is connected, due to store information related to the user's life. The use of control access techniques, which guarantee reliable authentication, authorization, and confidentiality of the services, does not ensure a holistic solution to the privacy problem. This difficulty happens due to the data needs to be disseminated in different parts of the network. In addition to privacy issues, another challenge facing the popularization of SG networks is security. Security problems on SG networks can cause disastrous effects on the network. According to [4], an SG network is vulnerable to cyber-attacks such as traffic analysis, social engineering, cracking, spoofing, denial of service, and others. If a security flaw exists in equipment connected to the network that could compromise the system, an update would be necessary to correct all devices, impacting a high monetary cost. To avoid security problems, the use of communication protocols that guarantee security in SG networks is essential.

For the data monitoring and communication in SG networks, different protocols exist for these areas. These protocols aim to ensure efficient solutions to the reliability and security of the network [5]. However, the use of different protocols fragments the development of new applications, generating different network architectures directed to the SG segment. The use of a protocol that satisfies the requirements of an SG network is necessary for the development of new applications.

The Open Smart Grid Protocol (OSGP) is a protocol widely used in SG applications. OSGP Alliance developed the OSGP and published as a standard by the European Telecommunications Standards Institute [6]. The protocol implements all layers of the OSI model and provides security through cryptographic methods for Smart Meters (SM). However, studies expose security flaws on the OSGP encryption method. The work presented by Kursawe and Peters [7] shows a structural weakness in the cryptographic process of OSGP. The main flaw observed was the use of RC4 encryption, with each new key generated for each message transmitted, only the first eight bytes of this new key is different from the others. Another problem observed was that is used only one key for authentication. This same authentication key is used to derive the encryption key, so if the authentication key is exposed, all encryption keys are compromised.

Security flaws are not exclusive of the OSGP protocol. As shown in [5], other SG protocols also have security flaws that can compromise the entire network. Conventional techniques of privacy and security are not sufficient to guarantee these requirements. For this, it is necessary to use an architecture that holistically guarantees security and privacy.

In 2008 Satoshi Nakamoto presented the Bitcoin system to the world. Bitcoin is a virtual currency, also known as cryptocurrency [8]. This technology works based on P2P communication among network users, eliminating the need for a third party to validate transactions between the peers of the network. To ensure integrity, security, privacy, and reliability of data transmitted over the network, bitcoin uses the technology known as the blockchain. Blockchain acts as a distributed reason book. The information is stored on blocks and validated through a consensus algorithm. The process of validating blocks is called mining. To encourage users to participate in the mining process, users that participate in the mining process receive a reward in cryptocurrency. Due to its characteristics, the blockchain got the attention of the applications developers.

Blockchain proved to be an innovative technology due to its characteristics, which can solve security and privacy issues [9]. It is possible to find blockchain usage in medical environments [10], on IoT scenarios [11] and in industrial environments [12]. The trend of the use of blockchain was not different for the SG scenario. Commercial solutions that use blockchain on SG scenarios already exist. Nowadays, the primary use of this technology consists of electrical energy trade between different consumers. However, different works are attempting to develop blockchain architectures for the SG scenario that guarantee users security and privacy.

With the development of blockchain architectures focused on the SG scenario, various authors propose entirely new solutions that lack the use of existing SG protocols. These solutions are difficult to implement because due to the complexity of adapting them to devices that already exist in SG networks. The use of existing protocols on new blockchain architectures can favor the implementation of this technology in SG networks.

Appendix C

Figure A3 illustrates the Energy Transfer SC. This SC is responsible for validating the energy trade between users. The algorithm is described detailed in Section 4.

```
pragma solidity ^0.5.1;
pragma experimental ABIEncoderV2;
import './Token.sol';
import './Storage.sol';
contract Transfer{
    Token token;
    Storage stor;
    struct EnergyOffer{
        uint energyQuant;
        uint energyValue;
    }
    mapping (address => EnergyOffer) public energyOffers;
    function buyEnergy(address _to, uint _quant) public{
        uint totalCost = energyOffers[_to].energyValue * _quant;
        require(energyOffers[_to].energyQuant >= _quant);
        energyOffers[_to].energyQuant -= _quant;
        token.transfer(_to, totalCost);
        stor.setTransLog(_to, totalCost, "003F00340000000006F52F5481599DF7BCF192C236");
    }
    function sellEnergy(uint _energyQuant, uint _energyValue) public{
        energyOffers[msg.sender].energyQuant = _energyQuant;
        energyOffers[msg.sender].energyValue = _energyValue;
    }
    function setTokenAddress(address _addr) public {
        token = Token(_addr);
    }
    function setStorageAddress(address _addr) public {
        stor = Storage(_addr);
    }
}
```

