A Review on Blockchain Technologies for Cyber-Resilient Automotives

Presenters

Prerana Cheguru

Sharani Regonda

Vaishnavi Rao

Delicia Fernandes

AGENDA

- Introduction to Blockchain
- The Need for Cyber-Resilience in Automotives
- Blockchain as a Solution
- Key Features of Blockchain for Automotives
- Use Cases & Applications
- Challenges and Limitations
- Comparative Analysis & Case Studies
- Future Prospects & Evolutions
- Conclusion & Call to Action

01

Introduction to Blockchain

1. Blockchain is a distributed ledger that uses cryptography to securely link transaction records.

2. Each new block contains a hash linking it to the previous block and transaction data.

3. Allows decentralized verification of information without a central authority using cryptography and consensus.

4. First introduced in 2008 with Bitcoin to record transactions.

5. Evolved for applications beyond cryptocurrencies including automotive systems to enhance security and cyber resilience.

02

Cyber-resilience in automotives

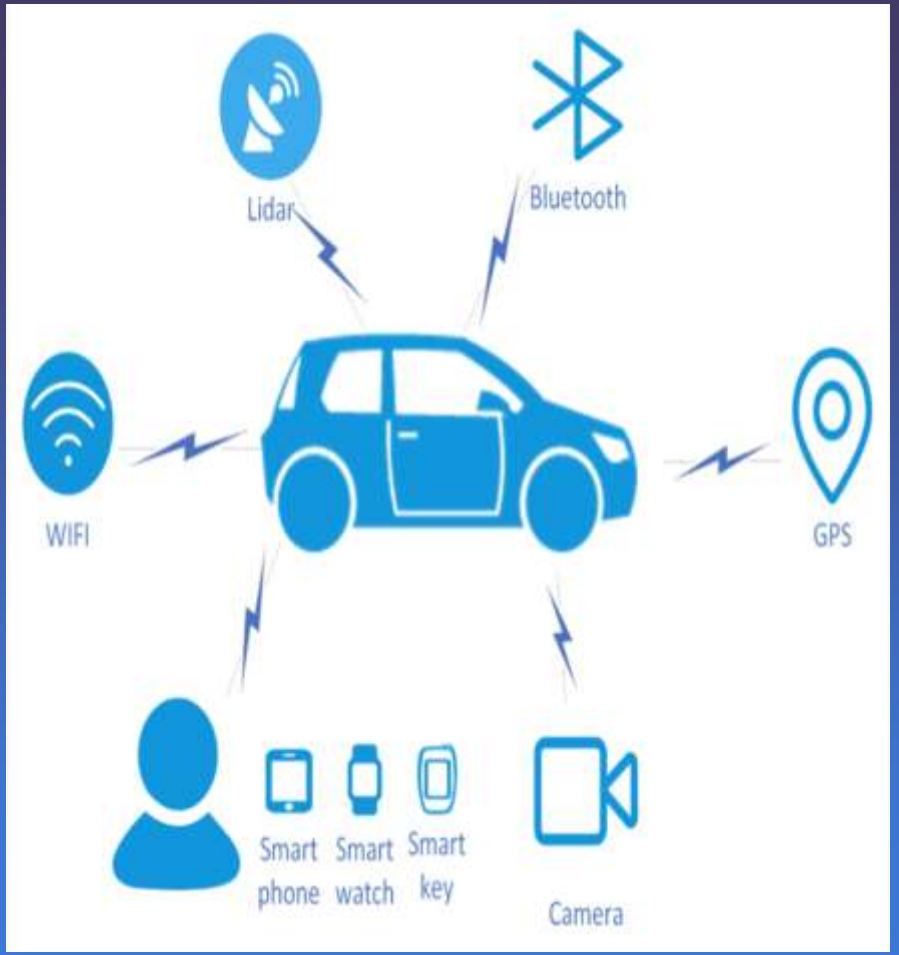
1. Vehicles are increasingly connected with internet-facing attack surfaces.

