AN INVESTIGATION INTO A DISTRIBUTED DIGITAL EVIDENCE STORAGE SYSTEM FOR UK POLICE FORCES

ABSTRACT

This work explores the major distributed technologies that could help to secure digital forensics evidence systems due to issues seen with current storage methods for this type of data. It explores various distributed ledger technologies, including the blockchain, the Arweave blockweave and the Hedera hashgraph, as well as distributed storage methods and secure proofs. There are some identified weaknesses with that using a more open, honest and reliable distributed system would improve, but it was ultimately found that a customised system would need to be designed with all 43 police forces in a consortium, hosting distributed storage and ledger nodes between all departments within all forces.

1 INTRODUCTION

Over the last few years there has been exponential growth in technological developments, exemplified by the advancements in social communication and cloud storage; With this comes an increase in the volume and complexity of heterogeneous data sources, not just seen on a single device but distributed across various virtual and physical locations. This means that the amount of digital data being gathered as evidence by police forces is increasing, with more data being potentially relevant to ongoing investigations (Vaughan and Baker, 2020). Secure storage methods are essential to preserving the confidentiality, integrity and availability of evidence.

It has been reported that police forces are lacking in technological resources, using outdated and poorly made technology, faltering behind the technological evolution that criminals are embracing. This is highlighted within the UK, in which the 43 different police forces have leaders with differing priorities on governance, tools and processes that are used and are reluctant to share this information with other teams (Muir and Walcott, 2021).

The security implications of distributed ledger technology have the potential to improve the sharing and storage of confidential digital forensics evidence while still preserving security through the use of cryptographic functions and distributed technologies. This project intends to explore different elements and approaches of distributed technologies that will ensure a high level of data security for the exponentially increasing storage requirements for evidence.

1.1 PROJECT REQUIREMENTS

The appropriate solution will require:

- Confidential data storage,
- Proof that the integrity of the data hasn't been compromised,
- Availability of evidence at all times,
- Immutability of data storage location,
- Non-repudiation of the user performing an action on data.

2 DIGITAL FORENSICS CHALLENGES

Police forces across the world are implementing new tools for evidence gathering, including video feeds from CCTV systems, body cams, drones, as well as more private data including biometrics, social media communications, office documents and emails; All of this evidence needs to be stored securely and immutably, while also remaining persistent within the storage system for as long as required (Koh, 2021). The increase in the variety of sources of evidence in recent years drives the demand for digital forensic work by 11-16% and is projected to continue growing (Vaughan and Baker, 2020).

One of the core issues in modern forensics is with regards to the increasing storage capacity of devices such as mobile phones or personal computers, as well as the growth in the number of said devices (Lillis, Becker and Scanlon, 2016). This results in very large storage systems being required to store the ever-growing volume of evidence in a manner that preserves privacy for all involved. The current systems in place do not utilise a singular collaborative storage system for all police forces in the UK, hindering the sharing of digital evidence between each force, leading to a fragmented policing system (Muir and Walcott, 2021).

Cloud computing has become more prevalent over the last few years with both business and personal users adopting some form of cloud into their daily structure. Currently, 35 out of 43 of the police forces in the UK utilise the Fotoware Digital Evidence Management System, which is a central repository for evidence that is searchable and accessible on any device. This system stores all digital evidence for each force in a secured central location, allowing access from any device at any time and enabling information sharing at several levels between police officers, investigators and prosecutors of each region (Fotoware, 2021).

Cloud storage has been seriously discussed as the next stage for police forces to implement, diminishing the need for on-premises evidence storage with clear benefits for storing digital evidence, including the scalability, accessibility and flexibility that is inherent to the cloud attempting to keep up with the growing volume of evidence (Muir and Walcott, 2021). There are also some core issues that could render cloud unsuitable for police data, including the data being controlled by a centralised third party, high storage costs, a single point of failure and most notably the potential for a third-party provider being compromised by threat actors (Guardian, 2021)(Chopra, 2021).

