International Journal of Geo-Information

MDPI

Article

B-GPS: Blockchain-Based Global Positioning System for Improved Data Integrity and Reliability

Seunghyeon Lee [1,†], Hong-Woo Seok [2,†], Ki-rim Lee [3] and Hoh Peter In [1,*]

[1] Department of Computer Science, Korea University, Seoul 02841, Korea; 2square@korea.ac.kr
[2] Department of Geoinformatic Engineering, Inha University, Incheon 22212, Korea; hwseok@inha.edu
[3] Department of Spatial Information, Kyungpook National University, Daegu 41566, Korea; geolee@knu.ac.kr
* Correspondence: hoh_in@korea.ac.kr
† These authors contributed equally to this work.

Abstract: When surveying national reference points using a global positioning system (GPS), appropriate work regulations pertaining to the surveying time must be observed. However, such data can be modified easily, so identifying non-compliance with work regulations and forgeries is challenging. If such incidents occur in cadastral surveys, it may result in financial damages to stakeholders, such as citizens and the state. Therefore, it is necessary to improve the reliability by ensuring the integrity of the GPS positioning data and allowing anyone to track them. In this study, a prototype system was developed to record GPS data and the corrections generated during survey processes using the Ethereum blockchain network. Blockchain is a distributed ledger system that prevents the manipulation of uploaded data without the need for a centralized institution by allowing anyone to check the data. Unlike in the past, the proposed system improves the data integrity and reliability for the entire survey process through blockchain, thereby ensuring transparency of the checks using smart contract addresses.

Keywords: blockchain; smart contract; GPS positioning; data integrity; data reliability

Citation: Lee, S.; Seok, H.-W.; Lee, K.-r.; In, H.P. B-GPS: Blockchain-Based Global Positioning System for Improved Data Integrity and Reliability. *ISPRS Int. J. Geo-Inf.* **2022**, *11*, 186. https://doi.org/10.3390/ijgi11030186

Academic Editors: Wolfgang Kainz and Peng Yue

Received: 11 February 2022
Accepted: 5 March 2022
Published: 9 March 2022

1. Introduction

A global navigation satellite system (GNSS) is a satellite-based navigation technology that determines the three-dimensional position at any time and location, and weather conditions developed by the United States (US) as GPS, Russia as GLONASS, Europe—known as Galileo, China—known as BeiDou, and so on. The positioning accuracy was dramatically improved with the development of these positioning systems [1]. Various types of positioning exist, such as static measurement, real-time kinematic (RTK), and smartphone location tracking. These systems are used in various fields that require precise positioning, such as those that involve drones of kinematic changes and in autonomous driving [2–6]. In both cases, correction information is received in real-time to estimate precise coordinates. The method of providing correction is divided into state–space representation (SSR) and observation space representation (OSR), such as single RTK and network RTK [7–9]. Moreover, there are other techniques, such as a satellite-based augmentation system (SBAS), wide area RTK (WARTK), and precise point positioning RTK (PPP-RTK) [10–12].

Geodetic surveys are currently being conducted using GNSS in various countries. In Korea, UK, and the USA, the survey and regulation of the operations of GNSS and network RTK usage are required within the accuracy of 3–10 cm. Depending on the grade, the USA requires accuracy up to 1 cm with the limited data latency to less than 2 s. Most network RTK techniques are used in GPS surveying are centralized systems, wherein the central server data of continuously operating reference stations (CORS) are also centralized. Accordingly, transmitting and receiving with the "Rover" are thus conducted based on this scheme [13].

In this process, the user can send "forged" ; the National Marine Electronics Association (NMEA) and the server can generate the Radio Technical Commission for Maritime Services (RTCM) message based on these data. Thus, there are limitations in that all of the data can be counterfeit [14]. There are several cases of manipulation of survey results in Korea and the USA, and the possibility of forgery and falsification by surveyors was confirmed during the survey using GPS. GPS not only identifies the location of an object, but it diversifies its role by analyzing the congestion level of traffic information and distributing the congestion level by routes in the vehicular navigation service. Considering these trends, positioning reliability improvement is also considered important. Samios et al. (2021) created an attack path for seismometers, accelerometers, and GPS receivers, and identified security vulnerabilities [15]. Thus, countermeasures are necessary because there are limitations in terms of the security and integrity of the GPS receiver and server-side data.

Research studies conducted on the identification of solutions of data forgery and falsification cases by centralized structures using blockchains is increasing. Unlike the traditional system, in which only a single group manages the database, the blockchain secures the integrity of the database by recording and storing data from multiple groups. Furthermore, by disclosing it to users, the transparency of data are secured. Kowaiski et al. (2021) confirmed the improvement of the trust relationship and security between business partners through blockchains in trade finance [16]. In turn, Majeed et al. (2021) improved blockchain technologies applied to smart cities and their reliability and security [17]. In turn, Li et al. (2021) proposed a framework using blockchain and improved positioning accuracy through data filtering [18].

Therefore, the current study was conducted to solve the problem of data forgery and falsification, which relates to the existing satellite survey system using the Ethereum blockchain. Assuming that there are no forged data in the communication between CORS and the server, and forged data in the communication between the user and the server, a blockchain-based decentralized satellite surveying system is implemented using data from the NMEA and RTCM. In the NMEA transmission/reception process, the received NMEA is transmitted to the server and recorded on the Ethereum network simultaneously. Subsequently, the RTCM received from the ground station is recorded on the Ethereum network, and correction is performed simultaneously. To this end, prototype software that communicates between the GPS receiver and the Ethereum blockchain network is produced, and the reliability and stability of this network is verified and compared with the existing system. It is crucial to prevent damage by securing the integrity of survey data, including surveyors and survey processes, but this has not been resolved in decades.

In this study, we solved this problem by uploading data to the blockchain in the process of obtaining the data at the software level. The contributions of this study are as follows: first, in the GPS positioning process, a blockchain-based positioning system is proposed to check data injection and compliance. Second, to improve the integrity of GPS data, blockchains using Keccak-256 functions, Merkle tree, and P2P-based consensus proof algorithms are applied to GPS positioning. Third, in order to improve the reliability of the GPS positioning process, the hash value on the blockchain makes it possible to verify the data source, the positioning record by the worker, and the positioning process of the positioning point. Fourth, the efficiency of introduction is evaluated by calculating the cost incurred when using the public blockchain.

The remainder of this paper is structured as follows. Section 2 presents some background on GPS positioning and blockchain technology, to illustrate the motivation of the study. Section 3 describes the flow of blockchain-based GPS positioning as proposed in this work, and presents a schematic, with explanations of the main algorithms in the software. Section 4 describes the checking of the operation of the software, and presents the results, as well as analyses of the cost and security concerns regarding the use of blockchain. Finally, Section 5 presents the conclusions of this study.