2. Threats include hacking vehicle systems, tracking/stalking drivers, and remotely disabling safety features.

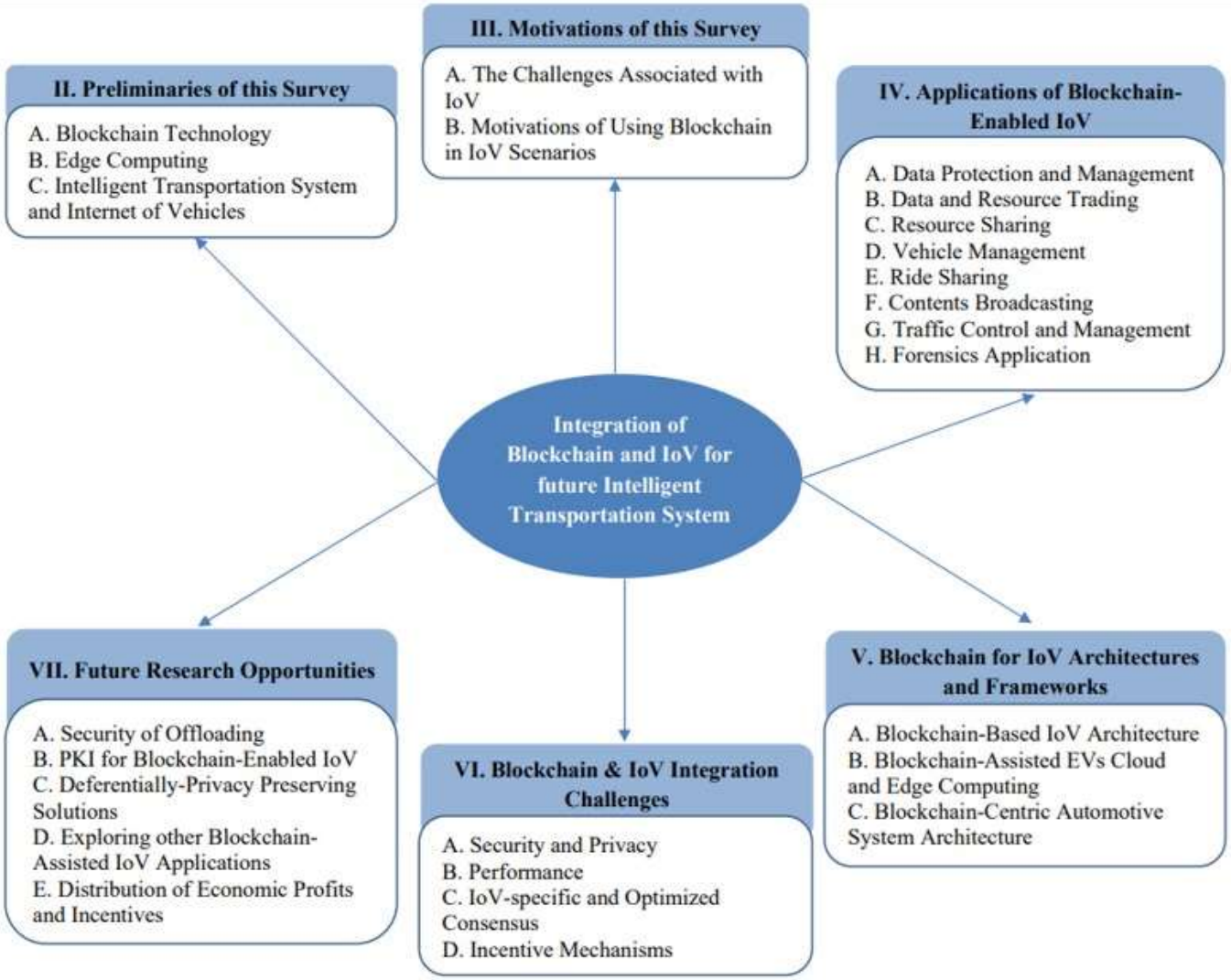
3. Past breaches showed ability to hack brakes, steering, and engine remotely.

4. Lack of security updates leaves many vehicles vulnerable for years.

5. Blockchain could help address issues like weak update mechanisms and single points of failure exploited in past attacks.



IoV


III. Motivations of this Survey
A. The Challenges Associated with IoV
B. Motivations of Using Blockchain in IoV Scenarios
II. Preliminaries of this Survey
A. Blockchain Technology
B. Edge Computing
C. Intelligent Transportation System and Internet of Vehicles
IV. Applications of Blockchain-Enabled IoV
A. Data Protection and Management
B. Data and Resource Trading
C. Resource Sharing
D. Vehicle Management
E. Ride Sharing
F. Contents Broadcasting
G. Traffic Control and Management
H. Forensics Application
Integration of Blockchain and IoV for future Intelligent Transportation System
VII. Future Research Opportunities
A. Security of Offloading
B. PKI for Blockchain-Enabled IoV
C. Deferentially-Privacy Preserving Solutions
D. Exploring other Blockchain-Assisted IoV Applications
E. Distribution of Economic Profits and Incentives
VI. Blockchain & IoV Integration Challenges
A. Security and Privacy
B. Performance
C. IoV-specific and Optimized Consensus
D. Incentive Mechanisms
V. Blockchain for IoV Architectures and Frameworks
A. Blockchain-Based IoV Architecture
B. Blockchain-Assisted EVs Cloud and Edge Computing
C. Blockchain-Centric Automotive System Architecture

03

Blockchain As A Solution

Decentralization:

1. Eliminates central points of failure.
2. Removes need for third-party intermediaries.

Tamper Resistance:

1. Data recorded on blockchain is nearly unalterable.
2. Distributed nature ensures data integrity.

Unforgeability:

1. Transactions are digitally signed.
2. Enhanced protection against impersonation.

Traceability:

1. Every block's data is cryptographically linked to the previous block.

Public Audit:

Transparent transaction verification by multiple nodes.

