**LITERATURE REVIEW**

1. **Livepeer Project[1]**

In “Livepeer Project” they discuss a decentralized live streaming video protocol based on blockchain using “Ethereum”. The Livepeer project aims to deliver a live video streaming network protocol that is fully decentralized, highly scalable, crypto token incentivized, and results in a solution which is cheaper to an app developer or broadcaster than using traditional centralized live video solutions. Decentralized applications (DApps) to be built in the form of largely static or infrequently updated web or mobile content, but at the moment DApps still lack the ability to include streaming media and data in an open. and a decentralized way . As the “ Livepeer Project” claims, the goal of their project is to decentralize live video broadcast over the internet. Although it is a secure platform based on the International Journal of Computer Applications (0975 – 8887) Volume 183 – No. 16, July 2021 21 blockchain technology, “Livepeer Project” has not suggested any mechanisms to auditability and intrusion detection[1] .

1. **SteemQ[2]**

A decentralized platform for STEEM SteemQ is a still on-going project aligned with “Steemit” decentralized social network which is based on blockchain technology. SteemQ is proposed to be a decentralized video platform for user- generated content based next-generation platforms on top of the new Blockchain and P2P technologies. The blockchain of choice is STEEM. This allows the developers to build on top of the same technology that powers Steemit, as well as inherit the benefits of an existing community, currency and platform. All STEEM social network accounts are automatically SteemQ accounts and vice-versa. The system aims to empower its users to the maximum extent possible while remaining resilient. SteemQ says that it uses IPFS as a core building block of the content distribution system of their prototype. IPFS is a great tool that does a few things really well. It provides a robust layer for managing, transporting, referencing, deduplicating, versioning and ensuring the integrity of the content. SteemQ suppose that they can secure the multi hashes by storing them on the immutable blockchain (i.e. STEEM’s posts become immutable after the first reward payout. STEEM’s transfers are much faster, being immutable and permanent within seconds, when the block is confirmed). This way they suggest that they can simultaneously guarantee the ownership and integrity of the content [2].

1. **Prov Chain[3]**

A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability In this paper, researchers have presented a concept called “ProvChain”, a blockchain based data provenance architecture to provide assurance of data operations in a cloud storage application, while enhancing privacy and availability at the same time. ProvChain uses the construction of the merkle tree technology for the provenance of data. A list of blockchain transactions will be used to form a block and the block needs to be confirmed by a set of nodes in order to be included in the blockchain. An attempt to modify a provenance data record will require an adversary to locate the transaction and the block. Blockchain’s underlying cryptographic theory will allow modifying a block record only if the adversary can present a longer chain of blocks than the rest of miners’ blockchain, which is quite difficult to achieve [3]. As the “ProvChain” claims, the goal of their project is to improve the provenance of data in the IoT based cloud environments. Although it is a secure platform based on the blockchain technology, “ProvChain” has not suggested any mechanisms to auditability and intrusion detection.[3]

1. **Blockchain-Based, Decentralized Access Control for IPFS[4]**

The weaknesses of blockchain can be overcome by moving the files containing personal data off-chain. This ensures files can be deleted as required and are not causing the chain to grow excessively fast. However, for data sharing between organizations the assurance that files have not been edited or changed must be retained. Moreover the blockchain tracks which entities have access to which data. IPFS stores files in a distributed way by splitting them into chunks which can be requested and transferred between nodes. Each file is identified by its cryptographic hash. Doing so makes it easy to ensure one has received the correct data by generating the hash of the concatenated file chunks and checking if it matches the hash that was requested. IPFS hashes identifying files that contain personal data can be stored on the blockchain instead of the data itself. Doing so enables compliance with GDPR legislation. The blockchain containing the hash ensures that the file has not been tampered with. The file itself being stored in IPFS means it can be deleted as required, by nodes removing it from their local storage. The hashes of files can be used to associate files with owners and access permissions. Chain growth is reduced as hashes are generally smaller than the data they represent, if SHA256 is used the on-chain storage required for a file of any size becomes 32 bytes. As such chain growth is vastly reduced. Enforcing Privacy: IPFS is designed to share information as widely as possible and does not attempt to restrict connections or data flow between nodes. The scenario considered herein deals with private data. IPFS cannot be allowed to share files with any nodes that request them, it must only share files with those that have permission according to the permissions recorded on the blockchain. As such, the provided solution is a modified version of IPFS that uses a smart contract which is capable of adding, removing and updating file ownership and accesses. Entities are identified by their Ethereum public key and files are identified by their unique cryptographic hash. The combination of blockchain assurance and a private network capable IPFS allows for compliance with current data protection and sharing legislation and reduces the cost of doing so.

1. **Performance Analysis of High-Definition Video Call over Secure Real Transport Protocol (SRTP)[5]**

Several studies have analyzed the effects of implementing security protocols like SRTP on voice and video call performance. Ismail and Yahya conducted experiments comparing HD video calls over secure (using SRTP) and non-secure channels in both wired and wireless LAN environments. They measured key performance indicators including jitter, Mean Opinion Score (MOS), and R-Factor. Their results showed that while the secure channel had slightly higher jitter and lower MOS/R-Factor scores, the differences were minimal and call quality remained acceptable when using SRTP encryption.