2. Background

2.1. GPS Positioning

As observation data, pseudorange, carrier-phase, and Doppler observations for each frequency are provided, and the pseudorange and carrier-phase are mainly used for navigation. The pseudorange is mainly used for smartphone navigation, etc., and it is possible to secure m-level accuracy for standalone positioning [19]. During the use of the carrier-phase, a dual-frequency GPS receiver is required to solve the integer ambiguity, and it is possible to secure cm-level accuracy through differential positioning with the reference station observations. Unlike the initial development of such a GPS for military purposes, the GPS is currently being used in various fields, such as geodetic surveying, autonomous driving, and a forecasting model [20]. In the case of a geodetic survey using GPS, precise positioning is possible within seconds–minutes. In the case of indirect leveling using GPS, 90% and 75% of time and costs are reduced, respectively, compared to the case of direct leveling through the level [21]. GPS surveying is divided into real-time and post-processing.

In real-time GPS surveying, the multi-reference station-based network RTK that overcomes the limitation of the baseline distance is preferred over the single RTK due to spatial decorrelation when the baseline distance increases [22]. In post-processing, GPS software, such as GipsyX/RTGx of NASA JPL and Bernese of Bern University, are used to acquire precise coordinates, where accuracy is mm-level. Real-time surveying can converge within a few seconds using RTCM messaging, such as Flächen–Korrektur parameter (FKP) correction or virtual reference station (VRS) observations, and coordinates with cm-level accuracy can be acquired. It was difficult to secure visible satellites in urban areas using only GPS/GLONASS, so the FIX rate of integer ambiguity during positioning was low. Through multi-GNSS (GPS/GLONASS/Galileo/BeiDou), the number of visible satellites is secured, and stability of the FIX rate is also improved [23]. Post-processing surveying can acquire precise coordinates, but it requires about two weeks of waiting because precise a final orbit product is required. The obtained coordinates are the antenna phase center (APC), which means the antenna receives the signal, and there is a difference from the geometric center of the antenna. Therefore, it is necessary to consider the variation according to the azimuth and elevation angle for each satellite provided through the ANTEX file.

In South Korea, the National Geographic Information Institute (NGII) provides single RTK and network RTK services as OSR correction through the NTRIP server and Geo++ SSRG services as SSR corrections [23]. Among these, for GPS surveying for geodetic surveying purposes,VRS and FKP methods are used among network RTK. When using network RTK, the user transmits NMEA to the server every second, and the server sets up a virtual reference station near the user and creates a virtual observation value or transmits a FKP correction to the user. The user conducts RTK using the given RTCM message, and the NMEA received from the user is used in future survey performance evaluations. Since SSR correction is not currently standardized, the formats of correction information provided by IGS and Geo++ are all different. In addition, as the verification of geodetic surveying has not been performed, it is not being used for geodetic surveying. Therefore, research is in progress targeting the simultaneous use of multiple users, such as autonomous driving.

These methods are performed at a single institution using a centralized server, making them more vulnerable to manipulation than decentralized systems, such as blockchain. An additional disadvantage is that the user must request disclosure every time, or establish a separate disclosure system for data verification. Anyone can check the data in the blockchain by providing the contract address without building a separate system.

2.2. Blockchain

Blockchain technology connects nodes based on a P2P network, and constructs a network using a distributed ledger [24]. This technology solves many problems of existing centralized systems [25–27]. Since more than 51% of nodes must be hacked for data manipulation, data integrity is guaranteed high stability, and in fact, the Bitcoin network is never "tampered". In addition, even if some nodes fail due to a DDoS attack, other nodes are maintained, and services are not paralyzed. The transparency that data are open to everyone solves the problem of information asymmetry. Therefore, with the question of the existing money system, a safe and transparent electronic money system was devised. In addition, by rewarding an unspecified number of nodes participating in the network with cryptocurrency, the degree of node participation is improved, and the stability of the network can be secured further. However, it could be mainly used for banking and payment systems to replace traditional currencies.

If the characteristics of the blockchain guarantee the integrity of the code and data generated by the program, various reliability problems that exist in existing computer systems can be solved. Ethereum, also called a second-generation blockchain, runs code written on a Turing completeness language called Solidity on a blockchain network [28]. Turing completeness languages are important because they can algorithmically solve any computable problem. Ethereum uses this to create an application that solves contract problems in the real world that could not be solved with the existing system. Given that this application uses decentralized nodes, it is called a decentralized application.

In addition, various blockchain frameworks exist, and are selected according to the purpose, closure, and speed of the service to be implemented. Furthermore, according to the restrictions on the participation qualification of nodes, three types of blockchains are largely determined: public, private, and consortium, and the consensus method between nodes is applied differently depending on the purpose [29]. Bitcoin and Ethereum are public blockchains, wherein an unspecified number of unspecified people can participate as nodes. At this time, the concept of cryptocurrency is attached because compensation for maintaining the node is required. However, in the case of private and consortium blockchains, only authorized nodes and users are allowed, such as the private network of the existing internet network configuration. Unlike public consortium blockchains, which entrusts server maintenance to anonymous users, it does not require compensation, such as cryptocurrency, because it uses existing resources.

Most devices are connected to networks to enable efficient control, a situation that may lead to facility damage and power supply problems in the case of power plants [30]. Since these issues arise from data manipulation, it is important to ensure data integrity. Algorithms and devices to address these issues have been researched, and trusted third-party solutions have been used to handle such problems [31–34]. However, it is not easy to ensure reliability using this approach, because all of these systems are centralized. Currently, blockchain networks are used to solve such problems in other fields [35–37]. The main limitation, with respect to the existing solutions, is that there is no method to reliably monitor malicious modifications to recorded data; however, blockchain was able to resolve this problem by ensuring integrity while simultaneously facilitating appropriate monitoring [38]. As this approach improves reliability, it can also be used to improve GPS positioning accuracy by using data between objects, such as self-driving cars [18,39]. However, there are cases where the blockchain is not suitable for rapid communication in an environment, such as internet of vehicles, because it consumes relatively high energy compared to the cryptography technique [40,41]. In addition, it is limited in that it has the same weakness as the 51% attack, in that it trusts all nodes without evaluating the reputation [42]. However, GPS surveying does not generate many transactions on the blockchain network and the 51% attack requires enormous costs, the attack occurs for financial gain, so cryptocurrency theft is the main target. In other words, even if the attack succeeds, no data are injected, and the blockchain used in this study has never been

successfully attacked. Therefore, blockchain was judged as the most suitable method to solve the problems introduced above in this study.

3. Blockchain-Based Global Positioning System

In this study, we developed and implemented a GPS positioning system using a smart contract of Ethereum to improve the integrity of GPS data. It receives NMEA data from the GPS receiver and transmits it to NTRIP Caster to receive RTCM data. The two data are then uploaded to the blockchain network, and the RTCM is transmitted to the GPS receiver for NTRIP-based position correction. By repeating this process for a certain period of time, the GPS receiver continuously corrects the position of the measured information to improve the positional accuracy, and all data are uploaded to the blockchain network. (Figure 1).