Non-repudiation:

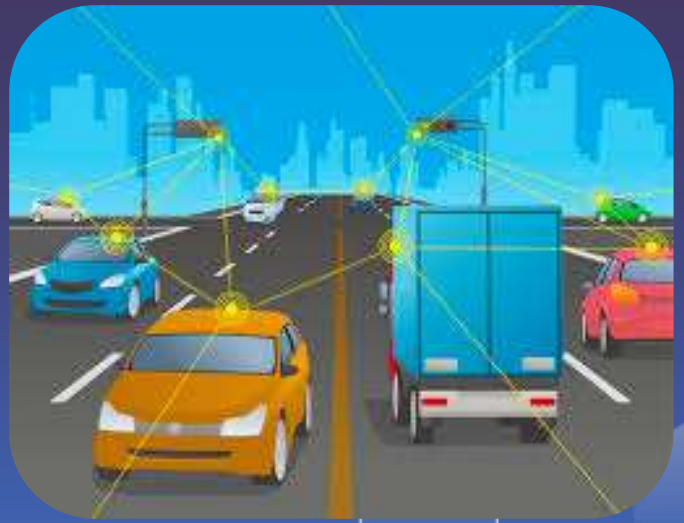
Ensures message senders can't deny their actions.

Simulation & Tools:

Tools like MIRACL and SUMO ensure robust simulations.

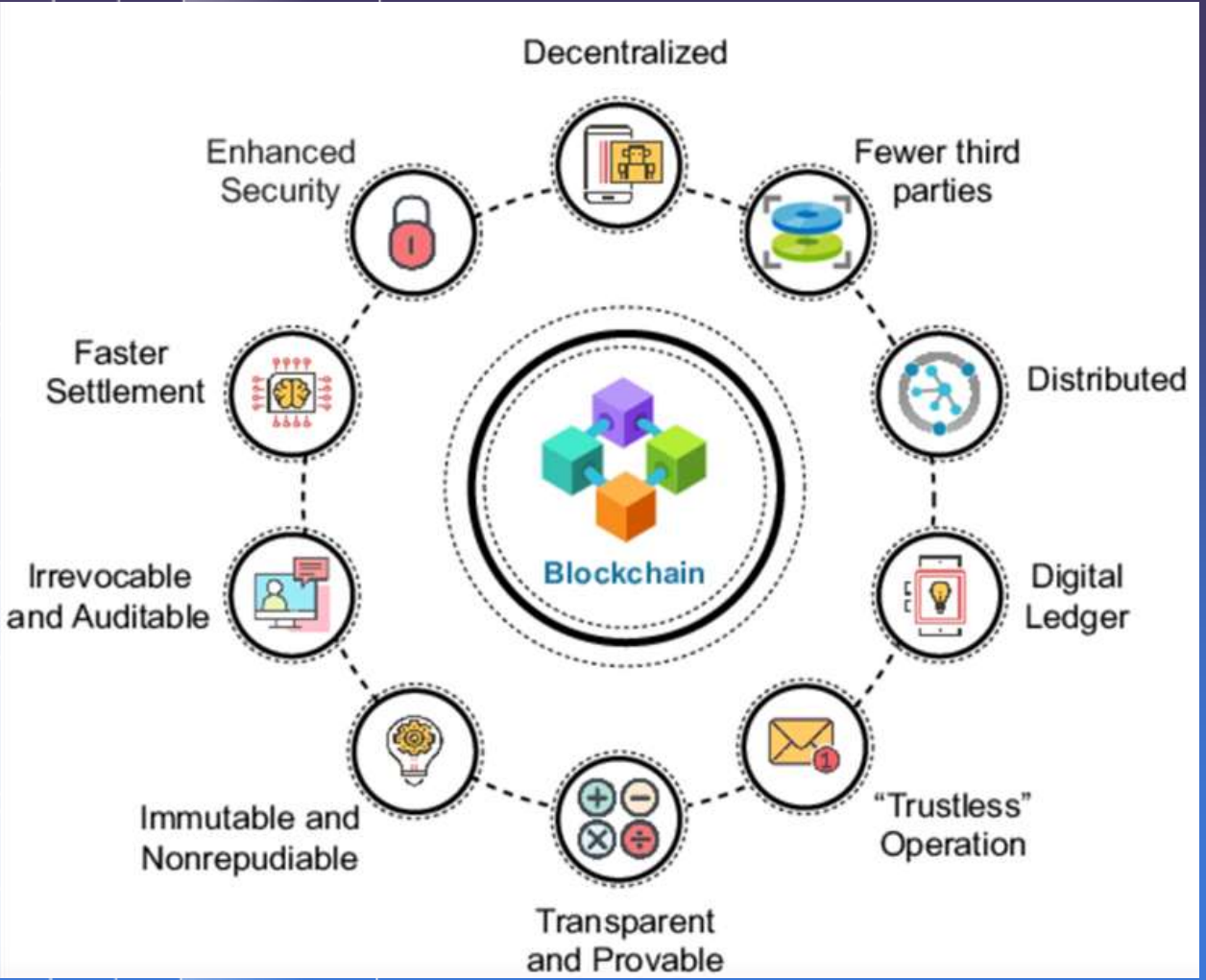
Cloud & Fog Computing:

Efficiently distributes computational tasks in vehicular networks.



