



The use of Smart Contract in Utility Business

¹MAKMUR A., ²VIAN ENDRAMANTO, ³GUNAWAN WANG

^{1,2}Information Systems Management Department, BINUS Graduate Program – Master of Information System Management, Bina Nusantara University, Jakarta, Indonesia.

¹makmur.a@binus.ac.id; ²vian.endramanto@binus.ac.id; ³gwang@binus.edu

ABSTRACT

PT PLN (Persero) as one of the state-owned companies in Indonesia, has the business of selling electricity as one of the core businesses of the company. Business. With customers in 2018 reaching 71.92 million customers, PT PLN (Persero) has entered into a power purchase and purchase contract with customers with the same number of 71.92 million customers. Smart Contracts are expected to be a substitute for written contracts because smart contracts do not require storage space for written documents and are safe from contract changes made by unauthorized parties because they are protected by cryptographic techniques.

Key words: Cryptographic PLN, Secure, Smart Contract

1. INTRODUCTION

PT PLN (Persero) as one of the state-owned companies in Indonesia, has the business of selling electricity as one of the core businesses of the company. The electricity customers of PT PLN (Persero) at the end of 2018 amounted to 71.92 million customers with 130,281 MVA connected power [1].

When viewed from the number of customers, the number of sales and purchase agreements (contracts) made by PT PLN (Persero) is equal to the same figure (71.92 million contracts) and all of them are still in writing. As is known, that making a contract of sale and purchase in writing, requires a lot of things, especially about how to save these contracts.

In the industrial era 4.0 which is currently developing, there is a blockchain technology that enables the creation of paperless and high-security smart contracts and can be one of the solutions to increase contract accountability between buyers and sellers, especially in power purchase contracts.

2. LITERATUR REVIEW

2.1 Blockchain

Blockchain is a technology that does not use third parties in exchanging information or entering into agreements. The technology is in the form of blocks and is interconnected and secured through cryptographic techniques. This technology can ensure the exchange of information that is very accurate and safe, because each block is interconnected, so if there is 1

block that is changed, then the block will not be part of the block above it. The description of the blockchain is as follows:

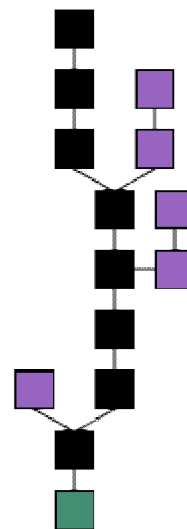


Figure 1: Blockchain

(<https://en.bitcoin.it/wiki/File:Blockchain.png>)

2.2 Smart Contract

A Smart contract is the application of code on the blockchain that aims to bind agreements or agreements between several parties. The Smart contract system is claimed to be able to increase trust due to the use of permanent code that cannot be changed, but due to its permanent nature makes smart contract more rigid than real contract (written contract), and to create this smart contract for engineers there are still limitations in the programming language.

Although there are currently constraints as described above, smart contracts have a tremendous opportunity to replace real contracts (written contracts) because smart contracts do not require storage space for written documents and are safe from contract changes made by unauthorized parties because they are protected by cryptographic techniques

2.3 Ethereum and Bitcoin

Smart contracts were popularized by Ethereum. Prior to that point, if we had a transaction in Bitcoin, we wouldn't be able to specify conditions on the transactions. For Example, Alice

who wants to sell her car, and Bob is looking to purchase it. He only wants to buy the car if Anna approves the condition of it, which is Bob's mechanic. Now, prior to smart contracts, mechanic approval would be dealt with outside of the network. Only the transaction would be recorded onto the network. Ethereum aimed to change this. There is a statement from Vitalik, one of the founders of Ethereum, "In a smart contract approach, "the benefit or profit is moved into a program, "and the program at that point runs this code, "and sooner or later, "it automatically approves a condition, "and it consequently determines "whether the benefit ought to go to one individual "or to the other individual, "or whether it ought to immediately refund "to the individual who sent it, "or some combination thereof." The real means is we're able to introduce conditional logic to determine where transactions go. If we go back to our example, we still have Alice who is looking to sell her car and Bob who is looking to purchase it. They have now agreed to enter into a smart contract, so Bob will transfer 30 Ethers should Anna approve the condition of the vehicle. So once she does this, the smart contract will automatically update, and it will transfer the coins to Alice, and it will be updated onto the ledger. In Fabric, the term chain code is used interchangeably with a smart contract. A chain code is the business logic that can be run by peers. It allows peers to query the ledger or manage ledger state with proposed transactions by various apps. The great thing about chain code is that it can be written in JavaScript, Golang, or Java. Unlike Ethereum, where the code is dependent upon the Ethereum virtual machine, chain code runs in its own docker container outside of the endorsing peers.

