IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 29, 2020, accepted July 9, 2020, date of publication July 15, 2020, date of current version July 29, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3009356

A Design for a Secure Energy Market Trading System in a National Wholesale Electricity Market

AKLILU DANIEL TESFAMICAEL[1], VICKY LIU[1], MATTHEW MCKAGUE[1], WILLIAM CAELLI[1], AND ERNEST FOO[2], (Member, IEEE)

[1]School of Computer Science, Queensland University of Technology, Brisbane, QLD 4000, Australia
[2]School of Information and Communication Technology, Griffith University, Brisbane, QLD 4111, Australia

Corresponding author: Aklilu Daniel Tesfamicael (aki.tesfamicael@hdr.qut.edu.au)

ABSTRACT Energy market trading systems are undergoing rapid transformation due to an increasing demand for renewable energy sources to be integrated into the power grid, coupled with the dynamic and evolving needs of future energy customers. In the current energy trading system, which is based on mega power generation, energy is traded by insecure means of communication based on mutual trust. In addition, electricity from both renewable and non-renewable sources is mixed in the grid, impeding customers' ability to definitively track the source of energy dispatched to their premises. Although blockchain technology has been studied for energy trading on a peer-to-peer microgrid trading, to our knowledge none of the previous work focused on using blockchain for trading energy in a national wholesale energy market in macrogrid. In this paper, we address security architectures required of the energy market trading system in an Australian context, we propose a cryptocurrency token-based structure and a smart contract that provides data confidentiality that verifies and audits transactional records. The proposed trading system architecture not only enhances overall system security but provides additional capabilities in the operation of the scheme so that sources of energy dispatched to customer premises are known. The energy market trading system we propose also presents higher security compared to existing trading systems.

INDEX TERMS Data security, distributed computing, power systems security.

I. INTRODUCTION

Market trading systems are used by energy generators, retailers and brokers to buy and sell electricity in the national wholesale electricity market. Currently, energy market trading systems are undergoing rapid change because of the continuing injection of renewable and non-renewable sources of energy into the macrogrid. A further factor concerns security of the increasing volumes of transactional data being generated. As more data are collected from the various market participants, it is imperative to provide data security because a data breach could have implications for national energy security.

In the Australian context, the Australian Energy Market Operator (AEMO) operates alongside Australia Energy Regulators (AER) and the Australian Energy Market Commission (AEMC). The AEMO predicts electricity demand nationwide and schedules electricity generators to meet that demand. Through a physical (spot) trading market the AEMO facilitates an agreement to buy and sell a fixed amount of electricity that is traded for immediate use. Through a contract trading market, generators can also make an agreement with customers or brokers (without AEMO involvement) that is traded on a longer-term engagement. Once the agreement is made by either of these trading markets, electricity is provisioned to customers through the macrogrid network nationwide.

This research focus is on macrogrid rather than the microgrid peer-to-peer energy trading. The difference between microgrid and macrogrid is that, microgrid is a group of decentralized (localized) energy micro generators that act as a single controllable or integrated entity with respect to the grid. However, macrogrid is the traditional centralized grid where large generators (power plants) dispatch electricity through a national power transmission and distribution network. Decentralized power generators in a microgrid mainly focus on the local energy needs. They generate electricity in

The associate editor coordinating the review of this manuscript and approving it for publication was Zhiyi Li.

a small scale where prosumers (producers/consumers), small businesses or communities generate electricity to meet their energy demand. They function either by being integrated to the grid, feeding the surplus energy generated, or in an isolated stand-alone situation. However, the centralized power generators, which mostly operate on fossil fuels, are integrated to the grid system dispatching electricity nationwide. Centralized power generators require a substantial investment in the plant operation and infrastructure setup, such as a complex power transmission and distribution network as well as power trading systems and operations. Electricity generated from the power generators is provisioned to customers through the transmission and distribution networks. The transmission network transfers power from power generation facilities to large electric load centers (substations) and interconnects states nationwide, while the distribution network takes power from the substations and dispatches it to customers. All electricity sales generated through the mega generators are traded through the national electricity market (NEM), which involves generators and retailers (through the AEMO), entering into contract to sell and buy energy through the transmission and distribution network in the macrogrid.