04

Key Features of Blockchain For Automotives


Decentralized
Enhanced Security
Fewer third parties
Faster Settlement
Distributed
Blockchain
Irrevocable and Auditable
Digital Ledger
Immutable and Nonrepudiable
"Trustless" Operation
Transparent and Provable

Decentralization: Blockchain operates on a decentralized network of nodes, eliminating the need for a central authority.

Immutable Ledger: Once data is recorded on a blockchain, it becomes tamper-resistant and immutable.

Enhanced Security: Blockchain employs cryptographic techniques to secure data and transactions.

Transparency: Blockchain provides a transparent and auditable ledger, allowing all authorized parties to access and verify data.

Smart Contracts: Smart contracts are self-executing agreements that automate processes and transactions when predefined conditions are met.

Vehicular Ad-hoc Networks (VANETs)

1. VANETs are wireless communication networks designed for vehicles on the road.
2. Their main purpose is to enhance road safety and transportation efficiency.
3. VANETs use Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication modes.
4. Challenges include intermittent connectivity, security, and scalability.

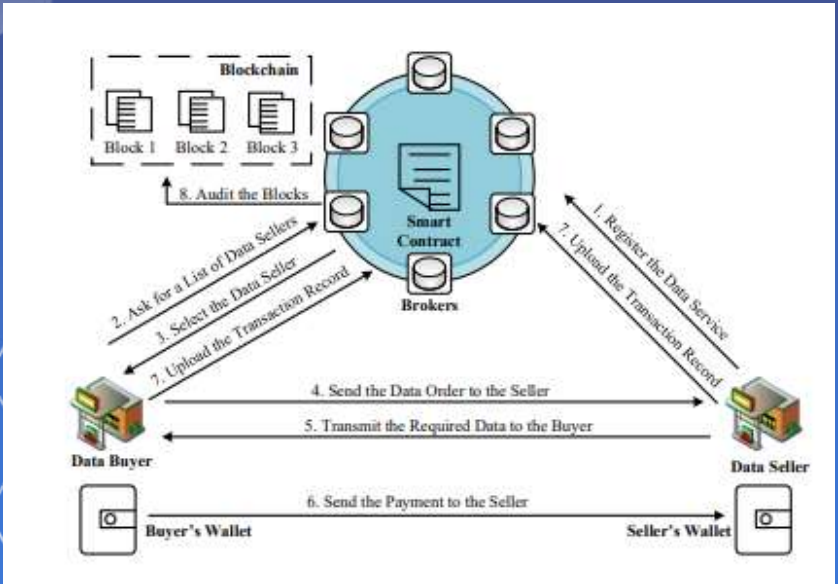
Mobile Ad-hoc Networks (VANETs)

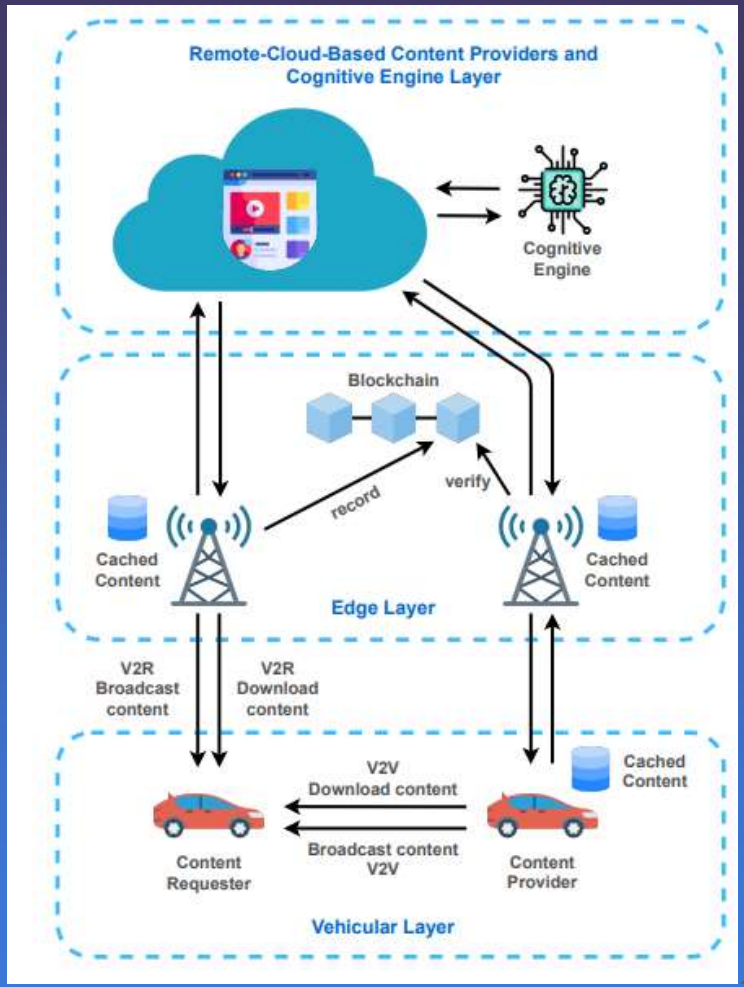
1. MANETs are decentralized wireless networks.
2. They have dynamic topologies and self-configure.
3. Nodes communicate wirelessly using specialized routing protocols.
4. Applications include military, disaster recovery, and IoT.

