

International Roaming Services Optimization Using Private Blockchain and Smart Contracts

Mark Renier M. Bailon, Lawrence Materum

Electronics and Communications Engineering Department, De La Salle University, Philippines,
mark_bailon@dlsu.edu.ph

ABSTRACT

International roaming is one of the many essential services a carrier enables on its customer's subscriber identity module (SIM) cards that allows its users to send and receive calls, messages, and e-mails whenever they travel to another country. From its beginnings in voice roaming in the last 1.5 decades up to today, international roaming has been a pivotal contributor to the sales of telecommunications carriers. It does however come at a high cost, which the users end up paying, due to numerous factors such as roaming agreements between home carriers and visited carriers as well as clearinghouses needed by companies to settle disputes in agreements between the carriers involved. This paper proposes a consortium blockchain approach coupled with smart contract application. The decentralized nature of a blockchain and the automation that smart contracts provide solves two of international roaming problems—intermediaries and high cost. Together with Tendermint—a consensus mechanism that requires no mining, implementation of the consortium blockchain can be done involving all carriers around the world with them being the privileged users and verify the transactions of two engaging carriers. With this setup, the blockchain is privatized yet still able to perform the essential functions of a blockchain, which are immutability, security, and transparency of data. The proposal can eliminate the need for continually changing roaming agreements and clearing houses that increase the price for the users as well as slow down the processing time making international roaming services much more efficient, user-friendly and cost-effective for both its consumers and carriers.

Key words: Blockchain, Consortium Blockchain, International Roaming, Non-mining Consensus, Smart Contracts.

1. INTRODUCTION

International roaming service is one of the many services in the telecommunications industry a mobile-internet service provider or carrier can offer. One of the helpful technological attainment in the Global System for Mobile Communications (GSM) Standard is that it paved the way for tri-band phones to operate outside its usual range of operation [1].

International roaming is a service that enables users to continue to use their home mobile number to send and receive calls, messages and e-mails as well as accessing the internet while in a different country, this includes LTE-advanced mobile technology services. This service is essentially a paid “extension” of a user’s home carrier retail voice and data services to the country they visit. The “extension” service is enabled by a wholesale roaming agreement between the user’s home carrier and the visited country’s carrier. All technical and commercial components required to enable the extension is covered in the roaming agreement.

Most international roaming services, however, charges its users with a large amount to cover the expenses a home carrier makes when making a roaming agreement with the visiting country’s carrier. Prices can range from \$50 to \$180 for the user depending on the duration of the extension [2]. Furthermore, these contracts will differ from one agreement to another. This difference is due to the non-centralized nature of a carrier’s adherence to their respective country’s regulations. Thus, requiring the aid of clearing houses to manage the agreement between the carriers as well as settle any dispute that may arise, result in, making some roaming services more expensive or more restrictive than others.

The most common solution for people would be to acquire a local SIM of the country they visit or an international SIM card that covers the countries they intend to visit in order to have access to call, SMS and data services. However, the difference in price between this option and an international roaming service is negligible and presents a diminishing return problem once the visit/travel is over.

This paper aims to ameliorate how current international roaming services operate in terms of its roaming agreements and clearing houses as well its seemingly high charges to its customers. The current set-up between carriers relies too heavily on clearinghouses that serve as the intermediaries. Roaming agreements frequently change due to regulations leading to delays, quality reduction and price overcharge all of which the users have no choice but to accept due to limited alternatives/options [1], [3].

Several projects have already been kickstarted to implement blockchain to improve international roaming with the use of blockchain. These are BubbleTone Application, Mobile Intercloud System with Blockchain, and Roaming Fraud Prevention. These projects are detailed as follows.

1.1 BubbleTone Application

Creators of the BubbleTone Blockchain have partnered with Allo Incognito to offer a blockchain based mobile application for the telecommunications market. Similar to the concept that aims in reducing user cost, the focus of the project aims to convert the SIM of the user to a temporary virtual SIM of the country they visit [4].

1.2 Mobile Intercloud System with Blockchain

The study focuses on developing a mobile intercloud system integrated with blockchain. It combines cloud, mobile, and blockchain based computing in one. This focuses in much broader concept in that it is a small step in attempting to merge all telecommunications carrier around the world into one prominent provider so that the concept of “roaming” is not even applicable anymore due to every mobile device being linked to a virtual terminal in a massive cloud that can connect to any user in it [4].