3 DISTRIBUTED LEDGER TECHNOLOGIES

3.1 CORE ELEMENTS

Distributed ledger technology (DLT) is a system used to record the transaction of digital assets across a peer-to-peer (P2P) network of users managed by distributed nodes. Blockchain technology is the most common type of DLT in which transaction data is aggregated into a block, timestamped, and recorded in permanent and immutable blocks of data (Nakomoto, 2018).

3.1.1 PERMISSIONS

The most commonly seen distributed ledger networks follow a permissionless and public system that anybody can join and participate within freely. This ledger of transactions is public and open to all users of the system, which allows for an honest and auditable ledger. The other types of distributed ledgers are managed, which follow a permissioned and private system that only those authorised to can join. This breaks down into two categories, private and federated. In a private system, a single authority decides who can be a node and their level of access, whereas a federated ledger is governed by a group of organisations rather than just one entity (Wegrzyn and Wang, 2021).

3.1.2 CRYPTOGRAPHY

Cryptography is used for the verification of transactions and ensuring homogeneity across a cluster of nodes. The data required is stored within the header of each aggregate of transactions and utilises a hash tree to verify the contents of data structures (Nakomoto, 2018). The most common hash tree used in DLT is the Merkle tree, where each leaf of the tree represents a transaction hash. Each leaf is concatenated to another and hashed together to form a new hash value. This happens until a single hash value is formed, representing the state of all transactions as seen in figure 1 (Buterin, 2021).

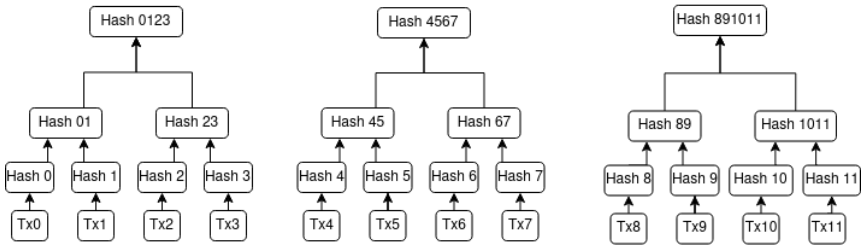

Figure 1: Merkle Tree Root Hash

3.1.3 CONSENSUS

Due to the lack of central governance in distributed ledger systems, a method of agreement between all nodes is essential to ensure consensus on the state of all transactions on the ledger (Aggarwal and Kumar, 2021). Public systems like Bitcoin and Ethereum utilise a trustless fault-tolerant mechanism, such as Proof-of-Work, in which a transaction is broadcast to all participating validator nodes and is aggregated into a block (Buterin, 2021). Each node performs validation of transaction data using an agreed-upon consensus mechanism (Castro and Liskov, 1999). If a majority of the nodes within the network agree upon a single homogenous state of the block, consensus will be achieved, the block will be appended to the ledger by the validator and all nodes will synchronise to the longest and most recent viable chain (Nakomoto, 2018). Private systems achieve consensus in a similar manner, but rather than all nodes having the potential to validate, only a preselected set of nodes are utilised (Bozkurt and Ucar, 2020).

3.2 DISTRIBUTED LEDGER STRUCTURES

3.2.1 BLOCKCHAIN

The most commonly incorporated structure is the linear blockchain, as seen below in figure 2, which creates an immutable cryptographic link from a new block to the existing chain of blocks (Nakomoto, 2018). This is used in many protocols, including Storj, Sia and Filecoin (Sia Docs, 2021) (Filecoin Docs, 2021) (StorjDocs , 2021).