The development of blockchain owes its introduction to the world to Bitcoin. In any case, while Bitcoin centrally focuses on sending and receiving digital money, different solutions have developed the utilization of blockchain beyond the payment system. One of the most well known is an open-source platform called Ethereum. It uses a cryptocurrency called ether to fund the execution of software code over a distributed peer-to-peer network. Ethereum was proposed in late 2013 by Vitalik Buterin, a cryptocurrency researcher and programmer. Unlike the allusive Satoshi Nakamoto of Bitcoin fame, Vitalik is very much real and known. Today, he continues to develop Ethereum with the global open-source community. Ethereum's peer-to-peer network is made up of participant computers collectively called the Ethereum Virtual Machine, or EVM. Just like Bitcoin, every computer has the complete blockchain installed. It's trustless and uses consensus and miners to add blocks. When a new transaction is added, it gets added to every computer. That's where the similarities largely end. Instead of currency as the end goal, Ethereum enables programmers to use a proprietary language called Solidity to write code that is distributed across the EVM and executed under certain conditions. In blockchain parlance, we call this code smart contracts. Smart contracts enable distributed applications known as apps. Most enterprise-class applications rely on expensive and redundant architecture. Everything from identity management to storage must be provided and supported. In addition, several layers of code to

ensure security, scalability, and logic create cost and performance overhead. For a developer, Ethereum provides the possibilities of a low-cost, massively scaled, and secure application platform right out of the virtual box. The EVM avoids censorship, downtime since it can't be turned off, fraud, and third-party interference. In particular, Ethereum applications can be trustless, not relying on the attendant challenges of governing authorities. The magic with Ethereum is that, when smart contracts are executed, there is a movement of cryptocurrency, in this case, ether that acts as a method of payment and authentication. The remarkable consequence of smart contracts is that they can technically live forever, executing any time conditions are met. Since the value of ether fluctuates, the cost of executing a smart contract can go up or down. In this way, a smart contract is more like a commodity. While we're still in the early days of application development, there are a number of ideas being pursued, including a voting system called Horizon State, a prediction market called Augur, a live broadcasting system called Livepeer, and a system for buying and selling event tickets called EventChain. These few give us a sense of the diversity we can expect in the future. Ethereum illustrates the enormous potential of blockchain technology. Rather than a technology limited to digital money, blockchain opens up a completely new way of thinking about developing, deploying, and executing software. While the future path for Ethereum and others is still somewhat unpredictable, the winners that emerge will be the creators of the next generation of the internet.

The real strength of Ethereum lies in the creation of smart contracts. One way to think of smart contracts is that they're like a special kind of a class. In this class, public functions can be called on externally. And data will be stored in the blockchain. One of the key differences between running this and another programming environment, however, is that when you call a write operation, it will cost gas, which is Ethereum. Keep in mind that some of these write operations will involve sending money as well. Every contract will run in its own address, its own box that stored in the account. This account will be similar to a wallet address that you might have starting with zero x and having some letters and numbers afterward. The original idea for Ethereum was essentially to do some coding that enables us to put money in holding bin, and this holding bin would require certain parameters to be met. And once those parameters will be met, it could then release the money to someone else or to a number of different people or return the money to the original individual who sent it. However, smart contracts have evolved considerably. They've evolved to encompass all kinds of code that are executed on a blockchain node. This means they're behaving much like a normal programming class or an executable service. So each smart contract is essentially a grouping of functions and state variables that reside on the blockchain and also can store data and interact with that blockchain opening unlimited possibilities to what we can do. Not just in terms of financial applications, but also in terms of decentralized applications. When creating a smart contract, it will be uploaded as a bytecode. This bytecode is then stored on the blockchain in the