Figure A3. Energy transfer Contract.

Article

A Cost Analysis of Implementing a Blockchain Architecture in a Smart Grid Scenario Using Sidechains

Iago Sestrem Ochôa [1,2,*], Luis Augusto Silva [1], Gabriel de Mello [1], Juan Francisco de Paz [3], Nuno M. Garcia [4,5] and Valderi Reis Quietinho Leithardt [1,4,6]

1 Laboratory of Embedded and Distributed Systems-LEDS, University of Vale do Itajaí, Itajaí-SC 88302-901, Brazil; luis.silva@edu.univali.br (L.A.S.); gabrieldemello@edu.univali.br (G.d.M.); iago.ochoa@edu.univali.br; valderi.leithardt@ubi.pt (V.R.Q.L.)
2 Departamento de Informática e Redes de Computadores, Instituto Federal Catarinense (IFC), Brusque 88354-300, Brazil
3 Expert Systems and Applications Lab, Faculty of Science, University of Salamanca, Plaza de los Caídos s/n, 37008 Salamanca, Spain; fcofds@usal.es (J.F.d.P.)
4 Departamento de Informática, Universidade da Beira Interior, 6201-001 Covilhã, Portugal; ngarcia@di.ubi.pt
5 Instituto de Telecomunicações, Universidade da Beira Interior, 6201-001 Covilhã, Portugal
6 COPELABS, Universidade Lusófona de Humanidades e Tecnologias, 1749-024 Lisboa, Portugal
* Correspondence: iago.ochoa@edu.univali.br

Abstract: Smart Grid systems have become popular and necessary for the development of a sustainable power grid. These systems use different technologies to provide optimized services to the users of the network. Regarding computing, these systems optimize electrical services by processing a large amount of data generated. However, privacy and security are essential in this kind of system. With a large amount of data generated, it is necessary to protect the privacy of users, because this data may reveal users' personal information. Today, blockchain technology has proven to be an efficient architecture for solving privacy and security problems in different scenarios. Over the years, different blockchain platforms have emerged, attempting to solve specific problems in different areas. However, the use of different platforms fragmented the market, which was no different in the smart grid scenario. This work proposes a blockchain architecture that uses sidechains to make the system scalable and adaptable. We used three blockchains to ensure privacy, security, and trust in the system. To universalize the proposed solution, we used the OSGP protocol and smart contracts. The results show that architecture security and privacy are guaranteed, making it feasible for implementation in real systems. Although scalability issues regarding the storage of data generated still exists.

Keywords: blockchain; sidechain; smart grid

1. Introduction

Smart Grid (SG) is a large-scale electrical network infrastructure mainly characterized by security, agility, and resilience, capable of handling new threats and unforeseen conditions. In 2005, the authors introduced this concept in [1], known as smart electrical networks. The agents that act on these networks can communicate and cooperate in a self-configuring mode, considering that a new element can join the network, or a random event can cause a requirement for correction. Although SG networks ensure efficiency in electrical systems, problems still exist for its implementation to be efficient in a holistic way.

