Intellectual Property Valuation Report

Understanding the Market Value of Intellectual Property

Blockchain-based Storage and Authentication

Sag. Ref: SR_202526_6760

Dec 09, 2025

Table of Contents

1 Executive Summary

Cyberattacks occur every 11 seconds, causing businesses to lose billions due to system downtime, ransomware payments, reputational damage, and falling stock prices. Centralized networks, which store sensitive data and intellectual property in a single location, remain particularly vulnerable, leaving organizations exposed despite significant cybersecurity investments. In view of these concerns, blockchain technology offers a compelling solution. As a distributed ledger system, it enables secure, immutable, and transparent recording of data and transactions, protecting critical information from hacking, theft, or other threats that compromise traditional centralized systems. Reflecting its growing relevance, Gartner forecasts that blockchain's business value will surge from $176 billion in 2025 to $3.1 trillion by 2030[1], driven by adoption across businesses, governments, and technology vendors worldwide.

The subject patent portfolio further strengthens this landscape by providing innovative methods for validating physical identification objects, securing satellite-based data communications, and granting property access via key fobs. With patents granted across the US, Japan, India, Great Britain, the EU, Australia, South Korea & Switzerland, a total of 33 countries, the portfolio demonstrates robust global validation and broad technological significance. With countries now passing laws to create digital only ID's, this data will need to be stored on a Blockchain infrastructure.

A brief overview of the exemplary technologies covered in the U.S. granted/allowed patents within the family is provided below.

- **US10878429B2:** This patent provides a method for verifying the authenticity of physical identification objects, such as UPC-labeled products, using blockchain technology. It stores user images, read-only images of physical identification objects, and associated digital identifiers on a blockchain. When a user requests access, they input a validation code, and the system verifies the user's image and matches the physical object's identifier.
- **US11257098B2:** This invention outlines a method for secure communication between two stations via satellite to control access to physical property. A server issues access keys, validates them, and ensures that only authorized stations can transmit or receive the keys. Validation histories are recorded in a Hyperledger, preventing unauthorized uplink communications.
- **US11836743B2:** This patent focuses on granting property access via a key fob integrated with blockchain logging. The key fob receives an encryption code from a mobile device and transmits it to a validation module at the property. Access is granted if the code is valid; otherwise, access is denied.
- **US12223517B2:** This patent enhances security for property access systems using electronic keys and blockchain-backed logs. An electronic key receives an encrypted code from a mobile device and transmits it wirelessly to a validator at the property. The validator grants or denies access based on the code's validity.

[1] https://www.gartner.com/en/doc/3855708-digital-disruption-profile-blockchains-radical-promise-spans-business-and-society

In addition to its patents, Silakab has developed **Clear Chek**, a SaaS blockchain application in MVP stage that converts paper and plastic IDs into secure digital credentials to protect against identity theft and fraud. The company is also developing an **Input Device blockchain application** in early design, aimed at securing access to vehicles, buildings, and other entry points.

MARKET TRENDS

The global Blockchain Technology market is expected to reach $ 31.28 billion by 2025 and $ 1,431.54 billion by 2030[2]. The escalating demand for secure and transparent transactions across many industries is driving market growth. Vendors in the market are focusing on increasing the customer base to gain a competitive edge in the industry. Therefore, key players are taking several strategic initiatives, such as mergers and acquisitions, and partnerships with other major companies.

- Some of the major players operating in the blockchain technology market include *IBM Corp., Microsoft Corp., The Linux Foundation, Blockchain Tech LTD, Chain, Inc, Circle Internet Financial Ltd., Deloitte Touche Tohmatsu, Digital Asset Holdings, LLC, Global Arena Holding, Inc., Monax Labs, Ripple etc.* Many of these companies already provide solutions for digital identity verification and property access management. Considering the advancements in solutions for digital identity verification and property access management, it is believed that more market players will be willing to adopt the technologies disclosed in the subject patent publications in the coming future.

FAIR MARKET VALUE CALCULATION

A Hybrid Approach has been followed to evaluate the appropriate Fair Market Value for the Patent Portfolio under review.

- The first part of this hybrid approach involves market analysis of the technology disclosed in the IP under study and understanding how much revenue would be generated by the implementation of in-scope technology. Several factors such as *Market Share, Adoption Rate, Annual Revenue, R&D Cost, Net Profit Margin, IP contribution to Net Profit, Tax and Duties, etc*., influencing the market are considered to arrive at an expected Fair Market value.
- The second part of this hybrid approach involves rigorous analysis of the Intellectual Property pertaining to the technology under study. Several factors that would affect the applicability of a patent are taken together to understand the actual worth of the Intellectual Property under study. For example – what problem is being solved by the patent, is the problem being solved prevalent in the market, availability of similar products in the market, etc.

Based on all the factors evaluated, **the fair market value for the subject patent portfolio is USD 5 billion.**

[2] https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market

2 Introduction

2.1 IP Valuation – An Overview

The current market value assessment exercise aims to determine the Net Present Value (NPV) that the patent portfolio pertaining to the given technology may generate for the patentee/licensee of the invention based on the present status and forecasting of the future value of the technology. The methodology followed in the current valuation exercise utilizes a financial model to understand/evaluate/determine various parameters such as the size of the market, market share, projected growth over time, etc. to estimate future cash flows that would be realized based on commercial exploitation of the patents in the portfolio. The valuation exercise considers the potential product revenue adjusted for the contribution of the patent to the product and additionally discounted based on the risk assessment of the patent (is the patent issued or still in the application phase, term of the patent, how easy it is to invent around, technological lifecycle, risk of successful patent challenge, etc.).

2.2 Technology under Focus

The subject patent portfolio covers facets relating to validating authenticity of a physical identification object and securing satellite data communications between first and second stations and granting access to property to a user of a key fob. A brief description of all the patent publications under study is illustrated below.

- **US10878429B2**

This invention outlines a method for storing user identification through a blockchain-based approach. It involves storing user images, read-only images of physical identification objects, and trackable digital identifiers in separate blockchains on servers. When a request for a read-only image arises, the user is prompted to input a code. Validating the code triggers capturing and comparing the user's image with the stored image in the blockchain. Upon a match, a trackable digital identifier is obtained from a scanned physical identification object. The system searches for this identifier and transmits the corresponding read-only image to the user's device via a secure protocol. A comparison between the scanned physical identification object and its read-only image determines its validity. If found invalid, a **block with information about the invalid object is added to the blockchain associated with the user**.

Specifically, a blockchain passport application is initiated by a mobile device when a user clicks on an app icon. The device then displays a scan button, allowing the user's camera or other scanning device to scan a passport barcode or other identification document to obtain scanned code information. The scanned code information is then searched for by a government server for passport information corresponding to the code. The information may include an image of the person, a portion of a passport document, or an electronic passport. The mobile device then gains read-only access to the passport information securely stored in a blockchain on a government server.

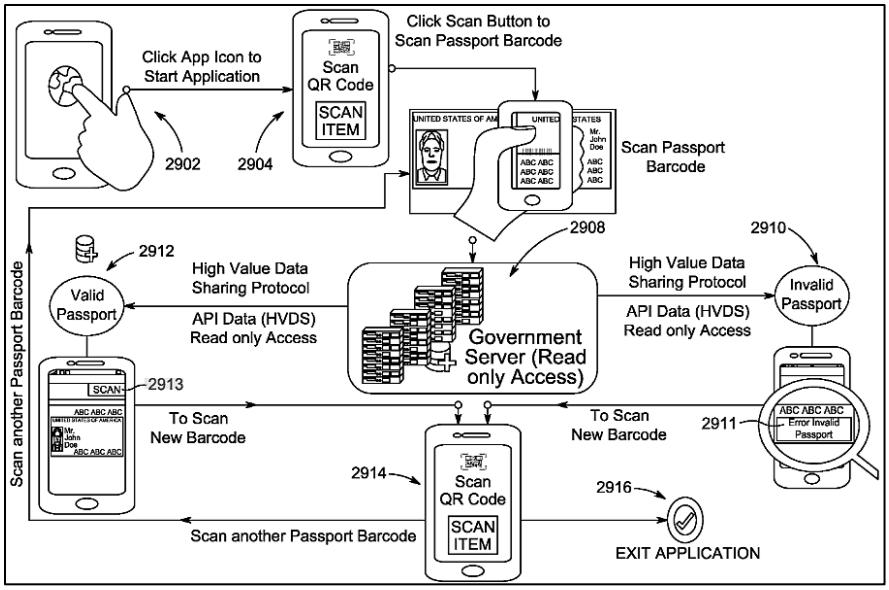


Figure 1 Exemplary figure from the patent depicting the invention

Additionally, after starting the application, the ID number and/or text is scanned, e.g., via OCR. Then, the application determines whether the ID is valid or not. If the ID is valid, ID proof details are displayed. If the ID is invalid, an error message is displayed (e.g., a message with the text: Invalid ID proof). Then, unless another ID proof needs to be scanned, the application is exited.

- **US11257098B2**

The invention describes a method for **securing satellite data communications** in a sequential manner. The first station transmits a request for an access key to access a property to a server through satellite. Upon receiving the access key from the server, the first station transmits it to a second station. Subsequently, the second station forwards this access key back to the server for validation. If the server successfully validates the access key, it transmits validation data to the first station via the satellite, permitting further satellite data communication between the first and second stations. Moreover, **the server maintains a validation history of the access key in a Hyperledger for record-keeping.** If the server fails to validate the access key, the satellite has the capability to deny data communications, ensuring a robust security protocol for the interaction between the two stations.

Specifically, the servers determine if the received access key from the first station matches the one sent to the second station. If they do, they validate the key and notify the first station. The first station then allows communication with the second station via satellite. If the key does not match, the first station denies communication. The first station denies communication with the second station. If the second station is a valid station, it may attempt to receive another access code from the servers. The satellite communication method repeats, and **in cases of validation and non-validation, servers create a block for these determinations and save it in the hyper-ledger**.