Ethereum network. The blockchain is immutable, which means that anytime we would want to make a change to the contract, we will have to move that contract to a new address. We can't edit what's at the original address, because that is now in a block that's already been processed. One thing to remember also is because of this the code is actually stored live, which means we are exposing our actual code. Now, on one hand, having that code available and sometimes people will upload not just the binary code, but they'll upload the original solidity code that they wrote the smart contract in for full transparency. This enables anyone who interacts with that contract to understand that it's not going to automatically take that ether and send it some mysterious Ethereum wallet. But because of this public availability of our code, it also means that our code must be written very well. It must be well-tested or savvy hackers can actually exploit the code. This happened in 2016 in what's now called the famous DAO Hack. Fifty million dollars worth of ether was drained from a contract and this caused a lot of turmoil in the community, whether or not they should write code to fix that hack. The debate still continues today. They did actually write codes so anyone who's using ETH, is running on the code base that had a fix for the DAO. However, there were a number of resisters and they're the ones who created what's called Ethereum Classic or ETC. So the bottom line is Ethereum represents a turing complete smart contract processing environment. And they talk about this a lot, really all that means is it's a programming language where we can do the things we'd expect to in a modern programming language. Everything is available, decentralized on the blockchain. It's public and it's unchangeable. Because it's built into the blockchain, financial applications are extremely easy to write in integrating any type of financial processing that comes quite naturally in the smart contract. And finally, we don't just have to store ether inside of a smart contract. You can store all kinds of data. In fact, any public variable that we create is going to be stored in the state of the Ethereum network and in the blockchain. Overall smart contracts are one of the key reasons that blockchain and distributed ledger technology are advancing beyond the use case of simply storing value or handling financial transactions. Being able to write code that resides in a blockchain allows for distributed functionality that is used to automate contract execution and provide back-end power to decentralize apps or DApps.

2.4 Energy Sector and Blockchain

Most of us take energy for granted. We turn on a light and it works. It powers our homes and the economies of the world. Over the past century, low-cost electricity has powered the biggest improvements in the quality of living for most people in history. But this incredible transformation has taken a toll. We've dug deep holes to extract coal, oil, and natural gas provide us with a steady supply of energy and a planetary hangover. From climate change to poor air quality to ground pollution and disease and poisons in our rivers and oceans and more, we've paid a hefty price. Still, our appetite for energy is increasing. Fortunately, a mix of power efficiencies in our devices, the promises of renewables such as solar, wind, and

thermal as well as safer nuclear options may create new opportunities that mix power abundance with lower cost and less impact on the planet. There is political and economic motivation to drive much more energy innovation. One of the most speculative areas is the role of blockchain technology in the energy sector. The energy sector like many others generates a high volume of transactions. There is a wide range of participants in any energy interaction. Consider energy generators, distributors, traders, regulators, and industrial end-users as the core players. In the flow of energy from the generation source to the consumer, there is a myriad of these stakeholders, additionally, billing and cash flow move between independent participants. It's a complex ecosystem that requires extensive trust and intermediaries. At a basic level, blockchain technology seems well suited to securely recording and storing transactions and thus increasing integrity and trust. In addition, an energy blockchain could provide secure storage of ownership records, in particular in the field of energy certification. Here are three use cases. First is the verification of renewable electricity and emission allowances. In the second case, a register that records and regulates the ownership and current state of assets such as smart meters, networks, and generation facilities. And the third, smart meter data could be shared with a wide variety of consumers without compromising privacy or security while also offering the opportunity to generate income from sharing. The next area is in the domain of energy billing. For example, billing for Electric Vehicles or EVs. As more people buy EVs, we'll eventually require an extensive network of perhaps millions of charging stations. When EV parks say in a supermarket parking lot, it's an opportunity for charging. While many payment systems exist, an efficient billing mechanism could be provided by the blockchain. As we explored in my blockchain basics course, the *stok*. Its solution enables secure, efficient blockchain transactions between devices without needing intermediaries, for example opening a bicycle lock with a smartphone. In fact, a startup called *Share&Charge* allows anyone who owns an EV charger to become a provider. This could be an excellent bridge option as the EV charger network gets built or perhaps it is the shape of things to come. Traditionally, there are major energy producers who provide energy either carbon or non-carbon based directly to customers or through a distribution provider, but this model which hasn't changed in decades has the potential for future disruption. In particular, when industries and homeowners begin to produce their own power using solar and wind, for example, a marketplace where the consumer also becomes the producer is well within the realm of possibility in just a few years. The potential trading and interactions between players become very interesting indeed. Let's assume that an entire sizable neighborhood of homeowners generates their own power. This neighborhood has microclimates so sometimes one side of the neighborhood is cloudy while the other side is sunny. When the cloudy side needs power and assuming the sunny side produces more than it needs, the excess power could be sold to the cloudy side. A great way to facilitate this will be to use a blockchain that uses smart contracts to manage the energy trades. Over time, homeowners would accumulate cryptocurrency that could be converted to say dollars or could