According to [2], one of the problems to be solved for the implementation of SG networks is the privacy issue. The work developed in [3] states that, in general, data privacy affects the security of who

In addition to supporting social welfare and philanthropy, Jackson believes Dogecoin can be used on the Internet as a "sweet spot" to thank others. In the beginning, though, Dogecoin was born out of a joke.
The founders say Dogecoin is not like Bitcoin, where people don't get involved for speculation, but to express feelings of sharing and concern. This also created that at the beginning of the dogecoin transmission channels are based on people-to-people sharing.
Restaurants in Maryland accept e-money dogecoin, MyFoxDC reported. Iron Rail Restaurant in Mount Savage, Maryland, officially accepts Dogecoin. Owner Terry Ii says the use of dogecoin has benefited restaurants, including the need not to pay for credit cards.
According to the records, the initial price of GRAM is $0.10. The circulation cost of the new GRAM will be $1 billion higher than the original.
According to reports, Dogecoin (DOGE) is a cryptocurrencies dedicated to the real practical value of money. With faster block intervals and extremely low rates, Dogecoin is better suited for small payments and online shopping. Dogecoin has been used by multiple merchants, allowing consumers to easily transfer money using DOGE.
Verge was originally created in 2014 under the name Dogecoin. It changed its name to Verge in 2016, but that doesn't change the fact that it's a dog coin fork. Dogecoin also became a branch of Litecoin, a well-known bitcoin.
the discounted price to buy back ALGO. If the investor trades for less than $1, the Algorand Foundation will buy back at less than $0.10.
The leading exchange in China, supports Bitcoin, Litecoin, Dogecoin.
Me: Hey, did you know that okcoin has plans to join dogecoin in the near future? I fully understand that if you don't want to discuss this, but I think I should ask: dogecoin has a very large user base and a very different population than Bitcoin and Litecoin. This will help attract new customers as well as a large volume.
Fire Coin has announced that it will list three trading pairs for Dogecoin: DOGE/BTC, DOGE/ETH, and DOGE/USDT.
7 day down 0.10%, the loss decreased;
Mars Finance APP (WeChat: hxcj24h) first-line reports, October 24, according to the official announcement, Binance.US announced that it will be launched on October 25 at 9:00 Dogecoin, dogecoin, the opening of the DOGE dollar pair, and said that the official opening of deposit channels.
On the one hand, F2Pool mines Dogecoin through merge mining and distributes Dogecoin to Wright miners to increase mining revenue. With the addition of Dogecoin, miners digging Litecoin

in the fish pond are basically equal to 0 fee. On the other hand, it is also thinking about whether there are other coins to mine the Litecoin mining machine in the hands of miners. F2Pool is currently online currency, there is a DGB (scrypt algorithm), which can be mined with Litecoin miners. Before the halving, DGB mining revenue may be 80% of Litecoin, but after the halving, it is quite 1.6 times that of Litecoin, which is relatively attractive and can help Litecoin miners through a relatively difficult time

But Bitcoin is too expensive, so cheaper Dogecoin is popular. Just a week after it went online, it became the second-largest tip currency. They're hoping that Facebook will accept Dogecoin so that your friends can not only like it, but also tip you by the way.

The founders say Dogecoin is not like Bitcoin, where people don't get involved for speculation, but to express feelings of sharing and concern. This also created that at the beginning of the dogecoin spread by people to share.

Decred, Dogecoin, Litecoin: Failed attempt to break up.

The Dogecoin community is responsible for the creation of the Dogecoin Foundation, a non-profit organization that promotes the use of Dogecoin through goodwill and charitable activities. These activities included a $30,000 DOGE donation to the Jamaican bobsleigh team at the 2014 Winter Olympics and an additional $30,000 to Kenya's Clean Water Initiative.

Dogecoin, first mined on December 6, 2013. It's worth $0.000328.

In a word: Dogecoin is a cryptocurrencies dedicated to the true practical value of money in English: Dogecoin English abbreviation: DOGEChinese Name: Dog Coin Project Introduction: Dogecoin has faster block spacing and very low rates, making Do.

It will go online on July 25 with an opening price of $0.10, according to the Singapore BOSS Exchange. The platform will airdrops 10,000 OSS pieces to new users.

We note that due to the use of splits and side chains, high volumes can be supported in a short period of time. This fact stems from the idea that if a user buys Dogecoin using Litecoin (within the framework of the world), the transaction will only communicate between the Dogecoin and Litecoin sidechains without affecting performance, such as Bitcoin or Ethernet sidechains.

Then the number of positions becomes 5000 x 51122 x 0.10, that is, you can only buy 0.10 bitcoins, and these bitcoins according to august 31 BTC market value of 0.10 x 47540 x 4754 yuan, a loss of 246 yuan.