05

Use-cases & Applications

1. Secure Over-the-Air (OTA) Updates
2. V2V and V2I Communication
3. Supply Chain Transparency
4. Vehicle Identity and Access Control



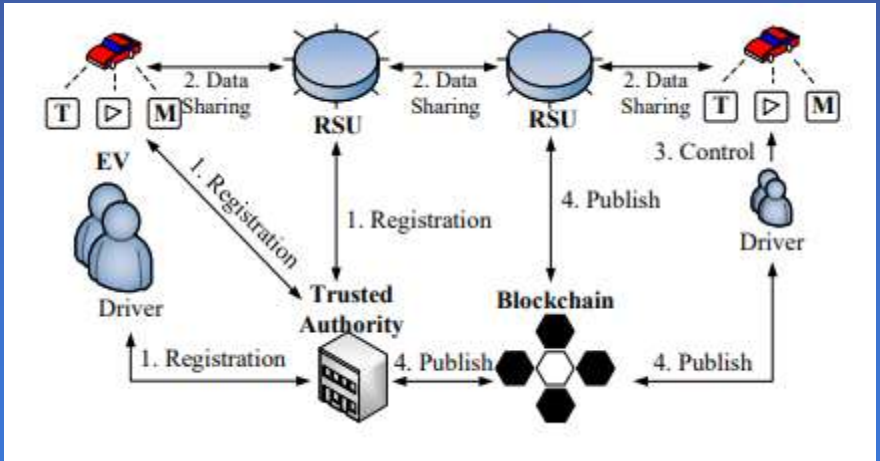


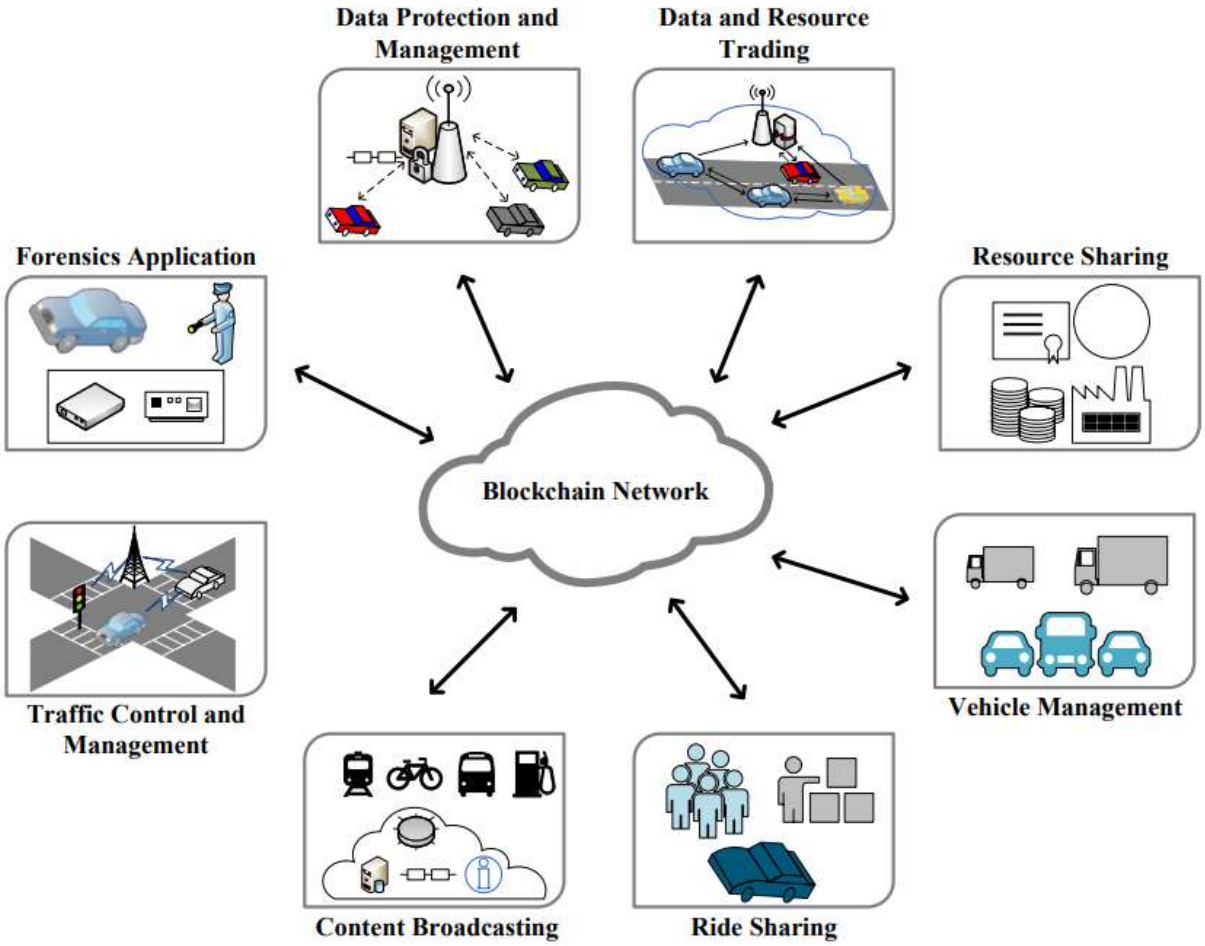
5. Automated Insurance Claims

6. Secure Data Sharing

7. Immutable Incident Records

8. Authentication and Authorization

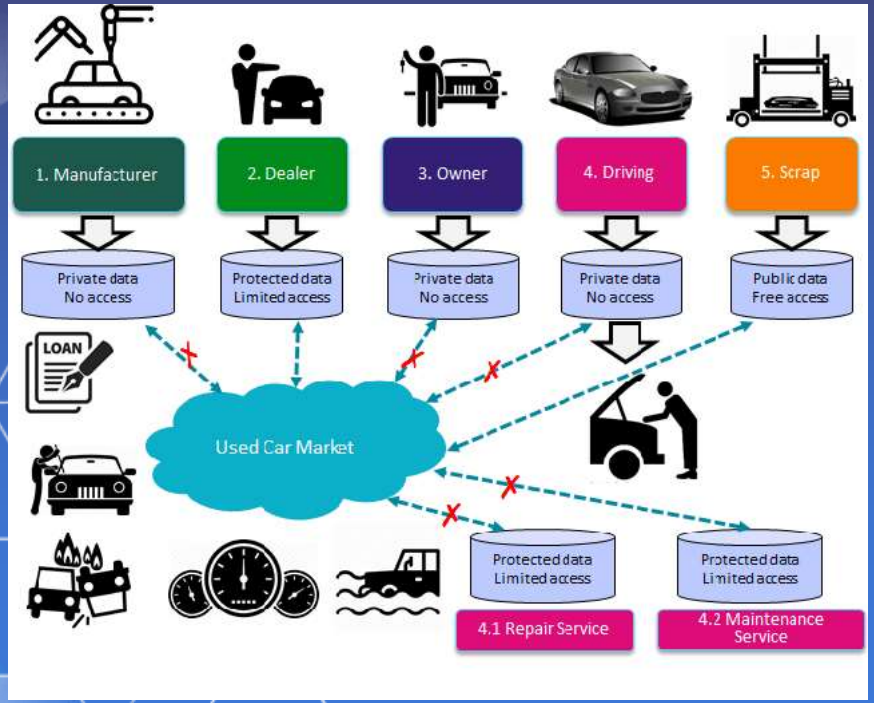



Data Protection and Management
Data and Resource Trading
Forensics Application
Resource Sharing
Blockchain Network
Traffic Control and Management
Vehicle Management
Content Broadcasting
Ride Sharing

07

Comparative Analysis & Case Studies

Summary comparison of previous survey articles on the A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry.



Stakeholder	Specific challenges
Car owners and lenders / buyers and sellers of pre-owned cars [127]–[129]	1) Lack of transparency regarding the car's history 2) Unpredictable car maintenance and repair costs 3) Lack of trust in the outcome of maintenance and repair jobs 4) Absence of informed buying options 5) Absence of car insurance options 6) Lack of trust in autonomous vehicles and IoT-connected vehicles 7) High-level transactional experience to consumers whilst reducing the costs incurred by them
Fleet management companies / Car leasing or sharing (car-sharing, ride-sharing or ride-hailing) companies [120], [130]	1) Lack of transparency regarding the car's history 2) Unpredictable car maintenance and repair costs 3) Lack of trust in the outcome of maintenance and repair jobs 4) Lack of interoperability with business partners 5) High operational costs, low margin 6) High costs in the car-sharing, ride-sharing and ride-hailing economy 7) Lack of trust in autonomous vehicles and IoT-connected vehicles
