An Overview of Blockchain Technology for Intellectual Property Management

Ikram Asghar, Oche A Egaji, Mark G Griffiths
The Centre of Excellence in Mobile and Emerging Technologies,
University of South Wales, Pontypridd, United Kingdom
ikram.asghar@southwales.ac.uk, alexander.egaji@southwales.ac.uk,
mark.griffiths@southwales.ac.uk

Abstract. Blockchain is a distributed digital ledger of cryptographically signed transactions grouped into a chain of blocks. The emergence of Blockchain has changed how information can be stored and processed securely. The research interest in Blockchain has significantly evolved as the technology has found applications beyond the finance industry. Blockchain has gone beyond the simple financial transaction application to include being used to securely share patient records, smart contracts, digital identity, and assets management. As the technology evolves, more and more industrialists and researchers explore its potential use in managing intellectual property. This paper explores the feasibility of adopting Blockchain for IP management, highlighting potential challenges and possible solutions.

Keywords: Blockchain, Smart Contract, IP Management, Consensus Mechanism, Mining.

1 Introduction

Distributed Ledger Technology (DLT) is essentially a decentralised database with no centralised administrator, usually maintained by multiple participants across the various nodes. Individual nodes can process and verify the validity of every item before creating a consensus among all participating nodes. DLT can record either static data, such as a registry or dynamic data, such as bank ledger/transactions. The types of DLT include Blockchain, Tangle, and Hashgraph. The most common among them is Blockchain, which is the technology that underpins cryptocurrencies such as Bitcoin and Ethereum. The term DLT and Blockchain are used interchangeably; however, DLT is the framework that formed the basis of Blockchain technology.

Blockchain is a distributed digital ledger of cryptographically signed transactions grouped into a chain of blocks. An individual block in the chain is linked to the previous block using a cryptographic hash function after it has been validated and undergone a consensus decision among participating nodes. New blocks are distributed across copies of the ledger within a network of participating nodes, and all conflicts are resolved via established principles. The chain continuously grows as new blocks are added, making the older blocks more challenging to modify. This functionality enables peer-to-

peer transactions and trust among users, eliminating the need for intermediaries. Resultantly, the Blockchain network is considered secured. The emergence of Blockchain has changed how information can be stored and processed securely.

Furthermore, Blockchain has gone beyond the simple financial transaction application to include being used to securely share patient records, smart contracts, digital identity, and asset management. Authors such as [1] have proposed an IP copyright protection algorithm to address traditional IP copyright management technology issues. The current state of the art, such as the i-Depot offered by the patent office, provides a centralised solution [2]. This solution has not tampered with proof as it relies on an individual institution that has to serve as the sole administrator. This paper explores the feasibility of adopting Blockchain for IP management, highlighting the potential challenges and possible solutions.

2 Research Methodology

The systematic research process used for this study is summarised in Figure 1. The research started with a broader area to identify relevant research gaps for Blockchain-related studies in current literature. Once the scope was identified for Blockchain and IP management, some keywords were also identified, which helped generate a search string. The search string elicits more studies from the top five academic databases, namely, IEEE, Sciencedirect, ACM, Scopus and Web of Science. Then critical studies are explored in detail to identify potential off the shelf solutions. These solutions are compared against commercially available Blockchain technologies, which help identify challenges with the current solutions. The research process completes with some conclusions of the study.

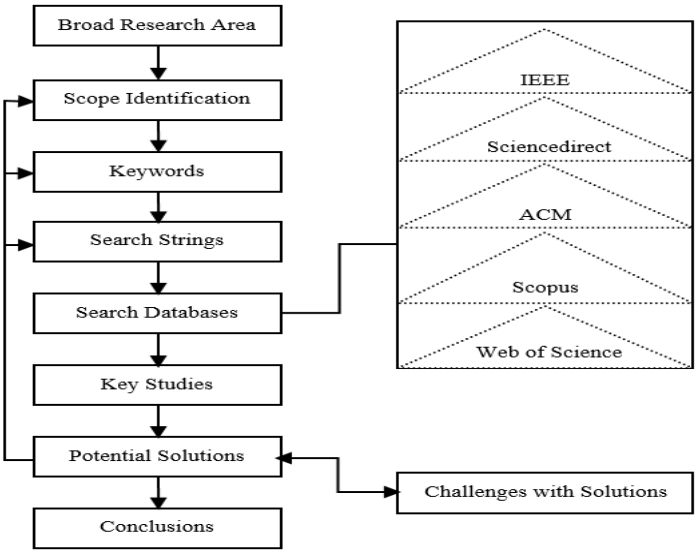

Fig. 1. Research Process Used for the Study

3 Literature Review

3.1 Blockchain

The first block in the Blockchain is called the genesis block, as it has no parent node. As shown in Figure 2, a block in the chain consists of a header and body. The block header includes block version (validation rule of the chain), Merkle tree (hash value of the transaction), timestamp (time in seconds), nBits (target threshold below which a block is valid), nonce (32-bit number updated for the hash calculation, usually starts from 0) and parent/previous block hash (256-bit hash value of the last block) [3]. Data types such as cryptocurrency transactions, contractual information, photos, videos and design documents can be added to the Blockchain. However, this is highly dependent on the Blockchain platform, e.g., there is a 1MB data storage limit per block in Bitcoin. Ethereum, on the other hand, has no limitation for direct file storage; however, it is not suited for large file storage, as this can affect performance. Most Blockchain applications built to support the proof of the existence of a document/Intellectual Property (IP) rely on the cryptographic hash value of the document, which is stored in the Blockchain at inception, and the actual document is encrypted before storing in a secure database. This is possible because Blockchain allows the users to add a message (payload) when processing a transaction, similar to adding a reference number to a bank payment [4].