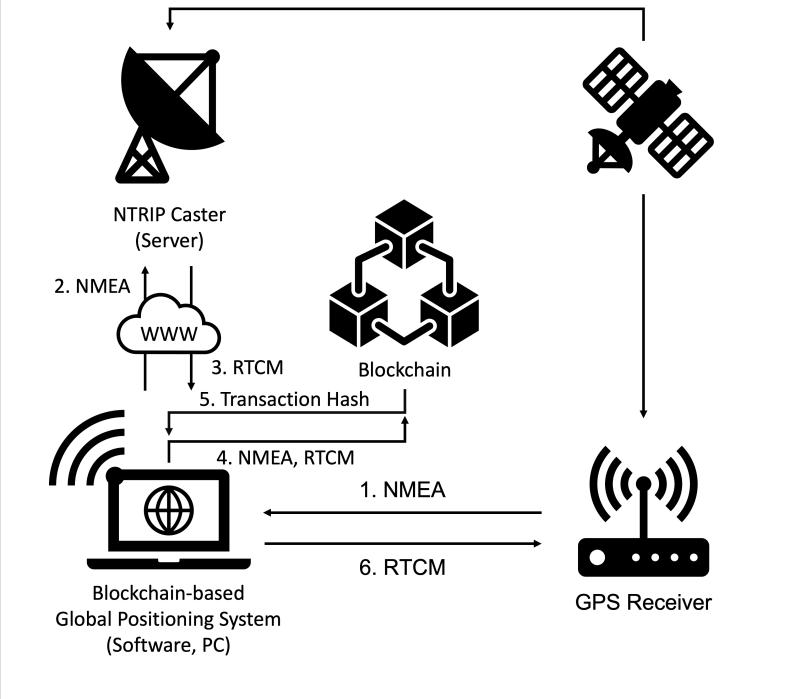

Figure 1. Overview of the blockchain-based global positioning system.

Transactions have several attributes: transaction hash refers to identifiers; contract addresses refer to survey points and survey processes; wallet addresses refer to surveyors; and data refer to NMEA and RTCM data. Unlike the traditional system, the entire process, other than the final result, can be checked for compliance with regulations pertaining to issues, such as survey time, and the work of surveyors can be traced (Table 1). Using this approach, even if a value in the system is manipulated, anyone can inquire about the transaction hash to perform integrity checks and track the original data.

Table 1. Hash role descriptions.

Hash Types	Descriptions
Transaction hash	The identifier of the positioning
Contract address	The identifier of the positioning point, which has transaction hashes
Wallet address	The identifier of the surveyor, which has transaction hashes

The integrity of all data are guaranteed by the blockchain. A blockchain generates transaction hashes using transaction attribute values, input data, and the Keccak-256 function, and creates a transaction root using the value of the transaction hashes and the Merkle tree. When a block is mined, a block hash is generated using the attribute values of the block, including the transaction root and the Keccak-256 function, and is used as one of the attributes of the following block, Figure 2. Therefore, as the block attempts to manipulate the data at a more extended point, the cost of injecting it increases exponentially. In this way, the blockchain prevents the injection.

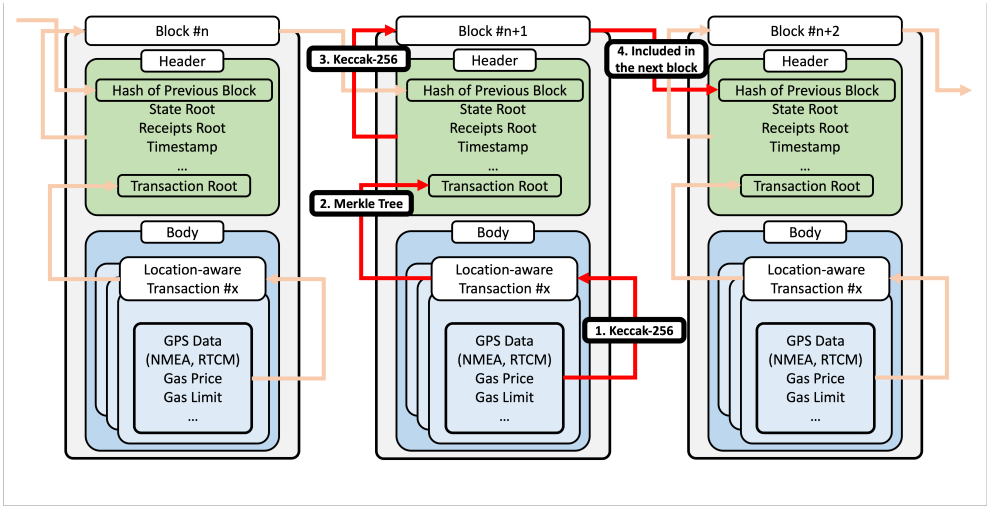

Figure 2. Connection of the block and transaction.

In this system, a low-cost GPS receiver (u-blox ZED-F9P) was used for GPS surveying [43]. We then developed software that send and receive the NMEA and RTCM data to the GPS receiver and NTRIP Caster. Moreover, it sent them to the Ropsten testnet of the Ethereum blockchain network for the experiment. The target network can be changed to the other network using the Ethereum virtual machine (EVM) for the actual case. It was developed on Python, and a smart contract that was executed on the Ethereum network was also developed with Solidity and inserted into the Python code. Python takes advantage of this by compiling the Solidity compiler and separating the application binary interface (ABI) and bytecode. Given that the smart contract is executed after the system operates using the user's Ethereum wallet, the wallet address remains, and the wallet address becomes a value that can identify the worker involved in the GPS positioning process.

In the original GPS survey process, Algorithm 2, which performs device initialization for surveying and connection with the NTRIP server, is started once, and Algorithm 3, which receives and corrects RTCM information and re-transmits NMEA information, is repeated for a specific time. In this study, Algorithm 1, a smart contract operating on Ethereum, was added. The Ethereum network connection and smart contract distribution, which is performed once in Algorithm 1, is executed in Algorithm 2, and data recording in the blockchain through smart contract execution is executed in Algorithm 3. Based on these, all data generated and used by GPS devices are recorded in the Ethereum network and integrity is secured.

Algorithm 1: Smart contract: ensure or return the surveyor, NMEA, RTCM.

Data: *Wallet Address*
Surveyor = *Wallet Address*
Function *1 : GPS Positioning*
  Data: *NMEA from Receiver*, *RTCM from Caster*
  NMEA = *NMEA from Receiver*
  RTCM = *RTCM from Caster*
end
Function *2 : Call the data*
  Result: *Surveyor*, *NMEA*, *RTCM*
end

Algorithm 1 is constructed to input the surveyor's address when the contract is deployed that stores the user's wallet address, when deploying a smart contract. Algorithm 1-1 (first function for GPS positioning) stores NMEA and RTCM, and Algorithm 1-2 reads operator and GPS information. It is defined as Algorithm 1-2 (second function for return the data). In the case of the construct, it is an area that is executed together with the distribution of the smart contract, and the user's wallet address is automatically saved as soon as Algorithm 1 operates. Algorithm 1-1 receives data from Algorithm 4 and stores them as data types. Subsequently, the GPS information and workers stored in this contract can be checked by Algorithms 1 and 2. Although the structure of Algorithm 3 is simple, it is a smart contract code written in Solidity and works on the Ethereum network. That is, the integrity of the GPS data and operator information stored in Algorithm 2 is guaranteed by Ethereum.