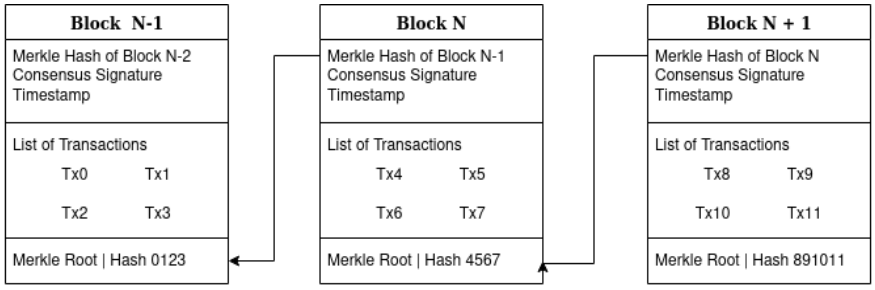

Figure 2: Structure of a Blockchain

3.2.2 BLOCKWEAVE

Arweave introduced a structure called a blockweave, which follows a graph-like structure, rather than linear. New blocks are linked to the previous block like traditional blockchains but also link to a secondary recall block from the history of the ledger to help provide unique consensus in Proof-Of-Access, demonstrated in figure 3 (Williams and Jones, 2019).

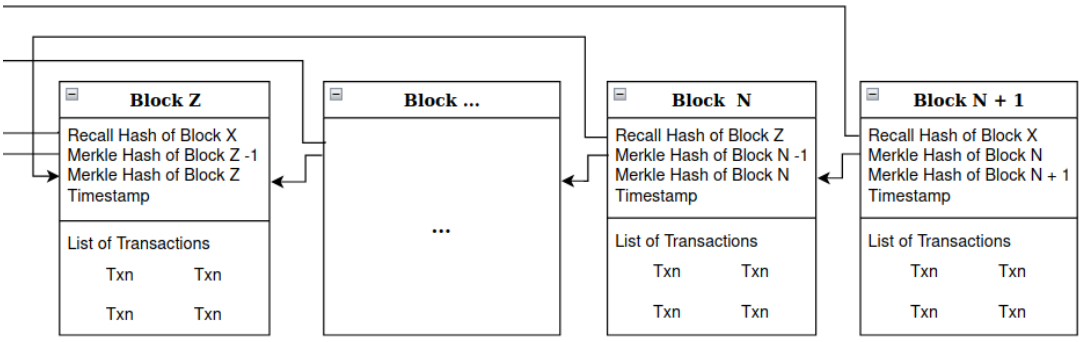

Figure 3: Structure of a Blockweave

3.2.3 HASHGRAPH

Hedera introduced a new structure, which improves upon the limitations seen with blockchain. Rather than each block of data being stored linearly and timestamped, the hashgraph structure enables multiple events, which are records of transactions, to be stored within a parallel structure (Hedera, 2021). Consensus is achieved via proprietary voting and gossip methods, improving scalability and lowering storage requirements (Khan, 2019).

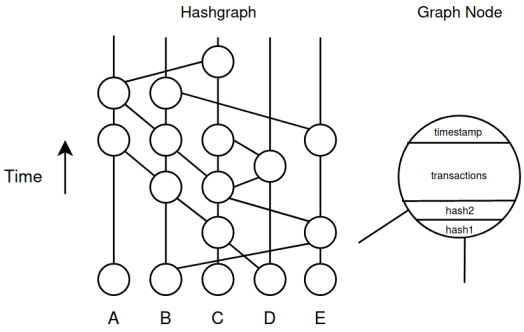

Figure 4: Structure of a Hashgraph

3.3 DISTRIBUTED DATA STORAGE

3.3.1 STORAGE SYSTEM

Within a blockchain, the blocks of data were designed to store the transaction metadata of digital assets; Each transaction requires a small storage capacity, evidenced by the 1MB Bitcoin blocks which are capable of storing many transactions per block (Croman and Decker, 2016). This enables an open and auditable system for the transaction of digital assets but is not suitable for storing mass amounts of data.

Current solutions such as Sia, IPFS and Storj focus on off-chain methods of storage and follow similar processes. The data being stored is sharded into many smaller segments, which are then encrypted using a symmetric key; This is stored on the client-side to ensure only they can decrypt the shards. These shards are distributed using a P2P protocol that matches the client with nodes that have excessive storage space and are looking to store data. Once stored, the location of where the shards are will be encrypted and uploaded onto a ledger, illustrated in figure 5 (Chopra, 2021); Due to the cryptographic functions in place, the client is the only entity that controls the keys and can decrypt the location of the shards to retrieve the data.