The energy market data transactions that trigger the provision of electricity from power generators to customers are not protected in the current trading system. There is no technological solution provided for data confidentiality and integrity. Energy market participants trade energy using insecure means of communication. Sometimes this is done by voice over the phone, by Microsoft Office Excel®based spreadsheet or through an instant messaging system. These are time-consuming processes and are open to human error that may result a breach of market data confidentiality, intentionally or unintentionally. For example, traders should not see each other's bid until it becomes public. Their bids should be kept confidential from each other and the public until all pre-dispatch market information relevant to a specific trading day becomes available to the general public, usually after the end of the trading day. Any breach of such market data confidentiality could have national security implications. As such, it is evident that guarding against improper information modification or destruction is of vital concern. Ensuring information non-repudiation and authenticity are key concerns in electricity generation and trading.

The objective of this research is to address the aforementioned challenges so that data collected for the use of electricity trade in the national electricity wholesale market are protected. Electricity trade in a wholesale market in the macrogrid is a more complex scheme than that of peer-to-peer energy trading in microgrid due to involving:

1) Different types of trading scheme in terms of spot and contract trading for mega power generation macrogrid energy trading.
2) The complexity of a mega power generation macrogrid trading scheme as it involves various stakeholders including energy generators, regulators, energy traders, wholesalers, retailers, brokers and customers.
3) The existence of operational dispatch and a five-minute settlement rule, in particular, for mega power generation macrogrid trading.
4) The electricity supply from mega power generation macrogrid includes non-renewable sources (coal or gas) and renewable sources (wind, solar or hydro). Mostly micro generation microgrids are based on rooftop solar power systems, which operate in a peer-to-peer trading scheme between prosumers and customers.

A. SCOPE OF RESEARCH PROJECT

The scope of this research is focused on providing security for transactional energy data when electricity in transmitted from generators to customers through the distribution and transmission network in a macrogrid. The ability of customers to access transactional energy data about the type and amount of energy dispatched to their premises is also within the scope of this research. These are the principal goals of this project. This project assumes that the types and amounts of energy the generators actually put into the overall system are accurate. Thus, the only focus of this research is the provision of data security when electricity is delivered to customers through the distribution and transmission network (rather than on energy generation). The architecture for enhanced availability and reliability of the energy market trading system in the macrogrid itself is outside scope of this paper.

To achieve the required result, this research uses the application of blockchain, such as a cryptocurrency token-based structure, and a smart contract as methods to address the transactional energy data security of such a system. A smart contract is capable of self-executing and enforcing a contract with terms of agreement between market participants to automatically fulfill the terms of the agreement once conditions are met, without the need for intermediaries. For instance, in the case of physical energy market trading, a smart contract can be used between generators and retailers and between retailers and customers. It can also be used between generators and customers in the case of contract energy market trading. The term 'digital token' is used in this paper for convenience. However, in this context the so-called token needs to be regarded as simply a transaction token and not as equivalent to conventional money.

The main purpose of this project is to design a framework for the trading system so that transactional data are auditable, verifiable and trackable when needed after the trading period is complete. This proposed system does not require real-time processing of high-volume data.

B. RESEARCH QUESTIONS AND CONTRIBUTION

The research questions investigated and reported upon in this paper may be stated as follows:

1) The current energy market trading scheme is based on mutual human trust. Without that, how do we build tamper-resistant security provisions into the trading system which are auditable and verifiable?

2) How can customers (energy consumers) be able to trace what percent of energy dispatched to their premises is, for example, from renewable sources?

The contribution of this paper is based on proposals for a secure mechanism enabling mutual trust in the system (a technological solution which is auditable and verifiable), rather than being based on human trust when trading energy through insecure means of trading systems or communications. In a fully trusted third-party (TTP) model, the AEMO would have access to all transactional data, and also have control. In our system we are removing some of the responsibilities regarding the audit of sales and payment mechanisms from the AEMO and transferring that responsibility instead to secure cryptocurrency schemes with the support of smart contracts that are capable of self-executing and enforcing a contract. This means that all market participants trading in the macrogrid can still fulfil their roles, as they currently do.

The key requirements of an energy market trading system, that this research project is based upon, are as follows:

1) Energy market trading system must provide confidentiality and integrity for energy trading. This is to sustain continued energy supply and sales. For example, all pre-dispatch energy market data relevant to a specific trading day must not be available to the general public before the end of that trading day.
2) Energy sources must be tracked during energy generation and energy dispatch so that renewable energies are separately identified from non-renewables.
3) Customers should have access to energy data transaction details so that the type of energy provisioned to their premises is known.

To address the above-mentioned challenges and key requirements, this paper provides a comprehensive review of the existing energy market trading system process and its security requirements in the Australian context, and makes the following contributions:

1) The application of blockchain and authentication mechanisms is proposed to protect transactional energy market data and maintain the confidentiality and integrity of information.
2) A new energy market trading system architecture is proposed which enables the tracking and monitoring of sources of energy (renewable versus non-renewable energy).