Car-sharing, ride-sharing or ride-hailing passengers [131], [132]	1) More affordable car rides 2) Better maintained cars 3) Lack of trust in autonomous vehicles and IoT-connected vehicles 4) Lack of a common mobility provider platform 5) Lack of instant payment
Car entrepreneurs [122], [130]	1) Expensive rates for car leasing and rental 2) Lower car-sharing, ride-sharing or ride-hailing partnership fees 3) Difficulties to set up business, unfair competition 4) Lack of trust in autonomous vehicles and IoT-connected vehicles 5) Lack of information sharing
Car dealers and retailers [122], [133], [134]	1) Updated car ownership records 2) Updated repair and maintenance records 3) Updated purchase records 4) Lack of trust in autonomous vehicles and IoT-connected vehicles 5) Lack of information sharing
OEM / Car manufacturers and suppliers [118], [122], [134]–[137]	1) Huge warranty claim costs 2) Enforcement of recommended maintenance and repair prices on the dealers 3) Customer complaints due to car dealers' violation of recommended maintenance prices set by car manufacturers 4) Lack of control of the car maintenance performed by authorized dealers 5) Weak customer loyalty 6) Cyber-attacks, system failure risks and enhanced security in autonomous vehicles and IoT-connected vehicles 7) Control of the logistics 8) Lack of information sharing
Insurance companies [138]–[140]	1) Inflexible and non-customized policy pricing 2) 5-10% of all claims worldwide are fraudulent [143] 3) Costly and inefficient claim management 4) Inaccurate customer policy pricing 5) Lack of oversight over the quality and pricing for a collision repair
Independent repair shops [129], [134]	1) Underutilized capacity 2) Customer retention 3) Low margins 4) Lack of brand confidence
After-market (producers, distributors and retailers of spare parts, garages) [134]	1) Inefficient stock management 2) Market for counterfeit spare parts 3) Lack of transparency in warranty monitoring and enforcement 4) Low margins 5) Lack of brand confidence