1.3 Roaming Fraud Prevention

Due to the data exchange between home carriers and visited carriers in current international roaming schemes, criminals can exploit delays in the exchange of information between the carriers to accumulate calls with stolen roaming SIMs. The project aims to use blockchain to create a system that can instantaneously block a SIM instead of having to wait for both carriers to resolve the issue. The removal of said delay between carriers saves both user and the carriers of any costs caused by the criminal [5].

While these projects focus more on integrating the blockchain between client and carrier, this proposed blockchain schema will focus more on a carrier-to-carrier relationship

2. BLOCKCHAIN

2.1 The Blockchain Concept

The core concept of a blockchain was initially for solving a growing problem on generating trust in an environment without trust, more commonly known as the Byzantine General Problem. It is the most critical underlying technology on one of the first cryptocurrencies—Bitcoin, and it has paved the way for the growth and success of decentralized network structures within numerous industries. Compared to a conventional database or network infrastructure that is dependent on a centralized server, a blockchain is not handled by one single entity but a multitude of users that verify, authenticate and ascertain that data being stored in the blockchain is genuine like a peer-to-peer operation [6], [7].

Each “block” in a blockchain contains a particular set of transactions, the cryptographic hash of the previous block and a timestamp. Once consensus is achieved amongst the peers in the network, a new block is then added and cannot be altered due to the three components stated. Other key characteristics of blockchain include but are not limited to:

1. Immutability: data stored within a blockchain is essentially tamper-proof as numerous P2P participants verify data entry
2. Accessibility: a fast and stable internet connection is all that is needed to do transactions in a blockchain whether it be mining, transacting or embedding
3. Transparency: every data and transactions that happen in a blockchain is visible to all peers and can be accessed, edited and viewed at any time
4. Privacy: transactions within the blockchain with regards to its peers can be handled with complete anonymity

Considering all these characteristics as mentioned above and finding a way to implement them into international roaming services will not only make things easier for users but also the carriers as blockchain solve the two crucial problems that are prevalent in international roaming, namely: potential overcharging and intermediary dependency.

Blockchain’s ability to ensure that data within in it is genuine and tamper-proof as well as transparent to any of the peers in the network will eliminate the need for carriers to rely on clearinghouses to settle any disputes that may occur. This ability in effect, will reduce costs significantly for both carriers and users. Users will also be able to have a smoother and easier way to enable international roaming services through their device due to blockchains accessibility [8], [9].

2.2 Consortium Blockchain

Depending on the needs of a company, a blockchain can be configured to operate where transactions, approvals, and verification can be done by anyone (public) or a group of selected individuals (private). It comes down to the company’s choice of whether security or privacy is their priority. For this study, we use a consortium or federated blockchain where access is limited to a group of individuals

A consortium blockchain – often called a semi-decentralized blockchain—is the middle ground between a sufficiently publicized blockchain like what Bitcoin uses and a privatized blockchain that non-cryptocurrency industries use. It offers privacy amongst its users like a public blockchain while still enforcing security and protection against “bad” players of the data within the blockchain like a

private blockchain thru its hybrid centralized-decentralized nature [10].

2.3 Telecommunications Applications

The telecommunications industry has had one of the most complex operations for the past decade. Within the industry itself involves many parties, vendors, customers, suppliers and their incorporated supply chain, network and database providers all of which face issues in transparency and trust due to the number of the entities involved. Blockchain technology as a whole will be able to solve many if not all of the gaps conventional centralized systems have today. Specific areas in which these can be applied to are as follows but are not limited to:

- Internal processes
- Smart connections
- Mobile money
- Identity management, and
- Fraud prevention,

The benefits of adopting blockchain in the telecommunications industry are numerous with but a fraction stated above. Long-term cost-benefit analysis is still needed as to whether all of these should have blockchain integrated within them as overhauling current business models present additional costs and risks [11], [12].