Through these contributions the proposed system is capable of providing and maintaining accurate energy related transactional data to support strategic planning and decision making at a national level. It also enables the tracking of customer energy consumption at different times of the day to help energy demand and supply management as well as pricing plans.

The importance of tracking sources of renewable energy in this paper has three objectives:

1) From the regulator's point of view (at the national level), governments wish to note and promote the development of renewable energy and be able to track progress towards achieving their renewable energy target.
2) From the consumers' point of view, customers have the option to purchase renewable electricity directly from their power supplier rather than installing solar panels on their own premises. Some customers are also looking for more sustainable energy options by sourcing their electricity from renewables. So, it is essential to demonstrate that their energy is indeed coming from their stipulated source.
3) From organizations' perspective, companies or organizations who embrace (wish to promote) renewable energy need to certify the proportion of their electricity that is being sources from renewables.

This research is based around the growing acknowledgement that such a trading system is an essential part of the national critical infrastructure involving reliable electricity transmission and distribution. Moreover, cybersecurity, crucial to national security, itself has become an essential protection paradigm for such a trading system.

The target audience for this research includes academic researchers as well as government, regulatory bodies, and energy market participants.

C. PAPER STRUCTURE

The remaining sections of the paper are organized as follows. Section II presents the security requirements of the energy market trading system, whilst Section III discusses related work. In Section IV we look at the current Australian energy market followed by section V which discusses the system design of our proposed energy market trading system. Section VI demonstrates the simulation design, followed by system design analysis in Section VII. Conclusions are outlined in section VIII.

II. ENERGY MARKET TRADING SYSTEM SECURITY REQUIREMENTS

In the energy sector, information is gathered from a variety of sources, such as information generated from the physical flow of electricity, information that the network traffic carries about sensors, smart readers, customers and other information that is recorded and stored for trading, compliance, auditing and monitoring purposes.

The key security requirements the energy market trading system must have are:

1) Confidentiality
   All energy market data related to sensitive or confidential institutional trading information must be protected from unauthorized disclosure. Unauthorized access to organizational data may result in a significant financial risk or loss.
2) Authentication
   The identity of the market participants must be verified before they start to trade energy in order to protect from impersonation attacks.

3) Integrity
Transactional energy market data must not be tampered with while information is passed and communicated between market participants during the trading period.

Information for energy sectors should not be modified without authorization and the source of information should be authenticated and time stamped. It is a requirement for the energy market trading system to ensure that only authorized market participants have access to accurate and complete market information when required. Information sharing should be restricted between market participants through various levels of security based on their function (role). If the security of information is compromised, incorrect information can be sent to the energy market. Accordingly, this can cause market instability, which ultimately affects the energy trade. The integrity of a trading system could have national security implications. As such, it is evident that guarding against improper information modification or destruction is of vital concern. Ensuring information non-repudiation and authenticity are key concerns in electricity generation and trading.

Having a secure energy market trading system could enable accurate energy prediction and pricing in real-time, as accurate information is passed and communicated between all market participants.

In this research, we assume that the physical protection of critical infrastructure such as process control systems and trading systems is already there. We assume that the generators and the market operators (such as the AEMO) have obligations to provide physical security for critical infrastructure. What we have provided is a mechanism that allows market participants to trade energy in a secure manner which is not usually provided by physical infrastructure security alone. This will be discussed in more detail in section V. Our security requirements take into consideration the above assumptions.

III. RELATED WORK

Providing a secure energy market trading system is what is required for energy generators, energy market regulators and customers, to buy and sell electricity in the energy market. As discussed above, security has become a major challenge in the existing trading system. The primary purpose of this review is to ascertain if there is compelling evidence that efforts exist towards the deployment of security mechanisms for mega power generation macrogrid energy trading. The scope of this review is limited to the application of distributed blockchain technology in the area of security for the energy market trade. Application of blockchain schemes in the areas of grid management, carbon credits tracking, energy storage, solar energy trading and electric vehicle charging are outside the scope of this review.

In recent years, the study of blockchain application in the energy sector has gained increasing interest both in academia and industry. Several articles have been published that discuss and review blockchain based energy trading focusing on peer-to-peer solar energy trading, renewable energy certificates (REC), grid management, carbon credits tracking, energy storage, etc. Recently 140 blockchain focused papers have been reviewed on the application of blockchains to the energy sector [1]. Part of this research outcome was to map the potential and relevance of blockchain applications in some areas of the energy sector. The authors further looked at the opportunities, challenges and limitations of blockchain technology in a number of cases, including peer-to-peer energy trading, electric vehicle charging, decentralized energy market, etc. These provide a step forward in identifying the areas where blockchain can be applied. However, there is more investigative work required in order to demonstrate any real benefits of blockchain technology in the energy sector.