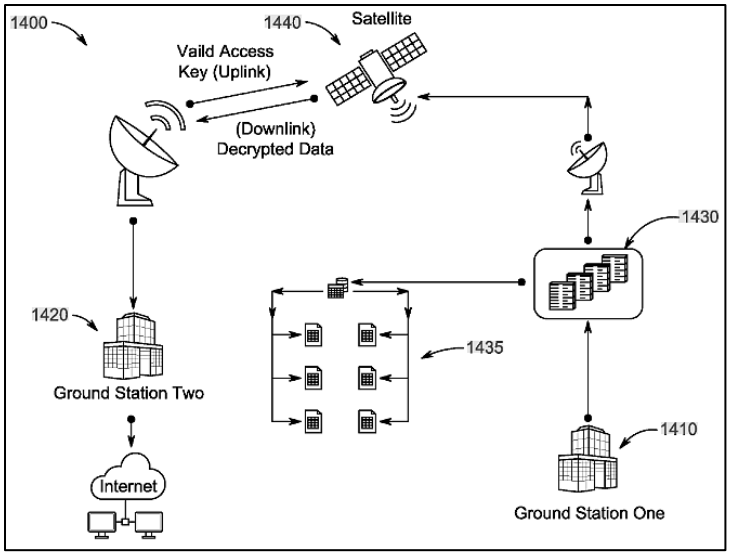


Figure 2 Exemplary figure from the patent depicting the invention

- **US11836743B2**

The invention describes a method for granting access to property to a user of a key fob. First, the key fob receives an encrypted code from a mobile device. Subsequently, the key fob transmits this encrypted code wirelessly to a validation module residing on a computing device within the property. Following this, the validation module determines the validity of the encrypted code, either granting or denying access accordingly. Once this determination is made, the computing device sends two crucial messages: an access message to the key for immediate action and a first access log message to the mobile device for record-keeping. Notably, the first access log message triggers the mobile device to dispatch a second access log message to a server. Lastly, upon receiving the second access log message, **the server updates the access log of the key fob in a Hyperledger**.

Specifically, the key fob system consists of a property, a smart device, a key fob, and a server connected through a network. The key fob grants access to the property upon receiving an encrypted code from the smart device. The entry can be a door, engine, or lock, depending on the property. For example, a land vehicle may have a door for entering or an engine to start. For aircraft or watercraft properties, the entry may be a door for controlling the aircraft or watercraft. For buildings or safes, the entry may be a door or lock. The smart device functions as a control device in the key fob system, capable of communicating with the key fob and the server via various methods, such as the internet wirelessly or wired, and with the key fob through Bluetooth. The key fob may have one or more buttons for accessing the property. For example, one button may be used to start an engine for land vehicles, watercraft, aircraft, or military vehicles. The key fob can be preprogrammed to pair with property via Bluetooth, eliminating the need for an internet connection. The same can be done with smart devices, also paired via Bluetooth. The server can store the access history of the key fob in property in a hyper ledger using blockchain technology. This allows the server to generate blocks for storing the access history and save them in the hyper-ledger stored on servers.

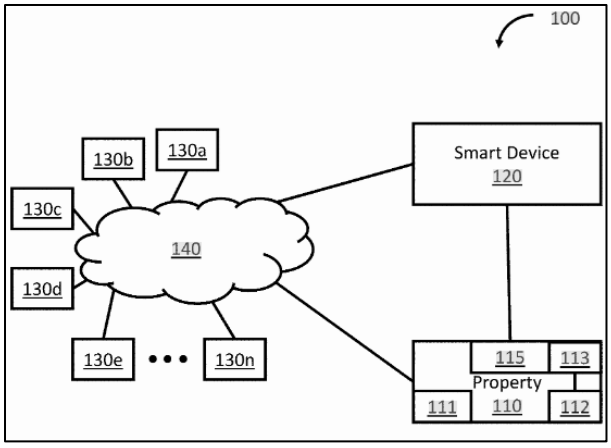


Figure 3 Exemplary figure from the patent depicting the invention

- **US12223517B2**

The invention describes a method for granting access to property to a user of an electronic key. First, the electronic key receives an encrypted code from a mobile computer. Subsequently, the electronic key transmits this encrypted code wirelessly to a validator running on a property computer. Following this, the validator determines the validity of the encrypted code, either granting or denying access accordingly. Once this determination is made, the computing device sends two crucial messages: an access message to the electronic key for immediate action and a first access log message to the mobile computer for record-keeping. The first access log message triggers the mobile computer to dispatch a second access log message to a server. Lastly, upon receiving the second access log message, **the server updates the access log of the electronic key in a hyper ledger**.

The patent describes a blockchain-secured smart access system that uses a smartphone, key fob (i.e., an electronic key), and server to control access to a property such as a car, building, or safe. The smartphone generates a unique encrypted digital key using public/private key encryption and sends it via Bluetooth to the paired key fob. The key fob then transmits this code to the property to request access. The property decrypts and verifies the code and granting or denying the entry. Further, it records each access attempt in a blockchain hyper ledger for security and traceability.

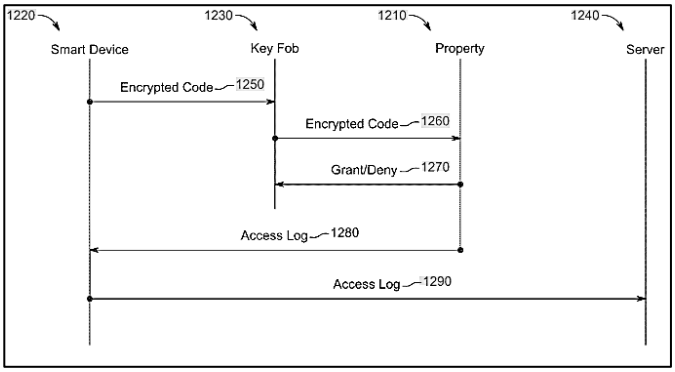


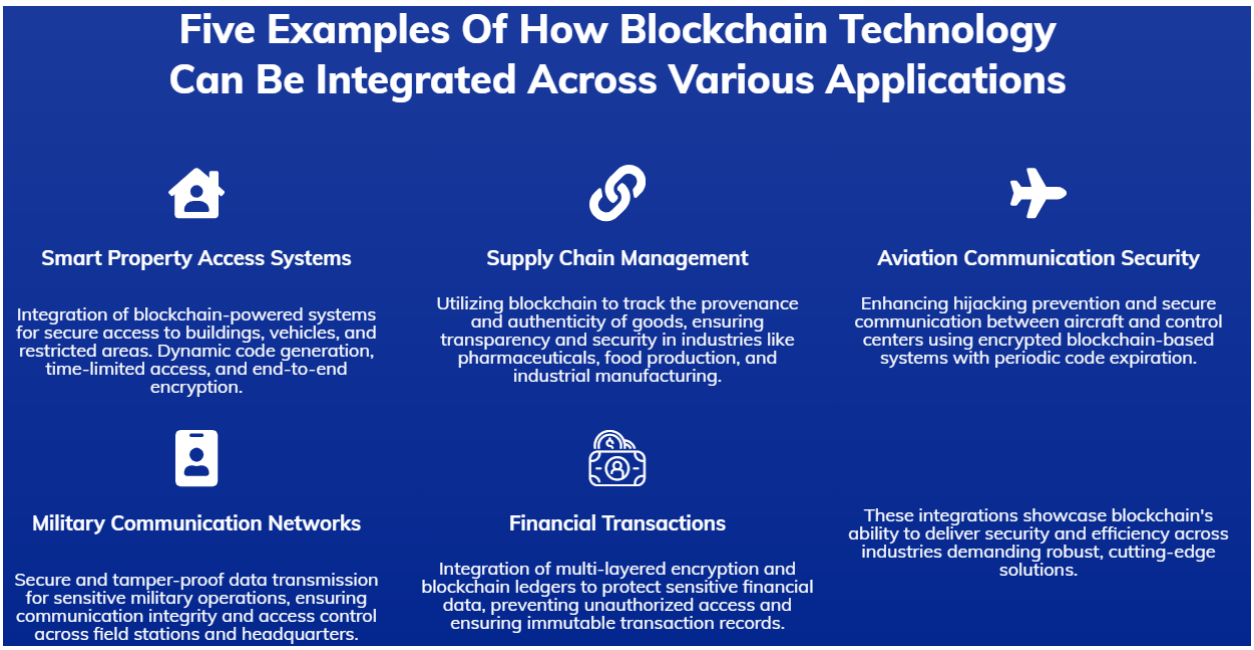
Figure 4 Exemplary figure from the patent depicting a communication procedure for a key fob system

2.3 Silakab Offerings and Market Reach

In addition to its patent portfolio,

- **Silakab Corp. has developed *Clear Chek*[3]**, a SaaS blockchain application currently in its MVP (Minimum Viable Product) stage. Clear Chek offers the ability to convert traditional paper and plastic IDs into secure, digital blockchain-based files, safeguarding sensitive information against identity theft, fraud, and cyber threats. By leveraging blockchain's immutable and encrypted architecture, Clear Chek ensures that sensitive information remains tamper-proof, traceable, and protected from hacking or unauthorized access. It provides governments, corporations, and individuals with a trusted platform for identity management and data security.
- **Silakab is also developing an *Input Device SaaS blockchain application***, which is currently in its early design stage. In addition, they are developing the Input Device application, which is currently in early development. This application extends blockchain security to physical access systems, protecting entry points for vehicles, buildings, trucks, and storage facilities.

The following diagram provides an overview of the potential global deployment and application areas for Silakab offerings.

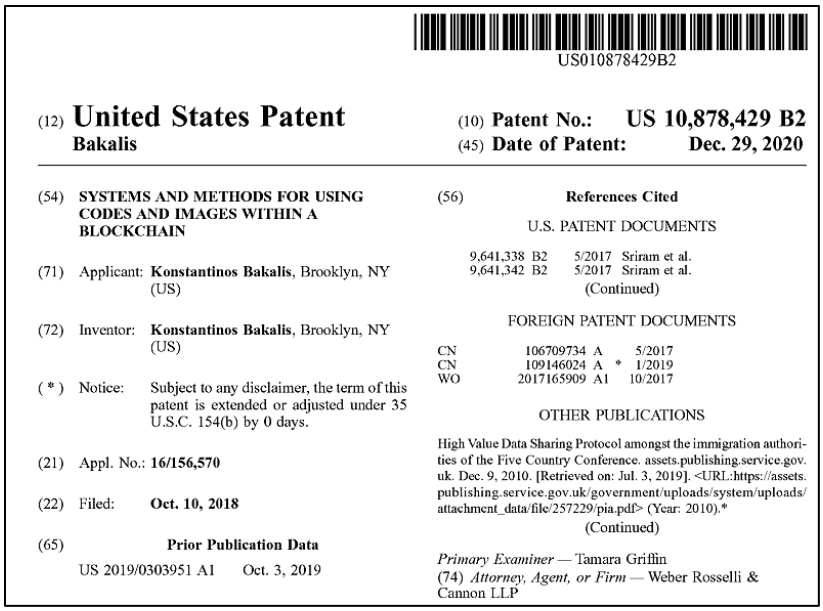


[3] https://silakab.com/

3 Impact of Subject Invention

3.1 Subject Patent Portfolio

Silakab holds a groundbreaking family of **blockchain patents** that are poised to transform the landscape of digital security. With four issued patents and a fifth pending approved, Silakab's intellectual property establishes a strong foundation for blockchain-driven innovation. These patents have been granted across major jurisdictions including the **United States, Japan, India, Great Britain, the European Union, Australia, South Korea & Switzerland, a total of 33 countries**, demonstrating global validation and broad technological relevance.