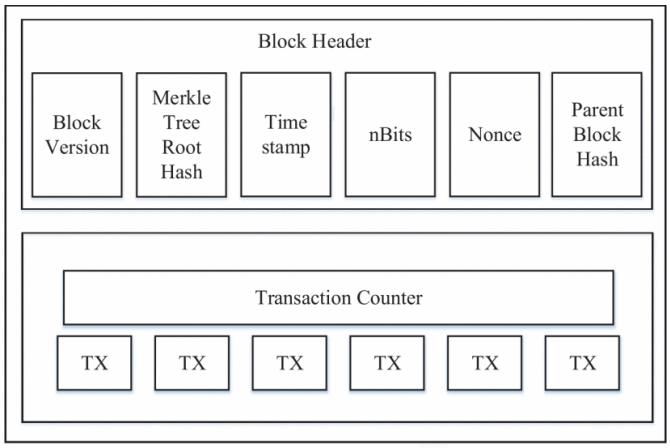

Fig. 2. Block Structure [4]

The Secure Hash Algorithm (SHA) with a fixed output string length of 256 bits (SHA-256) is the Blockchain's most commonly used cryptographic hash function. SHA-256 is a mathematical algorithm that takes a block of digital data as input and returns an output fingerprint (a message digest) of the data called a hash. The hash function will always give the same output for the same input. The SHA-256 is not an encryption algorithm, as it only computes a non-reversible hash value based on the input data (messages). Hence, it is essentially a one-way method [5, 6].

Blockchains are categorised based on the applied permission model of who can publish to the network. These categories can be Public, Private, Community/Consortium,

and Hybrid Blockchain. The Public Blockchain allows anyone to read and broadcast a transaction to the network. The Private Blockchain enables an organisation or subsidiary to read and publish to the Blockchain within the same group. The Community/Consortiums allow multiple groups from different organisations to form a consortium to write and post to the Blockchain. The Hybrid Blockchain combines any three (Public, Private and Community or Consortium) [7].

These categories of Blockchain can be further categorised as permissionless, permissioned or hybrid Blockchain, based on the need for authorisation. If anyone can join and publish to the network, it is called a permissionless Blockchain. However, if only a selected few can read or publish to the Blockchain, it is called a permissioned Blockchain, and a combination of both is the hybrid Blockchain. This implies the Blockchain can be configured to be permissionless for specific individuals and permissioned for others, depending on the central authority's level of control/oversight [8].

3.2 Consensus Mechanism

These are security protocols utilised by Blockchain to achieve agreement among multiple systems. There are various consensus mechanisms; however, this section focuses on the Proof of Stake (POS) and Proof of Work (PoW) consensus mechanisms commonly used in Ethereum and Bitcoin.

The Proof of Work (PoW) consensus mechanism is used by bitcoin to confirm transactions and create new blocks in the Blockchain. Particular nodes called miners with high computing resources create new blocks on the chain via mining. The miners compete to solve a computationally intensive puzzle to publish a block and be rewarded. The miners attempt to find the nonce with a hash value lower or equal to the difficulty level set by the network. The set difficulty level (the required number of zeroes at the beginning of the hash string) creates an average of 10 minutes between block creation. The miners can only update the 32-bit nonce in the block header to produce an acceptable 256-bit hash value. There are approximately 4 billion possible nonce-hash combinations to be mined before the correct nonce can be found. When the miner finds the correct nonce, they update the block and quickly broadcast their solution to the network. The puzzle is challenging to compute, but it is easy to verify the solution. This allows all other miners/nodes on the network to validate any proposed new block before adding it to the chain. The block will be rejected if the solution does not satisfy the puzzle. The POW consensus model is a resource-intensive and expensive process that results in an enormous waste of energy [8].

The Proof of Stake (POS) is an alternative consensus mechanism developed to mitigate POW's enormous waste of energy while retaining its positive attributes. The POS model is based on the premise that users are more likely to keep the system running according to protocol specifications based on the significance of their stake in the system. This is because the value of their stake can significantly diminish if users lose trust in the system. Hence, the likelihood of users publishing blocks to the chain is connected to the ratio of their stake to the overall stake in the network. The stake is usually the amount of cryptocurrency the user possesses in the network, and once staked, the user cannot spend the cryptocurrency [8, 9].

3.3 Blockchain Platforms

The Bitcoin platform launched in 2009 was the first decentralised digital cryptocurrency to revolutionise peer-to-peer money transfer without a central authority. The Bitcoin platform paved the way for the development of other Blockchain platforms. A typical Blockchain platform consists of the Cryptographic Services, Blockchain Runtime Environment, Blockchain Memory Store, Blockchain Secondary Storage, Smart Contract Module, Consensus Protocol Module and Blockchain Service Layer.