Algorithm 2: Connect to the GPS receiver and NTRIP caster.

Data: *Serial*, *NTRIP Caster*
Result: *Receiver*, *NTRIP Client*
while *Receiver is not connected* **do**
  Receiver = Connect through the *Serial*
end
while *Client is not connected* **do**
  NMEA = Parsing from *Receiver*
  NTRIP Client = Connect to *NTRIP Caster* using *NMEA*
end

Algorithm 2 initiates the execution and connection of the sensor using serial communication for GPS positioning. It is set to receive various types of information through connection and communication with the satellite at the same time the device is running, so GPS positioning starts. Subsequently, to connect with the NTRIP server, the input caster information is used to create the NTRIP client. In this study, the mount point VRS_V32 of the NGIS server was used. Thereafter, GNGGA was read from the information measured by positioning from the device and transmitted to the server through the NTRIP client to perform the initial connection. This is a general GPS positioning process. In this study, the connection of the Ethereum network and the execution of Algorithm 1-1 were added.

Algorithm 3: Connect to the Ethereum blockchain and deploy the smart contract.

Data: *Network URL*, *Wallet Address*, *Private Key*, *Contract Code*
Result: *Web3*, *Contract*
if *Web3 is not connected* **then**
  Web3 = Connect through HTTP provider with *Network URL*
end
Compiled Code = compile the *Contract Code*
ABI = Parsing from *Compiled Code*
Bytecode = Parsing from *Compiled Code*
TxHash = Transact the contract using *ABI*, *Bytecode*
while *Tx is not mined* **do**
  Tx = Wait for transaction receipt using *TxHash*
end
Contract = Defined using *ABI* and Address of *Tx*

NMEA and RTCM generated in the positioning process through Algorithm 1 were recorded on the Ethereum blockchain. However, this requires that the device is connected to the Ethereum network and deploys a smart contract. This algorithm manage this task. To achieve proof-of-concept, we entered the URL address of the test net. Additionally, the wallet address and private key were entered to execute the smart contract. Subsequently, connection to the network was established through the HTTP provider and a Web3 instance was created. The contract was then deployed using the ABI and bytecode extracted from the Web3 instance and the compiled Solidity code (Algorithm 3). Through the address of the deployed smart contract, the user (surveyor) can be identified, and GPS information can be tracked. After deploying, the receipt of the transaction was returned, which confirmed that the contract had been distributed correctly. Using only the address of the transaction that occurred in this process, the operator and GPS information whose integrity was secured in Algorithm 3 can be checked.

Algorithm 4: GPS positioning.

Data: *Web3*, *Contract*, *Receiver*, *NTRIP Caster*, *NTRIP Client*, *Deadline*
while *RunningTime* $\neq$ *Deadline* **do**
  NMEA = Parsing from *Receiver*
  if *NMEA is True* **then**
    RTCM = send *NMEA* to *NTRIP Caster* through *NTRIP Client*
    Tx Hash = Function 1 of Algorithm 1 with *NMEA*, *RTCM* using *Web3*
    NMEA = Send *RTCM* to *Receiver*
  end
end

To improve the integrity and reliability of GPS data and processes, Algorithm 4 performs blockchain-based GPS positioning for as long as the surveyor sets the time. When NMEA and RTCM data are input to the system through GPS surveying, through Algorithm 1, to record data on the blockchain and store the transaction hash value together in the system, this method prevents the injection of blockchain-based data and allows anyone to trace and prove the original data using hash values. For one survey point, a transaction hash occurs as long as there is a contract address and the time is set by the surveyor. Unlike the traditional system, data on the entire survey process can be tracked using this method.

4. Result

4.1. Results of Implementation

We implemented and developed a decentralized GPS positioning prototype system using the Ethereum blockchain. Solidity and Python were mainly used as development tools for smart contract application development. If the prototype works appropriately in the network, it also works in the main network or the test network. Thus, we experimented with the Ropsten test network.

The contract address deployed through Algorithm 3 is $0x4cDD2600bd83A308dF598F5FdA8D3Ef2BdFbf348$ (Figure 3). This address is generated each time the prototype is executed for GPS positioning at a new location, and all data generated by Algorithm 4 can be found at that address. One coordinate and record process corresponds to each contract address. It also contains the address of the wallet that deployed it, which allows us to identify the worker who operated it.

The deployed smart contract was recorded in block 1 and the first measured coordinate is the Tables 2 and 3. Subsequently, Algorithm 4 was executed 56 times to execute a total of 56 additional transactions (Figure 4).

Table 2. The first recording GPS positioning data.

Field	Value
NMEA Data	$GNGGA,025610.00,3735.2330935,N,12700.9212481,E,5,12,0.77,54.482,M,18.504,M,1.0,4095*5B
RTCM Data	\xd3\x00\t?_\xff\xe8\xde\x15\x18\x80H\xfa\xe4R\xd3\x00\x15 > \xef\xff\x03\xf8\xc5#6\xc5\tR\x1e\x13\x9f\x88\xfd\xabI\xfa\x00\x00h\xe8S\xd3\x00\x14@\x8f\xff \x00\x008\xba\xf0\x8b\xe5%JZ[\xb8\x8fR\xf0B\xc0\x94\x90\xc3\xd3\x00(@\x9f\xff \x0eGPPNULLANTENNA\x00\x00rTrimbleNetR9\x045.37\x00J\x9c\x84\xd3\x00\x14?\x0f\xff \x0eGPPNULLANTENNA\x00\x00\xc0e\x00\xd3\x00\x0cL\xef\xff\x8f\x03\x8a\x03?\x03P\x03MY\xac \x9d\xd3\x002@f\xc1\xa9\xff\xf0\xa7\x0c4 : \x00\x16\x0c\xac\x08\x08\x00\t\x05\x19\x06\x07\x00\x04\x82m\x02\x82\xc0\x02\x81gA\x81\xc0\x04\x02; \xe0\x80\x90\x00pF\x00@H\x00\x12

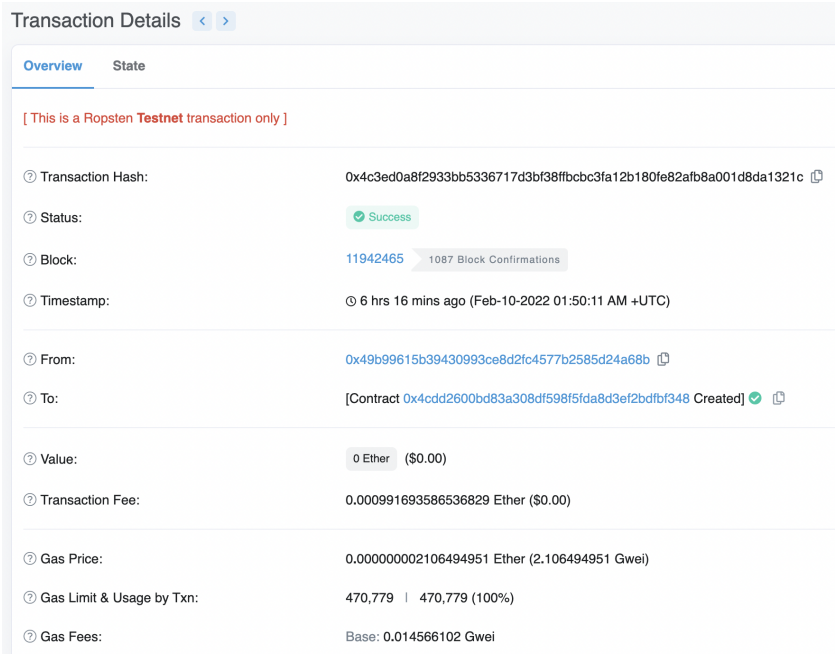

Figure 3. Block and transaction information by contract deploying.