US010878429B2

(12) **United States Patent**
Bakalis

(10) **Patent No.: US 10,878,429 B2**
(45) **Date of Patent: Dec. 29, 2020**

(54) **SYSTEMS AND METHODS FOR USING CODES AND IMAGES WITHIN A BLOCKCHAIN**

(71) Applicant: **Konstantinos Bakalis**, Brooklyn, NY (US)

(72) Inventor: **Konstantinos Bakalis**, Brooklyn, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/156,570**

(22) Filed: **Oct. 10, 2018**

(65) **Prior Publication Data**

US 2019/0303951 A1 Oct. 3, 2019

(56) **References Cited**

U.S. PATENT DOCUMENTS

9,641,338 B2 5/2017 Sriram et al.
9,641,342 B2 5/2017 Sriram et al.
(Continued)

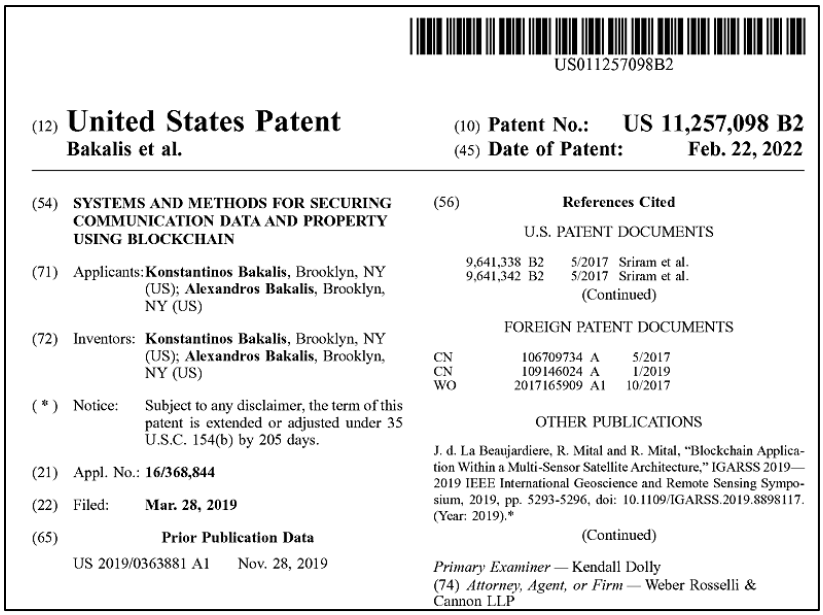
FOREIGN PATENT DOCUMENTS

CN 106709734 A 5/2017
CN 109146024 A * 1/2019
WO 2017165909 A1 10/2017

OTHER PUBLICATIONS

High Value Data Sharing Protocol amongst the immigration authorities of the Five Country Conference. assets.publishing.service.gov.uk. Dec. 9, 2010. [Retrieved on: Jul. 3, 2019]. <URL:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/257229/pia.pdf> (Year: 2010).*
(Continued)

Primary Examiner — Tamara Griffin
(74) *Attorney, Agent, or Firm* — Weber Rosselli & Cannon LLP



US011257098B2

(12) **United States Patent**
Bakalis et al.

(10) **Patent No.: US 11,257,098 B2**
(45) **Date of Patent: Feb. 22, 2022**

(54) **SYSTEMS AND METHODS FOR SECURING COMMUNICATION DATA AND PROPERTY USING BLOCKCHAIN**

(71) Applicants: **Konstantinos Bakalis**, Brooklyn, NY (US); **Alexandros Bakalis**, Brooklyn, NY (US)

(72) Inventors: **Konstantinos Bakalis**, Brooklyn, NY (US); **Alexandros Bakalis**, Brooklyn, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 205 days.

(21) Appl. No.: **16/368,844**

(22) Filed: **Mar. 28, 2019**

(65) **Prior Publication Data**

US 2019/0363881 A1 Nov. 28, 2019

(56) **References Cited**

U.S. PATENT DOCUMENTS

9,641,338 B2 5/2017 Sriram et al.
9,641,342 B2 5/2017 Sriram et al.
(Continued)

FOREIGN PATENT DOCUMENTS

CN 106709734 A 5/2017
CN 109146024 A 1/2019
WO 2017165909 A1 10/2017

OTHER PUBLICATIONS

J. d. La Beaujardiere, R. Mital and R. Mital, "Blockchain Application Within a Multi-Sensor Satellite Architecture," IGARSS 2019—2019 IEEE International Geoscience and Remote Sensing Symposium, 2019, pp. 5293-5296, doi: 10.1109/IGARSS.2019.8898117. (Year: 2019).*
(Continued)

Primary Examiner — Kendall Dolly
(74) *Attorney, Agent, or Firm* — Weber Rosselli & Cannon LLP


US011836743B2

(12) **United States Patent**
Bakalis et al.

(10) **Patent No.: US 11,836,743 B2**
(45) **Date of Patent: Dec. 5, 2023**

(54) **SYSTEMS AND METHODS FOR SECURING COMMUNICATION DATA AND PROPERTY USING BLOCKCHAIN**

(71) Applicants: **Konstantinos Bakalis**, Brooklyn, NY (US); **Alexandros Bakalis**, Brooklyn, NY (US)

(72) Inventors: **Konstantinos Bakalis**, Brooklyn, NY (US); **Alexandros Bakalis**, Brooklyn, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **17/672,429**

(22) Filed: **Feb. 15, 2022**

(65) **Prior Publication Data**

US 2022/0277317 A1 Sep. 1, 2022

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,366,696 B1 4/2002 Hertz et al.
9,641,338 B2 5/2017 Sriram et al.
(Continued)

FOREIGN PATENT DOCUMENTS

CN 106709734 A 5/2017
CN 109146024 A 1/2019
(Continued)

OTHER PUBLICATIONS

Anonymous: "Getting Smart: Contracts on the Blockchain", May 1, 2016 (May 1, 2016), XP055408890, Retrieved from the Internet: URL:https://www.iif.com/system/files/32370_132_smartcontracts_report_may_2016_vf.pdf; [retrieved on Sep. 21, 2017] I*p. 5*.
(Continued)

Primary Examiner — Kendall Dolly
(74) *Attorney, Agent, or Firm* — WEBER ROSSELLI & CANNON LLP


US012223517B2

(12) **United States Patent**
Bakalis et al.

(10) **Patent No.: US 12,223,517 B2**
(45) **Date of Patent: *Feb. 11, 2025**

(54) **SYSTEMS AND METHODS FOR SECURING COMMUNICATION DATA AND PROPERTY USING BLOCKCHAIN**

(71) Applicants: **Konstantinos Bakalis**, Brooklyn, NY (US); **Alexandros Bakalis**, Brooklyn, NY (US)

(72) Inventors: **Konstantinos Bakalis**, Brooklyn, NY (US); **Alexandros Bakalis**, Brooklyn, NY (US)

(73) Assignee: **Silakab Corp.**, Brooklyn, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **18/525,759**

(22) Filed: **Nov. 30, 2023**

(65) **Prior Publication Data**

US 2024/0296464 A1 Sep. 5, 2024

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,366,696 B1 4/2002 Hertz et al.
9,641,338 B2 5/2017 Sriram et al.
(Continued)

FOREIGN PATENT DOCUMENTS

CN 106709734 A 5/2017
CN 109146024 A 1/2019
(Continued)

OTHER PUBLICATIONS

Anonymous: "Getting Smart: Contracts on the Blockchain", May 1, 2016 (May 1, 2016), XP055408890, Retrieved from the Internet: URL:https://www.iif.com/system/files/32370_132_smartcontracts_report_may_2016_vf.pdf; [retrieved on Sep. 21, 2017] I*p. 5*.
(Continued)

Primary Examiner — Kendall Dolly
(74) *Attorney, Agent, or Firm* — Weber Rosselli & Cannon LLP

3.2 Market Applications/Advantages of Technology

A blockchain is a digital ledger of transactions maintained by a network of computers in a way that makes it difficult to hack or alter. Technology offers a secure way for individuals to deal directly with each other, without an intermediary like a government, bank or other third party. A list of records, called blocks, is linked together using cryptography. Each transaction is independently verified by peer-to-peer computer networks, time-stamped and added to the ledger. Once recorded, the data cannot easily be altered. Blockchain has various applications across different industries and settings. Below is listed some key market applications:

1. **Healthcare:** Traditional healthcare databases are typically centralized, making them vulnerable to single points of failure or cyber-attacks. Blockchain can provide secure and decentralized data storage and management. Blockchain can reduce patient identities, reducing the risk of identity theft and unauthorized access to sensitive healthcare information.
2. **Manufacturing:** Many manufacturing companies store information on parts, such as bar codes, QR codes, etc., in a database, which can be attacked by a cyber-attack, causing a loss of data. Blockchain can eliminate the risk of cyber-attacks by storing QR codes and bar codes in a block on the blockchain. The information becomes immutable. It cannot be altered or tampered with. This ensures the integrity of the QR codes over time.
3. **Government:** Utilizing blockchain in government processes can strengthen identification and authentication mechanisms, reduce the risk of fraudulent activity, and enhance the overall security and trustworthiness of government-issued identification systems. Government servers can store all the required data of a user in dedicated blockchains, which creates a transparent and immutable record of invalid identification attempts.
4. **IT Vendors:** Blockchain technology offers IT vendors a robust framework to improve transparency, security, and efficiency across various aspects of their operations. Data security and privacy are major concerns for IT vendors, as they store sensitive customer data and transactions on a blockchain, which ensures a high level of security.
5. **Travel and Leisure:** Many airline companies store data in traditional IT infrastructure, which can be vulnerable to cyber-attacks. By adopting blockchain, authorities can maintain tamper-resistant and auditable records, contributing to overall travel security. The decentralized nature of blockchain adds an additional layer of trust and transparency to the identification process in the travel and leisure industry.

Block chain offers numerous advantages across different industries and settings. Here are several key benefits:

1. **Enhanced security:** Blockchain can significantly alter the way sensitive data is viewed by creating a secure, end-to-end record that prevents fraud and unauthorized activity. It also addresses privacy issues by anonymizing personal data and using permissions to prevent access. The data is stored across a network of computers, making it difficult for hackers to view.