be used to directly purchase products. Several companies are already developing and testing this technology. Using theorem technology, Grid Singularity supports many of these use cases. Power Ledger is another cutting edge blockchain-based platform for energy trading. Electron in the UK is building a platform for microgrid trading and also for smart grid data management. Finally, SolarCoins are earned from homeowners who produce solar power. Authenticating the generation of power results in the collection of SolarCoins. The SolarCoin blockchain is a tradeable digital currency that can be converted into local currency or used directly with a variety of retailers. It's a model for incentivizing solar power usage. SolarCoin gets its value from being the product of power generation which produces proof of work. It's clear there's a lot of energy in the blockchain energy space.

2.5 Smart Contract Templates

According to Grigg’s Ricardian Contract framework, there are three key templates in a smart contract, namely "procedure, parameters and code". In this framework, execution parameters are extracted from the legal process and passed to the smart contract code that provides automated execution[2]. Example of the smart contract parameters written in javascript is shown below[3]:

```
Const SHA256 = require('crypto-js/sha256');
```

```
Class Block {
  Constructor (index, timestamp, data, previousHash = '') {
    this.index = index;
    this.timestamp = timestamp;
    this.data = data;
    this.previousHash = previousHash;
    this.hash = '';
  }
}
```

```
CalculateHash() {
  Return SHA256(this.index + this.previousHash +
  this.timestamp + JSON.stringify(this.data)).toString();
}
```

On those parameters, we can see that there is two hash that makes sure no one is able to change it because the hash is related to another hash (previous hash and now hash). Content of smart contract relies on the container of data, that can be set to define the contract itself.

3. SMART CONTRACT FOR ELECTRICITY BUSINESS

3.1.P2P trading system model of electricity blockchain

The upset towards the P2P power trade framework can be accomplished predicated for the modest scope vitality generators, where they may create, devour, and sell an abundance power limit like a commodity. The various leveled structure is rather supplanted by vitality exchanges and understandings. Right now, loads including household and business clients are fit for associating with both the retail for

end clients and discount showcase from the ordinary force generators[4]. This paper proposes a distributed power exchanging framework that sanctions prosumers to exchange vitality while guarantees the general system quality with its structured agreement component.

3.2.Overview of P2PEBT (P2P Electricity Blockchain Trading) system

As appeared in Figure. 2, in the customary force network framework (Figure. 2a), the power stream is various leveled, and the power trade process depends on the retailers to take part in the value exchange process. So as to adjust the current customary force framework, we can allude to the Figure. 2b that we receive the traditional force conveyance framework. The framework reconstruction lies in the center to the low voltage level where the force loads are appointed in microgrid containing renewables, little force storage. Other than giving the discount showcase in the customary framework, value-based vitality empowers the coordination of retail clients using continuous tranching exchanges to be executed naturally by blockchain installed framework, thus diminishing the brought together highlights of the cutting edge matrix framework [5].