Ref.	Year	Federated Learning	Blockchain	IoVs Based on Federated Learning	IoVs Based on Blockchain	IoV Based on Blockchain-Enabled Federated Learning
[3]	2019	✓	✗	✗	✗	✗
[4]	2020	✓	✓	✗	✗	✗
[5]	2020	✓	✗	✴	✗	✗
[6]	2020	✓	✗	✗	✗	✗
[7]	2020	✓	✗	✗	✗	✗
[8]	2020	✓	✗	✗	✗	✗
[9]	2020	✗	✓	✗	✴	✗
[10]	2021	✓	✗	✗	✗	✗
[11]	2021	✓	✗	✗	✴	✗
[12]	2021	✗	✓	✗	✴	✗
[13]	2021	✓	✗	✗	✗	✗
[14]	2021	✓	✓	✗	✗	✗
[15]	2020	✗	✓	✗	✓	✗
Proposed	**2021**	✓	✓	✓	✓	✓

Summary comparison of previous survey articles on the Internet of Vehicles (IoVs). '✓' indicates that the topic is covered, '✗' indicates that the topic is not covered, and '✴' indicates that the topic is partially covered.

Algorithm 1: Pseudocode for the *Firmware Update* contract

```
1  contract FirmwareUpdate
2      mapping(address => int) Reputation
           // Mapping for distributors
           reputation
3      mapping(address => int) UpdatedAVs
           // Mapping for AVs with the No.of
           obtained updates
4      function FirmwareUpdate(_PK, _VK, _ACi,
         _Pi, X)
5          PK ← _PK // Proving Key
6          VK ← _VK // Verifying key
7          ACi ← _ACi // authentication code
8          Pi ← _Pi // ABE Policy
9          MaxUpdate ← X // Max. No. of download
               per Update
10     function RecieveProof(σagg, PK[ ], C[ ]
       keys[ ])
11         address [] RecievedAVs // Received AV
               list
12         for s ← 0 to PK.lengh do
13             if verifySig(pk_M, PK[s], C[s])
14                 return
15             end
16             if UpdatedAVs[PK[s]] > MaxUpdate
17                 return
18             end
19             hs ← H(keys[s])
20             CVs ← H(ACi, hs)
                RecievedAVs.push(Pairing(PK[s], CVs))
21         end
22         if Pairing(g1, σagg)=Prod(RecievedAVs)
23             UpdateReputation(msg.sender,
                PK.length)
24             for i ← 0 to PK.lengh do
25                 emitEvent("KeyRevealed", PK_i,
                    keys[i])
26                 UpdatedAVs[PK_i]←
                    UpdatedAVs[PK_i]+1
27             end
28         end
29     function UpdateReputation(Dist, N)
           // increase reputation distributors
30         Reputation[Dist]← Reputation[Dist]+=N
```

Algorithm 1: Pseudocode for the Firmware Update contract

Category	Explanation	Use cases
Static registry	Distributed database for storing reference data	• Proof of ownership • Traceability • Patents
Identity	Distributed database with identity related information	• Identity fraud • Identity records
Smart contracts	Trigger automated and self-executing actions when predefined conditions are met	• Insurance-claim payout • Cash-equity trading
Dynamic registry	Distributed database that is updated with asset transactions	• Supply chain • Fractional investing
Payment infrastructure	Dynamic distributed database that is updated with payment transactions	• Cross-border payments • Peer-to-peer payments • Insurance claims
Several categories	Use cases composed by several of the previous groups Standalone cases not fitting in any of the previous categories	• Initial Coin Offering (ICO) • Blockchain as a Service (BaaS)