2. **Greater transparency**: Blockchain technology can significantly improve the way sensitive and crucial data is viewed. It creates an end-to-end encrypted record, preventing fraud and unauthorized activity. Privacy issues are addressed by anonymizing personal data and using permissions to prevent access. Blockchain stores information across a network of computers, making it difficult for hackers to view data. It also provides greater transparency by recording transactions and data identically in multiple locations, allowing all network participants with permission to see the same information. Transactions are immutable and time- and date-stamped, enabling members to view the entire transaction history, virtually eliminating fraud opportunities.
3. **Instant traceability:** Blockchain technology provides an audit trail for asset provenance, aiding industries with concerns about environmental or human rights issues or counterfeiting. It allows direct sharing of provenance data with customers, exposing weaknesses in supply chains. Traceability data can also reveal weaknesses in supply chains, such as goods waiting for transit at loading docks.
4. **Increased efficiency and speed**: Blockchain streamlines traditional paper-heavy processes, reducing time, human error, and third-party mediation. Transactions can be completed faster and more efficiently, with documentation and transaction details stored on the blockchain, eliminating the need for paper exchange and reconciling multiple ledgers, resulting in quicker access to the stored details.
5. **Immutability:** Blockchain uses hashing techniques to store each transaction on a block that is connected to each other, so it has tighter security. Data cannot be tampered with in blockchain technology due to its decentralized structure so any change will be reflected in all the nodes so one cannot do fraud here; hence it can be claimed that transactions are tamper-proof.
6. **Cost Reduction:** As blockchain needs no third man, thus, it reduces the cost for the businesses and gives trust to the other partner.

Furthermore, a couple of patents in the family comprise the use of satellite communication for data communications. Secure Satellite data communication is the transmission of information between two or more points via communication satellites orbiting the Earth. Satellites act as relay stations in space, receiving signals from ground-based stations and retransmitting them to other ground-based locations. It plays a crucial role in enabling long-distance and global communication, particularly in areas where traditional terrestrial communication infrastructure is impractical or unavailable. Below are illustrated a few applications of satellite communication systems.

- **Military and Defense Systems:** Military applications often involve secure communication for accessing sensitive physical assets. Secure satellite data communication can ensure that only authorized stations can communicate and access equipment or systems.
- **Maritime Communication and Navigation:** Secure satellite communication is vital for maritime applications including safe navigation, tracking vessels, and transmission.

- **Global Connectivity for IoT Devices:** Internet of things (IoT) devices in various industries, such as utilities, transportation, and logistics, rely on secure satellite data communications to ensure global connectivity and the safe transfer of data between devices.
- **Land Surveying and Mapping:** Land surveyors rely on satellite communication to transfer mapping data, boundary measurements, and topographic information. This facilitates real-time collaboration among surveying teams and helps in updating maps with accurate geospatial data.
- **Aerospace and Aviation:** Secure satellite data communications facilitate safe air traffic management, real-time aircraft tracking, and communication between ground control and aircraft.

Secure satellite data transfers provide significant benefits in a variety of sectors and contexts. Here are a few important advantages:

1. **Wide scope:** Satellite communication can cover a wide range of the Earth's surface, including inaccessible and hard-to-reach ranges. This makes it a perfect solution for communication in regions where terrestrial communication framework isn't accessible or not cost-effective to introduce.
2. **High-speed communication:** Satellite communication can transmit information at high speeds, permitting quick and efficient communication. Usually particularly valuable for applications that require real-time information transmissions, such as video conferencing or remote sensing.
3. **Reliability:** Satellite communication is profoundly reliable because it isn't influenced by climate conditions or characteristic catastrophes that can disturb earthly communication foundations. This makes it a prevalent choice for basic applications such as military communication or emergency response.
4. **Secure Data Transfer:** Secure satellite communication employs encryption and authentication protocols, ensuring the confidentiality and integrity of the transmitted data. This is vital for sensitive applications like military operations and healthcare.
5. **Global Positioning:** Satellites contribute to global positioning systems (GPS), supporting navigation and location-based services which are integral in sectors like transportation, logistics, and emergency response.
6. **Support for IoT and M2M Communication:** Satellites play a crucial role in supporting the Internet of Things (IoT) and machine-to-machine (M2M) communication, providing connectivity for a myriad of devices and sensors.

These applications and advantages collectively make secure satellite data communications a valuable and versatile solution for addressing communication challenges in diverse settings and industries.

4 Industry/Market Research

The industry research aims to answer some obvious questions such as how big the industry is in terms of revenue, who are the leading technology players, what is the growth rate, etc. To begin with, the first step is to identify the critical information required and analyze various sources for gathering said critical information. For this purpose, different product directories, industry catalogs, reference books, or other available literature are analyzed. Further, different publicly available literature through the web is surveyed with respect to the market to ascertain a product's novelty and the competitive advantages or disadvantages. Our patents appeal to many sectors including property protection, building protection and vehicle theft protection.

Apart from online literature, it is also helpful to take note of the companies providing similar products in the said domain since they could be potential licensees should one choose to go further in the commercialization process. It is also a motive to understand the lifecycle of the subject technology. The data below has been surveyed from different sources to understand the market landscape.

4.1 Market Size – Global Blockchain Technology Market

The patents/inventions under consideration relate to blockchain technology used for validating the authenticity of physical identification objects, securing satellite data communications between first and second stations, and granting access to property through a key fob or electronic key. Thus, to estimate the fair market value of the portfolio, we explored several market reports dealing with Blockchain Technology. All these reports have comparable market statistics and owing to the presence of sufficient information required for calculating the market value, we have consulted a market report from Grand View Research *(Report)* for gathering data points related to the market. Considering the remaining life term of the patents, the market has been forecasted from the year 2025 to 2038 for the current valuation study.

GLOBAL BLOCKCHAIN TECHNOLOGY MARKET SIZE

Grand View Research estimates that the global blockchain technology market size was USD 31.28 billion in 2024 and is projected to reach USD 1,431.54 billion by 2030, growing at a CAGR of 90.1% from 2025 to 2030 [4].

Blockchain's decentralized and immutable ledger system ensures the integrity and transparency of transactions, making it especially appealing to sectors such as finance, healthcare, and supply chain management. Businesses across these domains are increasingly integrating blockchain solutions to enhance security and transparency in their operations.

The digital identity segment is expected to grow the fastest in the coming years. This is happening because people and organizations increasingly need safe and reliable ways to prove who they are online. As more

[4]https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market

activities such as banking, healthcare, and government services move to digital platforms, traditional identity methods are no longer enough.

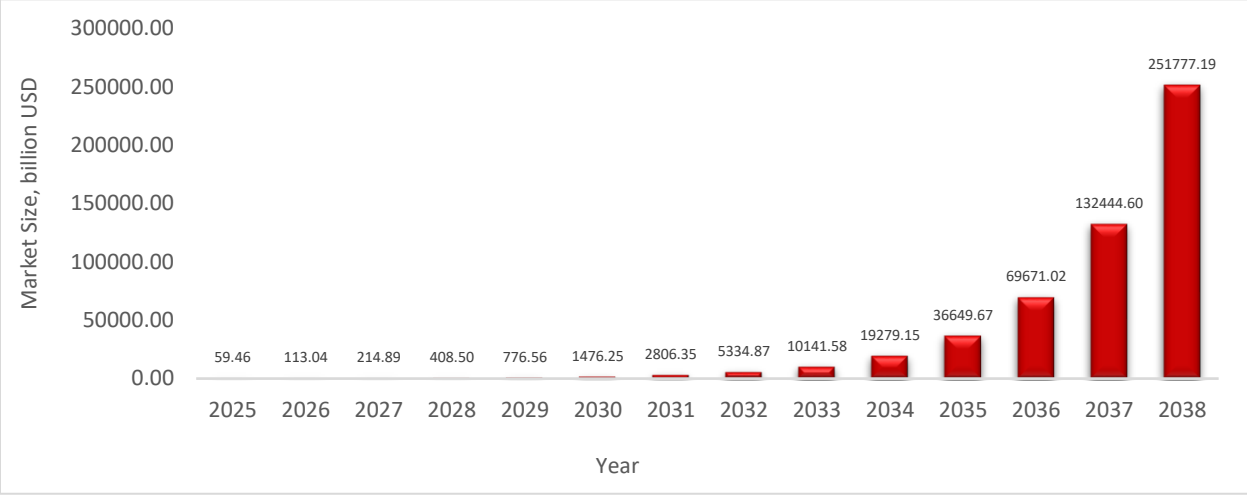


Figure 5 Global Blockchain Market Size

OTHER GEOGRAPHICAL INSIGHTS

- North America blockchain technology market dominated globally in 2024 and accounted for 37.4% of the global revenue. The region boasts a robust ecosystem of tech startups, established corporations, and leading research institutions, creating a fertile ground for blockchain development. Silicon Valley has been a hot spot for blockchain startups and venture capital investments. Moreover, North America is home to a diverse range of industries, from finance and healthcare to supply chain management and energy, all of which recognize the transformative potential of blockchain technology.

- The U.S. blockchain market is projected to grow at a strong CAGR from 2025 to 2030, supported by regulatory progress and rising government adoption for digital identity and supply chain security. A mature tech ecosystem, strong venture capital activity, and partnerships between startups and major financial institutions are accelerating large-scale innovation.
- The APAC region is expected to witness the fastest CAGR, driven by government support in China, Japan, and India. These countries promote blockchain for transparency and efficiency across industries.
- Europe's market is set for strong growth due to robust regulations like MiCA, which build trust in blockchain systems. Sustainability initiatives also drive blockchain adoption in energy trading and carbon tracking. Cross-border EU collaboration supports innovation in logistics, trade, and public services.

COMPETITIVE LANDSCAPE / KEY PLAYERS

Major market players are spending a lot of money on R&D to increase their product lines, which will help the blockchain technology market grow even more. Market participants are also taking a range of strategic initiatives to grow their worldwide footprint, with key market developments such as new product launches, mergers and acquisitions, contractual agreements, increased investments, and collaboration with other organizations.

Major companies in the blockchain technology market include[5]:

- *Microsoft Corporation*
- *IBM Corporation*
- *The Linux Foundation*
- *Blockchain Tech LTD*
- *Chain*
- *Circle Internet Financial, LLC*
- *Deloitte Touche Tohmatsu Limited*
- *Digital Asset Holdings, LLC*
- *Global Arena Holding, Inc (GAHC)*
- *Monax Labs*
- *Ripple*

These organizations collectively shape market trends by focusing on innovation, enterprise adoption, and the integration of advanced technologies. Many of these companies actively pursue strategies such as new product launches, acquisitions, and strategic partnerships to strengthen their competitive position.