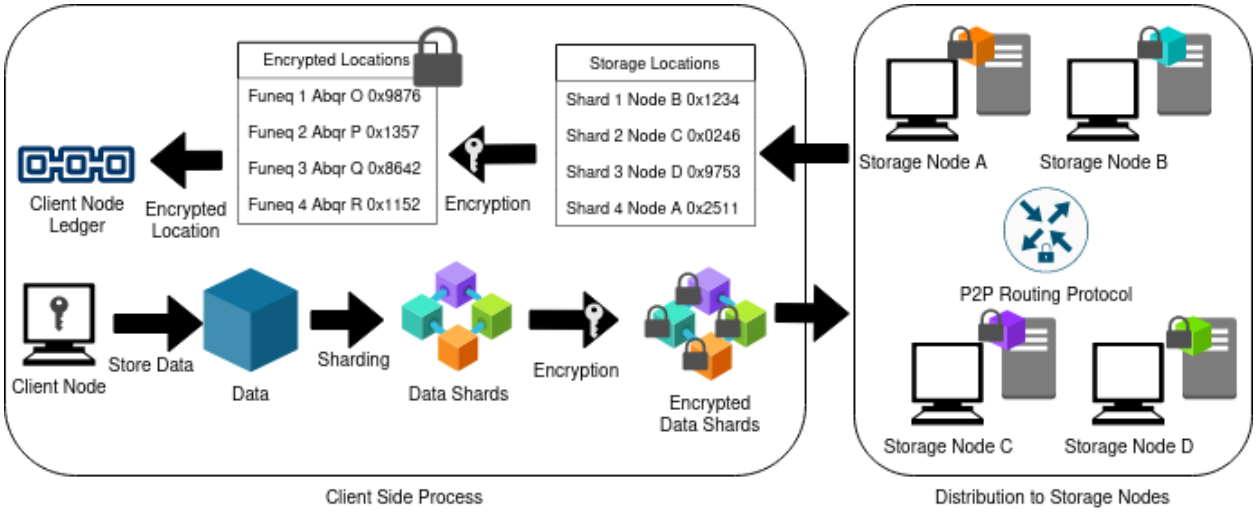

Figure 5: Off-Chain Data Sharding and Storage Upload.

3.3.2 STORAGE PROOFS

Distributed ledger data storage generally lives off-chain, which means that users require verification that enough nodes are storing the requested data completely and correctly. There are various methods currently being implemented in distributed storage projects including Filecoin's Proof-Of-Spacetime and Proof-Of-Replication, Sia's Proof-Of-Storage and Arweave's Proof-of-Access, which is incorporated into the consensus mechanism (Filecoin Docs, 2021) (Sia Docs, 2021) (Williams and Jones, 2019).

4 COMPARATIVE ANALYSIS OF DISTRIBUTED SOLUTIONS

An analysis of the different distributed solutions discussed within the literature review will be performed to assess the suitability of alternatives to store highly confidential digital evidence. (Sia Docs, 2021) (StorjDocs , 2021) (Swarm, 2021) (Williams and Jones, 2019) (IPFSDocs, 2021} (Daniel and Tschorsch, 2021).

4.1 LEDGER PERMISSIONS ANALYSIS

	Access	Identity	Management	Security	Speed	Availability
Permissionless	Anybody	Pseudonymous	Decentralised management	Consensus Mechanism	Slow	Open read/write
Federated	Multiple Groups	Known trusted participants	Semi-centralised management	Voting/ Multi-Party Consensus	Fast	Permissioned read/write
Permissioned	Singular Group	Known trusted participants	Central management	Voting/ Multi-Party Consensus	Fast	Permissioned read/write

Permissionless ledgers enable anybody to access, read and write to the ledger with a pseudonymous identity and are managed by an agreed-upon consensus mechanism. Permissioned ledgers are managed by a singular central entity deciding who can join, read and write to the ledger, utilising voting-based or multi-party consensus mechanisms. Federated ledgers are similar to permissioned ledgers but are controlled by many private groups sharing management of the ledger (Khan, 2019) Only known and trusted entities should be able to access the evidence ledger. A public ledger would be unsuitable due to the lack of confidentiality in which anybody can view the blocks on the ledger, whereas a federated ledger would ensure that only authorised groups can (Wegrzyn and Wang, 2021).