3. SMART CONTRACT

3.1 Smart versus Traditional Contract

Conventional International roaming services rely heavily on roaming agreements between the carriers, which profoundly affect the cost of the service for the users. Furthermore, these contracts may change due to regulations concerning one of the participating carriers causing unavailability of service for a set amount of time until a new agreement can be made, resulting in inconvenience on the users. Unlike standard contracts that outline terms and conditions of a relationship between two parties and enforced by specific laws, a smart contract directly implements a relationship via a cryptographic code. Smart contracts are protocols developed to digitally verify, authenticate, enforce, and facilitate the status and performance of a contract. They allow trustworthy transactions between two parties without the need for an intermediary to enforce and provide nonrepudiation whenever a dispute occurs [11].

B. Ethereum

Smart contracts originated from a blockchain known as Ethereum. Through its virtualization platform, individual users were able to develop self-driven contracts that can be executed under either a decentralized, semi-decentralized, or centralized control.

This automatized nature of the contracts coupled with the transparency and immutability that the blockchain in which

the smart contract is embedded into allows parties forming a contract to lessen costs, increase efficiency and consistency [13].

4. CONSENSUS

In conventional centralized systems such as databases, a particular entity oversees handling all functionality of the database such as maintenance and facilitation. Tasks such as adding, deleting, and updating of specific data or records are performed by this entity, which is considered the sole in-charge of the data. Such functionality raises a few concerns regarding the immutability of the data this entity governs as they are the only ones that can perform any modifications.

Blockchains, on the other hand, that operates in a decentralized and self-regulating nature work on a global peer-to-peer scale. Involvement of peers ranging from thousands to even millions verifies and authenticates the transactions that occur within the blockchain. This involvement generally results in the consensus of the blockchain network. The consensus in a blockchain network is a “state” in which all peers agree that an entire transaction, data, or query is legitimate [14].

Given a blockchains dynamic nature, it requires a reliable, fast, and secure way to generate a consensus. A consensus mechanism or a set of regulations that determine the contribution of a peer within the network is needed to achieve the agreement.

Many consensus mechanisms have been developed since the blockchain implementation. Such a consensus is what is known as proof of work (POW); it is the consensus mechanism behind Bitcoin and several other cryptocurrencies. POW requires that a peer or a miner has done the necessary amount of work to qualify them to add new transactions in a blockchain. POW, however, requires a lot of computing power as well as energy consumption to function correctly [15].

Proof of stake (POS) is another popular consensus mechanism. Unlike POW, POS requires little computing power and can increase processing time. Instead of a necessary amount of work, POS investigates how much “stake” one peer has in maintaining a blockchain network. The higher the “stake,” the more likely it is for a peer to qualify them to add new transactions. Unfortunately, this comes with a few disadvantages such as the increased risk of being controlled by an entity since once peer can theoretically save up on “stake” and gain control of the blockchain network, this is more commonly known as a 51% attack [16].

5. TENDERMINT – A NON-MINING APPROACH

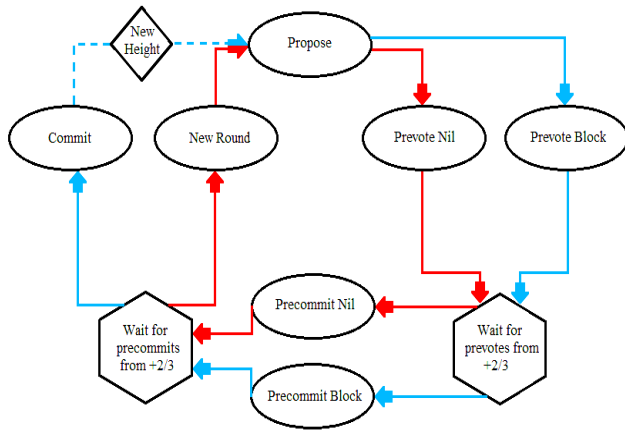


Figure 1: Tendermint Consensus Overview [15]

For consensus to be achieved in a public blockchain, most require a specific “proof” before a peer can alter or add to the blockchain. However, in privileged or private blockchains achieving proof is not necessarily needed since the peers within are registered before they can even perform anything in the blockchain.

Tendermint is a consensus mechanism which allows a blockchain and its peers to achieve consensus without the need for “mining.” It is a software that securely replicates the status of an application to its connected nodes. Every node on the network will see a single transaction at the same time and lock on to the state of the network after a transaction is done, with this all nodes are updated and have a copy of the status of the blockchain to which they can then verify and authenticate. Statistically, Tendermint is still able to operate efficiently, even when 33% of the nodes fail at some arbitrary point [15].