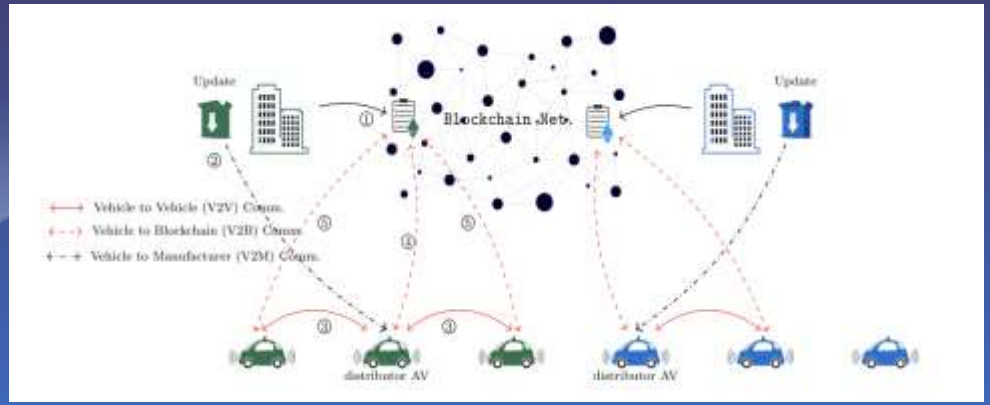
Case Studies:

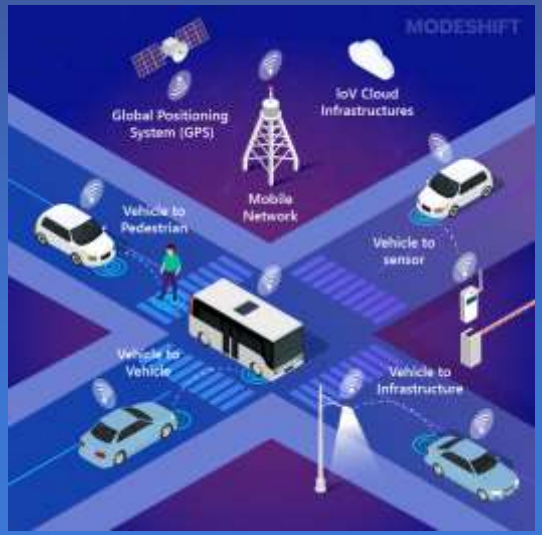
1. **Firmware Updates in Autonomous Vehicles**
2. **Federated Learning in IoV**
3. **Blockchain in Cyber-Physical Systems**
4. **Applications of Blockchain in IoV**

08

Future Prospects & Evolutions

1. IoT & AI Integration
2. Augmented Reality (AR) & Virtual Reality (VR) Integration
3. Supply Chain Transparency
4. Peer-to-Peer Models
5. Enhanced Security Frameworks

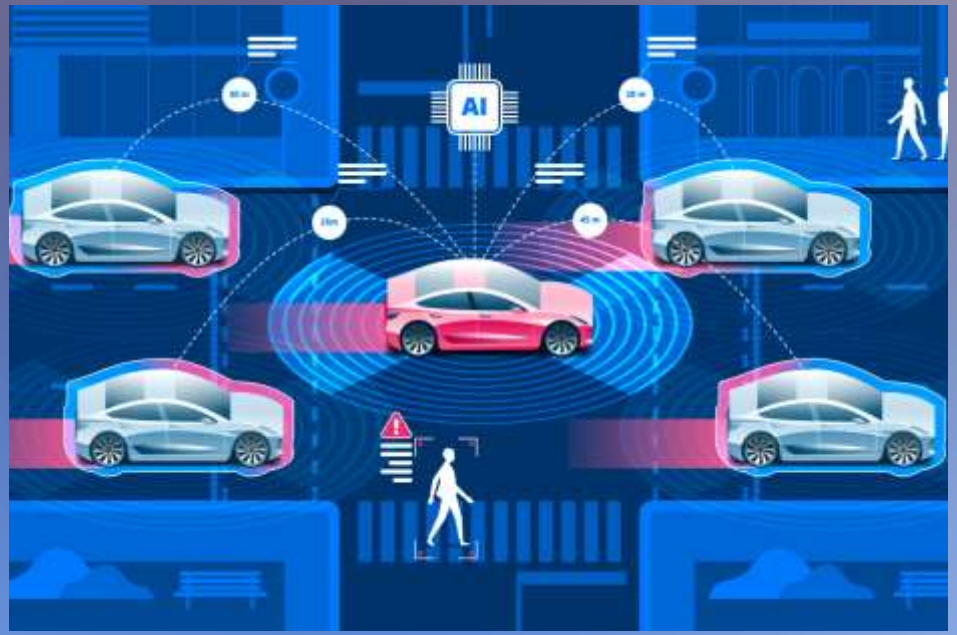




09

Conclusion & Call to Action

As vehicles evolve into more connected, intelligent entities, the synergy of blockchain and IoV will be instrumental in shaping a future of transportation that is not only smart and efficient but also secure and trustworthy.



THANKS