4.2 LEDGER STRUCTURE ANALYSIS

	Consensus	Scalability	Validation	Data Format
Blockchain	PoW, PoS, Voting Based, etc	100-10,000 Tx/S	Hash pointer to the previous block	Block
Blockweave	Proof-of-Access	~5,000 Tx/S	Hash Pointer to previous block and recall block	Block
Hashgraph	Gossip & Virtual Voting	~500,000 Tx/S	Gossiping to random nodes to share events	Event

Each proposed DLT uses consensus to ensure that the data is shared accurately. Consensus is required to create new data blocks or events, with blockchain ledgers using Proof-Of-Work, Proof-Of-Stake and Voting based mechanisms, whereas Blockweave uses the Proof-Of-Access consensus as discussed in section 3.2.2. Hashgraph uses a unique protocol of gossiping, and each gossip event is shared between two nodes as seen in figure 4 (Hedera, 2021). Hashgraph was deemed an unsuitable structure for the size of this project, as only 43 organisations will be using it and do not require the large transaction speed of roughly half a million Tx/s or the gossiping consensus model designed for decentralised projects.

4.3 DISTRIBUTED STORAGE ANALYSIS

	Sia	IPFS & Filecoin	Storj	Arweave	Swarm
Confidentiality	Threefish Symmetric Encryption	None	AES-256-GCM Encryption	AES-256-GCM/ Private key for Private Files	Modified Symmetric Block Cipher
Integrity	Proof-of-Storage	Content Addressing, Proof-of-Spacetime	Satellite Nodes, Proof-of-Storage	Blockweave/ Proof-of-Access	Content Addressing
Availability	Reed Solomon Erasure Codes, Replication & Incentives	Replication & Incentives through Filecoin	Reed Solomon Erasure Codes & Incentives	Blockshadow Replication & Incentives	Reed Solomon Erasure Codes, Replication & Incentives
Storage Format	Chunks	Blocks	Segments	Files	Chunks
File Lookup	Hash Pointer	Distributed Hash Table, Opportunistic	Central	Opportunistic	Distributed Hash Table

4.3.1 STORAGE SYSTEM ANALYSIS

Sia, Storj and Swarm make use of symmetric encryption algorithms to ensure high confidentiality and privacy of data once sharded into pieces. Integrity focused methods are integrated into the storage protocols to ensure that data has not been altered during storage; Swarm and IPFS utilise content addressing systems where changes to data result in a new storage address. Storj uses a centralised satellite node to act as a mediator between the storage nodes and the user.

One of the methods seen to be commonly used to increase the availability of the data is to create data redundancy to ensure that a single point of failure does not render the data inaccessible. Arweaves blockshadowing decouples transactions from blocks and replicates a ‘shadow’ of only a few kilobytes and can be used to reconstruct a block. Sia, Storj and Swarm make use of another redundancy approach, the Reed Solomon Erasure Encoding . This reduces storage overhead by encoding the data into the k, n erasure code in which there is n number of data shards and any k number of shards are required to recover the original chunks/segments of data (Ollo, 2018).

4.3.2 STORAGE PROOFS ANALYSIS

Filecoin, Sia and Arweave make use of data proof algorithms to enable integrity verification that large volumes of data are being retained accurately and correctly across the nodes. Filecoin utilises a Proof-of-Spacetime, which allows a node to verify storage space over a period of time, whereas projects like Sia and Storj uses a continuous check that the data is still being retained in the form of Proof-of-Storage (FilecoinDocs, 2021). Arweave’s unique blockweave and Proof-of-Access consensus ensure availability through the random historical recall block, which encourages storing as much data as possible for the greater potential to mine blocks and receive cryptocurrency incentives.

