Journal of Digital Art Engineering & Multimedia Vol.11, No.3, September (2024), pp.367-374
ISSN 2508-9099(p) 2672-1198(e) *http://dx.doi.org/10.29056/jdaem.2024.09.08*

Private Blockchain을 이용한 전기자동차 충방전장치의 운영과 관리에 관한 연구

Operation & Management of Charging and Discharging system for Electrical Vehicle With Private Blockchain

이성욱[1]

Sunguk Lee[1]

요 약

현재 전기자동차는 과도기적 단계를 지나 전체 자동차 판매량의 약 20%를 차지하고 있다. 이에 발맞추어 전기자동차 충전기반시설 또한 급격히 늘어나고 있다. 현재의 전기자동차 기반시설은 오직 전기자동차의 배터리를 충전하는 목적으로 이용되고 있는 실정이나 전기자동차의 배터리를 새로운 분산전원으로 이용하려는 스마트그리드 기술에 대한 관심이 점점 높아지고 있다. 이를 위해서 Vehicle to Grid (V2G)기술이 여러 산업체와 학계로부터 연구되고 있으며 전기자동차와 전력서비스제공자 사이의 신뢰성 높은 통신은 V2G 시스템의 필수적인 요소이다. 본고에서는 블록체인을 이용한 V2G시스템의 인증과 운영체계를 제안한다. 공개키 암호 알고리즘과 디지털서명을 이용하여 메시지의 기밀성과 서비스 당사자 상호간의 인증을 지원한다. 모든 거래 내역은 모든 참여자들이 공유하고 사용자의 개인정보는 블록에 기록되지 않으며 사용자의 익명성을 보장한다. 또한 특정 노드가 블록을 관리하는 Private Blockchain방식을 사용하여 시스템의 효율성을 높였다.

핵심어 : 전기자동차, 스마트그리드, V2G, 블록체인, 보안

Abstract

Currently, electric vehicles (EVs) have passed the transitional stage and account for around 20 % of sales volume in the total vehicle market. The charging infrastructure for electric vehicles is also rapidly increasing with increasement of EVs. The current infrastructure for EV is used only to charge batteries of EVs, but interest to use EV's batteries as new distributed power resources with help of smart grid technology is increasing To realize this idea the Vehicle to Grid (V2G) technology which needs secure communication channel has been researched by various industries and academia. This paper proposes authentication and operating scheme of V2G system with blockchain network. The public key cryptography and digital signature algorithm are used to support for security of communication and authentication between EVs and the service provider. All transaction details which do not have private information are shared by all participants. The proposed scheme supports for anonymity of service user and security of

1 Department of Multimedia Engineering, Hannam University, Daejeon, Korea
e-mail: sulee0612@hnu.kr

* 이 논문은 2023학년도 한남대학교 학술연구비 지원에 의하여 연구되었음.

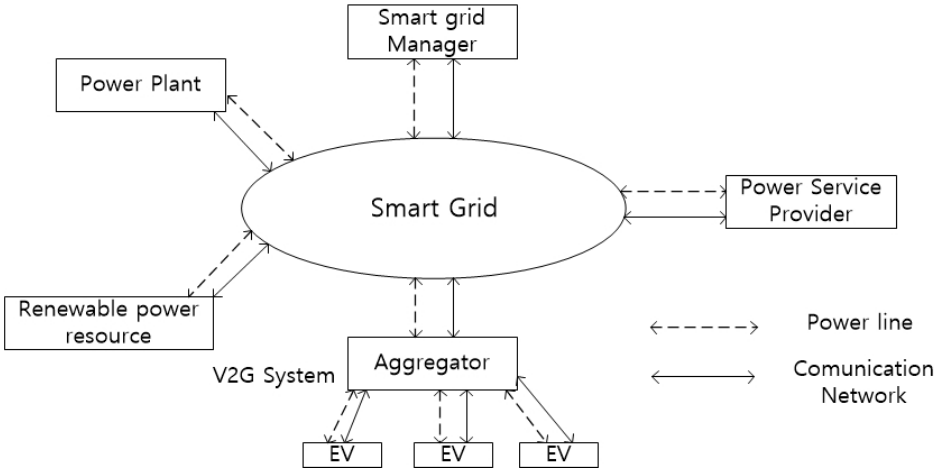
Received(July 23, 2024), Review Result(1st: August 11, 2024), Accepted(September 9, 2024), Published(September 30, 2024)

private information. This scheme also provides the high efficiency of operation with help of private blockchain network with a managing node.