Table 3. Transaction information of first GPS positioning.

Field	Value
Tx Hash	0x205393a698c8fd6a966f88a68b9b8a16ea9e499027174a53c0c8f8cc0c02b85c
Worker ID (Wallet Address)	0x49B99615B39430993Ce8D2fC4577b2585d24a68B
Point ID (Contract Address)	0x4cDD2600bd83A308dF598F5FdA8D3Ef2BdFbf348
Gas Used	348,221
Tx Data	0xee198295000000000000000000000000000000000000000000000000000000000000000040000000000000000000000000000000000000000000000000000000000000000c0000000000000000000000000000000000000000000000000000000000000000005724474e4747412c3032353631302e30302c333733352e323333303933352c4e2c31323730302e393231323438312c452c352c31322c302e37372c35342e3438322c4d2c31382e3530342c4d2c312e302c343039352a3542000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000108d300093f5fffe8de15188048fae452d300153eefff03f8c52336c509521e139f88fdab49fa000068e853d30014408fff000038baf08be5254a5a5bb88f52f042c09490c3d30028409fff0e4750504e554c4c414e54454e4e4100000d5472696d626c65204e6574523904352e3337004a9c84d300143f0fff0e4750504e554c4c414e54454e4e410000c06500d3000c4cefff8f038a033f0350034d59ac9dd300324066c1a9fff0a70c343a00160cac0808000905190607000482 6d0282c00281674181c004023be0809000704600404800201 23c74e0d3002c40775e3fff853060a0b000804840404800482828586800 1c1034181e001c101c080a0006038f0a0b800884c03a69af0000000000000000000000000000000000000000000000000000000000000000

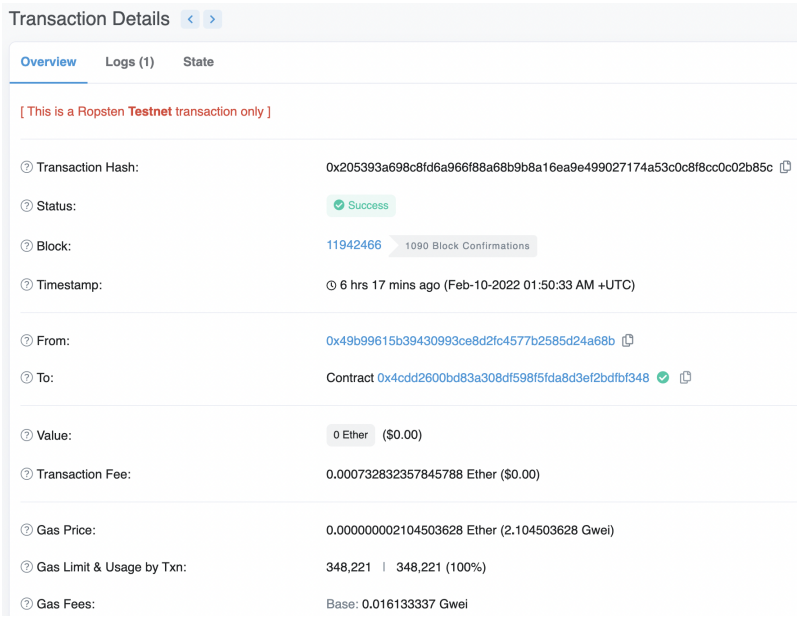

Figure 4. Transaction information of the first recording GPS positioning data at Etherscan explorer.

The last recorded coordinates are seen in Tables 4 and 5. Algorithms 1–3 were executed to see the value recorded in the contract. It was confirmed that the measured coordinate and the value recorded in the Ethereum network matched (Figure 5).

Table 4. The last recording GPS positioning data.

Field	Value
NMEA Data	$GNGGA,030002.00,3735.2333839,N,12700.9215485,E,5,12,0.63,55.661,M,18.504,M,1.0,4095*5C
RTCM Data	Error at LaTeX. We'll send it to Editorial office.

Table 5. Transaction information of last GPS positioning data.

Field	Value
Tx Hash	0x1b7903fbf8970bacd165737289895b1e106f2b2a9ed15b76cfcaba65d3bd99c6
Worker ID (wallet address)	0x49B99615B39430993Ce8D2fC4577b2585d24a68B
Point ID (contract address)	0x23F21cf7154C470Da3d850899CDedeA29d7AF9a9
Gas Used	147,262
Tx Data	0xee1982950000000000000000000000000000000000000000000000000000000040000000000 00000000000000000000000000000000000000000000000c000000000000000000000000 000000000000000000000000000000000000005724474e4747412c3033303030322e30302c 333733352e323333333833392c4e2c31323730302e393231353438352c452c352c31322c302e 36332c35352e3636312c4d2c31382e3530342c4d2c312e302c343039352a35430000000000000 0000000000000000000000000000000000000000000000000000000000000000 185d300b6446fff69950d820007b18000420000000000040088807fffffa6a8ada4a9ab 3009a4e05af4cff9f8440b28165050657fcd859b2338a96302fd260b0c48677cd067a0fb 4409a7e37846ee4de8edefdee9bd337c3084b1021b4e086f9c21c5679455de4ebdf93abde 4e6e85b99e1708d85c2921708b7a237fe8de1fa3951e8e9a86bc8e1b12a86c5661b15 c7bbe75ef4c8fbd475ef5467ffffffffffffffffffffff80000061af1a619ed9cb55d565aefa 5d96b8d97e5705c0120d300c3464fff699432c00007fb609a1800000000200200007 ffff553ec0be3fbbbf3dc13c25272b2a2a4880c771e77c5533dc390a9dc457c85c02b 8fea1ee3f3bbdcc0462073be353bf9ede5d9aff5e3e45e98cd1f5e6e7cae7afbf67fae 603f0179ed56214281dd0b07459bf9d04fe72640723001a143f1aa3fc6d03dc82ef 73033fba89ff387fd44b9f5208ff4b3ffd5f87f6cc2fe04c7d8a17037b402f3cff563dc 0c037ffecfffffffffffffff99f0000014591d33d73578614596df3d18e385d54d300f5af 92000000000000000000000000000000000000000000000000000