A Blockchain platform can be Stateless or Stateful depending on the smart contract functionality. The Stateless Blockchain platform primarily focuses on publishing transactions to the chain and has some other Blockchain functionalities. The architecture is independent of the smart contract logic layer. The Stateful Blockchain architecture consists of the smart contract and the other Blockchain functionality in the logic layer [7]. Some of these platforms are open-source; hence, the smart contract functionality can be built on a stateless Blockchain. However, it might not be as efficient as Stateful platforms specifically designed to incorporate smart contracts in their logic layer. The various Blockchain platforms available and their technical specifications are shown in Table 1.

Table 1. Blockchain Platform Specification [7]

No.	Blockchain	Start Year	Private/Public/ Consortium/ Hybrid	Permissionless/ Permisioned/ Hybrid	Consensus Mechanism	Statlessess /Stateful
1	Bitcoin	2009	Public	Permissionless	Proof of Work (PoW)	Stateless
2	Ethereum	2015	Public	Permissionless	PoW/ Proof of Stake (PoF)	Stateful
3	Hyperledger fabric	2016	Consortium	Permissioned	Supports pluggable consensus like Practical Byzantine Fault Tolerance (PBFT), Raft, Pow, PoS	Stateful
4	Corda R3	2015	Consortium	Permissioned	Validity consensus, Uniqueness Consensus, pluggable consensus	Stateful
5	Quorum	2016	Consortium	Permissioned	QuorumChain pluggable consensus (PoS, Raft, Istanbul-BFT)	Stateful
6	IOTA	2015	Public	Permissionless	PoW	Stateless
7	Ripple	2012	Consortium	Permissioned	XRP Ledger	Stateless
8	Kadena	2016	Hybrid	Hybrid	Consensus Protocol	Stateful
9	Tezos	2018	Public	Permissioned	BFT Raft, ScalableBFT	Stateful
10	Sawtooth	2016	Hybrid	Hybrid	Proof-of-Stake	Stateful
11	NEM	2015	Hybrid	Hybrid	Pluggable consensus algorithms – Proof of Elapsed Time (PoET), PBFT	Stateless
12	MultiChain	2015	Private	Permissioned	Proof of Importance	Stateless
13	HydraChain	2016	Hybrid	Hybrid	PoW	Stateful
14	BigChainDB	2016	Hybrid	Hybrid	PBFT	Stateless
15	OpenChain	2015	Hybrid	Hybrid	BFT	Stateless

3.4 Smart Contracts

The smart contract is "a computerised transaction protocol that executes the terms of a contract" [10]. They aim to automate the execution of contractual agreements at a low transaction fee when the predefined conditions are met without the need for a third party. The concept of a Smart Contract has extended the application of Blockchain technology [11]. Smart contracts have unique primary addresses on the Blockchain network and can be triggered when transactions are addressed to them. Smart contracts are executed by nodes in the network and must be deterministic. Hence, the execution outcome should be similar for all nodes in the network, and the outcome of the execution are stored in the Blockchain [8, 12, 13].

Smart contracts are limited to machine-readable terms as no artificial intelligence is involved. Hence, it works better with conditions affecting numbers without any need to translate natural language into codes. Smart contracts are classified into 'smart contract code' and 'smart legal contract' [14]. The smart contract code is a collection of executable codes that have been verified and deployed on the Blockchain. A smart contract code's ability depends on the technical features of the Blockchain upon which it is implemented and the programming language used to express the contract. The smart legal contract applies the technology to complement or substitute legal contracts. This does not necessarily mean all aspect of the contract is presented in a computer programmable format. Instead, it does suggest that all parties involved have decided that some elements of the key terms will benefit from being represented in computer programming format [13]. The ability of the technology to create binding legal agreements is dependent on the existing legal framework and how the legal, political and commercial institutions decide to adopt the technology. The practicality and usefulness of any smart legal contract are dependent on three factors [14].

- Trust the users have in the technology
- Legislatures that recognise the adoption of the technology
- Interpretable by the courts

The misgivings amongst policymakers/regulators due to Blockchain's association with Bitcoin (and its association with money laundering) affect users' trust in the technology. Blockchain's use in dubious trading sites and the need to write legislation to accommodate the technology are also factors. There are also legal issues with the immutable nature of the chain; what happens if regulators/courts demand an illogical/illegal transaction to be overturned [15]. Resolving these issues might take several years as the technology is still in its infancy.

Another author has reviewed the potential challenges in smart contracts' legal and practical enforceability within civil and common law jurisdictions. The author evaluated their position under Australian, English, French and American contract law; and reasoned there are still unanswered questions about the legal enforceability of a smart contract. Businesses are advised to factor in issues around the legal status of a smart contract before adopting them. Legal and practical enforceability questions will linger until smart contracts are widely tested in court [16].

A systematic study categorised 16 non-legal challenges faced by smart contracts into (i) Blockchain mechanism, (ii) virtual machine and (iii) contract source code level [17].

The Blockchain mechanism and the contract source code account for most of the issues associated with the smart contract due to the design challenges of the Blockchain (scalability, security, privacy) and human-error factors (lack of knowledge, programming mistakes, mistypes, etc.). The commonly identified issues by half of the authors they reviewed are 'unpredictable State', 'Generating Randomness' and 'Programming smart contracts. The unpredictable state relates to the uncertainty of knowing when the contract will be invoked after a transaction is sent to the Blockchain. This could be a potential problem because of the possibility that another transaction that alters the contract's state is executed first and when there is a Blockchain fork [17]. Other non-legal issues associated with smart contract includes codifying issues, scalability, the throughput of transactions, performance issues, privacy and security issues, and consumption of resources (energy) [12, 18]. This has contributed to the reluctance of users to adopt Blockchain technology. There are also non-legal factors, including low awareness and understanding of the technology among lawmakers, IP offices or lawyers (barrier of social acceptance), and lack of internationally accepted standardisation [19].