Authors in [2] also used blockchain technology to address the security issues of energy trade in a smart grid. They have developed a token-based energy trading system called PriWatt. Through this system, the authors claim to be able to trade energy securely in a smart grid on a peer-to-peer network. A case study was used to provide evidence for their research in measuring the performance and security of the system. To reach a consensus in such a system they applied a proof-of-work (PoW) mechanism. Multi-signature and anonymous encrypted messaging structures have also been used. In a similar concept, authors in [3] studied the privacy of users in smart grid throughout the billing process and reporting of energy transactions. Other literature [4]–[7] claims to provide security and privacy solutions for a smart grid through different mechanisms: using an authenticated method of anonymous meter reading, the use of homomorphic encryption to secure data in transit and the use of privacy crypto transaction proofs called zero-knowledge to prove the fee of the electrical meter is correct without revealing other transactional data of the customer. The focus of all the aforementioned publications is on localized grids (microgrids), which are different from our research. Our research focus is on mega power generation energy market trading, such as a macrogrid. Trading on macrogrid generation is complex as it involves different types of trading schemes.

As to the research on application of blockchain based cryptocurrency in the energy sector, there are a number of researchers leaning towards privacy. Since the introduction of ''Bitcoin'' in 2008 [7] numerous cryptocurrencies studies exist. One of them that is believed to have stronger privacy and anonymity guarantees is Zcash [8] and [13]. It uses zero-knowledge proofs to allow validity of a transaction without revealing any other information beyond validating identity. Zcash enables optional privacy features for transactions so that sender and receiver addresses, and the amount of money transacted, are private. The addresses beginning with a ''t'' (t-addrs) are considered transparent and are like bitcoin transactions. ''Shielded'' transactions are used with addresses beginning with a ''z'' (z-addrs), and these are fully anonymous. Zcash has been further studied in [8] and demonstrated its privacy and anonymity features. It has been suggested that Zcash provides strong anonymity and privacy for users that

want to transact digital coins privately. On the other hand, authors in [40] studied the necessary properties and security requirements of Ring Confidential Transaction (RingCT) for Monero that achieves anonymity on all three facets of its transactions through ring signatures, stealth addresses, and RingCT. Though Zcash and Moreno have been studied by many scholars separately, no study has been conducted to evidence their integration with the Ethereum blockchain to provide privacy to Ethereum's smart contract. They do not provide smart contracts by themselves either. In most well-known smart contracts, such as Ethereum, privacy is not preserved by themselves, the sender and recipient of each transaction and its data are public, making it easy for competitors to see each other's financial and confidential data. However, there are other protocols, anonymous zero-knowledge transactions efficient communication (AZTEC) and Zether, that are studied by authors in [37], [38] that can be used as a plug-in solution to the Ethereum blockchain to preserve privacy and anonymity for Ethereum's smart contract. Authors in [39] also demonstrated when AZTEC protocol is used with Ethereum's smart contract then Ethereum's public ERC-20 token converts into a confidential AZTEC note form to preserve its privacy.

There are also a number of papers [9]–[15] with studies on privacy and anonymity, such as Zerocash and Zerocoin digital coin cryptocurrencies that aim at addressing the privacy weakness of Bitcoin. Other digital coins [16]–[22] have also been explored and demonstrated to provide better privacy and anonymity properties compared to Bitcoin.

Recent work in [23] and [24] introduced the concept of NRGcoin, a digital currency for renewable energy trading based on the concept of a decentralized blockchain application. Their experiment is based on a peer-to-peer trading concept that prosumers (people with rooftop solar panels) inject solar energy to a grid and trade using a digital coin. The smart meter counts one NRGcoin for every 1-kilowatt hour (KWh) of renewable energy the prosumer solar system injects into the grid. In a similar manner, authors in [27] extended a recently developed trading workflow called PETra and proposed a design solution that addresses the anonymity of the transactions both on the network communication and distributed ledger layers. PETra uses digital tokens representing the quantity of energy generation and consumption. They used a similar concept to that of Zcash. Once information is processed by the blockchain network, prosumers can trade by hiding their identity using anonymized addresses.