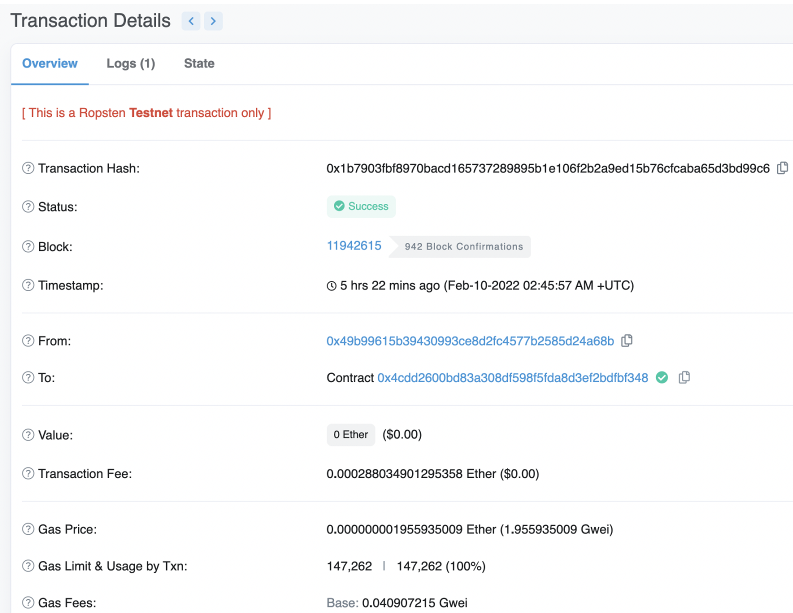

Figure 5. Transaction information of the last GPS positioning at Etherscan explorer.

4.2. Security Analysis

Integrity: in this study, location-based transactions were created and uploaded to the blockchain using NMEA from GPS surveys and RTCM received from NTRIP Caster, to improve the integrity of GPS data. The matching of GPS data stored in the blockchain and data stored in the system were verified using the data uploaded to the blockchain through the Etherscan explorer (Figure 6). Location-based transactions can use hash values for transactions produced through the Keccak-256 function as identifiers. Changing data leads to changes in transaction hash values, providing a means of monitoring integrity. The blockchain also prevents injection using a method that must be agreed upon by more

than 51% of nodes. The integrity of all data generated during the GPS surveying process is thus guaranteed.

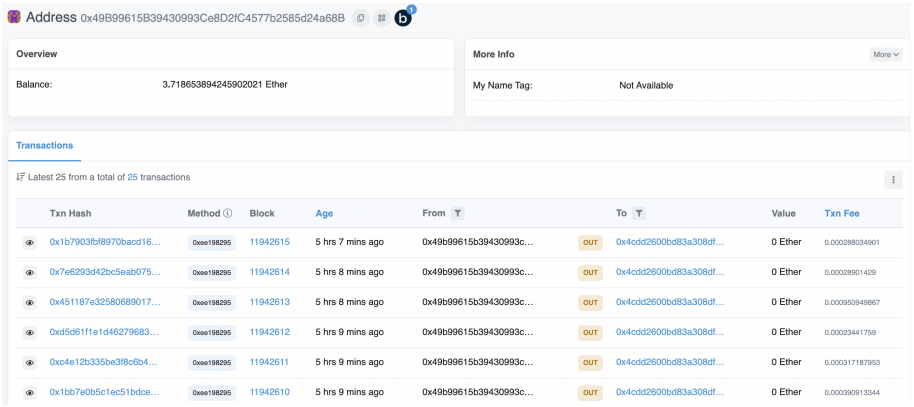

Figure 6. Verification of the uploading to a blockchain through Explorer.

Reliability: it was confirmed that reliability was improved by allowing anyone to prove GPS data using hash values on the blockchain. In this study, the transaction hashes occur for each Algorithm 4, and NMEA and RTCM data are stored (Figure 7). Therefore, even if a user reports a result in the form of a file, data can be tracked using only the transaction address. The algorithm proposed in this study distributes one contract to one location to be measured, and generates one transaction per point (Figure 8). When the system is executed to produce 60 surveys at one point, 60 transactions occur, and are connected to one contract address. In the past, if only one point could be received as a final result, the contract address could be used to track whether regulations, such as overall data, and survey working hours for one location could be observed (Figure 9). Wallet addresses can distinguish between workers. All transactions and contracts that occurred can be queried, so that all of the surveyed behaviors of the workers could be tracked (Figure 10).

Figure 7. Tracking the GPS data and point and worker by the transaction hashes.

Figure 8. Mapping the GPS data parsed from the transaction hash.

Point ID(Contract Address)	Transaction Hash
0x4cDD2600bd83A308dF598F5FdA8D3Ef2BdFbf348	0x205393a698c8fd6a966f88a68b9b8a16ea9e49902717...
0x4cDD2600bd83A308dF598F5FdA8D3Ef2BdFbf348	0xe891f9e023e61bb39b1e596d95013bf42b3b9858c018...
0x4cDD2600bd83A308dF598F5FdA8D3Ef2BdFbf348	0x176622c61e73431c5eb5474f016de12faaaf563f94ec...
0x4cDD2600bd83A308dF598F5FdA8D3Ef2BdFbf348	0xad85fa5c73cd4fc0f7abd0fc3704dc81ffa4ad007796...
0x4cDD2600bd83A308dF598F5FdA8D3Ef2BdFbf348	0x858db67e55e63d5dec64daf3f6f178b65170306e5f9e...
...	...
0xF42b8A2C6196E701DDcB341d21e18Ee0e1E1abD5	0x70f1b6185b822299607b8de4eb6b1a76fbdfc93a5362...
0xF42b8A2C6196E701DDcB341d21e18Ee0e1E1abD5	0x33f19b5853c64aaa06afee7aca50dac7043bfbd4261f...
0xF42b8A2C6196E701DDcB341d21e18Ee0e1E1abD5	0x821a97f5af8a4b0e8e24aa2cdcf8e655fdb425305042...
0xF42b8A2C6196E701DDcB341d21e18Ee0e1E1abD5	0xe3388a5be4539912d0d7b44e3652350d48e12c57d9d2...
0xF42b8A2C6196E701DDcB341d21e18Ee0e1E1abD5	0xa19ff961596d26023b5b4a2c0811d871b91b61df0219...

Figure 9. The transaction hashes by the contract addresses.