5 PROPOSED DISTRIBUTED SOLUTIONS

The proposed solutions aim to solve security and interoperability issues of regular third-party evidence management systems used by UK Police Forces. Solutions must follow the project requirements set out in section 1.1, which were analysed through a SWOT evaluation to explore each proposals strengths and weaknesses and how they can be used for or against them.

A federated ledger was chosen to implement the system as each member of the police force consortium will have read and write access to the immutable store of evidence. Making use of the semi-centralised structure will ensure that each authorised police force can store and access confidential case data but no one else. The blockweave structure was deemed to be the most suitable ledger structure to be used by a federated police evidence management system due to its inherent ability to promote immutable and integrity focused data retention for a longer period of time or even permanently. This is essential as fresh evidence is almost always required for a sentence appeal, and having an incomplete view of evidence has previously led to clear miscarriages of justice (Elks, 2008). The storage system being proposed is an on-chain system, making use of the federated permissions and the blockweave ledger structure to form a consortium derivative of the Arweave protocol. The blockweave network structure helps promote the availability of data through the Proof-of-Access consensus which requires recall to a random block in the ledger history, as well as Proof-of-Existence to prove that data is being retained by storage nodes. The data will be distributed via blockshadows to be shared at a highly compressed rate to all participating nodes, ensuring that data redundancy, thus availability is high.

5.1 FEDERATED PERMISSIONS SWOT ANALYSIS

SWOT Analysis of Federated Ledger	
Strengths	**Weaknesses**
1. Multiple diverse groups can form a central consortium. 2. Only permissioned members of these groups can join. 3. Increased translation speed compared to public ledgers. 4. Only requires small groups of validators to transact. 5. Cheaper transaction costs than public chains. 6. More energy efficient than costly Proof-of-Work.	1. Trust is required for the system to run smoothly. 2. The federated ecosystem is still in development. 3. Transaction speed varies by the number of nodes. 4. No decentralisation of the ledger. 5. Smaller number of nodes data availability concern.
Opportunities	**Threats**
1. High level of verification of data. 2. Offer a highly scalable solution. 3. Enable business interactions to be more efficient. 4. Allows for regulated systems that each group follows. 5. Can incorporate data confidentiality for all groups.	1. Trust is not inherent across organisations 2. If nodes are not active, Tx speed slows down. 3. Authorised nodes will be able to see all transactions. 4. Large groups of the consortium could combine to potentially alter a record.

5.2 BLOCKWEAVE LEDGER STRUCTURE SWOT ANALYSIS

SWOT Analysis of Blockweave Ledger Structure	
Strengths	**Weaknesses**
1. Providing a reliable record of transactions. 2. Proof-of-Access based on Proof-of-Work protocol. 3. Each transaction is cryptographically linked to a key. 4. Integrity through collision-resistant transactions. 6. Average speed of 5000 Tx/S. 7. High grade AES-256-GCM Symmetric Encryption	1. Data can never be deleted/edited from the ledger. 2. Lower confidentiality inherent to the system. 3. Consensus is designed for an open permanent web. 4. Lower Tx/S than Hedera. 5. The Proof-Of-Access consensus is based on energy-intensive Proof-Of-Work puzzle consensus.
Opportunities	**Threats**
1. Blockweave could offer a data chain of custody. 2. Incentivisation for the storage and serving of data. 3. Proof-of-Access encourages transaction data permanence and availability. 4. Persistence of long-term storage to be used in appeals. 5. Access control to enable key access for private files.	1. Smaller clusters of nodes may struggle over time to keep up with data demands. 2. Cryptographic vulnerabilities inherent to blockchains. 4. Users may be able to access data they are unauthorised to due to lack of access controls.