Dogecoin features price charts, via TradeView.

Jackson Palmer, co-founder of Dogecoin, advises MOBIUS.

each function. The setStorageAddress() function sends the data to the storage contract to store the transaction information on BlockSEC.

Figure 5 illustrates the operation of the proposed architecture in different situations. The illustrated scenario consists of the integration of different SG zones and the connection of different environments through the proposed architecture. To exemplify the use of the architecture, different application scenarios are used, such as privacy preference register (i), energy trade (ii), and monitoring (iii).

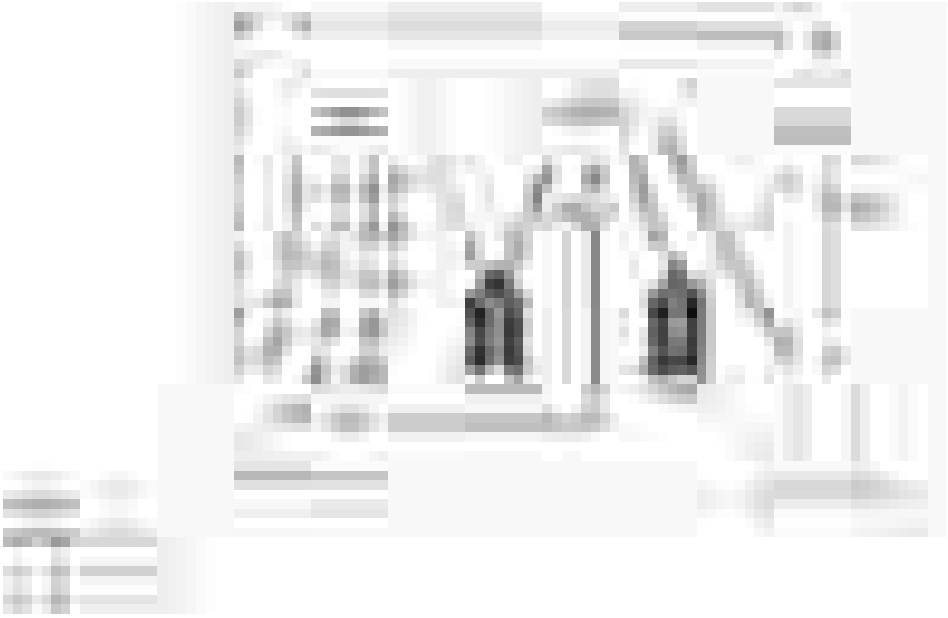

Figure 5. Application Scenario.

In situation (i), a user registers his SM in the system through an UI. The systems registers a wallet address for each SM. At this moment, the user sets his privacy preferences. The privacy preference information is registered on the PPC and stored in BlockPRI. Only the contract owner can change privacy preferences defined. Figure 6 illustrates this process.

