mp1:

The paper provides an overview of blockchain architecture and discusses various consensus algorithms used in different blockchains. It also explores the use of blockchain in cloud storage and the enhancement of security measures.

The paper mentions Ripple as a consensus set of regulations that uses collectively-relied on subnetworks in the big community. It also discusses Tendermint as a Byzantine agreement algorithm and private blockchain as a centralized network. It further discusses different categories of cloud services offered such as infrastructure, platform, and application.

[

2

]

The paper highlights the role of cloud service providers in establishing connections between the client's networks and their own data storage and backup systems. It also raises concerns about the involvement of a third party and the potential risks of data theft or tampering. It suggests that using blockchain technology can address these concerns.

[

3

]

The paper mentions the use of blockchain technology in various fields and services, such as financial markets, IoT, supply chain, voting, and storage. It also discusses the security issues associated with blockchain, including the risk of cybercrime.

[

4

]

The paper discusses the differences between public, private, and consortium blockchains in terms of read permission, immutability, and efficiency. It highlights the advantages of public blockchains in terms of transaction visibility and tamper resistance. It also mentions that private and consortium blockchains can be more efficient due to fewer validators.

mp2:

Blockchain technology offers considerable benefits in easing paperwork processing, identification of counterfeits and products, facilitation of origin tracking, and operationalization of the Internet of Things in supply chain.

Blockchain can be categorized into permissionless, permissioned, and private blockchains, with permissionless blockchains being fully public peer-to-peer networks and permissioned blockchains functioning as a federation. The concept of distributed ledger technologies (DLT) encompasses broader variations of blockchain.

[

3

]

Blockchain technology promises to address trust issues and enable secure and authenticated information exchange in supply networks, leading to rapid implementation of pilot projects and changes in the supply chain industry.

mp3:

Zhou et al. conducted a survey on the security and privacy concerns of cloud computing providers, focusing on availability, confidentiality, integrity, control, and auditing characteristics. They also discussed out-of-date privacy acts and problems related to multi-location storage.

Vaquero et al. provided insight into IaaS clouds security, categorizing security studies according to the Cloud Security Alliance (CSA) top threats to cloud computing. They analyzed security from the networking, virtualization, and physical sides of cloud IaaS networks.

Subashini and Kavitha studied the security of service delivery models in cloud computing, with a particular focus on the SaaS model. They also presented an overview of current security solutions reported in the literature.

Ahuja and Komathukattil presented a survey on common threats and associated risks to clouds, as well as approaches to tackle those threats and risks. They also discussed security models of leading cloud providers.

mp4:

The paper discusses the need for a data provenance framework in cloud computing and proposes BlockCloud, a blockchain-empowered data provenance architecture for the cloud computing platform. It also presents a proof-of-stake (PoS) consensus mechanism for BlockCloud to alleviate computational requirements.

[

1

]

The paper highlights the importance of accountability and auditability in cloud computing for maintaining provenance and mentions efficient logging techniques, data-integrity proofs, and checksumming as traditional methods.

[

2

]

It mentions that blockchain-based provenance creates a separate provenance layer in cloud systems, facilitating functionalities such as identity management, transaction tracking, and contract execution. The blockchain layer holds the provenance data, identity information, and executable contracts.

[

3

]

The paper discusses the validation process for ensuring the integrity of transactions in the blockchain. It mentions the reconstruction of the Merkle tree from transaction hashes and the comparison of the computed Merkle root hash with the hash of the leader's block.

[

4

]

The paper also mentions the application of blockchain technology in the electronics industry for cyber supply-chain provenance, addressing risks such as counterfeits, unauthorized production, tampering, and theft. It emphasizes the need for tools and technologies to provide provenance assurance in the cyber supply chain.