Keyword : Electric vehicle, Smart grid, V2G, Blockchain, Security

1. 서론

이산화탄소와 대기오염물질을 줄이기 위한 세계적인 노력의 하나로 세계 각국은 친환경자동차인 전기자동차(Electric Vehicle)의 보급에 힘써왔으며 과도기적 과정을 거쳐 이제는 전기자동차가 시장에서 자동차 판매량의 상당부분을 차지하고 있다 [1]. IEA에서 발간한 Global EV Outlook 2024에 다르면 따르면 2023년 세계 전기자동차의 판매량은 약 35% 증가하여 1,400만대(시장판매량의 약 18%) 달했으며 2024년도에는 약 1,700만대에 이를 것으로 예상하며 이는 전 세계에서 판매되는 자동차의 약 20%에 달하는 수치이다 [1]. 이처럼 빠른 전기자동차의 증가에 따라 전기자동차의 충전기반시설도 급속도로 만들어지고 있으며 단순한 전기자동차의 충전만을 위한 기반이 아니라 스마트그리드 기술과 연계하여 전기자동차의 배터리를 새로운 신재생에너지원으로 사용하려는 기술이 Vehicle-to-Grid(V2G) 로 많은 연구가 이루어지고 있다 [2][3]. [그림 1]은 스마트그리드와 연계한 V2G 시스템의 개략전인 구성을 보여주고 있다.



[그림 1] V2G 시스템 개념도

[Fig. 1] Configuration of V2G system

현재로는 전기자동차의 단순한 충전만을 위한 기반시설들이 운용중이다. 관공서나 주유소에 설치된 급속의 공용충전장치들이 설치되어 있으며 가정에서 전력공급자와 계약을 통한 완속의 가정용 충전장치가 사용되고 있다. 단순히 전기자동차의 충전을 위해 전력을 구매하는 현재의 시스템의 경우 일반 주유소의 단말과 같은 단순한 과금 기능만으로 충분하다. 하지만 전기자동차의 배터

리를 분산에너지원으로 사용하려는 V2G 시스템은 전기자동차의 주행정보, 배터리 정보, 전력정보 등의 실시간의 여러 부가적인 정보가 필요하며 과금을 위한 민감한 개인정보도 제공되어야 한다 [4][5]. 이를 위해서 정보전송을 위한 네트워크 기술이 필요하며 중앙의 관리자가 있는 중앙집중형 네트워크를 사용한 V2G 시스템은 기존의 보안 체계와 인프라를 사용하기 쉬우며 서비스의 관리가 용이해진다 [4]. 하지만 전용시스템과 전용망을 포함한 별도의 기반시설을 구축하여야 하여 비용적인 측면에서 부담이 큰 실정이다. 중앙인프라나 관리자 없이 참여 노드들만으로 정보를 저장하고 인증을 포함한 거래를 안전하게 할 수 있는 기술로 블록체인에 대한 연구가 활발히 진행되고 있다. 블록체인은 중앙화된 기반시설 없이 참여 노들들만으로 데이터를 공유하고 인증하는 분산형 데이터베이스 시스템이다 [5].

본고에서는 사용자의 개인정보보호와 익명성을 보장할 수 있는 블록체인을 기반으로 하는 V2G 시스템을 제안한다. 2장에서는 블록체인의 형태와 작동방법에 대해 알아보고 3장에서는 제안한 블록체인을 이용한 전기자동차 충방전시스템에 대해 설명한다. 마지막으로 4장에서 끝을 맺는다.

