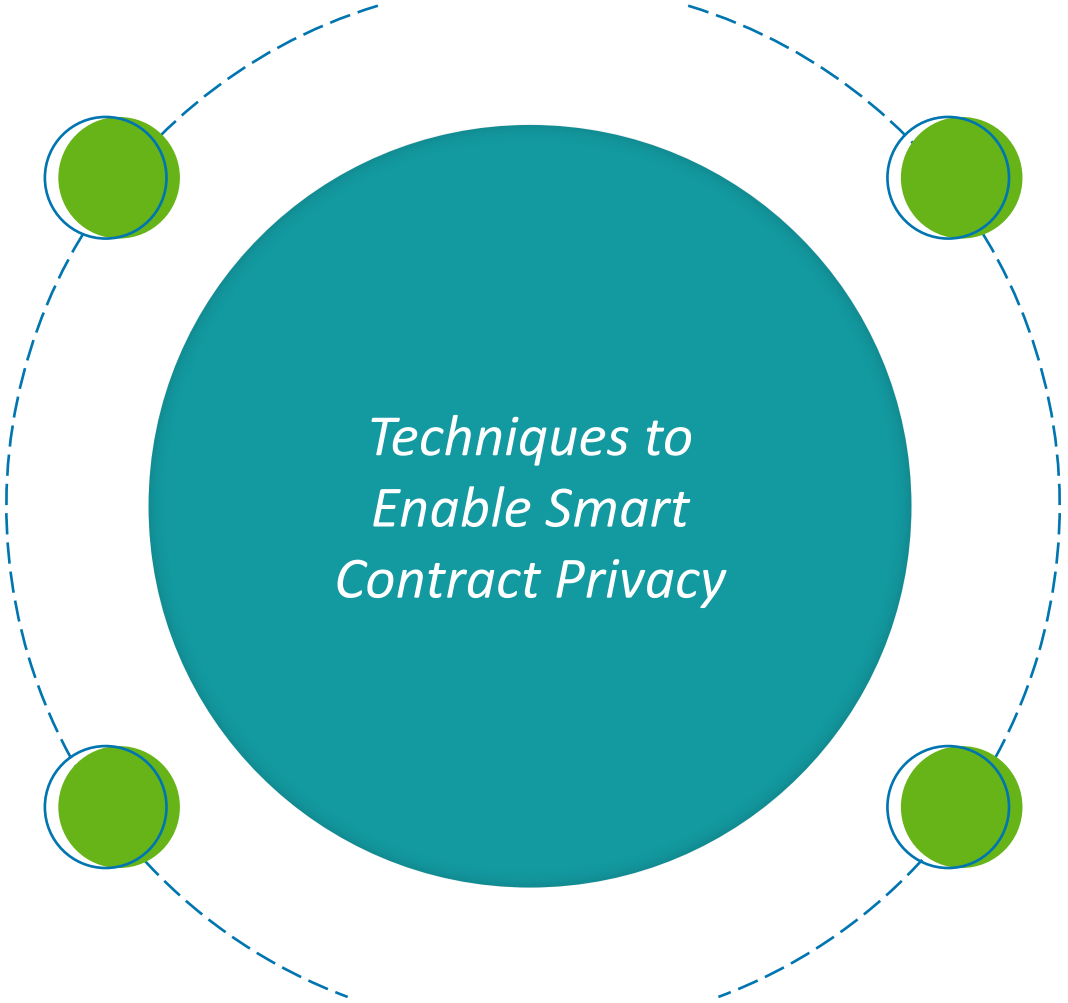
Techniques/Frameworks To Address Smart Contract Security, Privacy & Confidentiality

EKIDEN

Ekiden is a hardware based protocol that aims at bringing Scalability and Confidentiality characteristics to smart contracts in Blockchain.

BULLET PROOF

Bulletproofs are zero knowledge proofs to build confidentiality in a non trusted setup.