These findings align with earlier work by Alexander et al. (2009)[6] who evaluated SRTP's impact specifically on VoIP performance. They found that SRTP added only "negligible overhead" and did not significantly affect VoIP quality metrics like packet inter-arrival time and jitter. Similarly, Adomkus and Kalvaitis (2008)[7] concluded that while SRTP could slightly degrade some VoIP performance parameters, its use was still "necessary" for voice encryption.

However, other researchers have observed more noticeable performance impacts from implementing call security. Sureshkumar and Dutta (2010)[8] measured increases in call setup time, memory utilization, and queue size when enabling security features for VoIP calls. Their work suggests that additional processing required for encryption/decryption can impact system resources and call initiation.

1. **P2P Media Streaming with HTML5 and WebRTC[9]**

The potential of WebRTC to support P2P streaming lies in its ability to establish direct communication between browsers using UDP-based protocols. This real-time communication can enable browsers to act as both content consumers and distributors, reducing the dependency on central servers. The application of WebRTC in video streaming, particularly VoD, could decentralize media distribution, thereby reducing infrastructure costs for service providers​.

One major performance bottleneck is the computational load associated with cryptographic hashing, such as the generation of MD5 hashes used to verify video file integrity. These operations consume significant CPU resources, which can slow down content delivery and affect the user experience, especially on devices with limited processing power. Performance comparisons between browser versions show a tenfold difference in handling MD5 computations​. Improvements in JavaScript implementations and potential standardization of more efficient hashing algorithms could address these issues.

The feasibility of implementing a P2P VoD service using HTML5 and WebRTC has been partially demonstrated through experimental setups. Initial results suggest that handling video streams on desktop and near-future mobile devices is achievable. Still, significant optimization is required to ensure seamless performance across various platforms​. HTML5’s built-in video elements, combined with the Offline Application Caching API, offer some flexibility by allowing videos to be stored and played even when the user is offline​.

1. **Development of a secure video chat based on the WebRTC standard for video conferencing [10]**

WebRTC is a standardized technology that enables real-time peer-to-peer communication, allowing browsers to exchange audio, video, and data without the need for additional plugins. Its primary advantage lies in the fact that it ensures security by using protocols such as Secure Real-Time Transport Protocol (SRTP) and Datagram Transport Layer Security (DTLS) for encryption and authentication​. These protocols play an essential role in protecting data transmissions, providing privacy, and preventing replay attacks.

The literature highlights the growing relevance of WebRTC in video conferencing applications due to its ability to turn browsers into fully-fledged video communication terminals. This has made WebRTC a crucial tool for modern communication, particularly because of its cross-platform nature and browser support, which eliminates the need for installing extra software​.

1. **Secure High Definition Video Conferencing [11]**

The Secure Real-Time Transport Protocol (SRTP) is a profile of RTP designed specifically to address security concerns in real-time media transmission. SRTP employs AES (Advanced Encryption Standard) for encrypting media payloads, ensuring confidentiality without compromising performance. Additionally, it uses Hash-based Message Authentication Codes (HMAC) to safeguard the integrity of RTP packets​.

However, SRTP requires a method for exchanging cryptographic keys, which is where the Multimedia Internet Keying (MIKEY) protocol comes into play. MIKEY allows secure key exchange during the media negotiation process, and its integration with SIP makes it an ideal solution for securing video conferencing sessions. MIKEY supports multiple authentication mechanisms, including pre-shared keys, public key encryption, and Diffie-Hellman key exchange, offering flexibility depending on the level of security required​

1. **Blockchain-Based E-Voting System[12]**

Blockchain's potential for e-voting lies in its ability to ensure:

* **Transparency**: Every vote can be recorded on a public ledger, which is immutable and verifiable.
* **Immutability**: Once votes are cast and added to the blockchain, they cannot be changed or deleted.
* **Security**: Blockchain’s decentralized nature reduces the risk of hacking or tampering, as an attacker would need to compromise a majority of nodes in the network.

The authors of the paper highlight several requirements for a blockchain-based e-voting system:

* **Voter Privacy**: The system must prevent any third party from linking a vote to the voter’s identity. Technologies such as Zero-Knowledge Proofs (ZKPs) are often proposed as a solution to achieve this​(Research-Paper-BBEVS).
* **Vote Verification**: Voters should be able to verify that their votes have been recorded correctly without revealing their identity.
* **Coercion Resistance**: The system must protect voters from being forced to vote in a certain way by an external party.
* **Decentralization**: No single entity should control the system; instead, multiple independent nodes should participate in verifying and recording votes .

1. **Blockchain Private File Storage-Sharing Method Based on IPFS[13]**

IPFS is a peer-to-peer file system that stores and shares files in a distributed manner. It uses content-based addressing to locate files based on their unique hash value rather than their physical location. This method increases data availability and reduces redundancy​. The integration of blockchain with IPFS enhances security by recording file metadata, including file hash and ownership, on the blockchain while storing the actual file on IPFS. This hybrid model ensures that the file content remains immutable and easily traceable without overburdening the blockchain with large amounts of data.