5.3 BLOCKWEAVE ON-CHAIN STORAGE SWOT ANALYSIS

SWOT Analysis of On-Chain Blockweave Storage	
Strengths	**Weaknesses**
1. Offering immutability of data. 2. Blockshadow enables compression and availability. 3. Provides Proof-of-Existence of a piece of data. 4. More reliable access to data than cloud services. 5. Use of Private Keys for Private Files 6. Stores file completely and holistically.	1. Data is stored in large blocks and is by default openly accessible to any participants of the network. 2. The blockshadows used for data replication are not sharded, providing a lesser element of confidentiality. 3. Evidence data cannot be deleted or altered on the permanent storage system.
Opportunities	**Threats**
1. Could provide access to evidence for new groups as agreed upon by the consortium. 2. Strong verification protocols to ensure data is being uploaded correctly and completely. 3. Large blocks of data can be distributed across the network in a few kilobyte blockshadow. 4. Data accuracy needed to verify evidence can be ensured through collision-resistant hashing algorithms (Scanlon and Kechadi, 2014).	1. Incorrectly entered evidence could threaten ongoing cases. 2. Concern about ever changing data protection regulations with regards to police retention. 3. Concern with non-essential evidence being collected and being immutably and permanently stored on the blockweave.

6 CONCLUSION

The current systems in place for digital evidence management in the UK relies upon either cloud storage or Fotoware which is a centralised project with minimal interoperability built in. There have been anecdotal instances of small groups of forces uploading their evidence to a Fotoware system making use of active directory services to enable access control to enforce trust. This enables better national cooperation by providing access to the same system, and can even have wide international implications in years to come (Koh, 2021).

The proposed system introduces many strong security protocols to ensure that data on the ledger cannot be altered and the data will remain persistent and available. The inherent cryptographic protocols utilised in blockchain technology such as the public/private key encryption, as well as the federated permissions means that the evidence being uploaded is seen to be confidential as only those authorised to access it are able to. The data integrity for the transactions in each block is provided through the use of Merkle Root Trees, as well as using cryptographic blockshadows to enable an exact replication of the block. Proof-Of-Access and Proof-Of-Existence provides the system with a higher level of availability and integrity in that the nodes are incentivised to store the data for as long as possible as part of the consensus mechanism, and store the data accurately as well.

Although the solution provided will certainly focus on improving the data security for specific elements, there are also weaknesses to using this system that need to be highlighted. The current Blockweave - Proof-of-Access combination encourages data to be stored permanently. The issue with using a data permanence storage solution for digital forensics data is the length of time certain data should be retained, as although some data will and should be kept for future investigations, most of the data being stored will be irrelevant and introduces concerns with data privacy and GDPR regulations. As data regulations are constantly being altered and updated, new regulations could cause issues with the permanence of this solution.

Solutions designed for a niche consortium of groups should not be designed based on protocols and elements of projects designed for the open sharing of data. The desired solution for this project would be a custom-built solution inspired by other technologies and designs that enables data records to be stored for as long as required. This would need to be worked in a completely collaborative manner with the 43 Police Forces in the UK to ensure that the solution is effective and certain measures such as data access and retention are discussed and implemented correctly while still preserving the security of the data.

7 BIBLIOGRAPHY

Vaughan, J. and Baker, N., 2020. *Digital Forensic Science Strategy.* [online] npcc.police.uk. Available at: <https://www.npcc.police.uk/Digital%20Forensic%20Science%20Strategy%202020.pdf> [Accessed 25 November 2021].

Muir, R. and Walcott, S., 2021. *Unleashing the value of Digital Forensics*. [online] police-foundation.org.uk. Available at: <https://www.police-foundation.org.uk/2017/wp-content/uploads/2010/10/value_of_digital_forensics.pdf > [Accessed 25 November 2021].

Nakomoto, S., 2018. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [online] ussc.gov. Available at: <https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf> [Accessed 25 November 2021].

Buterin, V., 2021. *Ethereum Whitepaper*. [online] ethereum.org. Available at: <https://ethereum.org/en/whitepaper> [Accessed 26 November 2021].

Aggarwal, S. and Kumar, N., 2021. Consensus mechanisms. *Advances in Computers*, pp.211-226.

Castro, M. and Liskov, B., 1999, February. Practical byzantine fault tolerance. In *OSDI* (Vol. 99, No. 1999, pp. 173-186).