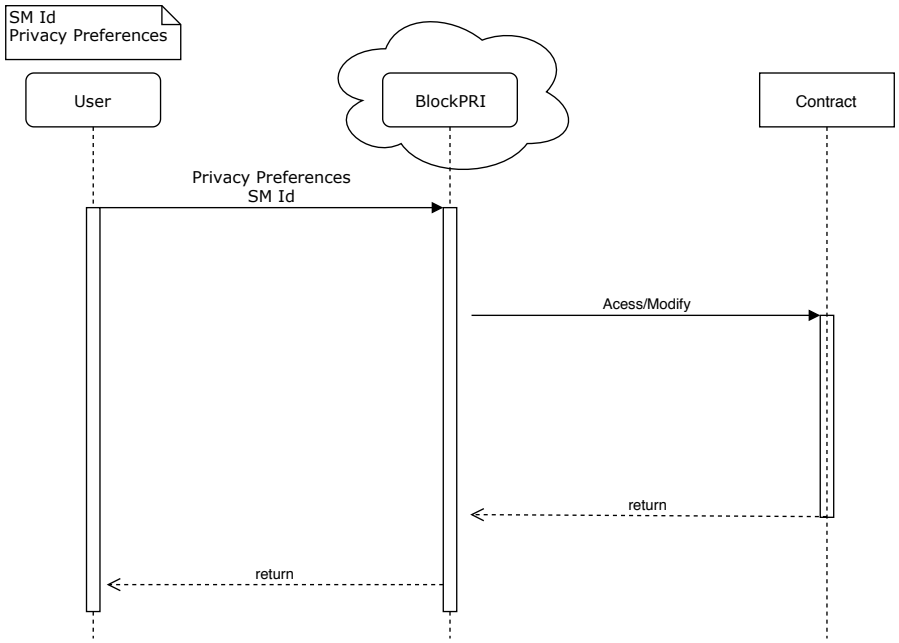

Figure 6. Privacy preferences registering.

To solve the problems previously presented, in this article, we propose a blockchain architecture focused on the SG scenario that uses sidechain. Our architecture uses the OSGP protocol integrated into three different blockchains, proposing to guarantee privacy and security in SG networks holistically. Our architecture allows users to define their privacy preferences in a tamper-proof way, using a privacy blockchain. The access to the information of each user by the electric company is stored in storage blockchain to ensure the reliability of the system. In this way, users and companies benefit from the use of this type of architecture.

The principal contribution of this article is on the definition of a blockchain architecture that uses a protocol widely used in the SG scenario, supporting the implementation of this architecture on existing systems. Regarding the functionalities of our architecture, it provides security, reliability, and privacy for users through the use of different blockchains. Our architecture also provides scalability for SG applications, implementing the architecture in a sidechain concept, specifically designed to enable large-scale application development using the OSGP protocol.

The paper is structured as follows. Section 2 presents the background with the fundamental concepts to understand this work. Section 3 shows the related works. Section 4 exhibits the methodology used in the development of the proposed architecture and the details of our architecture. Section 5 illustrates the results obtained through the tests developed. Finally, section 6 shows the conclusions obtained with the development of this work.

2. Background

In this section are presented the fundamental concepts to understand our architecture. In Section 2.1 we present the SG concept focusing on security and privacy issues. We also show the blockchain concept as a solution to security and privacy problems in section 2.2. In Section 2.3 we outline the advantages of using the Ethereum blockchain in application development, the concept of sidechain, and how it can revolutionize blockchain technology.

2.1. Smart Grid

According to [13], an SG system is the integration of information technology with the generation, transmission, and distribution systems of electrical energy. It is possible to describe four characteristics of an SG system: (i) Increase efficiency and profitability of the system. (ii) Supply tools for the consumer to manage energy use. (iii) Optimization of the resilience and quality of energy of the system. (iv) Development of new technologies such as renewable energy generation (solar, wind, and others), storage of energy (batteries), and electric vehicles.

One of the critical features in an SG network is that consumers also become producers (or prosumers); this happens because they can produce renewable energy in their houses through alternative sources. Analyzing this from an extended perspective, they acquire the responsibility of generating electricity with the same quality of traditional generation sources. According to the essential characteristics of the SG networks before mentioned, with decentralized prosumers, three of these characteristics are guaranteed [14].

To ensure efficient management of energy usage, SG networks need to allow the prosumers to perform real-time monitoring of electricity consumption and generation. In this way, they can choose to store or sell the energy excess produced for other SG network users. SG networks require the development of communication infrastructures that support the growth and density of the system, guaranteeing the quality of service necessary for the operation for large scale applications.

The Smart Meter (SM) is the critical part of an SG network. An SM is responsible for collect, process, and manage the information obtained about the electrical usage on a residence. They are also responsible for collecting data from the electricity grid. The functionalities of an SM are various, these functionalities are intended to provide the consumer a wide range of information such as, the amount of energy consumed in real-time, amount of energy used in the last hour, week and month (and how

in the transaction cheaper. The first is high supply and low demand, denoting excess production. The second is the importance of monitoring when in an exchange with a dealership. In Situation 2, when dealing specifically with this aspect, there is no difference in price, since the privacy options are disabled, but in Situation 4, having the options enabled made it even possible to cheap the transaction.