Tendermint is made up of two key components: an application interface known as Application Blockchain Interface (ABCI) and the engine for the blockchain consensus known as the Tendermint Core.

5.1 Application Blockchain Interface (ABCI)

Essentially what allows transactions on the blockchain to be read and written by any programming language is the ABCI. Compared to most consensus mechanisms of blockchains that come with a built-in scripting language, users of Tendermint can develop and write in whatever language and development environment they want [16].

The ABCI is also responsible for maintaining the Unspent Transaction Output (UTXO) database as well as validate any cryptographic signatures that transactions have. Client access to the UTXO for queries and authentication purposes is also handled by the ABCI. Lastly, the ABCI is responsible for preventing any transactions from an attack that is known as double spending.

5.2 Tendermint Core

For immutability to be achieved by any blockchain, all peers within the network must have the same and the most recent copy of the blockchain to reference if a transaction is authentic. The consensus engine that Tendermint uses is called the Tendermint Core. This mechanism ensures that the transactions that happen within the blockchain recorded and maintained by each peer in the network in a specific order. It shares block status and transaction details in all nodes and establishes a sanctioned order of transactions [16].

5.3 Consensus Overview

Peers within the blockchain are referred to as validators. The validator’s role is to propose blocks of transactions and vote which amongst it is to be committed in a chain; this proposal process is done in a round robin manner. It is possible for a block not to be committed in which case a new validator will have a chance to propose a block. A particular internal “fee” is still imposed in the system to prevent foul play amongst the validators and promote cooperation [15], [16].

The voting process is split into a pre-vote and pre-commit. A block is considered committed when it garners more than 66% of the validator’s pre-commit votes (Fig. 1). It is possible for validators to fail in committing a block. This event could be due to the current proposer to be offline or experiencing low bandwidth. In the event, this failure happens Tendermint allows the other validators to decide to skip the elected proposer.

Validators have to wait a specific amount of time to receive a block with a complete proposal before they can proceed to a next block. Tendermint is considered a weakly synchronous protocol due to the validator’s reliance on a timeout. Other parts of the protocol, however, are asynchronous, and the validators only commit a block once more than two-thirds of them have confirmed [16]

Tendermint ensures that validators will never commit two conflicting blocks at the same level by enforcing locking rules that regulate the path that is followed in the network flow. When a validator pre-commits, they are bound to that block and must pre-vote for the block it locks on. Only when there is a polka for a next block can that validator unlock and pre-commit again [16].

5.4 Cooperation within the network

Since transactions within an individual block are divided among the validators themselves, a bad player may arise and exclude proper signatures or include bad ones when proposing the next block. Consider the following scenario. Let f_k be the fee to be divided in the block k ($k = 1, 2, 3, \dots, \in \mathbb{N}^+$), v_i be the voting power of Validator i , where the total voting power is given as follows.

$$v_1 + v_2 + v_3 + \dots + v_n = 1 \tag{1}$$

The share of Validator i on the block k is $f_k v_i$. Validator 1 is the selected proposer for block 1 and wants to exclude Validator 2's signature. The stake would be Validator 2's share of the fees amounting to $f_1 v_2$. Making this exclusion would benefit Validator 1 by:

$$f_1 v_2 \frac{v_1}{1 - v_2} \tag{2}$$

Suppose it is Validator 2's turn and wants to retaliate and exclude Validator 1's signature on block 2. Then Validator 1 would lose $f_2 v_1$. Validator 1 will only gain an advantage if the "fees" in block 1 are higher than the "fees" in block 2.

$$f_1 v_2 \frac{v_1}{1 - v_2} > f_2 v_1 \tag{3}$$

However, since Validator 1 and Validator 2 can only get to be a proposer for on block each, neither of them will gain a substantial benefit since all block contains an equal amount of "fee" ($f_1 = f_2 = f_3 \dots$). The same can be said if a particular validator has multiple accounts and voting power, the exclusion and retaliation would amount to no substantial gain for any validator [16].

Thus, changing voting power and excluding signatures would be overall detrimental to validators since by excluding one another they give more power to validators that do not exclude in the blockchain leading them to end up losing advantage instead of gaining.