2. 블록체인

2.1 블록체인의 개요와 종류

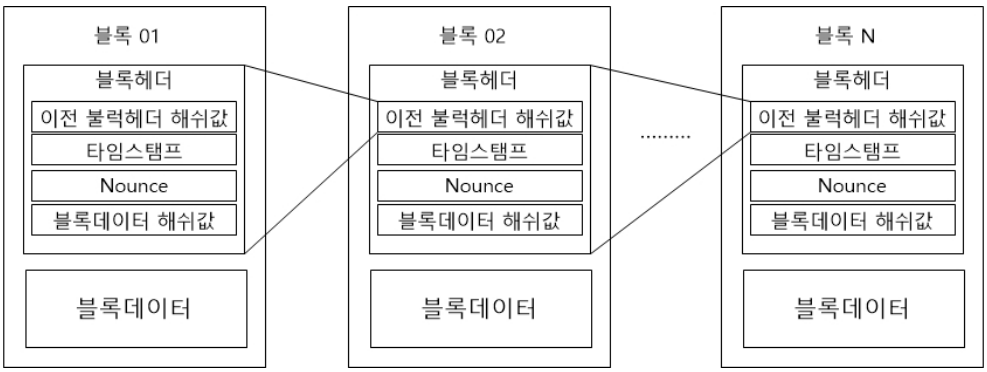
블록체인은 2008년 Satoshi Nakamoto의 Bitcoin 이라는 논문에 처음 소개된 개념이다. Nakamoto는 중앙기구나 금융기관의 영향력 없이 거래당사자들만 참여하여 직접 믿고 거래를 할 수 있는 암호화화폐(Cryptocurrency)인 비트코인을 소개하였다 [6]. 이 거래를 가능하게 하기 위해서는 모든 노드들이 모든 거래의 내용을 가지고 있고 이를 확인해 주는 분산된 데이터베이스 역할을 해주어 한다. 이를 위해서는 참가 노드들이 모두 연결된 분산형 네트워크 즉 블록체인을 구성해야하며 비트코인은 이 블록체인을 구성하는 대가로 제안되었다.

블록체인은 네트워크의 관리방법에 따라 Public Blockchain, Private Blockchain 그리고 Consortium Blockchain 으로 구분된다 [7]. 일반적으로 블록체인이라 칭하면 Public Blockchain 으로 누구나 블록체인에 참여 하여 거래를 할 수 있으며 거래를 확인해주는 데이터베이스 역할도 수행하게 된다. 이 형태는 Nakamoto가 제안한 형태로 관리자 없이 네트워크가 생성 운용되며 신분의 노출 없이 익명성이 보장된다. Private Blockchain 은 관리자 노드가 참여하는 경우로 Public Blockchain에 비해서 훨씬 빠른 속도로 거래를 처리할 수 있다. Consortium Blockchain 은 Private Blockchain이 여러 개 연합하여 이루어진 블록체인이다.

2.2 블록체인의 구조와 작동방식

이장에서는 관리노드 없이 누구나 참여할 수 있는 Nakamoto가 제안한 Public Blockchain의 구조

와 거래처리방식에 대해 설명한다. 블록체인에 참여한 참여노드는 온라인 거래(transaction)를 수행하고 자신이 수행한 이 거래와 다른 모든 거래의 내역의 내역을 원장(ledger)으로 만든다. 이 원장을 참여자 모두에게 브로드캐스팅하고 모든 참여 노드들은 이 거래 원부를 저장함으로써 이 거래의 내역을 확인하고 인증하게 된다. 이 원부를 블록 형태의 파일로 보고 거래 원부의 내역을 모두 연결하여 저장하는 것을 블록체인이라 한다. 이 블록은 거래의 내용을 가지는 블록데이터 (Block Data) 부분과 블록 헤더(Block Header)로 구성이 된다. [그림 2]는 블록체인의 구성을 보여 주고 있다.



[그림 2] 블록체인의 구성

[Fig. 2] Blockchain System

블록헤더 부분에는 이 블록의 번호, 앞 블록의 블록헤더의 해쉬값, 타임스탬프, 데이터 블록의 해쉬값 그리고 Nounce 로 구성이 된다. 앞 블록헤더의 해쉬는 SHA-256을 이용하여 256비트의 숫자 값을 가진다. Nounce 는 블록체인에 새로운 블록을 생성할 수 있는 기회를 갖기 위한 퍼즐 문제를 푸는데 사용된다. Nakamoto 는 조건을 만족 시키는 Nounce을 발견한 노드가 새로운 블록을 생성하도록 제안하였으며 새로운 Nounce 값을 발견한 보상으로 주어지는 것이 잘 알려진 비트코인이다.

최근에 생성된 블록은 바로 전의 블록의 블록헤더의 해쉬값을 가진다. 따라서 처음 생성된 블록의 블록헤더 부분의 정보부터 바로 전 블록의 블록헤더의 정보가 계획 해쉬되어 저장이 된다. 이러한 방식으로 최근에 생성된 블록은 처음 생성된 블록부터 모든 블록의 정보와 연결된 블록체인을 형성하게 된다. 만약 누군가가 거래 내용을 위조하게 된다면 블록헤더의 해쉬값이 달라지기 때문에 정당하지 않은 거래임을 바로 확인할 수 있다.