Even though it can be theoretically admissible in most legal systems, it will require experts to assert the fundamentals of the technology and its trustworthiness, which can often be an expensive and time-consuming task. There have been reported cases in China where the plaintiffs won in court using electronic evidence preserved on the Blockchain [20]. According to [19], the EU and Turkish laws allow individuals to present Blockchain records as timestamp evidence in a court. The overview of legislation supporting Blockchain and its use cases by some governments is shown in Table 2 and Table 3. However, [21] argues that the Blockchain database will not be protected under EU copyright law because the information stored on the chain influences platform-based functionality.

Table 2. Overview of Legislations supporting Blockchain Technology [22]

Location	Legislation	Effect	Status
Vermont (US)	HB868	Admissibility of Blockchain data in court	Signed by Governor on 06 February 2016 https://legislature.vermont.gov/bill/status/2016/H.868
EU	Regulatory framework (910/2014/EU)	Admissibility of electronic signatures and timestamps in European courts	Effective – 23 July 2014 https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014
Arizona (US)	HB2417	Admissibility of Blockchain signatures, smart contracts and definition of ownership	Signed by Governor on 29 March 2017 https://legiscan.com/AZ/bill/HB2417/2017

The International Organisation for Standardisation (ISO) is currently developing standards for Blockchain and distributed ledger technology called ISO/TC 307 [23]. Regulators might be more inclined to give Blockchain the required legal status once the ISO has set up this framework. This will encourage the adoption of Blockchain by rights holders for creating/preserving evidence for their IP claim. Also, [24] reckon the exponential increase of disruptive technology will make clients ask legal professionals to deal with issues in areas that lawyers do not fully understand. The author proposed introducing innovative technology of the future to law students at university to help

them better navigate possible legal gaps in the future market. This will provide the legal professional with the much-needed legal knowledge in the decentralised world. Thus, enabling them to adjust to the evolving technology innovation rather than creating obstacles.

Table 3. Overview of Governments' use case of Blockchain technology [22]

Location	Project	Use Cases	Blockchain platform
Estonia	X-Road	Secured government databases; Transparent healthcare records system; Public notary service	Proprietary (permissioned) and Ethereum
Delaware (US)	Delaware Blockchain Initiative	Storage of state archival records; Document filling with smart contract integration	Assemble (permissioned)
Georgia	-	Property registry	Bitcoin
Sweden	-	Property registry	Bitcoin
Illinois (US)	Illinois Blockchain Initiative	Property registry	Proprietary structure on top of Bitcoin
Russia	Digital Ecosystem	Communication between FAS and Companies	Unknown
Dubai	Dubai Blockchain Strategy	Paperless city transactions	Unknown

The best possible solution to having a legally binding contract under the current law is combining smart contracts with traditional contracts. In this way, the terms of the programmable contract are presented with a smart contract, while the rest remain as a traditional contract; hence, the traditional contract should be the primary source of interpretation while the smart contract serves as a supplement [13].

3.5 Blockchain in IP Management

Blockchain can be adopted to foster IP traceability as part of Open Innovation's problem-solving process [25]. This involved protecting ideas and the systematic development process from conception to completion. The authors adopted the 'Design Thinking Process' stages as individual interfaces to capture and digitally record verbal, written/sketched, and even modelled or constructed outcomes. The Design Thinking Process is a six-stage process (understand, observe, define, ideate, prototype, test) used by designers to organise their fact-finding and decision making. The outcomes are recorded and linked to the content creator. The generated hash (a unique fingerprint) for each digital artefact is embedded in the bitcoin Blockchain using the OriginStamp decentralised trusted timestamping service. The embedded Blockchain information can be used to guarantee proof of existence and proof of origin. Hence, this provides a verifiable tamperproof record of the entire innovation process from idea conception to the beginning of production.

A Secure Additive Manufacturing Platform (SAMPL) was proposed to enable a complete transparent chain of trust for the various stages in the manufacturing process using Blockchain [26]. The authors used Blockchain technology to manage the IP of the 3D print supply chain to prevent IP theft. They suggested installing the secure element (similar to those in a copy machine to avoid copying money) in the machines that

control the 3D printer's communication to the Blockchain. The connection of the 3D printers to the Blockchain will form a chain of trust between the copyright holders and the service providers. The entire process is stored on the Blockchain, from generating the 3D printing data via a trust service provider (3D printers with the secure element) to the labelling of the printed components with an RFID chip. The Ethereum Blockchain was used in the implementation because of its quality tools, documentation and capability to map complex workflow with smart contracts. The licensor and licensee record the licensing and licence consumption in the Blockchain, managed with a smart contract. This was carried out through transactions, and the public/private-key procedure secured the signature based on the industry-standard Elliptic Curve Digital Signature Algorithm (ECDSA). The private key of the licensor and licensee are stored in the wallet; they are used to create the digital signature.