Blockchain-based decentralized file storage solutions, such as Storj and Filecoin, utilize IPFS for file storage and blockchain for maintaining metadata and incentives for storage providers. These systems demonstrate how blockchain can address issues of file integrity and ownership while ensuring scalability and accessibility .​

**REFERENCES**

[1] [D. Petkanics, "LivePeer Project overview," 2018.](https://github.com/livepeer/wiki/blob/master/WHITEPAPER.md)

[2] [Furion, "SteemQ - A Decentralized Video Platform for STEEM," 2016.](https://steemit.com/steemq/@furion/steemq-a-decentralized-video-platform-for-steem)

[3] [Data provenance assurance in the cloud using blockchain by Sachin Shetty, Val Red, Charles Kamhoua, Kevin Kwiat, Laurent Njilla . Proceedings Volume 10206, Disruptive Technologies in Sensors and Sensor Systems; 102060I (2017)](https://www.spiedigitallibrary.org/conference-proceedings-of-spie/10206/1/Data-provenance-assurance-in-the-cloud-using-blockchain/10.1117/12.2266994.short#_=_)

[4] [Blockchain-Based, Decentralized Access Control for IPFS Mathis Steichen, Beltran Fiz, Robert Norvill, Wazen Shbair and Radu State University of Luxembourg, SnT, SEDAN , The 2018 IEEE International Conference on Blockchain (Blockchain-2018)At: Halifax, Canada](https://www.researchgate.net/publication/327034734_Blockchain-Based_Decentralized_Access_Control_for_IPFS)

[5] [Performance Analysis of High-Definition Video Call over Secure Real Transport Protocol (SRTP) Nor Rahimah Ismail and Saadiah Yahya , Faculty of Computer Science & Mathematic, University Technology MARA, Shah Alam, Selangor](https://myjms.mohe.gov.my/index.php/dismath/article/view/13703)

[6] [An evaluation of Secure Real-Time Transport Protocol (SRTP) performance for VoIP](https://www.researchgate.net/publication/221204875_An_evaluation_of_Secure_Real-Time_Transport_Protocol_SRTP_performance_for_VoIP)

[January 2009 DOI:10.1109/NSS.2009.90 Source:DBLP](https://www.researchgate.net/publication/221204875_An_evaluation_of_Secure_Real-Time_Transport_Protocol_SRTP_performance_for_VoIP)

[Third International Conference on Network and System Security, NSS 2009, Gold Coast, Queensland, Australia, October 19-21, 2009](https://www.researchgate.net/publication/221204875_An_evaluation_of_Secure_Real-Time_Transport_Protocol_SRTP_performance_for_VoIP)

[Authors: Andre L. Alexander , Alexander L. Wijesinha , Ramesh K Karne](https://www.researchgate.net/publication/221204875_An_evaluation_of_Secure_Real-Time_Transport_Protocol_SRTP_performance_for_VoIP)

[7] [Adomkus, T. and E.Kalvatis, “Investigation of VoIP Quality of Service using SRTP Protocol”, Telekomunikacijų katedra, Kauno Technologijos Universitetas, 2008.](https://www.researchgate.net/publication/228760699_Investigation_of_VoIP_Quality_of_Service_using_SRTP_Protocol)

[8] [Sureshkumar V. Subramanian and Rudra Dutta, “Comparative Study of Secure vs Non-Secure Transport Protocols on the SIP Proxy Server Performance: An Experimental Approach”, 2010 International Conference on Advances in Recent Technologies in Communication and Computing](https://ieeexplore.ieee.org/document/5656775)

[9] [P2P Media Streaming with HTML5 and WebRTC Jukka K. Nurminen, Antony J. R. Meyn, Eetu Jalonen, Yrjo Raivio and Raul Garcıa Marrero, Department of Computer Science and Engineering, Aalto University, Finland](https://ieeexplore.ieee.org/document/6970739?denied=)

[10] [Development of a secure video chat based on the WebRTC standard for video conferencing Elena Revyakina1, Don State Technical University (DSTU), Rostov-on-Don, Russian Federation](https://www.e3s-conferences.org/articles/e3sconf/abs/2023/26/e3sconf_uesf2023_07017/e3sconf_uesf2023_07017.html)

[11] [Secure High Definition Video Conferencing , Master of Science Thesis , Guillem , Cabrera Añón](https://upcommons.upc.edu/handle/2099.1/5334)

[12] [Blockchain-Based E-Voting System By Friðrik Þ. Hjálmarsson; Gunnlaugur K. Hreiðarsson; Mohammad Hamdaqa; Gísli Hjálmtýsson](https://ieeexplore.ieee.org/document/8457919/authors#authors)

[13] [Blockchain Private File Storage-Sharing Method Based on IPFS Peng Kang, Wenzhong Yang , and Jiong Zheng](https://pubmed.ncbi.nlm.nih.gov/35890780/)