Nakamoto가 제안한 블록체인에서는 새로운 블록을 생성하는 노드를 정하는 방법으로 Proof of Work의 합의알고리즘을 사용하고 있다. 이 방식은 새로운 Nounce 값을 발견하는 참가자만이 새로 발견한 Nounce값을 포함하여 새로운 블록을 생성하고 이를 전체 네트워크에 브로드캐스팅 한다.

이 블록을 받은 다른 참가자 들은 발견된 Nounce가 적절한지는 판단하고 적절할 경우 자신의 블록체인에 새로 받은 블록으로 업데이트 하게 된다. Proof of Work 방식은 참가자가 새로운 거래 즉 새로운 블록을 생성하기 위해서는 매우 많은 양의 연산을 수행하여야 해서 참가자들에게 매우 큰 부담을 주게 된다 [8]. 또한 적절한 시간에 거래를 생성하기에 매우 많은 시간이 소요되어 암호화 화폐의 경우를 제외하고 일반적인 비즈니스 분야에서는 사용하기에 적절치 않을 수 있다. 이러한 제약을 극복하기 위해 여러 합의 알고리즘들이 연구되고 있다 [9].

3. 블록체인 기반의 V2G 시스템

이장에서는 블록체인을 기반으로 한 V2G 시스템의 구성, 인증 그리고 운용 메커니즘을 제안한다. 거래의 효율과 인증의 문제점 때문에 순수한 블록체인 대신 관리자노드의 개입을 최소화한 Private Blockchain 방식의 전기자동차 충방전시스템을 제안한다.

모든 전기자동차는 계산능력과 통신 능력을 가지고 충방전 기반시설과 서비스 제공자와 통신을 수행할 수 있다. 이러한 기능이 없는 전기자동차의 경우는 운전자의 스마트폰을 대신 사용할 수 있으나 서비스에 제약이 있을 수 있다. 거래 즉 배터리를 충전하거나 배터리의 전력을 판매하려는 전기자동차는 블록체인 참여 모듈 혹은 소프트웨어를 작동시켜 블록체인의 구성원으로 참여하게 된다.

하나의 충방전 기반시설은 하나의 Private Blockchain 네트워크를 구성한다. 전력서비스제공자는 이러한 블록체인을 하나의 분리된 네트워크로 관리하거나 연합 형태인 Consortium Blockchain 형태로 전체 충방전 기반시설을 관리한다. 이 Private Blockchain 네트워크는 관리자노드가 참여하며 이 관리자 노드는 전력서비스 제공자와 연결되어 전력충방전 기반시설에 포함되어 전력서비스 운영과 블록체인의 관리를 담당한다.

Step 1 : 블록체인 참여와 계정생성

하나의 충방전 기반시설을 관리하는 관리자노드는 비대칭암호화 알고리즘인 RSA나 ECC를 이용하여 공개키와 사설키를 만든다. 동일한 전력서비스제공자가 운영하는 충방전 인프라에서는 같은 키(Key)쌍을 사용할 수도 있다. 관리자노드는 전력서비스 참가자 전체에게 전력서비스제공자의 ID와 자신의 공개키 (Public Key)인 Kpub_admin를 브로드 캐스팅한다. 처음 이 전력서비스제공자에게 서비스를 제공받는 사용자도 자신의 공개키 Kpub_user 와 개인키 Kp_user 를 작성하고 자신의 ID (ID_user)와 공개키 Kpub_user를 관리자가 전송한 공개키 Kpub_admin 로 암호화 하여 관리자노드에게 보낸다. 사용자ID는 차량의 VIN 번호나 차량운전자의 전화번호를 이용할 수 있다. 관리자노드는 사용자ID와 사용자의 공개키를 전력서비스제공자에게 보내고 서비스제공자는 사용자ID에 임의의 솔트(salt)값을 더해서 해쉬(Hash)한 고객인식번호 H(ID_user,salt)를 생성하고 사용자ID, 사용자