[5]https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market

4.2 Market Share & Adoption Rate

Given the nature of the patented blockchain technologies, the market share has been estimated by considering the role these inventions can realistically occupy within the broader global blockchain ecosystem. The blockchain market might comprise other technologies and/or features (i.e., market alternatives) that would not overlap with concepts of blockchain solutions related to the subject inventions. Considering the breadth of technologies that make up the global blockchain ecosystem and acknowledging that the subject inventions address a well-defined segment within this expanding market, it is reasonable to assume that the addressable market for these patented technologies would fall within a modest range, typically between **0.1% to 0.5%** of the global blockchain market. For the purpose of valuation, a midpoint estimate of **0.2%** has been selected as a conservative and reasonable figure. This value reflects both the potential applicability of the inventions and the competitive environment, where numerous alternative technologies exist that do not intersect with the concepts covered by the subject patents.

Furthermore, achieving a high product adoption rate is key to the success of any product. The adoption rate is one of the important factors in determining the market value of a product. Importantly, the rate at which a product is taken up has a great effect on the revenue that goes to the developer of the product. As often happens, initial uptake is low, and adoption grows slowly as people become aware of the product, try it out, and use it[6].

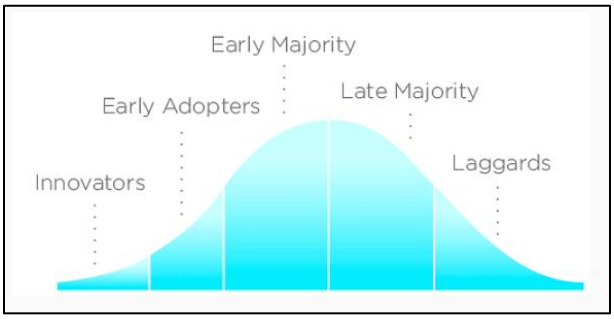


Figure 6 Generalized Adoption Curve for a New Product[7]

From the market research, it is observed that many companies are working in the blockchain domain (please refer to Section 4.3) and many products in the market offer digital identity verification and property access management solutions. To model potential growth in market adoption over the forecast period, the adoption rate for the patented technologies has been assumed to increase incrementally by **4%, 8%, and 12%,** respectively, over successive four-year intervals. This approach reflects the possibility of accelerated uptake as the technologies gain recognition, licensing agreements are executed, or integration into commercial solutions expands. By incorporating these incremental adoption rates, the

[6] https://fullenrich.com/glossary/product-adoption-rate

[7] https://www.cutter.com/article/measuring-adoption-new-business-technologies-489531

valuation captures a range of realistic growth scenarios and provides a more nuanced view of the potential market penetration and associated revenue over the patent lifecycle.

PRELIMINARY CALCULATIONS

Blockchain Technology Market (billion USD)							
Factors	**2025 (A)**	**2026 (B)**	**2027 (C)**	**2028 (D)**	**2029 (E)**	**2030 (F)**	**2031 (G)**
Global Blockchain Technology Market Size (~90.1% CAGR)	59.5	113.0	214.9	408.5	776.6	1476.2	2806.3
% share of this technology (<1%) + adoption increase by 4, 8, and 12% the forecasted years.	0.0020	0.0021	0.0022	0.0022	0.0023	0.0025	0.0027
Annual Revenue (Gross)	0.12	0.24	0.46	0.92	1.82	3.73	7.66

Blockchain Technology Market (billion USD)							
Factors	**2032 (H)**	**2033 (I)**	**2034 (J)**	**2035 (K)**	**2036 (L)**	**2037 (M)**	**2038 (N)**
Global Blockchain Technology Market Size (~90.1% CAGR)	5334.9	10141.6	19279.2	36649.7	69671.0	132444.6	251777.2
% share of this technology (<1%) + adoption increase by 4, 8, and 12% the forecasted years.	0.0029	0.0032	0.0036	0.0040	0.0045	0.0050	0.0056
Annual Revenue (Gross)	15.72	32.28	68.73	146.34	311.58	663.38	1412.42

4.3 Present Market Applicability

EXISTING PRODUCTS & TECHNOLOGIES

According to a recent survey, enterprises are particularly optimistic about blockchain adoption. The study revealed that nearly 90% of businesses surveyed have already implemented blockchain technology to some extent, and 87% are planning to invest in it in the coming years[8]. The integration of **Artificial Intelligence (AI) and blockchain** is transforming the landscape of digital identity management. By combining blockchain's immutable, decentralized ledger with AI-driven analytics, organizations can create secure, verifiable, and intelligent identity systems. Blockchain ensures that identity data is tamper-proof, traceable, and controlled by the user, while AI enables real-time verification, anomaly detection, and predictive risk assessment. Together, these technologies provide a robust framework for digital identity, enhancing security, reducing fraud, and streamlining access management for individuals, enterprises, and government agencies. The synergy of AI and blockchain not only strengthens trust in digital transactions but also enables scalable, automated identity solutions in a rapidly evolving digital ecosystem[9].

The adoption of blockchain technology in the enterprise landscape is happening faster than anticipated. Some of the exemplary companies with their products, somewhat in-line with the subject patents, have been listed below. Based on the conducted quick product search, it is observed that there are existing solutions for authenticity verification and access control to a property that are used for authentication and access for a user.

*(**Note**: It should be noted that this analysis is not an infringement search but rather an indicative assessment highlighting use of blockchain technologies in the existing market products.)*

Nonetheless, increased venture capital funding and investment in blockchain technology, widespread implementation of blockchain solutions in banking and cyber security, widespread adoption of blockchain solutions for payment, access verification, digital identities, and rising government initiatives are all contributing to the high growth rate of the blockchain market. Considering the advancements in blockchain services, it is believed that more market players would be willing to adopt the technology disclosed by the subject invention in the coming future. It is also believed that blockchain will be the most promising technologies in the coming years, and the current insistent research work being done in this domain certainly indicates that the subject patents hold good futuristic potential.

[8] https://linkedin.com/pulse/why-90-enterprises-adopting-blockchain-paul-lucki/
[9] https://consensys.io/blockchain-use-cases/digital-identity

Few related market products/technologies with respect to US10878429B2:

1. EVERNYM

Evernym is a digital identity company that uses distributed ledger technology to create secure and verifiable digital identities. Evernym's platform allows users to create and manage their own digital identities, which can be used to validate their identity and access services without having to share their personal information. Evernym also offers a solution for verifying the authenticity of government-issued IDs. Evernym's solution works by storing a hash of the government-issued ID on the distributed ledger technology. For example, whenever a user wants to verify their identity, they can simply share their digital identity with the verifier. The verifier can then compare the hash of the government-issued ID on the distributed ledger technology to the hash of the digital identity that the user is sharing. If the two hashes match, then the verifier can verify that the user's digital identity is authentic.

2. IDSCAN.NET

IDScan.net has introduced Digital Identity Validation (DIVE) API which is a tool used for verifying user identities digitally. It uses a combination of ID scanning and selfies to securely and accurately verify a user's identity. For example, when a user opens or clicks on a link sent via SMS, the user is redirected to IDScan.net web page. The user is then prompted to take three images: the front of their ID, the back of their ID, and an optional selfie. Once the user has captured the required images, they submit them to the IDScan.net DIVE API. The IDScan.net DIVE API uses a combination of computer vision techniques (OCR) and machine learning algorithms to verify the identity of the user. The DIVE API first analyzes the captured images to ensure they meet the requirements and are free from anomalies. The DIVE API then phrases the ID document using both PDF417 barcodes and Machine-Readable Zones (MRZ) to extract relevant information such as name, date of birth, and expiration date. The DIVE API also uses advanced machine learning algorithms to verify authenticity of the ID document. It checks for visual security features, document integrity, and inconsistencies in the extracted data. The DIVE API utilizes liveness detection techniques to ensure that the user is a real person and not attempting to use a fake ID or photograph and after the verification is complete, the IDScan.net DIVE API returns the results to the website.

3. IBM

IBM has introduced blockchain for digital identity and credentials which allow individuals, organizations, and institutions to manage, share, and verify digital identities and credentials. Individuals create their digital identities on the blockchain by providing their personal information and verifying their identity with a trusted issuer. Organizations and institutions issue credentials to blockchain which include diplomas, certifications, licenses, and other forms of proof of achievement and affiliation. Individuals can share their credentials with others by providing a link to their blockchain profile. Verifiers can then check the validity of the credentials on the blockchain.

4. DOCK.IO

Dock.io is a blockchain based solution for managing digital identities by providing secure, tamper-proof, and verifiable credential issuance, storage, and verification. The solution utilizes a combination of cryptography a blockchain technology to ensure the integrity and authenticity of digital identities. Each individual or entity is assigned a unique DID (Decentralized Identifiers), which serves as a digital address that represents their identity on the Dock blockchain. DIDs are similar to usernames but are cryptographically linked to an individual's private keys, ensuring ownership and control over their identity data.

5. NEC

NEC is a digital identity management through blockchain which provides a significant improvement in security, speed of transaction and user experience. The solution offers various applications in the real world, such as empowering individuals to control their personal data, addressing the challenges faced by refugees without proper documentation, eliminating bureaucratic passport creation processes, enhancing security and privacy of medical records and intellectual property, and simplifying KYC processes. By storing digital identity on a shared ledger, banks can access relevant data with customer consent, facilitating compliance with regulations and ensuring the protection of patient data. This solution also simplifies KYC processes, allowing banks to access relevant data with customer consent and perform due diligence.

6. ACCENTURE

Accenture has developed a digital identity prototype to modernize identity management for organizations and individuals. Utilizing blockchain and biometrics, the system simplifies establishing, tracking, and maintaining digital identities, making them more efficient, user-friendly, secure, and less susceptible to fraud. The system is interoperable with other databases, ensuring data remains in its original location, and works with mobile, connected, or standalone devices.

7. WIPRO

Wipro has introduced Decentralized Identity platform which is powered by blockchain and enables individuals, entities, and devices to hold their identity in a secure wallet that can be used to prove their identity, leveraging the trustable verifiable credentials that are issued to them by various entities. The solution allows authorized issuers to grant identity information to identity subjects like Verifiable Credentials, which are based on the subject's user records. Verifiers create a verification template with a QR code list of issuers, and the subject scans the code to retrieve the relevant credential. The subject selects attributes from the credential, ensuring the validity and ownership of the claims without the verifier reaching out to the issuer.

8. MICROSOFT

Microsoft Entra Verified ID with Face Check allows organizations to verify identities instantly and securely by combining verifiable credentials with facial verification. When identity proof is needed, a verifier displays a QR code that the user scans with the Microsoft Authenticator app to access their digital credential, such as a passport or employee ID. For assurance, Face Check prompts the user to take a live selfie. Azure performs a liveness test and compares selfies with the credential photo, generating a confidence score without storing any images. The application then sends a digitally signed proof and the Face Check result to the verifier, who validates the signature, issuer, and credential status. If all checks pass, the user's identity is confirmed and access is granted.