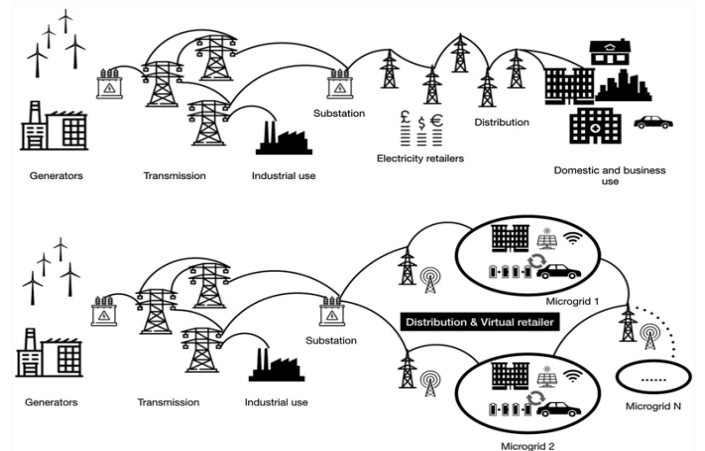


Figure 2:Model comparison of Electricity trading system.

a Traditional power distribution system.

b Proposed decentralized power trading system using microgrids

In the P2PEBT framework, all parts in the microgrids, for example, residential clients, batteries, sunlight-based boards are equipped for drawing and infusing power into the force organize. The power resource is expected as a savvy property as responsibility for the resource can be constrained by brilliant agreements. The upside of regarding power as the savvy property is that it very well may be controlled by means of computerized gadgets and the advantage possession move can be accomplished requiring little to no effort. The requests for purchasing and selling power are characterized as exchanges, in which the data is communicated in the lattice framework through a suitable remote system [6]. The exchanges can likewise be executed among retail and discount markets which level the open door for all parts. Also, the trading strategy must record for the transmission and dispersion limits and other physical imperatives on the matrix.

As examined over, the P2PEBT framework adjusts to the accompanying principles [7]:

1. **Adaptable** The essential parts of the P2PEBT framework is taken as the reference to the present market arrangements, which additionally have been adjusted to receive the blockchain innovation. P2PEBT framework remains the trustworthiness of the customary model and conforms to the market rules.
2. **Efficient** The exchange procedure takes out the association of the outsider contrasting with the customary retail process, in this manner the measure of time expended is diminished while the proficiency is improved in a straightforward trade way.
3. **Flexible** The proposed model sends an open exchanging stage which permits more vitality prosumer types to enter the trade showcase in an increasingly adaptable way.
4. **Cost-successful** The new power framework fabricates an immediate association among purchasers and venders while guaranteeing the general force organize soundness, which augments the monetary return for both the matrix framework administrators and individual clients.

3.3.P2P trading model in P2PEBT system

As portrayed in Figure. 3, the microgrid segments are the hubs in the P2PEBT framework and they can distribute exchanges as indicated by their requests. The requests of purchasing and selling power are typified as exchanges in the P2PEBT framework, where every exchange period is characterized as Tround. Tround is the ideal opportunity for mining another square in the blockchain which is characterized by the agreement natives. What's more, every hub is equipped for setting the cost for the power exchange to boost clients to adjust the organic market, meanwhile, to decrease the force age and utilization tops. For every exchange (TXi) that is distributed by the prosumer I in the P2PEBT system[8].

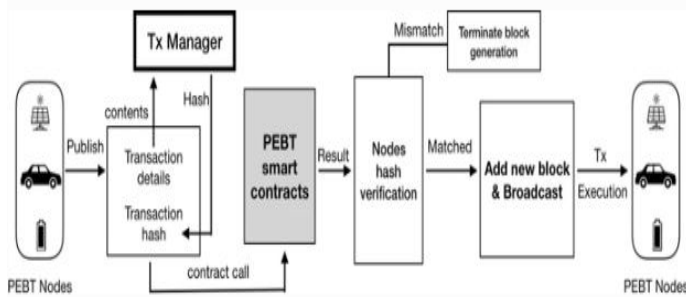


Figure 3:Structure of proposed P2PEBT system transaction process

1. *Transaction Initialization.* So as to ensure user’s’ privacy, the exchange payload is encoded by the exchange supervisor where the real substance of the exchange is introduced by hash. In P2PEBT, the exchange subtleties must be gotten to by the arrangement hubs and the genuine substance can be uncovered by personality enlistment with the exchange director.
2. *Transaction aggregation.* After the culmination of request planning, all exchanges are totaled including the measure

of power and anticipated serving time. The framework will check the absolute power requests and call smart contracts to execute transaction exchange.