6. PROPOSED BLOCKCHAIN SCHEMA: RESULTS AND DISCUSSIONS

6.1 Current/Conventional Schema

Current international roaming service relies on an inter-carrier relationship that operates on a centralized database. This central database has two key components: the roaming agreement and the clearing houses. Roaming agreements handle what both the home carrier's and visited carriers' responsibility is when enabling a user to have access to international roaming service.

Clearinghouses ensure that both parties involved in the agreement commit to it (Figure 2) and shall settle any disputes. As stated before, this set-up, however efficient it may result in a charging rate that is too much for the user and can be optimized with blockchain implementation.

6.2 Proposed Schema

The schema will consist of two significant interactions, a carrier's registry into the blockchain network and the user's request for international roaming service. Carrier registry will involve further processing than current blockchain

implementations (see Figure 3 and the registration steps). On

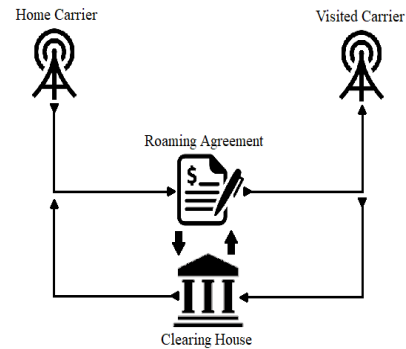


Figure 2: Conventional international roaming scheme between two carriers

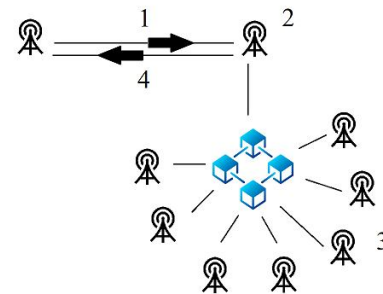


Figure 3: Carrier registration to the blockchain. The numbers correspond to the steps. In this example, there are seven carriers/mobile operators. The six carriers are connected to their blockchain network represented by the blue blocks.

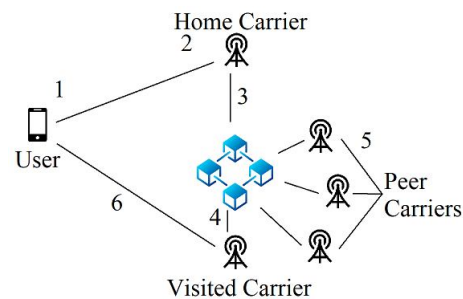


Figure 4: User registration for international roaming service. The numbers correspond to the steps. In this example, there are five carriers connected to their blockchain network.

the other hand, the user request focuses more on the smart contract formation, retention, and termination, as outlined in the steps given below (see accompanying Figure 4).

Carrier Registry Steps:

- (i) The carrier interested in joining the blockchain network sends a request to the nearest carrier that is part of the

network. Depending on the peers/validators in the network, requirements will vary on what they need from the interested party.

(ii) The nearest carrier receives the request along with the requirements and pushes it into the network along with its digital hash and identity; this carrier becomes the proposer for the entry of a new block in the network.

(iii) All the peers/validators will vote accordingly depending on the requirements submitted. The rules of pre-vote and pre-commit will apply in this stage and must be satisfied, or the block entry will be forfeited.

(iv) Once the vote is done, the carrier that received the request will send a status to the interested carrier and shall be provided with its digital hash and identity if they are allowed to join the blockchain network.

User Request Steps:

(i) User enables roaming on their device so that a connection request can be sent to the home carrier. If there is no existing contract, enabling roaming will automatically forward digital hash, identity, profile and the country the user is visiting the home carrier along with a charge that will be deducted once the contract is established.

(ii) The home carrier checks if an existing contract enabling roaming is already within the network.

(iii) If no contract exists, the home carrier will forward the user's digital hash, identity, and profile to the visited carrier. The contract is initiated and sent to the blockchain network as well for verification and approval.

(iv) Visited carrier verifies the hash and identity and approves/disproves the smart contract and sends the status of the contract to the blockchain network.

(v) Peer carriers within the network process the transaction into the blockchain network. Blockchain status is updated and is sent via the Tendermint Consensus mechanism.