9. TRINSIC

The Trinsic Identity Acceptance Network is a decentralized identity platform designed to let individuals and organizations verify digital credentials securely. Trinsic shows how users can present verifiable credentials such as a driver's license, employee ID, or certificate directly from their digital wallet when interacting with a verifier (like a business or government portal). The process starts when a verifier displays a QR code requesting proof of a specific credential. The user scans the QR code using the Trinsic Wallet app, which holds their credentials. The app sends a cryptographically signed presentation to the verifier, proving the information's authenticity without exposing unnecessary personal data. The Trinsic network acts as a trust layer between issuers (who create credentials), holders (individuals who control them), and verifiers (who need to check them). All verification happens instantly using decentralized identifiers (DIDs) and verifiable credential standards, ensuring that users stay in control of their data while verifiers can confidently confirm authenticity.

10. VERIDOC GLOBAL ID

VeriDoc Global is an anti-fraud document verification system that uses blockchain and QR code technology to ensure that any ID or document viewed by a user is the true, original version issued by an authorized source. When an organization creates an ID or document, VeriDoc generates a unique cryptographic hash (a digital fingerprint) for that file. This hash is then stored securely on a blockchain and

also embedded into a QR code printed on the physical or digital ID. To verify authenticity, the user can scan the QR code using a smartphone app. The app retrieves the original, verified version of the ID from the blockchain and displays it on the screen. The user can then visually compare the ID they're holding with the verified version to confirm it hasn't been tampered with. Because blockchain records are immutable, they can't be altered or deleted. Any attempt to forge or modify the ID would result in a mismatch between the document's QR code and the blockchain record. This makes VeriDoc's system highly effective at preventing counterfeit IDs and fake certificates. Its applications extend across multiple domains, including identity cards, driver's licenses, academic certificates, medical records, legal documents, and financial papers.

11. DOCUSHIELD

DocuShield provides a blockchain-powered verification system that confirms document authenticity without exposing or sharing the actual content. When a document is created or received, it remains securely stored within the organization's infrastructure and is never uploaded or shared externally. The system generates a unique cryptographic hash, which serves as a digital fingerprint of the document. This hash does not contain any document data but can prove its integrity since even the smallest change would produce a completely different hash. The generated hash is then recorded on a private blockchain ledger, ensuring that the proof of authenticity cannot be altered or deleted. When verification is required, the system recalculates the document's hash and compares it with the blockchain record. If both match, the document is confirmed as genuine and untampered. Every verification action is logged in real time, providing a transparent audit trail for accountability and security without compromising the privacy of the original document.

Few related market products/technologies with respect to US11257098B2, US11836743B2 and US12223517B2:

Presently available products or features have not yet adapted Hyperledger for storing the history of the access key and access log.

1. TESLA

A Tesla key fob is a device that allows a user to lock and unlock when the key fob is within a short distance. This feature uses a low-power radio signal to detect the presence of the key fob and communicate with the vehicle's sensors. The Tesla key fob also contains an RFID chip that is used to authenticate the key fob when it is placed against the B-pillar of the vehicle or tapped on the center console.

Tesla also allows its users to unlock their cars by using the Tesla mobile app. The Tesla mobile app enables drivers to manage various aspects of their cars, and it can also be used to lock, unlock, and start a vehicle. Tesla's app can remotely unlock and start all its vehicles, such as models X, Y, S, and 3. To unlock a Tesla car, the user must ensure that both the app and car are connected to a cellular network. Additionally, mobile access should be activated on the touchscreen. For example, users should open the Tesla app and

tap Controls, followed by Unlock. Whenever a user taps yes on the confirmation pop-up window, it will instantly unlock the car doors.

2. HID GLOBAL

The HID Mobile Access solution allows users to use a mobile device as a credential to access doors, networks, services, and more. For example, employees can unlock their office using their iPhone or Apple Watch by adding an employee badge to their Apple Wallet. Further, employees can access office doors, elevators, turnstiles, multifunction printers, and much more using just their iPhone or Apple Watch. Employee badges in Apple Wallet integrate into the HID access control systems. Employees just need to hold their iPhone or Apple Watch near the reader to unlock it. In the HID Mobile Access solution, credentials (access key) are stored on the mobile device (Apple wallet), the request for access key is not sent to the server.

3. BMW

BMW Digital Key utilizes near-field communication such as NFC chips in smartphones or smart watches to communicate with BMW NFC antennas. Whenever a user places their phone or smart watch near the NFC antenna on the driver's door handle, the vehicle will recognize it and unlock the door. The user can then start the engine by placing the smart phone and smart watch on the NFC antenna in the center console.

4. NISSAN

Nissan offers remote door lock and unlock feature which operates through a combination of radio frequency (RF) technology and transponder embedded within the vehicle's key fob or a smart phone app (Nissan connect). For example, the driver opens the Nissan connect service app on their smartphone and selects 'Remote door Lock/Unlock' option. The app establishes a secure connection with the vehicle's telematics module, which is typically connected to the vehicle's cellular network. The driver then enters the PIN for the remote lock/unlock feature, ensuring security and preventing unauthorized access. The app sends a secure communication to the vehicle's telematics module, instructing it to send a lock/unlock signal to the dashboard. The dashboard processes the signal and unlocks the door.

5. VOLKSWAGEN

Volkswagen makes use of a transponder system in the remote key fob that communicates wirelessly with the car's computer. The transponder sends a unique signal that the car can identify signal that the car can identify, and when the key fob is pressed, the car unlocks or locks the doors. This feature allows drivers to lock or unlock their car doors, start, or stop their engines using a smartphone. This feature provides a variety of safety features, such as Automatic Crash Notification, and stolen vehicle locator. For example, a user can use Remote Access to unlock the vehicle doors and turn on notifications for stolen vehicle locator and crash notification.

6. AUDI

Audi Advanced Key is a keyless entry technology designed for car drivers, allowing them to start or open their cars without having to reach for their keys. The Audi Advanced Key connects proximity sensors in car doors and trunk lids, activated by a radio pulse generator within five feet of the vehicle. When using a door handle or trunk, the Audi automatically unlocks. Audi also allows its users to access their vehicles through the Audi app. The Audi app uses Bluetooth to connect with the vehicle. Once the vehicle is connected, the user can use the app to lock and unlock doors, start the vehicle's engine, and more. For example, to unlock the doors, the user needs to open the app and tap the 'Unlock' button. The app then sends a signal to the vehicle, which unlocks the door.

7. HYUNDAI

Hyundai's Digital Key 2 system allows users to unlock, start, and share access to their vehicles using a smartphone, eliminating the need for a physical key. The system uses advanced Near-Field Communication (NFC) and Ultra-Wideband (UWB) technology to recognize when the user is nearby and automatically unlocking the doors. Here, the smartphone securely stores the digital key in its memory and transmits it to the vehicle's onboard control unit (ECU) via NFC, Bluetooth Low Energy (BLE), or UWB. The ECU validates the digital key before granting access, and once validated, it unlocks the vehicle.

Below are presented a few Satellite Communication Services where the subject inventions might be applicable.

8. INMARSAT

Inmarsat offers secure satellite communication services for the aviation, maritime, defense, enterprise, and government sectors. The Inmarsat solution provides aircraft positioning data for air traffic management, enabling planes to fly closer together and facilitating communication between pilots and controllers. Inmarsat Classic Aero offers surveillance through the Automatic Dependent Surveillance Contract (ADS-C) and communications through Controller Pilot Data Link Communications (CPDLC), meeting ICAO requirements. SB-S from Inmarsat is a secure broadband with speed IP connection for operations and safety communications, providing the same services as Classic Aero and enabling

operational efficiencies such as engine monitoring, real-time weather, telemedicine, and preventive maintenance.

9. INTELSAT

Intelsat provides satellite communication services worldwide, serving sectors like media, broadband, government and mobility. Intelsat's secure global network offers broadband mobile connectivity at speeds that surpass traditional narrowband solutions, enabling enroute communications, intelligence, surveillance, reconnaissance, disaster recovery, and remote operations. Intelsat's aeronautical solutions utilize high-throughput satellite technology and its network to provide reliable, high-performance connectivity for governments and emergency response teams.

10. VIASAT

ViaSat is a satellite broadband service that also provides secure communications for government and commercial applications. ViaSat offers defense satellite communications, tactical networking, and cyber security solutions to provide a comprehensive approach with performance advantages, including multi-band, flexible SATCOM terminals and EW-resistant networks, ensuring resilient, end-to-end communications across domains and missions. Viasat's real-time HD video and broadband maritime communications services offer Search and Rescue (SAR) missions, whether searching for missing persons or locating lost aircraft, vessels, or wreckage. These services offer operational advantages, speeding up progress and increasing the likelihood of success in global SAR efforts.

11. SES S.A.

SES is a global satellite operator offering a range of satellite operators offering a range of satellite communication services which includes secure data transmission for government, aviation and maritime applications. SES's commercial maritime offering utilizes a fleet of high-throughput satellites and the Skala Global Platform ground system, enabling ships of all sizes to benefit from exceptional maritime connectivity. SES offer network services for digital transformation, cloud connectivity, and crew safety.

Further, we have seen multiple companies such as Eutelsat Group (Eutelsat + OneWeb), Thales Alenia Space, Hughes Network Systems, Telesat, Globalstar, and Cobham SATCOM that, similar to the companies discussed above, provide a wide range of satellite systems and secure space communication solutions supporting defense, government, and commercial missions. These organizations deliver capabilities such as resilient satellite networks, high-throughput broadband services, mobility connectivity for aviation, encrypted communication platforms, that ensure reliable and secure data transmission across global operating environments.

5 Evaluation Method

5.1 A Hybrid Approach to Calculate Fair Market Value

A Hybrid Approach has been followed to evaluate the appropriate Fair Market Value for the patents under study.

- The first part of this hybrid approach involves market analysis of the technology as covered by the IP understudy, understanding how much revenue would be generated by the implementation of the subject technology, whether the technology is fresh or obsolete in the market, and risk factors, etc. Along with this, many other factors influencing the market are considered to arrive at an expected Fair Market value.
- The second part of this hybrid approach involves rigorous analysis of the Intellectual Property under study. The first part of the hybrid approach would indeed give us an expected revenue from the commercial exploitation of technology. However, different factors affect the applicability of a patent. These factors need to be taken together to understand what is the actual worth of the Intellectual Property which is under study. For example – what problem is being solved by the patent is the problem being solved prevalent in the market, availability of similar products in the market, etc.