Table 3. Token Cost in Different Situations

	Demand	Generation	Privacy Preferences	Trade Type	Energy Ammount	Price (SGT)
Situation 1	75	25	Disabled	CP	50	30
Situation 2	25	75	Disabled	CC	50	20
Situation 3	75	25	Enabled	CP	50	30
Situation 4	25	75	Enabled	CC	50	10

5.3. Smart Contract Cost

Table 4 shows the deploy cost of each contract developed. We used the Ropsten TestNet to evaluate all contracts. The Storage contract, which is responsible for storing information, which is the most expensive functionality in a blockchain, had the highest cost in ETH. The other contracts have a lower cost because the functions used in each of them do not have the main purpose of storing data, but access control.

Table 4. Deploy Cost by Contract

Contract	Cost (ETH)
Access	0.001413
Storage	0.003389
Transfer	0.001417
Token	0.001862

In Table 5, we show the relationship of a function to its contract and the cost of operation. As can be seen, the predominance of the most expensive ones is almost entirely from Storage class functions, since they are blockchain write operations (even getters, since the use of functions results in saving the corresponding get-log operation to the address). Transfer functions also had some cost, even if less excessive.

Table 5. Function Cost

Function	Contract	Cost (ETH)
setTranslog	Storage	0.000821
buyEnergy	Transfer	0.000536
getEnergyUsage	Storage	0.000519
getTranslog	Storage	0.000447
sellEnergy	Transfer	0.000452

5.4. Privacy violation test

In Figure 10 we demonstrate, by the console, the result of an attempt of unauthorized access to the data stored in the storage. First, we define an address as being an electrical company to try to access. Then, another address is registered and stored on BlockPRI, with the distributor mode disabled, as well as the settings that allow access to data stored in the blockchain. Finally, we had the distributor address try to access the historical data of the consumer who chose to protect himself. The result of the

Appendix B

Figure A2 illustrates the Storage SC. This contract is responsible for check the preferences stored in PPC and perform an action based on these preferences. The algorithm is described detailed in Section 4.

```
pragma solidity ^0.5.1;
pragma experimental ABIEncoderV2;
import "./Access.sol";
contract Storage {
    Access access;
    struct AccessLog {
        address accessOrigin;
        uint accessTime;
        uint accessDay;
    }
    struct TransactionLog {
        address transDest;
        uint transValue;
        string transCode;
    }
    struct EnergyUsage {
        uint usageDay;
        uint usageQuant;
    }
    struct ConsumerInfo {
        AccessLog[] accessLog;
        TransactionLog[] transLog;
        EnergyUsage[] energyUsage;
        uint currentEneryUsage;
    }
    mapping (address => ConsumerInfo) public consumerInfos;
    function setAddress(address _addr) public{
        access = Access(_addr);
    }
    function setTransLog(address _transDest, uint _transValue, string memory _transCode) public{
        consumerInfos[msg.sender].transLog.push(TransactionLog(_transDest, _transValue, _transCode));
    }
    function getTransLog(address _consumerAddr) public returns (TransactionLog[] memory){
        require(access.getConsumerPrefs(msg.sender).isDistributor == true);
        require(access.getConsumerPrefs(_consumerAddr).canMonitorTransf == true);
        consumerInfos[_consumerAddr].accessLog.push(AccessLog(msg.sender, 0, 0));
        return consumerInfos[_consumerAddr].transLog;
    }
    function getEnergyUsage(address _consumerAddr) public returns (EnergyUsage[] memory){
        require(access.getConsumerPrefs(msg.sender).isDistributor == true);
        require(access.getConsumerPrefs(_consumerAddr).canMonitorCons == true);
        consumerInfos[_consumerAddr].accessLog.push(AccessLog(msg.sender, 0, 0));
        return consumerInfos[_consumerAddr].energyUsage;
    }
    function getCurrentEnergyUsage(address _consumerAddr) public returns (uint){
        require(access.getConsumerPrefs(msg.sender).isDistributor == true);
        consumerInfos[_consumerAddr].accessLog.push(AccessLog(msg.sender, 0, 0));
        return consumerInfos[_consumerAddr].currentEneryUsage;
    }
}
```

Figure A2. Storage Contract.