(vi) Visited carrier integrates the profile of the user to their local network and allows the user to connect and access the carrier's services

7. CONCLUSION

Overall, blockchain implementation within any branch of telecommunication can be beneficial. Due to its flexibility in adjusting for privacy or security coupled with its famous immutability and transparency characteristics, blockchain can significantly reduce cost, increase efficiency and decrease unnecessary processing time caused by intermediaries and

inconsistent and unstable written contracts.

With this specific proposed scheme, international roaming, one of telecommunications key contributors to its income source can be improved in such a way both user and local and foreign carriers can reduce their expenditures by removing roaming agreements and clearing houses that significantly raise the cost in the conventional way of international roaming.

Smart contracts can essentially replace law firms due to their discrete, strict, and non-reputable nature. Disputes of any kind are settled within the contract, and no party can claim otherwise due to multiple peers validating every transaction that goes thru the blockchain network.

Consensus mechanisms provide a way for immutability to happen. Specifically, in this work, the cellular phone roaming service is keyed through the Tendermint Consensus due to its flexibility in terms of coding and simplicity in its architecture. Carriers that want to participate in the network need to contact one administrator and provide necessary documents and other requirements to be part of the blockchain network and participate in the proposed international roaming schema.

Users, by merely enabling roaming in their devices can request access for international roaming, select a preferred quality of the service from the home carrier and the rest is processed smoothly throughout the network without having to go through intermediaries that bump the price of otherwise cheap and reliable service.

REFERENCES

1. E. Sutherland, **International roaming charges: over-charging and competition law**, Telecommunications Policy, vol. 25, no. 1–2, pp. 5–20, 2001.
[https://doi.org/10.1016/S0308-5961\(00\)00084-7](https://doi.org/10.1016/S0308-5961(00)00084-7)
2. GlobeTelecoms, **International Postpaid Roaming**, www.globe.com.ph/international/roaming/postpaid.html, 2019.
3. Bubbletone, **Bubbletone to Use Blockchain Technology as a Solution to International Roaming**, cryptovest.com/news/bubbletone-to-use-blockchain-technology-as-a-solution-to-international-roaming, Jan. 2018.
4. Y. H. Ho, Z. Cheng, P. M. F. Ho, and H. C. Chan, **Mobile Intercloud System with Blockchain**, in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, 2018, vol. 1.
5. E. Priezkalns, **Blockchain Proposed as Solution to Roaming Fraud**, commsrisk.com/blockchain-proposed-as-solution-to-roaming-fraud/, Oct. 2018.

6. G. Adamson and J. Mohan, **Introduction to Blockchain**, *ieeetv.ieee.org/ieeetv-specials/introduction-to-blockchain?*, Dec. 2016.
7. L. Nekrasenko, A. Kalinichenko, A. Brzozowska, and B. Lazurenko, **Decentralized social and economic network as an alternative economic relations development in society**, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, no. 1, pp. 308–313, 2019.
<https://doi.org/10.30534/ijatcse/2019/5481.12019>
8. Z. Ramzan, **Bitcoin**, *www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-overview*, 2013.
9. M. Di Piero, **What is the blockchain?**, *Computing in Science & Engineering*, vol. 19, no. 5, pp. 92–95, 2017.
<https://doi.org/10.1109/MCSE.2017.3421554>
10. O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, **Consortium blockchains: Overview, applications and challenges**, *International Journal On Advances in Telecommunications*, vol. 11, no. 1&2, 2018.
11. A. Hertig, **How do Ethereum Smart Contracts Work?**, *www.coindesk.com/information/ethereum-smart-contracts-work*, 2019.
12. S. Haji, Q. Tan, and R. S. Costa, **A hybrid model for information security risk assessment**, *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 1, 2019.
<https://doi.org/10.30534/ijatcse/2019/1981.12019>
13. M. Barret, **Smart Contracts and Ethereum Explained**, *www.clerro.com/guide/462/smart-contracts-and-ethereum-explained*, Mar. 2019.
14. C. Hammerschmidt, **Consensus in Blockchain Systems**, *medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe*, Jan. 2017.
15. Tendermint, **What is Tendermint?** *tendermint.com/docs/introduction/introduction.html*, Aug. 2018.
16. J. Kwon, **Tendermint: Consensus without mining**, *Draft v. 0.6*, fall, 2014.