Another study proposed using private Blockchain technology to manage product development information and processes with a particular use case in additive manufacturing [27]. The paper utilised a multi-agent system Blockchain technology to verify and distribute manufacturing IP. It entails using Blockchain to store IP or production phase data among designers and engineers, managers and stakeholders within and outside the organisation. The transaction on the Blockchain is signed with the sender's private key to prevent a change in its content by participating stakeholders. The data relating to the products, such as the CAD files and all other technical information/documents, are stored in a cloud-based repository. Hence, a verifiable cryptographic hash is generated for the blocks by combing the checksum of the CAD file's public key of the sender and recipient to reduce the likelihood of fraud. The barriers associated with online open innovation, focusing on Intellectual Property Rights (IPR) and the potential solution via building a smart online platform are outlined in [28]. The authors developed safe online Network Innovation Rooms (NIR) for collaboration between SMEs. Once the SMEs decide to collaborate, they must digitally sign an NDA before entering the secure and safe collaborative environment to disclose what IP or information is to be timestamped and stored in a Blockchain as their contribution to the NIR. The NDA is implemented as a smart contract using the Ethereum platform. It explicitly describes the IP and co-creations to be protected and their restrictive usage within the NIR.

Blockchain can be a potential solution for issues faced using the Building Information Modelling (BIM) technology in construction management, such as confidentiality, provenance tracking, multiparty aggregation, traceability, inter-organisational record keeping, change tracking, data ownership, etc. [29]. Another author proposed an architecture that combines Blockchain and IoT in managing IP. Their proposed approach is a peer-to-peer system with the Blockchain architecture in the cloud, which can connect to various IoT devices deployed [30].

Other research by [31] proposed an IP protection framework for microfilms using Blockchain technology. Microfilms are short films played on media platforms. The authors proposed storing the microfilms' names and scripts on the Blockchain as they are the main distinguishing factor between microfilms. Another paper utilised Blockchain to manage intellectual property in the fashion industry [32].

4 Potential off the Shelf Solutions

The section explores some of the existing or most recent third-party platforms for IP management. These include Binded, Proof of Existence, Bernstein, The Coalition of Automated Legal Applications Intellectual Property Group (COALA IP), and Secure Public Online Ownership Ledger (SPOOL) on Ascribe.

4.1 Binded

Binded started in 2017, and it utilised Blockchain to protect the copyrights of images. It was ideally suited to photographers who want to protect their images' IP. The user can sign up to the web platform and upload images to their private copyright vault either via their computer or from a platform such as Instagram. The platform then creates a unique fingerprint for every image in the private vault and permanently stores them in the Blockchain. They provide a copyright certificate for the content creator as proof of the content/ownership, which can protect against copyright infringement. The platforms also enable copyright owners to search online for matching images and potentially pursue copyright infringement online. They claim to have grown to over 15,000 members before being bought by Pixsy, which has a similar mission to protect copyright for artists. The platform has migrated to Pixsy [33].

4.2 Proof of Existence

This online service anonymously stores the Proof of Existence of any document on the Blockchain. This is carried out by storing the document's fingerprint in the Blockchain. The documents are not stored in their database or on the Blockchain. The document's fingerprint is created using the SHA-256 and embedded in the Bitcoin Blockchain to certify the document. This is carried out by generating a unique Bitcoin transaction that contains the document fingerprint (Hash value) using the OP_RETURN script. This is a Bitcoin script opcode used to make transaction output provably not spendable and allows for adding a small amount of text, the document's fingerprint in this instance, and a marker to identify all the transactions. Once the transaction completes, the document is proven to exist from the confirmed transaction [34].

4.3 Brenstien

This online web application allows content creators to create a digital trail of their innovation using the Bitcoin Blockchain and the national timestamping authorities. The platform provides the proof of existence, ownership and content development over time of any digital asset of any size or format. The platform utilises in-browser encryption for all uploaded documents to the local storage, requiring an encryption key to access the assets. The content creator only knows this encryption key and is not shared with Bernstein. Similar to Binded and Proof of existence, the fingerprint of the digital asset is certified and saved in the Blockchain. The platform enables proof of development by

chaining the certificates of the creative process together [35]. This is similar to [25], but every document iteration is frozen over time.

4.4 The Coalition of Automated Legal Applications - Intellectual Property Group (COALA IP)

This group was formed to address the issues of IP licensing for content creators using Blockchain. The group aims to build a free, open, easy-to-use platform capable of digitally recording assets and their required metadata, assigning and licensing rights, mediating a dispute, and authenticating claims made by others. The white paper containing the technical specification of COALA IP is available in [36].

4.5 The Coalition of Automated Legal Applications - Intellectual Property Group

This platform was created to protect the ownership of digital assets using the Bitcoin Blockchain. The platform features include the registration of ownership, transfer of ownership, and the right of owners to assign other individuals permission to sell on their behalf [37]. The ascribe service is no longer active as they encountered challenges such as scaling, user experience, interoperability and security, which affected the platform's adoption. This led to the creation of BigChain, which is the group's current focus. BigChainDB is a queryable distributed database with Blockchain characteristics. The platform enables enterprises and developers to deploy Blockchain proof of concepts. According to the founders, the comparison of Bitcoin Blockchain, Distributed Database and BigChainDB's performance is shown in Table 4. The platform was created by combing a distributed database (MongoDB) with a production-ready consensus engine (Tendermint) [38].