Williams, S. and Diordiiev, V., 2019. *Arweave Yellowpaper*. [online] Arweave.org. Available at: <https://www.arweave.org/yellow-paper.pdf}> [Accessed 27 November 2021].

Wegrzyn, K. and Wang, E., 2021. *Types of Blockchain: Public, Private, or Something in Between*. [online] Foley. Available at: <https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between> [Accessed 27 November 2021].

Chopra, T., 2021. *SDC2021: Analysis of Distributed Storage on Blockchain*. [Youtube] Available at: <https://www.youtube.com/watch?v=gVYXeCVhA1c> [Accessed 28 November 2021].

SiaDocs. 2021. *Sia Docs*. [online] Available at: <https://support.sia.tech/get-started-with-sia/intro> [Accessed 28 November 2021].

FilecoinDocs. 2021. *How Filecoin Works*. [online] Available at: <https://docs.filecoin.io/> [Accessed 28 November 2021].

IPFSDocs. 2021. *IPFS Documentation*. [online] Available at: <https://docs.ipfs.io> [Accessed 28 November 2021].

StorjDocs. 2021. *What is Storj DCS*. [online] Available at: <https://docs.storj.io/dcs}> [Accessed 28 November 2021].

Croman, K. and Decker, C., 2016. On Scaling Decentralized Blockchains. *Financial Cryptography and Data Security*, pp.106-125.

Scanlon, M. and Kechadi, T., 2014. Digital Evidence Bag Selection for P2P Network Investigation. *Lecture Notes in Electrical Engineering*, pp.307-314.

Koh, E., 2021. *How 4 UK Police Forces Centralized their Digital Evidence Management*. [online] Fotoware.com. Available at: <https://www.fotoware.com/blog/how-4-uk-police-forces-centralized-their-digital-evidence-management> [Accessed 15 December 2021].

Lillis, D., Becker, B. and Scanlon, M., 2016. *Current Challenges And Future Research Areas For Digital Forensic Investigation*. [online] Markscanlon.co. Available at: <https://markscanlon.co/papers/CurrentChallengesAndFutureResearchAreas.pdf> [Accessed 16 December 2021].

Fotoware. 2021. *Digital Evidence Management from FotoWare*. [online] Available at: <https://www.fotoware.com/en/digital-evidence-management-system}> [Accessed 18 December 2021].

Guardian. 2021. *US Amazon web services outage*. [online] Available at: <https://www.theguardian.com/technology/2021/dec/15/amazon-down-web-services-outage-netflix-slack-ring-doordash-latest> [Accessed 18 December 2021].

Bozkurt, A. and Ucar, H., 2020. Blockchain Technology as a Bridging Infrastructure Among Formal, Non-Formal, and Learning Processes. *Blockchain Technology Applications in Education*, pp.1-15.

Hedera. 2021. *Hello future* . [online] Available at: <https://hedera.com}> [Accessed 18 December 2021].

Khan, F., 2019. *What are the different types of DLTs & how they work? | DataDrivenInvestor*. [online] DataDrivenInvestor. Available at: <https://www.datadriveninvestor.com/2019/02/14/what-are-the-different-types-of-dlts-how-they-work/> [Accessed 19 December 2021].

Swarm, 2021. S*warm | storage and communication infrastructure for a self-sovereign digital society* [online] Available at: <https://www.ethswarm.org/swarm-whitepaper.pdf> [Accessed 19 December 2021].

Daniel, E. and Tschorsch, F., 2021. *IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks*. [online] arXiv.org. Available at: <https://arxiv.org/abs/2102.12737v2> [Accessed 23 December 2021]

Ollo, J., 2018. *Replication is bad for storage: Erasure codes for fun.* [online] Storj.io. Available at: <https://www.storj.io/blog/replication-is-bad-for-decentralized-storage-part-1-erasure-codes-for-fun-and-profit> [Accessed 27 December 2021].

Elks, L., 2008. *Righting Miscarriages of Justice?*. [online] JUSTICE. Available at: <https://justice.org.uk/righting-miscarriages-of-justice> [Accessed 30 December 2021].