3. *Consensus commitment.* The accord component is applied to the exchanges to choose a pioneer of the present procedure. The pioneer communicates square information and its proof-of-Benefit (PoB) to other approved hubs. The hubs at that point review the square information to check whether the hash coordinates its nearby records in the hubs hash confirmation process. On the off chance that the hash results are coordinated, hubs will acknowledge the new information square and continue to the subsequent stage. In the event that not, at that point the new block generation process will be ended, and the system will wait for the following round.
4. *Block generation.* The concurred exchange information is then communicated to the entire system and just members being chosen in the new square can unscramble the square substance to execute the exchanges. At that point, the encrypted block contents can be executed in the system.

3.4.Proposed Templates

After knowing the key templates of a smart contract, we proposed parameters of smart contract for electricity business in Indonesia is shown below :

No	Parameters
1	Index
2	Timestamp
3	Data : - NIK/IDCustomer - NameCustomer - NIK/ID Seller - Amount Transaction
4	Previous Hash
5	Hash

4. CONCLUSION

From the description above, we can conclude that to make a smart contract for electricity business needs parameters as follows :

- Index
- Timestamp
- Data Contract (Contract Content)
- Previous Hash
- Hash

This is minimal parameters that must be include when we are going to make a smart contract for electricity business in Indonesia. Further research also can be made to make sure the very important parameters that can be applied in electricity business smart contract.

The power business is experiencing significant developments that works unquestionably more than the framework update, where individuals center more around inexhaustible and

practical vitality. Right now, proposed a proof-of-advantage accord convention in the blockchain framework and further introduced the P2PEBT framework that works with retailers in the power market to limit the force change in a day. By accomplishing the target, the soundness is improved with progressively leveled power utilization and the activity cost is as needs be decreased comparing to the new circumstance activity. We broke down the condition of-craftsmanship blockchain innovation and the accord instruments including proof-of-work and proof-of-stake where the inspiration is related to regard to the drawbacks in these systems. At that point, the PoB is proposed alongside the P2PEBT framework to help retailers taking an interest in the power exchanging with neighborhood peers. Security examination has indicated that the proposed instrument is fit for ensuring the exchange execution against potential assaults and adjusting to the power exchanging situation. Reenactment results present the charging and releasing interest changes utilizing the P2PEBT framework and further infers the capacity of the proposed system to generously diminishing the PF value.

REFERENCES

- [1] PT PLN (PERSERO), “Annual Report,” 2018.
- [2] C. D. Clack, V. A. Bakshi, and L. Braine, “Smart Contract Templates: essential requirements and design options,” pp. 1–15, 2016.
- [3] Xavier Simply Explained - Savjee Youtube, “Creating a blockchain with Javascript (Blockchain, part 1),” 2017.
- [4] M. Andoni *et al.*, “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” *Renewable and Sustainable Energy Reviews*. 2019.
<https://doi.org/10.1016/j.rser.2018.10.014>
- [5] B. T. Patterson and D. E. Geary, “Real-Time transactional power management in a microgrid mesh network: The enernet,” in *INTELEC, International Telecommunications Energy Conference (Proceedings)*, 2016.
<https://doi.org/10.1109/INTLEC.2016.7749106>
- [6] M. Pilkington, “Blockchain technology: Principles and applications,” in *Research Handbooks on Digital Transformations*, 2016.
- [7] C. Liu, K. K. Chai, X. Zhang, and Y. Chen, “Peer-to-peer electricity trading system: smart contracts based proof-of-benefit consensus protocol,” *Wirel. Networks*, 2019.
<https://doi.org/10.1007/s11276-019-01949-0>
- [8] Y. Zhang and J. Wen, “The IoT electric business model: Using blockchain technology for the internet of things,” *Peer-to-Peer Netw. Appl.*, 2017.
<https://doi.org/10.1007/s12083-016-0456-1>