Table 4. BigChainDB, Bitcoin Blockchain, Distributed Database Comparison [38]

	Bitcoin Blockchain	Distributed Database	BIGCHAIN DB
Immutability	√		√
No Central Authority	√		√
Assets Over Network	√		√
High Throughput		√	√
Low Latency		√	√
Rich Permissioning		√	√
Query Capabilities		√	√

Other available Blockchain IP solutions include Po.et, Creativechain.org, IPSeeds.net, Stampery.com, Witcoin.io [39] and Amazon Manage Blockchain [40]. The Amazon Manage Blockchain was developed using the Hyperleger Fabric and Ethereum Blockchain framework. Additionally, Monograph's IP management platform was built explicitly to protect the digital asset for artists and secure royalties when the content is used [41].

5 The Challenges of Using Blockchain for Intellectual Property

The Chamber of Digital Commerce, a world trade industrial representation for Blockchain and digital assets, outlined an innovation guide to IP Strategy, protecting innovation and avoiding infringement [42]. The potential technical challenges/limitations to be resolved before using Blockchain to manage the intellectual property from an operational perspective can be classified into authenticity, provenance and royalty [43].

5.1 Authenticity Problem

Most Blockchain intellectual property applications require converting some IP into a hash key stored in a distributed ledger. This proves that valuable work exists at the moment in time in the Blockchain. More value can be added to this information by including additional details about the right holder's proof of ownership.
Several third-party services have utilised digital certificates (Blockchain 'Timestamping') and a common IP metadata protocol to provide evidence of ownership. The fundamental problem with using third party services is that the authenticity of the information entered during registration, which is not native to the Blockchain, cannot be guaranteed. This is referred to as the 'garbage in, garbage out' problem in a data sense. Hence, it is unclear how conflict can be resolved without a trusted third party if the copyright ownership information is incorrectly entered deliberately (by bad actors) or mistakenly (human error). Until authentication is resolved, the practical application of the Blockchain in IP can only be via a permissioned network that requires the validation of the entered information before they are published on the Blockchain [43].

5.2 Provenance Problem

Assuming the authentication issue has been resolved, the next challenge is how to record the transfer of IP ownership on the network. Most copyrighted works are based on pre-existing work with their authors and right owners. More so, copyright ownership tends to change over time. Creating a chain of all these different owners presents additional complexity [44]. There is a requirement for Blockchain to transfer ownership without a trusted third party and prevent piracy by issuing a digital certificate or a secret key to access the digital content.

However, this presents another issue of provenance as Blockchain cannot prevent 'double spending' and other authorised replications outside the network. An example could be transferring physical assets like land or a painting without updating the distributed ledger. A bad actor can also assess the digital assets when possessing the private key. Hence, the ledger stops being reliable when an IP transfer occurs outside the network without any mechanism to update the ledger. Until the provenance issue is resolved, the practical application of the technology should include issuing a transferable certificate, where the right to exclude unauthorised use is dependent on a trusted third party like a government institution rather than the Blockchain. This implies the embedding of terms of services/contract that complies with local law into the chain; to be used to resolve ownership disputes in court [43]. Other solutions suggested include

the work presented in the paper [45]. The authors proposed a benchmark framework for managing intellectual property using a hybrid Blockchain. They offered a combination of consortium and private Blockchain properties and a definition of attribute-based access control. They claimed the hybrid-based model could potentially solve challenges such as provenance and authenticity posed by Blockchain for IP management [45].

5.3 Royalty Stability Problem

Resolving authentication and provenance issues will make adopting Blockchain for IP management feasible. However, several trusted third parties help manage the secondary users of physical and digital intellectual property. Their high service charge diminishes the royalty payment to the IP owners. These have resulted in services directly connecting IP owners with consumers via Blockchain. The services manage IP usage and payment records by secondary users. This is common in the music industry, and some of the existing services include Ujo Music, Peertracks, Monegraph and Bittunes [46]. Also, Etheruem provides a platform for IP management called DAapps [43]. The major challenge of adopting this approach in royalty payment is the extreme volatility of cryptocurrencies, making it challenging to have a fixed consumable price/value on the Blockchain. Until the royalty stability problem is resolved, IP owners and consumers must be willing to accept the trade-off between efficiency and price stability.

6 Conclusions of the Study

Although the introduction of Blockchain in IP management has its advantages, it also possesses some challenges that must be addressed before the solution can be effective for IP management. As outlined by [44], some of these challenges include where the actual copyright work will be stored (either on the Blockchain or a decentralised cloud storage platform). Numerous design constraints exist with the available Blockchain architectures for storing a large digital file. Storing data or files on the Blockchain can slow down the network because of the proof of work mechanism for validating a transaction, making the whole process of large file-sharing or storage on the network a non-starter. Appropriate use of the Blockchain will entail storing items that can only be captured in small text like the document hash. Hence, there are two potential solutions to adopting Blockchain for IP management workflow. The first requires a secure database to store the encrypted IP documents and embed the Blockchain's cryptographic hash and metadata.