ENIGMA

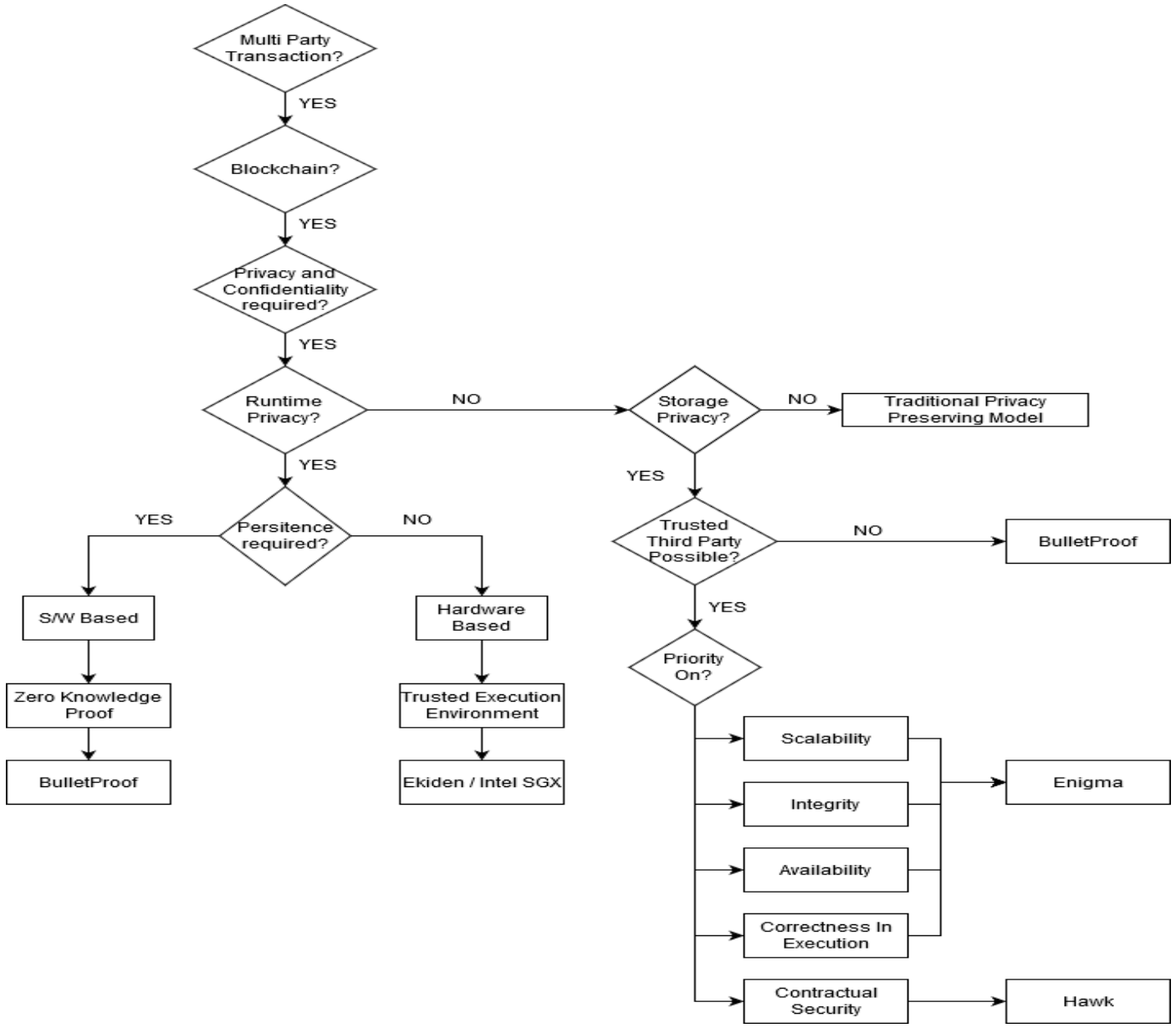
Enigma is a decentralized computation platform capable of preserving privacy.

HAWK

Hawk is a framework developed to bring in privacy in smart contracts.

BOSCH

PROPOSED METHODOLOGY - Decision Framework



IEEE - Decision Framework and Detailed Analysis on Privacy Preserving Smart Contract Frameworks for Enterprise Blockchain Applications

Observations

Intel SGX is the most matured hardware based technology in this space

Zero knowledge proof based techniques are being adopted mostly in the blockchain enterprise networks

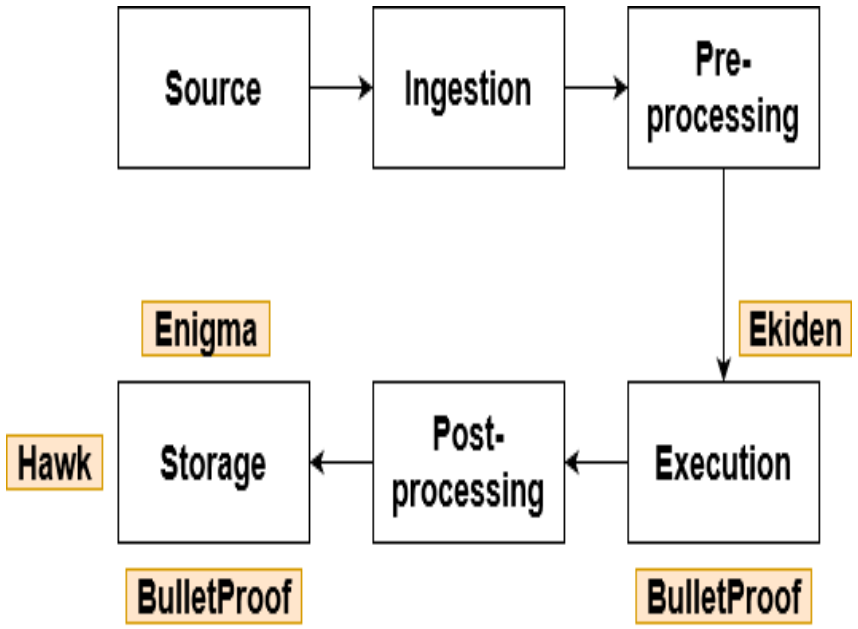
Homomorphic Encryption is another evolving technique to address confidentiality needs . way are not always straight forward to use especially for string based operations