공개키, 사용한 솔트값을 고객 리스트에 추가한다. 이 고객인식번호는 서비스제공자가 고객을 식별하기 위한 것으로 민감한 고객정보를 노출하지 않고 고객을 식별할 수 있다. 이러한 절차를 거쳐서 새로운 사용자는 블록체인에 참여하게 되고 서비스를 이용할 수 있다. 블록체인네트워크에의 참여는 오직 관리자 노드만을 통해서 수행하여 부적절한 노드의 참가를 막는다. 이와 같이 공개키 기반 기술과 해쉬 알고리즘을 통해 민감한 정보를 노출시키지 않고 블록체인 등록을 할 수 있다. 이 시스템에서는 관리자노드는 사용자의 어떠한 정보도 저장하지 않고 서비스제공자는 사용자의 ID, 공개키, 솔트 값만을 가진다.

Step 2 : 충방전서비스

사용자가 전력을 구매할 경우 즉 충전서비스를 사용할 경우에는 자신의 ID와 신용카드정보과 같은 결재 정보를 관리자노드의 공개키로 암호화한 다음 사용자 자신의 개인키로 다시 암호화 한다. 즉 관리자노드의 공개키로 암호화 된 정보에 사용자가 디지털서명을 하여 관리자 노드로 전송한다. 이 메시지는 받은 관리자 노드는 사용자의 공개키로 복호화 하여 신원을 확인하고 자신의 개인키로 다시 복호화 하여 메시지를 확인한다. 그 후 관리자 노드는 충방전시스템에 충전 서비스를 제공하라는 신호를 보내고 충전이 시작된다. 충전 완료우 받은 결재 정보로 결재를 하고 충전량과 과금 정보를 사용자에게 알려준다.

전력을 판매하는 경우에는 사용자가 자신의 ID, 송금 받을 계좌정보, 판매량을 포함한 메시지를 관리자노드의 공개키로 암호화한 후 다시 사용자 자신의 개인키로 암호화 하여서 관리자 노드로 전송한다. 디지털서명으로 신원을 확인하고 메시지를 복호화 하여 서비스의 내용을 확인한다. 이를 서비스제공자에게 보내서 승인을 받은 후 관리자 노드는 현재 전력가격, 전력구입량, 금액 정보를 사용자에게 보내고 서비스를 시작한다. 방전서비스 종료 후 구입한 전력량을 확인하고 금액을 지급한다.

Step 3 : 블록의 생성 및 체인구성

전력서비스 즉 전력의 판매나 구매 거래가 성립되면 이 거래는 원장에 기록이 된다. 이 거래 원장 즉 블록들은 허가된 참가자 즉 전기자동차와 전력서비스 제공자에만 저장되고 Private Blockchain을 이루게 된다.

거래원장 즉 블록은 충방전 서비스가 제공될 때 관리자노드에서 작성을 한다. 사용자측인 전기자동차는 연산능력이 부족한 경우가 많기 때문에 관리자노드에서 블록의 작성을 진행해주는 것이 시스템의 유지 및 운용에 더 유리하다. 관리자노드는 블록의 데이터부분에 고객인식번호 H(ID_user,salt), 거래내역 (충전 or 방전),거래시간, 거래전력량, 거래시점의 전력가격, 결재된 서비스 가격, 서비스위치(혹은 관리자노드의 ID)를 기록한다. 헤더부분에는 블록번호, 앞 블록의 불록헤더

의 해쉬값, 시간정보, 블록 데이터의 해쉬값을 가진다. 이 블록을 식별하기 위한 블록 번호는 sequence number - 고객인식번호H(ID_user,salt) 로 구성한다. 블록생성 순서대로 작성되는 sequence number 와 고유한 고객인식번호를 조합하여 특정고객의 거래내역의 관리를 보다 용이하게 해준다.

관리자노드는 작성된 블록을 자신의 개인키로 디지털 서명하여 사용자와 전력서비스제공자에게 전달한다. 사용자와 전력서비스제공자는 거래원장 확인 후 이상이 없으면 자신의 개인키로 디지털 서명하여 reply message를 관리자 노드에 보내고 이상이 있을 경우 이상사실을 알려서 관리자노드가 다시 거래를 검토하고 블록을 새로 작성하도록 한다. 관리자 노드는 확인이 완료된 새로운 블록을 자신의 개인키로 암호화 하여 전체 블록체인 네트워크 참여자들에게 브로드 캐스팅한다. 전체 블록체인 참여자는 관리자노드의 디지털 서명을 확인하고 부차적인 합의 과정 없이 거래의 원장 (블록)을 저장하고 블록체인에 추가한다.