Worker ID(Wallet Address)	Transaction Hash
0x49B99615B39430993Ce8D2fC4577b2585d24a68B	0x205393a698c8fd6a966f88a68b9b8a16ea9e49902717...
0x49B99615B39430993Ce8D2fC4577b2585d24a68B	0xe891f9e023e61bb39b1e596d95013bf42b3b9858c018...
0x49B99615B39430993Ce8D2fC4577b2585d24a68B	0x176622c61e73431c5eb5474f016de12faaaf563f94ec...
0x49B99615B39430993Ce8D2fC4577b2585d24a68B	0xad85fa5c73cd4fc0f7abd0fc3704dc81ffa4ad007796...
0x49B99615B39430993Ce8D2fC4577b2585d24a68B	0x858db67e55e63d5dec64daf3f6f178b65170306e5f9e...
...	...
0x834844CefEeEc34305d14ad9c20D887891eDa935	0x70f1b6185b822299607b8de4eb6b1a76fbdfc93a5362...
0x834844CefEeEc34305d14ad9c20D887891eDa935	0x33f19b5853c64aaa06afee7aca50dac7043bfbd4261f...
0x834844CefEeEc34305d14ad9c20D887891eDa935	0x821a97f5af8a4b0e8e24aa2cdcf8e655fdb425305042...
0x834844CefEeEc34305d14ad9c20D887891eDa935	0xe3388a5be4539912d0d7b44e3652350d48e12c57d9d2...
0x834844CefEeEc34305d14ad9c20D887891eDa935	0xa19ff961596d26023b5b4a2c0811d871b91b61df0219...

Figure 10. The transaction hashes by the wallet addresses.

4.3. Cost Analysis

The gas used in the deploying of smart contracts shown in this experiment was 348,221 gas, and the GPS positioning function was calculated as an average of 267,316 gas (Table 6). It slightly depends on the transmitted data. Therefore, performing GPS positioning for 56 times includes the deploying of smart contracts using "15,317,889 gas". In the case of the view function, gas is not required, because it is a function that returns only the result without the calculation. The more considerable the amount of data recorded on the blockchain, the more gas is used, so the gas usage tends to increase according to the length of the RTCM message (Figure 11).

Table 6. Cost of smart contract execution.

Field	Cost (Gas)
Deploying	348,221
GPS Positioning (Function 1, Avg)	267,316
GPS Positioning (Function 1, 56 times)	15,317,889

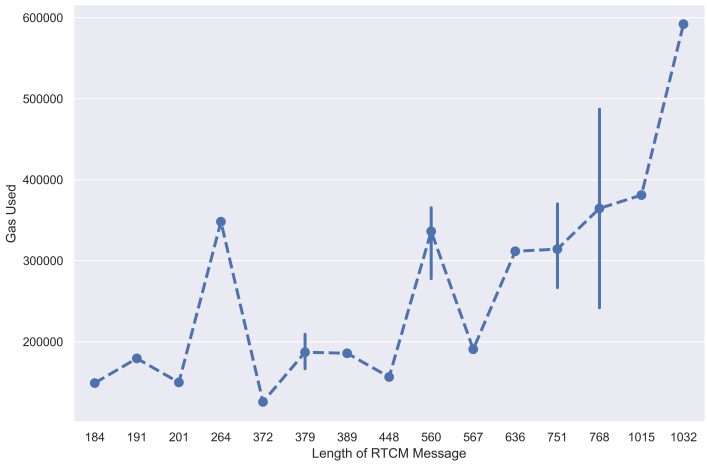

Figure 11. Gas usage of transactions according to the length of the RTCM message.

5. Discussion and Conclusions

In this study, we proposed a system that uploads the GPS positioning process to the blockchain network, using smart contracts, and ensuring data integrity. The Ropsten testnet of Ethereum networks were used, but they can work in the same way on Ethereum's main network and many other blockchains using EVM. All users were able to check GPS data at a specific location, as well as workers and processes, using the provided contract address. These concerns can be addressed earlier if such information is written together in areas vulnerable to easy manipulation and financial damage, such as cadastral surveys. Therefore, the government needs to prevent legal disputes and improve administrative efficiency by operating a blockchain network that records such GPS information. In addition, based on the structure of the existing algorithm, it was suggested that the blockchain could be applied in a simple method, such as by putting information on the blockchain network and wallet to be used in the existing survey software and smart contracts. However, networks such as Ethereum and Binance Smart Chain may involve prohibitively high costs, and Klaytn requires a reasonable level of costs. This concern can be addressed by using various blockchains using Solidity-based smart contracts. Furthermore, if a part of the ground station system is operated as a private blockchain, the cost concern will be resolved entirely. Therefore, future research will focus on cost issues and the configuration of the blockchain network.

Author Contributions: Conceptualization, Seunghyeon Lee; methodology, Seunghyeon Lee and Hong-Woo Seok; software, Seunghyeon Lee and Hong-Woo Seok; investigation, Ki-rim Lee; writing—original draft preparation, Seunghyeon Lee and Hong-Woo Seok; writing—review and editing, Seunghyeon Lee, Hong-Woo Seok and supervision, Hoh Peter In. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Research Foundation (NRF) of Korea grant funded by the Korean government (MSIT), no. NRF-2021R1A2C2012476.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Li, X.; Ge, M.; Dai, X.; Ren, X.; Fritsche, M.; Wickert, J.; Schuh, H. Accuracy and reliability of multi-GPS real-time precise positioning: GPS, GLONASS, BeiDou, and Galileo. *J. Geod.* **2015**, *89*, 607–635. [CrossRef]
2. Kwak, J.; Sung, Y. Autonomous UAV flight control for GPS-based navigation. *IEEE Access* **2018**, *6*, 37947–37955. [CrossRef]