The second approach involves using file sharing solutions that mimic the Blockchain's decentralised and cryptographic properties (StorJ, Filecoin, and The Interplanetary Files System (IPFS), etc.) for file storage. Then, the hash of the document is stored in the Blockchain. IPFS is a peer-to-peer file-sharing protocol where each node stores a collection of the hash. IPFS keeps track of files and their respective versions in the network by giving the files and data blocks a unique fingerprint. The IPFS only stores the hash of the file, which can be used to find the location of the actual file. Therefore, the file can be accessed by anyone possessing the hash key. This is a potential security

risk, making IPFS unsuitable for IP sensitive files unless an additional layer of security/encryption is applied to the uploaded file to limit access. This can be done via Asymmetric Encryption, which uses the cryptographic public and private keys. Access to the files can be managed by encrypting the files with the public keys of the potential recipient. Therefore, any unauthorised access to the hash key of the file by malicious users is pointless as they cannot access the file's content. Hence, an appropriate application of IPFS for IP management would be storing the IPFS cryptographic hash key of the file in the Blockchain network. The file can be retrieved by first querying the Blockchain network to get the cryptographic hash and sending a query to the IPFS with the retrieved hash. The IPFS will return the original file uploaded to the network.

This paper has aggregated knowledge about Bolckchain and its use for IP management. Blockchain, its types, advantages, disadvantages, potential solutions, and challenges to these solutions have been discussed in detail. Therefore, this paper can be a roadmap for future researchers to explore this area further.

Acknowledgements. The authors would like to acknowledge the European Regional Development Fund (ERDF) and the Welsh Government for funding this project (WEFO 82127 & WEFO 80849).

References

1. Xiao, L., Huang, W., Xie, Y., Xiao, W., and Li, K.-C.: 'A blockchain-based traceable IP copyright protection algorithm', IEEE Access, 2020, 8, pp. 49532-49542
2. Modic, D., Hafner, A., Damij, N., and Zajc, L.C.: 'Innovations in intellectual property rights management: Their potential benefits and limitations', European Journal of Management and Business Economics, 2019
3. Aste, T., Tasca, P., and Di Matteo, T.: 'Blockchain technologies: The foreseeable impact on society and industry', computer, 2017, 50, (9), pp. 18-28
4. Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H.: 'An overview of blockchain technology: Architecture, consensus, and future trends', in Editor (Ed.)^(Eds.): 'Book An overview of blockchain technology: Architecture, consensus, and future trends' (Ieee, 2017, edn.), pp. 557-564
5. Wolrich, G.M., Yap, K.S., Guilford, J.D., Gopal, V., and Gulley, S.M.: 'Instruction set for message scheduling of SHA256 algorithm', in Editor (Ed.)^(Eds.): 'Book Instruction set for message scheduling of SHA256 algorithm' (Google Patents, 2014, edn.), pp.
6. Naik, R.P., and Courtois, N.T.: 'Optimising the sha256 hashing algorithm for faster and more efficient bitcoin mining', MSc Information Security Department of Computer Science UCL, 2013, pp. 1-65
7. Shrivas, M.K., and Yeboah, D.T.: 'The disruptive blockchain: Types, platforms and applications', in Editor (Ed.)^(Eds.): 'Book The disruptive blockchain: Types, platforms and applications' (2018, edn.), pp.
8. Yaga, D., Mell, P., Roby, N., and Scarfone, K.: 'Blockchain technology overview', arXiv preprint arXiv:1906.11078, 2019

9. Tosh, D., Shetty, S., Foytik, P., Kamhoua, C., and Njilla, L.: 'CloudPoS: A proof-of-stake consensus design for blockchain integrated cloud', in Editor (Ed.)^(Eds.): 'Book CloudPoS: A proof-of-stake consensus design for blockchain integrated cloud' (IEEE, 2018, edn.), pp. 302-309
10. Szabo, N.: 'Smart contracts: Building blocks for digital markets. EXTROPY J. Transhum', Thought, 1996, 18, pp. 50-53
11 Szabo, N.: 'The idea of smart contracts', Nick Szabo's papers and concise tutorials, 1997, 6, (1), pp. 199
12. Alharby, M., and Van Moorsel, A.: 'Blockchain-based smart contracts: A systematic mapping study', arXiv preprint arXiv:1710.06372, 2017
13. Hsiao, J.I.: 'Smart contract on the blockchain-paradigm shift for contract law', US-China L. Rev., 2017, 14, pp. 685
14. Stark, J.: 'Making sense of blockchain smart contracts', Coindesk. com, 2016
15. Yeoh, P.: 'Regulatory issues in blockchain technology', Journal of Financial Regulation and Compliance, 2017
16. Giancaspro, M.: 'Is a 'smart contract'really a smart idea? Insights from a legal perspective', Computer law & security review, 2017, 33, (6), pp. 825-835
17. Macrinici, D., Cartofeanu, C., and Gao, S.: 'Smart contract applications within blockchain technology: A systematic mapping study', Telematics and Informatics, 2018, 35, (8), pp. 2337-2354
18. Kamboj, D., and Yang, T.A.: 'An exploratory analysis of blockchain: applications, security, and related issues', in Editor (Ed.)^(Eds.): 'Book An exploratory analysis of blockchain: applications, security, and related issues' (The Steering Committee of The World Congress in Computer Science, Computer …, 2018, edn.), pp. 67-73
19. Gürkaynak, G., Yılmaz, I., Yeşilaltay, B., and Bengi, B.: 'Intellectual property law and practice in the blockchain realm', Computer law & security review, 2018, 34, (4), pp. 847-862
20. Helpdesk, C.I.S.: 'IPR protection for AI technology & application of blockchain in China', in Editor (Ed.)^(Eds.): 'Book IPR protection for AI technology & application of blockchain in China' (2019, edn.), pp.
21. Bacon, J., Michels, J.D., Millard, C., and Singh, J.: 'Blockchain demystified: a technical and legal introduction to distributed and centralized ledgers', Rich. JL & Tech., 2018, 25, pp. 1
22. Rivière, J.-M.: 'Blockchain technology and IP–investigating benefits and acceptance in governments and legislations', Junior Management Science, 2018, 3, (1), pp. 1-15
23. Cha, H., Lee, W., Choi, Y., Lee, J., and Lee, K.: 'International standardization on blockchain', Electronics and Telecommunications Trends, 2019, 34, (2), pp. 110-120
24. Fenwick, M., Kaal, W.A., and Vermeulen, E.P.: 'Legal education in the Blockchain revolution', Vand. J. Ent. & Tech. L., 2017, 20, pp. 351
25. Schönhals, A., Hepp, T., and Gipp, B.: 'Design thinking using the blockchain: enable traceability of intellectual property in problem-solving processes for open innovation', in Editor (Ed.)^(Eds.): 'Book Design thinking using the blockchain: enable traceability of intellectual property in problem-solving processes for open innovation' (2018, edn.), pp. 105-110
26. Holland, M., Stjepandić, J., and Nigischer, C.: 'Intellectual property protection of 3D print supply chain with blockchain technology', in Editor (Ed.)^(Eds.): 'Book Intellectual property protection of 3D print supply chain with blockchain technology' (IEEE, 2018, edn.), pp. 1-8