Thus, this overall Hybrid Approach proceeds in three steps:

1. **Market Evaluation of Portfolio**
   Output: A figure representing expected revenue

2. **Intellectual Property Evaluation of Portfolio**
   Output: A weighted factor (0.00 to 1.00)

3. ***Net Fair Market Value = Step 1 Output X Step 2 Output***

6 Calculation of Fair Market Value

6.1 Step 1: Market Evaluation of Technology

The approach followed in this evaluation involves market analysis of the technology covered by the IP under study in the forecast years (2025-2038); to understand how much revenue would be generated by the implementation of the subject technology, along with consideration of many other factors influencing the market to arrive at an expected value. All the below values are in billions of USD.

Factors	2025 (A)	2026 (B)	2027 (C)	2028 (D)	2029 (E)	2030 (F)	2031 (G)
Annual Revenue (Gross)	0.12	0.24	0.46	0.92	1.82	3.73	7.66
R&D Cost ~10%	0.01	0.02	0.04	0.07	0.15	0.30	0.61
Annual Revenue (Net)	0.11	0.22	0.43	0.85	1.67	3.43	7.05
Net Profit margin ~10%	0.01	0.02	0.04	0.08	0.17	0.34	0.70
Average IP contribution in Net Profit (32%)	0.004	0.007	0.014	0.027	0.053	0.110	0.23
Tax and Duties ~21%	0.001	0.001	0.003	0.006	0.011	0.023	0.05
Profit after Tax	0.003	0.005	0.011	0.021	0.042	0.087	0.18
Discount Rate ~10%	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Discount Factor for the NPV Calculation	0.91	0.83	0.75	0.68	0.62	0.56	0.51
Adjusted NPV after Discount Factor	0.003	0.005	0.008	0.015	0.026	0.049	0.091
Product Factor	0.30	0.30	0.30	0.30	0.30	0.30	0.30
Net Present Value (NPV)	0.001	0.001	0.002	0.004	0.008	0.015	0.027

Factors	2032 (H	2033 (I)	2034 (J)	2035 (K)	2036 (L)	2037 (M)	2038 (N)
Annual Revenue (Gross)	15.72	32.28	68.73	146.34	311.58	663.38	1412.42
R&D Cost ~10%	1.26	2.58	5.50	11.71	24.93	53.07	112.99
Annual Revenue (Net)	14.47	29.70	63.23	134.63	286.65	610.31	1299.43
Net Profit margin ~10%	1.45	2.97	6.32	13.46	28.67	61.03	129.94
Average IP contribution in Net Profit (32%)	0.46	0.95	2.02	4.31	9.17	19.53	41.58
Tax and Duties ~21%	0.10	0.20	0.42	0.90	1.93	4.10	8.73
Profit after Tax	0.37	0.75	1.60	3.40	7.25	15.43	32.85
Discount Rate ~10%	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Discount Factor for the NPV Calculation	0.47	0.42	0.39	0.35	0.32	0.29	0.26
Adjusted NPV after Discount Factor	0.171	0.318	0.616	1.193	2.309	4.469	8.650
Product Factor	0.30	0.30	0.30	0.30	0.30	0.30	0.30
Net Present Value (NPV)	0.051	0.096	0.185	0.358	0.693	1.341	2.595

6.2 Other Considered Factors

Market Size, **Market Share**, **and Adoption Rate** are already discussed in Section 4.1 and Section 4.2 Other legends used in the above calculation of the fair market value are as follows:

- **Annual Revenue (Gross):** This is the product of the global market size and the market share with the increasing adoption of the subject patented technology. This figure will give an idea of how deeply the subject technology would penetrate the market.
- **R&D Cost:** These are the costs utilized in innovative activities undertaken by corporations in developing new services or products or improving existing ones. Research and development expenses can be defined as an expense arising from studies and product development processes.

  Based on market research, it is seen that prominent market players in the blockchain technology market put a considerable amount of their net revenue into the research and development of new technologies. For example, IBM and Microsoft put around 11.9% and 11.5% of their revenue in R&D activities. However, IBM and Microsoft might utilize the said R&D percentage amount for various other activities as well besides blockchain technology. Additionally, smaller and medium-sized enterprises typically invest a lower percentage of revenue in R&D, whereas dedicated blockchain-focused firms may invest a higher proportion. To account for this diversity and capture a representative estimate across the market, we have considered the average R&D expenditure in the blockchain technology domain to be approximately **5-10%** of revenue. For this analysis, we have used an **8% (0.08)** R&D allocation.

  Refer to the table below for detailed calculations.

S. No	Company	R&D share percentage
1	**IBM Corporation**	For 2024, R&D Expenses: $ 7,479 million and Total Revenue: $ 62,753 million R&D Percentage = (R&D Expenses / Total Revenues) × 100 = (7,479/62,753) × 100 = 11.9% *Source: https://www.ibm.com/downloads/documents/us-en/1227c12d3a38b173 (Page 46)* *Source: https://discern.io/metric/rd-expenses-as-a-percentage-of-revenue/ (Formula)*
2	**Microsoft Corporation**	For 2025 (Year Ended June 30), R&D Expenses: $ 32,488 million and Total Revenue: $ 281,724 million R&D Percentage = (R&D Expenses / Total Revenues) × 100 = (32,488 /281,724) × 100 = 11.5% *Source: https://www.microsoft.com/investor/reports/ar25/index.html*
3	**RYVYL**	For 2024, R&D Expenses: $ 3,848 thousand and Total Revenue: $ 55,998 thousand R&D Percentage = (R&D Expenses / Total Revenues) × 100 = (3,848/55,998) × 100 = 6.87% *Source: https://www.nasdaq.com/press-release/ryvyl-reports-q4-2024-and-full-year-2024-financial-results-and-provides-business*

- **Annual Revenue (Net):** This is the revenue calculated after deducting the R&D cost.

  Net Profit Margin: The net profit margin (NPM), or simply net margin, measures how much net income or profit is generated as a percentage of revenue. The profit margin is the profit earned by the entities concerned after reducing all company expenses from the Annual Revenue. During the financial analysis, it was observed that while some companies achieve high net profit margins (NPM) of up to 40%, smaller and medium-sized organizations generally report lower margins. Overall, blockchain companies tend to maintain profit margins in the range of 5-15%. Therefore, to account for the broad spectrum of company sizes, from small to large corporations, a conservative NPM of approximately **10%** has been considered for the current study.

  Refer to the table below for detailed calculations.

S. No	Company	Net Profit Margin percentage
1	**IBM Corporation**	For 2024, Net income: $ 6,023 million and Total Revenue: $ 62,753 million = (Net income / Total Revenues) × 100 Net Profit Margin = (6,023 /62,753) × 100 = 9.6% *Source: https://www.ibm.com/downloads/documents/us-en/1227c12d3a38b173 (Page 46)* *Source: https://www.investopedia.com/terms/n/net_margin.asp (Net Profit Margin Formula)*
2	**Microsoft Corporation**	For 2025 (Year Ended June 30), Net income: $ 101,832 million and Total Revenue: $ 281,724 million = (Net income / Total Revenues) × 100 Net Profit Margin = (101,832 /281,724) × 100 = 36.14% *Source: https://www.microsoft.com/investor/reports/ar25/index.html*
3	**The Linux Foundation**	For 2023, Net income: $ 10.81 million and Total Revenue: $ 196.03 million = (Net income / Total Revenues) × 100 Net Profit Margin = (10.81 / 196.03) × 100 = 5.52% *Source: https://projects.propublica.org/nonprofits/organizations/460503801*
4	**DTCC**	For 2024, Net income: $481,494 thousand and Total Revenue: $2,485,973 thousand = (Net income / Total Revenues) × 100 Net Profit Margin = (481,494 /2,485,973) × 100 = 19.36% *Source: https://www.dtcc.com/annuals/2024/files/DTCC-Annual-Report-2024-Print.pdf (page 72 of PDF)*

- **IP Contribution to Net Profit:** At the lower end, the IP is considered to contribute 25% to the net profit margin[10,11], considering other expenditures for selling a product in the actual market. This contribution can be higher considering the breadth of coverage of the IP portfolio. Considering the breadth of the subject portfolio, we have considered the value of this parameter as 32% (0.32).
- **Tax and Duties:** These refer to the taxes, duties, excise, and other fixed costs that are incurred by the entities. Every country has their own tax structure[12,13,14,15,16.] For example, The United States imposes a tax on the profits of US corporations at a rate of 21 percent. Thus, 21% of the absolute profit would be spent in the form of taxes. These figures for Europe, and Asia-Pacific, are between 15 and 25%. For the current study, we have considered this factor to be average **21% (0.21)**.
- **Profit after tax:** It is the true profit earned via IP after adjusting it for various tax-related fixed costs.
- **Discount Factor:** The discount factor considers the risks that have an impact on the generation of the future revenue or income stream. The risk factor or the discount rate considers the overall market risk, the specific industry risk, and the risks associated with specific IP assets and operations being considered.

  Discount Factor = 1 / (1 + r)^n, where "r" is the discount rate and "n" is the number of periods.

  The discount rate is the key factor in business valuation that converts future dollars into present value as of the valuation date. Companies with larger cash flows are likely to be more valuable, as are those with cash flows that are growing at a faster rate. Now, if the future cash flows are less certain, they are deemed to be riskier, which reduces the value of the business. The discount rate "discounts" future cash flows to a present value. Specifically, in patent valuation, the discount rate is a risk- and time-adjusted rate used to convert uncertain future patent-related income into a current dollar value.

  As per market statistics, a **discount rate of 10%** is generally accepted as a reasonable estimate for approximating the long-term value of a patent portfolio[17, 18,19].

---

[10] https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/gvi-profitability.pdf
[11] https://www.royaltyrange.com/home/blog/what-are-patent-licensing-royalty-rates
[12] https://taxsummaries.pwc.com/united-states/corporate/taxes-on-corporate-income
[13] https://taxfoundation.org/data/all/eu/corporate-tax-rates-europe-2024/#:~:text=On%20average%2C%20the%20European%20countries,was%2023.45%20percent%20in%202023.
[14] https://taxfoundation.org/data/all/global/corporate-tax-rates-by-country-2023/#:~:text=South%20America%20has%20the%20highest%20average%20statutory%20corporate%20tax%20rate,all%20regions%20at%2019.80%20percent.
[15] https://taxsummaries.pwc.com/united-arab-emirates/corporate/income-determination#:~:text=A%209%25%20effective%20tax%20rate,of%20the%20UAE%20CT%20Law.
[16] https://tradingeconomics.com/country-list/corporate-tax-rate?continent=africa
[17] https://patentpc.com/blog/how-to-use-the-income-approach-to-accurately-value-ip?utm_source=chatgpt.com
[18] https://www.copperpodip.com/post/adapting-weighted-average-cost-of-capital-wacc-for-accurate-patent-valuation?utm_source=chatgpt.com
[19] https://mercercapital.com/article/understand-the-discount-rate-used-in-a-business-valuation/

- **Adjusted NPV after Discount Factor:** It is the Net Present Value after considering the amount for the Risk factor.
- **Product Factor:** The Product factor implies how important the subject technology is to the overall product. A value of 1 would mean that the subject technology is completely relevant to all the parts of the product.