블록발행 후 관리자노드에 저장된 사용자의 모든 정보는 삭제되고 전력서비스제공자와 사용자만이 사용자의 사용자ID, 공개키 그리고 고객인식번호 생성에 사용된 Salt값을 저장한다. 생성된 블록에는 민감한 개인정보는 저장되지 않고 오직 고객인식번호와 거래내역만 기록되어 있어 전력서비스제공자와 본인만이 이 블록의 당사자가 누구인지 알 수 있다. 재방문하여 전력서비스를 사용할 경우에는 자신의 ID와 기록된 salt 값으로 고객인식번호를 생성하여 이를 이용하여 전력서비스를 사용한다.

4. 결론

본고에서는 민감한 개인정보의 보호를 고려하여 Private Blockchain을 이용한 전기자동차 충방전 기반시설의 운용과 관리방안을 제안하였다. 비트코인으로 잘 알려진 Public Blockchain 네트워크는 모든 참가자가 동일한 자격을 가지고 합의 과정을 거쳐야 블록을 추가할 수 있기 때문에 체계적이고 빠른 처리가 필요한 비즈니스 부분에는 알맞지 않다. 제안한 방식은 관리자노드가 존재하는 Private Blockchain형태로 PKI를 기반으로 사용자, 관리자노드 그리고 전력서비스제공자 사이의 통신을 보호하고 관리지 노드가 서비스 종료 후 블록을 발행하게 된다. 이 과정에서 사용자의 인식을 위해서 salt값과 사용자ID의 해쉬값을 이용하여 이 거래의 당사자를 확인하고 사용자와 전력서비스 제공자 이외에는 이 거래가 누구의 거래인지 알지 못하게 익명성을 보장한다. 또한 블록에는 거래내역을 제외한 어떠한 개인정보도 기록되지 않으므로 개인정보유출에 대한 위험도 줄어든다.

References

[1] “Global EV Outlook 2024 Moving towards increased affordability”, International Energy Agency (IEA), Paris, France, April 2024, [Online]. Available: https://www.iea.org/reports/global-ev-outlook-2024.

[2] C. Liu, K. T. Chau, D. Wu, S. Gao, “Opportunities and Challenges of Vehicle-to-Home, Vehicle-to-Vehicle, and Vehicle-to-Grid Technologies”, Proceeding of IEEE, vol. 101, no. 11, November 2013, pp. 2409-2427, doi: 10.1109/JPROC.2013.2271951.

[3] S. Hahih, M. Kamran, U. Rahid, “Impact analysis of vehicle-to-grid techology and charging strategies of electri vehicle on distribution networks-A review”, Journal of Power Sources, vol. 277, March 2015, pp. 205-214, doi: 10.1016/j.jpowsour.2014.12.020.

[4] Z. Yang, S. Yu, W. Lou, C. Liu, “P2: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid”, IEEE Transaction On Smart Grid, vol. 2, no. 4, December 2011, pp. 697-706, doi: 10.1109/tsg.2011.2140343.

[5] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, K. Ren, “A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks”, IEEE Networks, vol. 32, no. 6, November 2018, pp. 184-192, doi: 10.1109/MNET.2018.1700269.

[6] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electric Cash System”, bitcoin.org, https://bitcoin.org/bitcoin.pdf, (accessed July 1, 2024)

[7] Y. Jiang, S. Ding, “A High Performance Consensus Algorithm for Consortium Blockchain”, IEEE 4th International Conference on Computer and Communications(ICCC), December 7-10, 2018, Chengdu, China, pp. 2379-2386, doi: 10.1109/CompComm.2018.8781067.

[8] D. Yaga, P. Mell, N. Roby, K. Scarfone, “Block chain Technology Overview”, National Institute of Standards and Technology(NIST), Gaithersburg, MD, USA, NISTIR8202, October 2018, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf.

[9] S. Pahlajani, A. Kshirsagar, V. Pachghare, “Survey on Private Blockchain Consensus Algorithm”, IEEE 1st International Conference on Innovations in Information and Communication Technology(ICIICT), April 25-26, 2019, Chennai, India, pp. 1-6, doi: 10.1109/ICIICT1.2019.8741353.