27. Papakostas, N., Newell, A., and Hargaden, V.: ‘A novel paradigm for managing the product development process utilising blockchain technology principles’, CIRP Annals, 2019, 68, (1), pp. 137-140
28. De la Rosa, J.-L., Gibovic, D., Torres, V., Maicher, L., Miralles, F., El-Fakdi, A., and Bikfalvi, A.: ‘On intellectual property in online open innovation for SME by means of blockchain and smart contracts’, in Editor (Ed.)^(Eds.): ‘Book On intellectual property in online open innovation for SME by means of blockchain and smart contracts’ (2016, edn.), pp.
29. Turk, Ž., and Klinc, R.: ‘Potentials of blockchain technology for construction management’, Procedia engineering, 2017, 196, pp. 638-645
30. Lin, J., Long, W., Zhang, A., and Chai, Y.: ‘Using blockchain and IoT technologies to enhance intellectual property protection’, in Editor (Ed.)^(Eds.): ‘Book Using blockchain and IoT technologies to enhance intellectual property protection’ (2019, edn.), pp. 44-49
31. Tsai, W.-T., Feng, L., Zhang, H., You, Y., Wang, L., and Zhong, Y.: ‘Intellectual-property blockchain-based protection model for microfilms’, in Editor (Ed.)^(Eds.): ‘Book Intellectual-property blockchain-based protection model for microfilms’ (IEEE, 2017, edn.), pp. 174-178
32. Sacha, G.: ‘Blockchain and its relevance to intellectual property law in the fashion industry’, Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne, 2019, 29, pp. 201-213
33. Binded, https://binded.com, last accessed 27 April 2022
34. Proof of Existence, https://proofofexistence.com/, last accessed 27 April 2022
35. Brenstein, https://www.bernstein.io/, last accessed 27 April 2022
36. Coala IP, https://www.coalaip.org/, last accessed 27 April 2022
37. Shrier, D., Wu, W., and Pentland, A.: ‘Blockchain & infrastructure (identity, data security)’, Massachusetts Institute of Technology-Connection Science, 2016, 1, (3), pp. 1-19
38. BigChainDB, https://www.bigchaindb.com/, last accessed 27 April 2022
39. De La Rosa, J.L., Torres-Padrosa, V., El-Fakdi, A., Gibovic, D., Hornyák, O., Maicher, L., and Miralles, F.: ‘A survey of blockchain technologies for open innovation’, in Editor (Ed.)^(Eds.): ‘Book A survey of blockchain technologies for open innovation’ (2017, edn.), pp. 14-15
40. Saghiri, A.M., HamlAbadi, K.G., and Vahdati, M.: ‘The internet of things, artificial intelligence, and blockchain: implementation perspectives’: ‘Advanced applications of blockchain technology’ (Springer, 2020), pp. 15-54
41. Monegraph, https://monegraph.com/, last accessed 27 April 2022
42. Council, B.I.P.: ‘A Blockchain Innovator's Guide To IP Strategy, Protecting Innovation & Avoiding Infringement’, in Editor (Ed.)^(Eds.): ‘Book A Blockchain Innovator's Guide To IP Strategy, Protecting Innovation & Avoiding Infringement’ (2018, edn.), pp. 1-46
43. Ito, K., and O’Dair, M.: ‘A critical examination of the application of blockchain technology to intellectual property management’: ‘Business transformation through blockchain’ (Springer, 2019), pp. 317-335
44. Savelyev, A.: ‘Copyright in the blockchain era: Promises and challenges’, Computer law & security review, 2018, 34, (3), pp. 550-561
45. Halloush, Z.A., and Yaseen, Q.M.: ‘A blockchain model for preserving intellectual property’, in Editor (Ed.)^(Eds.): ‘Book A blockchain model for preserving intellectual property’ (2019, edn.), pp. 1-5
46. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., and Santamaria, V.: ‘To blockchain or not to blockchain: That is the question’, It Professional, 2018, 20, (2), pp. 62-74.