3. Meng, X.; Wang, H.; Liu, B. A robust vehicle localization approach based on gnss/imu/dmi/lidar sensor fusion for autonomous vehicles. *Sensors* **2017**, *17*, 2140. [CrossRef] [PubMed]
4. De Miguel, M.Á.; García, F.; Armingol, J.M. Improved LiDAR probabilistic localization for autonomous vehicles using GNSS. *Sensors* **2020**, *20*, 3145. [CrossRef]
5. Wakker, W.J.; van der Molen, P.; Lemmen, C. Land registration and cadastre in the Netherlands, and the role of cadastral boundaries: The application of GPS technology in the survey of cadastral boundaries. *J. Geospat. Eng.* **2003**, *5*, 3–10.
6. Kavaliauskas, P.; Židanavičius, D.; Jurelionis, A. Geometric Accuracy of 3D Reality Mesh Utilization for BIM-Based Earthwork Quantity Estimation Workflows. *ISPRS Int. J. Geo-Inf.* **2021**, *10*, 399. [CrossRef]
7. Abidin, H.Z.; Haroen, T.S.; Adiyanto, F.H.; Andreas, H.; Gumilar, I.; Mudita, I.; Soemarto, I. On the establishment and implementation of GPS CORS for cadastral surveying and mapping in Indonesia. *Surv. Rev.* **2015**, *47*, 61–70. [CrossRef]
8. Fotopoulos, G.; Cannon, M.E. An overview of multi-reference station methods for cm-level positioning. *GPS Solut.* **2001**, *4*, 1–10. [CrossRef]
9. Bar-Sever, Y.; Bell, B.; Dorsey, A.; Srinivasan, J. *Space Applications of the Nasa Global Differential GPS System*; Jpl Technical Reports; Institute of Navigation: Portland, OR, USA, 2003.
10. Conker, R.S.; El-Arini, M.B.; Hegarty, C.J.; Hsiao, T. Modeling the effects of ionospheric scintillation on GPS/Satellite-Based Augmentation System availability. *Radio Sci.* **2003**, *38*, 1. [CrossRef]
11. Hernández-Pajares, M.; Juan, J.M.; Sanz, J.; Orús, R.; García-Rodríguez, A.; LColombo, O. Wide area real time kinematics with Galileo and GPS signals. In Proceedings of the 17th International Technical Meeting of the Satellite Division of The Institute of Navigation, Long Beach, CA, USA, 21–24 September 2004; pp. 2541–2554.
12. Wabbena, G.; Schmitz, M.; Bagge, A. PPP-RTK: Precise point positioning using state-space representation in RTK networks. In Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation, Long Beach, CA, USA, 13–16 September 2005; pp. 2584–2594.
13. Snay, R.A.; Soler, T. Continuously operating reference station (CORS): History, applications, and future enhancements. *J. Surv. Eng.* **2008**, *134*, 95–104. [CrossRef]
14. Iqbal, M.U.; Lim, S. Legal and ethical implications of GPS vulnerabilities. *J. Law Inf. Technol.* **2008**, *3*, 178.
15. Samios, M.; Evangelidis, C.P.; Serrelis, E. Assessment of Information Security Vulnerabilities in Common Seismological Equipment. *Seismol. Soc. Am.* **2021**, *92*, 933–940. [CrossRef]
16. Kowalski, M.; Lee, Z.W.; Chan, T.K. Blockchain technology and trust relationships in trade finance. *Technol. Forecast. Soc. Chang.* **2021**, *166*, 120641. [CrossRef]
17. Majeed, U.; Khan, L.U.; Yaqoob, I.; Kazmi, S.A.; Salah, K.; Hong, C.S. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. *J. Netw. Comput. Appl.* **2021**, *181*, 103007. [CrossRef]
18. Li, C.; Fu, Y.; Yu, F.R.; Luan, T.H.; Zhang, Y. Vehicle position correction: A vehicular blockchain networks-based GPS error sharing framework. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 898–912. [CrossRef]
19. Lee, H.C. Development of GNSS Precise Point Positioning Algorithm Based on Real-Time CLAS Messages Provided by QZSS. Master's Thesis, Inha University, Incheon, Korea, 2021.
20. Ansari, K. Real-Time Positioning Based on Kalman Filter and Implication of Singular Spectrum Analysis. *IEEE Geosci. Remote Sens. Lett.* **2021**, *18*, 58–61. [CrossRef]
21. *National Geographic Information Institute Achievement Report*; National Geographic Information Institute, Ministry of Land, Infrastructure and Transport: Suwon, Korea, 2017.
22. Wübbena, G.; Bagge, A.; Schmitz, M. Network-Based Techniques for RTK Applications. In Proceedings of the GPS Symposium, GPS JIN, Tokyo, Japan, 14–16 November 2001.
23. Seok, H.W.; Park, K.D.; Kim, Y.G.; Lee, H.C. Accuracy Evaluation of Multi-GNSS Network-RTK Surveys Operated by National Geographic Information Institute. In Proceedings of the IPNT Conference, Yeosu, Korea, 11–13 November 2020.
24. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 23 November 2021).
25. Viriyasitavat, W.; Da Xu, L.; Bi, Z.; Sapsomboon, A. Blockchain-based business process management (BPM) framework for service composition in industry 4.0. *J. Intell. Manuf.* **2020**, *31*, 1737–1748. [CrossRef]
26. Dashkevich, N.; Counsell, S.; Destefanis, G. Blockchain application for central banks: A systematic mapping study. *IEEE Access* **2020**, *8*, 139918–139952. [CrossRef]
27. Wüst, K.; Gervais, A. Do you need a blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology, Zug, Switzerland, 20–22 June 2018; pp. 45–54.
28. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper. 2014. Available online: https://ethereum.github.io/yellowpaper/paper.pdf (accessed on 23 November 2021).
29. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Yellick, J. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth Eurosys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
30. Kesler, B. The vulnerability of nuclear facilities to cyber attack; strategic insights: Spring 2010. *Strateg. Insights* **2011**, *10*, 15–25.
31. Yang, Q.; An, D.; Min, R.; Yu, W.; Yang, X.; Zhao, W. On optimal PMU placement-based defense against data integrity attacks in smart grid. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1735–1750. [CrossRef]

32. Malan, D.J.; Welsh, M.; Smith, M.D. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. In Proceedings of the 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, CA, USA, 4–7 October 2004; Volume 27, pp. 71–80.
33. Ghaeb, J.A.; Smadi, M.A.; Chebil, J. A high performance data integrity assurance based on the determinant technique. *Future Gener. Comput. Syst.* **2011**, *27*, 614–619. [CrossRef]
34. Huang, P.; Fan, K.; Yang, H.; Zhang, K.; Li, H.; Yang, Y. A collaborative auditing blockchain for trustworthy data integrity in cloud storage system. *IEEE Access* **2020**, *8*, 94780–94794. [CrossRef]
35. Zhao, Q.; Chen, S.; Liu, Z.; Baker, T.; Zhang, Y. Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. *Inf. Process. Manag.* **2020**, *57*, 102355. [CrossRef]
36. Hang, L.; Kim, D.H. Design and implementation of an integrated iot blockchain platform for sensing data integrity. *Sensors* **2019**, *19*, 2228. [CrossRef]
37. Wei, P.; Wang, D.; Zhao, Y.; Tyagi, S.K.S.; Kumar, N. Blockchain data-based cloud data integrity protection mechanism. *Future Gener. Comput. Syst.* **2020**, *102*, 2228. [CrossRef]
38. Choi, M.K.; Yeun, C.Y.; Seong, P.H. A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology. *IEEE Access* **2020**, *8*, 118732–118740. [CrossRef]
39. Song, Y.; Fu, Y.; Yu, F.R.; Zhou, L. Blockchain-enabled Internet of Vehicles with cooperative positioning: A deep neural network approach. *IEEE Internet Things J.* **2020**, *7*, 3485–3498. [CrossRef]
40. Mahmood, A.; Siddiqui, S.A.; Sheng, Q.Z.; Zhang, W.E.; Suzuki, H.; Ni, W. Trust on wheels: Towards secure and resource efficient IoV networks. *Computing* **2022**, 1–22. [CrossRef]
41. Sharma, V. An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV). *IEEE Commun. Lett.* **2022**, *23*, 246–249. [CrossRef]
42. Sayeed, S.; Marco-Gisbert, H. Assessing blockchain consensus and security mechanisms against the 51% attack. *Appl. Sci.* **2019**, *9*, 17889. [CrossRef]
43. U-Blox ZED-F9P-02B. U-Blox F9 High Precision GNSS Module. Data Sheet. 2021. Available online: Https://www.u-blox.com/sites/default/files/ZED-F9P-04B_DataSheet_UBX-21044850.pdf (accessed on 2 February 2022).