BOSCH

Robert Bosch Engineering and Business Solutions Pvt Ltd

Typical Data Flow – Framework Mapping

Data Flow Based Comparison



Comparison of Privacy techniques

	Ekiden	Enigma	Bulletproof	Hawk
Integrity	Yes	Yes	No	No
Availability	No	Yes	Yes	No
Privacy	Yes	Yes	Yes	Yes
Persistence	No	Yes	Yes	Yes
Performance	High	Low	Low	Low
Correctness in execution	Yes	Yes	No	No
Scalability	Yes	Yes	No	No

BOSCH

*with over **135 years** of experience in the industry, we, at Bosch, speak your language and understand your needs, thus providing solutions designed in partnership with you & delivered to address the realities of your business environment*

– Robert Bosch

THANK YOU

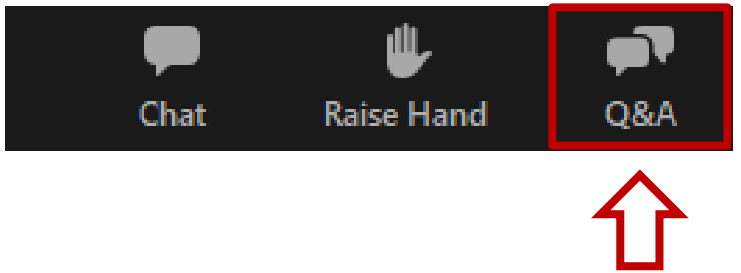
Invented for life

BOSCH

Q&A time

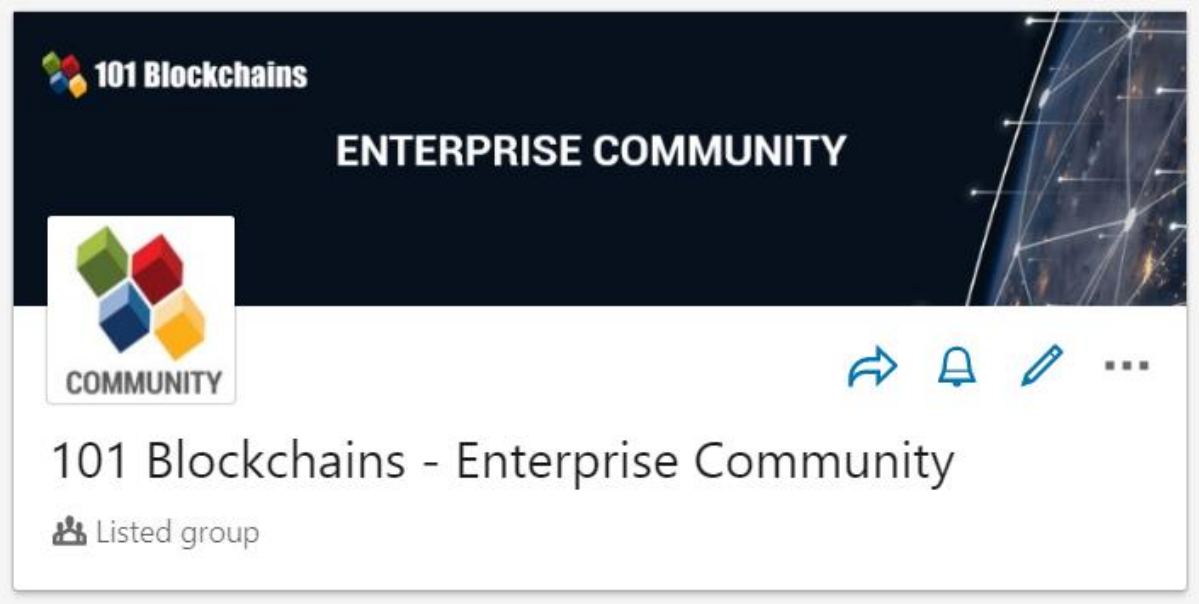
101 Blockchains

Use the **Q&A** tab to ask your questions



Join our Group on LinkedIn

https://www.linkedin.com/groups/12400295/



101 Blockchains

ARE YOU READY TO JOIN THE BLOCKCHAIN REVOLUTION?

- www 101blockchains.com
- contact@101blockchains.com
- in linkedin.com/company/101blockchains
- in https://www.linkedin.com/groups/12400295/

© 2020 101 Blockchains. All rights reserved. This document may not be distributed, transmitted or reproduced in any form or by any means without 101 Blockchains' prior written permission. While the information contained in this document has been obtained from sources believed to be reliable, 101 Blockchains disclaims all warranties as to the completeness or accuracy. Although 101 Blockchains research may address business, financial, investment and legal issues, 101 Blockchains does not provide any business, financial, legal or investment advice and this document should not be construed or used as such. 101 Blockchains shall not be responsible for any loss sustained by any person who relies on this publication.