  A **product factor of 30%** has been considered reasonable for this valuation, reflecting the proportional contribution of the patented technologies to the overall functionality of commercial blockchain-based products. While the subject inventions represent meaningful enablers such as innovations ledger-based digital identity storage and user authentication; the complete operation of blockchain products typically depends on multiple backend components including network protocols, distributed ledgers, encryption modules, cloud infrastructure, and user interface layers. Accordingly, a 30% product factor provides a balanced and defensible estimate, recognizing the significance of the patented technologies to product differentiation and performance, while appropriately discounting the numerous other technical and operational components required to deliver the end product.
- **Net Present Value (NPV):** The Adjusted NPV takes into consideration the product factor.

NET NPV = Adding Adjusted NPV values (A-N) for all the forecast years i.e., 2025 to 2038

= **USD 5.38 billion**

6.3 Step 2: Intellectual Property Evaluation of Technology

The Intellectual Property has been evaluated based on the following pointers to calculate an IP factor that determines the overall value. The IP factor as calculated for the subject patent(s) is analogous to a percentile score given to the subject patent(s) with respect to an ideal IP in the related technology space. To keep parity between different parameters, we have assigned different weightages to different parameters. For example, parameters such as infringement and licensing potential have been assigned a weightage of 2 whereas parameters such as legal aspects and geographical coverage have been assigned a weightage of 0.5. Moreover, each parameter has been assigned a score from 1 to 5.

1. **PRACTICAL APPLICABILITY** **(Weightage: 1.5; Score: 5)**

   This factor represents whether the invention covers a practically/commercially viable solution that is ready to be introduced in the market. This factor would be rated from 1 to 5, where 1 represents that the invention in its existing form may not have substantial commercial applicability, and 5 represents that the disclosed invention presents a commercially viable solution with very minimal, or no changes required as such.

2. **TECHNOLOGY INFLUENCE** **(Weightage: 1; Score: 4)**

   This factor represents the impact of the invention on the existing solutions/technology existing in the market. This factor would be rated from 1 to 5 based on the disruptive nature of the subject invention – whether the subject invention is solving a common problem and would only act as an alternative to the existing solutions or whether it can completely replace the existing solutions. For example, 1 could mean that the disclosed invention would have an insignificant impact as there are already existing solutions that are being widely used/accepted, and 5 would mean that either there are no existing solutions or that the technology would be significantly advantageous/better than the current solutions.

3. **DEVELOPMENTAL STAGE** **(Weightage: 1; Score: 5)**

   This factor represents the developmental stage of the subject invention, i.e., whether the idea is at a very nascent stage with no testing being performed to test the applicability of the invention, or if the subject invention is already being implemented in the market. This factor would be rated from 1 to 5, where 1 represents that just a rough idea exists presently with no testing done yet, and 5 represents that the subject invention already has a market presence.

4. **BREADTH OF TECHNICAL COVERAGE** **(Weightage: 1.5; Score: 5)**

   This factor represents whether the subject invention disclosure has a multitude of aspects that can be covered via multiple patents or whether the invention has very few aspects that have already been covered by the patents. This factor would be rated from 1 to 5, where 1 represents that there are very few aspects that the subject invention discloses and the same has already been covered in

the existing patent(s), and 5 would represent that the subject invention potentially has a variety of aspects that are either already covered via multiple patents or can be covered via additional continuation applications.

5. DEMAND TREND **(Weightage: 2; Score: 5)**

This factor represents the market demand for the subject invention/idea. This factor would be rated from 1 to 5, where 1 represents that the subject technology is outdated and there is no current market demand for the same, and 5 represents that the current market demand for the subject technology is very high or is on a rise.

6. GEOGRAPHICAL RELEVANCE **(Weightage: 2; Score: 5)**

This factor represents the potential applicability of the subject invention with respect to the nature of markets and/or jurisdictions, i.e., whether the invention is applicable to a very low, local, or specialized market, or whether the invention seems to have a very high, international, or very broad market. This factor would be rated from 1 to 5, where 1 represents that the subject invention will have applicability to only a local or a specialized market, and 5 represents that the subject invention seems to have applicability to a very broad market across multiple jurisdictions.

7. CROWDEDNESS **(Weightage: 1.5; Score: 4)**

This factor represents the quanta of competition of the subject invention in the existing market scenario, i.e., whether there are many or only a few similar existing products and technologies in the market. This factor would be rated from 1 to 5, where 1 represents that the subject invention will have an extremely difficult penetration in the market owing to the heavy competition, and 5 represents that the market penetration will be extremely easy due to the non-existence of products and technologies analogous to the subject invention.

8. GEOGRAPHICAL COVERAGE **(Weightage: 2; Score: 5)**

This factor represents the overlap of the protection that the subject technology has in terms of geographical relevance (jurisdictions with a majority share of the given market). This factor would be rated from 1 to 5, where 1 represents that the subject technology has coverage only in limited jurisdictions, and 5 represents that the subject technology has been covered in all the important jurisdictions for the given market.

9. INVENTION R&D **(Weightage: 0.5; Score: 4)**

This factor represents the extent of R&D required to achieve a market-ready product, in terms of difficulty and expense. This factor would be rated from 1 to 5, where 1 represents that the extent of R&D required would be very high, and 5 represents that the extent of R&D required would be very low.

10. MANUFACTURING/DEVELOPING **(Weightage: 1; Score: 5)**

This factor represents the extent of efforts required for manufacturing/practicing the invention or product. This factor would be rated from 1 to 5, where 1 represents that a dedicated manufacturing facility/plant will need to be set up (for example) for manufacturing/practicing the invention or product, and 5 represents that no specially equipped manufacturing facility/plant is required, and the existing manufacturing/developing resources would be sufficient to practice the invention.

11. PROFITABILITY **(Weightage: 1; Score: 5)**

This factor represents the profitability/revenues that the subject invention is likely to gather. This factor would be rated from 1 to 5, where 1 represents that the expected revenue/profitability is likely to be very low, and 5 represents that the expected revenue/profitability is likely to be very high.

12. INFRINGEMENT **(Weightage: 2; Score: 3)**

This factor represents whether there are existing market products that seem to be implementing the claimed invention. This factor would be rated from 1 to 5, where 1 represents that the subject invention does not seem to have any infringement yet, and 5 represents that the technology has widespread infringement or is a Standard Essential patent.

13. LICENSING POTENTIAL **(Weightage: 2; Score: 5)**

This factor represents whether the companies would be willing to obtain a license for the subject invention to implement the claimed invention in their products (for example). This factor would be rated from 1 to 5, where 1 represents that the subject invention will have a low chance that another company will seek the license the invention, and 5 represents that the invention holds a very good licensing potential.

14. LEGAL **(Weightage: 0.5; Score: 5)**

This factor represents whether the technical subject matter/invention/idea when productized will comply with applicable laws within the applicable jurisdictions or whether changes will need to be made to make the product compliant with the applicable laws. This factor would be rated from 1 to 5, where 1 represents that the product based on the subject matter would clearly be non-compliant with the applicable laws even after any amendments, and 5 would mean that the product would be compliant with the laws without any changes.

15. POSSIBLE HAZARDS **(Weightage: 0.5; Score: 5)**

This factor represents the possible hazards or side effects the invention/idea/product is likely to have on the environment/society. This factor would be rated from 1 to 5, where 1 represents that the invention/idea/product could be very dangerous for the environment/society, and 5 represents that the invention/idea/product would be very safe.

Sr. No.	PARAMETER	WEIGHTAGE	SCORE	WEIGHTED SCORE	MAXIMUM WEIGHTED SCORE
1	Practical Applicability	1.5	5	7.5	7.5
2	Technology Influence	1	4	4	10
3	Developmental Stage	1	5	5	5
4	Breadth of Technical Coverage	1.5	5	7.5	5
5	Demand Trend	2	5	10	7.5
6	Geographical relevance	2	5	10	7.5
7	Crowdedness	1.5	4	6	7.5
8	Geographical coverage	2	5	10	10
9	Invention R&D	0.5	4	2	5
10	Manufacturing/Developing	1	5	5	5
11	Profitability	1	5	5	5
12	Infringement	2	3	6	10
13	Licensing potential	2	5	10	10
14	Legal	0.5	5	2.5	2.5
15	Possible hazards	0.5	5	2.5	2.5
		CUMULATIVE SCORE		**93**	**100**
		IP FACTOR		**0.93**	

Scoring Description:

0 – 25: The monetization potential is very less for this patent.
26 – 50: The monetization potential is moderately high, and the invention somewhat solves the existing problems.
51 – 81: The monetization potential is high, and it is feasible to solve the existing problems using the invention.
81+: The monetization potential is very high. An overlapping market solution is already present in the market, but the present solution could replace existing solutions.

6.4 Step 3: Fair Market Value

Step 3 Output = Step 1 Output X Step 2 Output

= $ 5.38 billion x 0.93
= $ 5.001 billion

Based on all the calculations,

The Fair Market Value for the subject patent family under study is USD 5 billion

Non-Disclosure and Disclaimer

Non-Disclosure

Elevate or any of its subsidiaries, or any of their directors, officers, employees, agents, or representatives (together, "PERSONNEL") undertakes that all the client information shall be treated as confidential information and no part of such information will be used for any purpose whatsoever outside the intended scope of completing the search. Elevate will not use or share any part of the confidential information with third parties without your prior written approval.

Disclaimer

The patent valuation exercise is designed to provide an estimated fair market value for the subject patent portfolio. A robust and tested methodology has been followed in the analysis to deliver the most accurate information possible. However, some parameters considered in the study may be subjective and the results could vary based on different interpretations or perspectives. The methodology adopted by Elevate, along with various interpretations taken, have been documented in this report. We do not accept liability for any financial losses, missed opportunities, third party claims or any other adverse outcomes resulting from the utilization of this report.

About Us

Elevate is a global law company offering integrated legal operations, consulting, technology, and intellectual property solutions. Through its multi-disciplinary teams, which combine lawyers, engineers, technologists, and business experts, Elevate delivers cost-optimized, risk-mitigated outcomes for corporations, law departments, and leading law firms.

Elevate assists law firms, in-house legal teams, inventors, researchers, and businesses in making informed decisions related to IP, contracts, compliance, litigation, and business law through intelligent, scalable, and tech-enabled solutions.

Operating from a global footprint and supported by robust technology platforms, Elevate spans the full lifecycle of IP management and broader legal operations – from strategy and risk mitigation, through creation, maintenance, and monetization of IP, as well as contract lifecycle, litigation support, legal spend management, and compliance