In regard to authentication, there are numerous publications that focus on certificate-based authentication for user verification. In [28] the authors propose a new public key cryptography infrastructure (PKI) called Certcoin that leverages the consistency offered by blockchain-based cryptocurrencies. They have demonstrated that this new PKI provides a stronger identity retention guarantee than any PKI's used in practice. However, this concept lacks experimental results to verify its practical application in a real-world scenario.

TABLE 1. Distribution of energy market terms and participants.

Stakeholders	Description
Australian Energy Market Commission (AEMC)	The AEMC sets rules for Australian electricity marketing.
Australian Energy Market Operator (AEMO)	The AEMO predicts electricity demand nationwide and schedule for electricity generators to meet that demand. The AEMO operates alongside the Australia Energy Regulator (AER) and the Australian Energy Market Commission (AEMC).
Australian Energy Regulator (AER)	The AER enforces compliance with the national electricity laws and rules.
Brokers	Brokers help customers and businesses to attain the best deal for their electricity needs from the generators.
Contract Traders	Traders who sell a fixed amount of electricity at a more stable price to secure required levels of volume on a longer-term basis.
Customers	Customers purchase electricity supplied by generators through a transmission network.
Exchange traded futures	Electricity traded on registered exchanges.
Generators	Owners of a power plant that generate and sell electricity to retailers, brokers or directly to customers.
National Electricity Market (NEM)	The NEM is an interconnected electric system in the wholesale market through which generators and retailers trade electricity.
Network Service Providers (NSP)	Entities who own, operate, or control electricity transmission networks.
Physical (spot) Traders	Traders who sell electricity supplied to the market for short-term trades.
Retailers	Retailers buy wholesale electricity from generators and sell to residential, commercial and industrial customers.

Most recent research [28]–[36] has also focused on the distributed PKI solution using blockchain, but has not practically assessed the performance impact of this application to the real-time requirement of energy trading. However, much successful work has been done on decentralized PKI's in other areas where real-time is not a requirement.

At the time of writing this paper, we have not found any papers that primarily focus on security in the energy trading system for a mega power generation macrogrid scheme. Most of the research we identified on the energy sector was on distributed blockchain applications in a peer-to-peer energy trading scheme. This is in a localized microgrid energy generation system between prosumers and customers. However, this research focus is to build security systems for the market participants in mega power generation energy market trading that involves complex trading scheme.

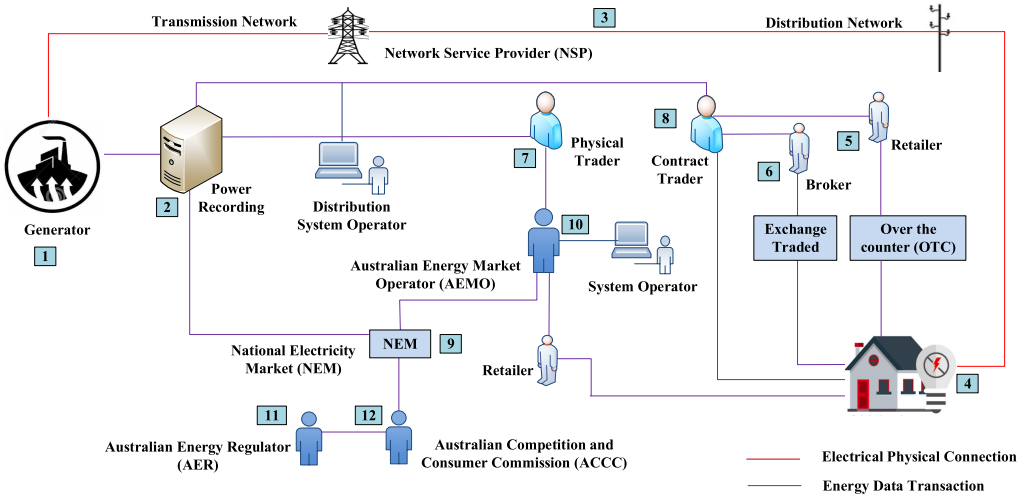

FIGURE 1. Energy market participants relationship.

IV. AN OVERVIEW OF CURRENT AUSTRALIAN ENERGY MARKET

The Australian energy sector has operated for more than 100 years, but it is just in the last 20 years that the industry has started to reform [42]. Most of the restructuring consists of reorganization of the electricity market and formalization of electricity industry regulation. Historically, the electricity sector was dominated by coal-fired power stations, but in recent years renewables are growing at a rapid pace. Presently, Australia generates 91 per cent of its electricity from burning fossil fuels, of which 75 per cent is from coal and 16 per cent from natural gas. Only nine per cent of electricity is generated through renewables [43]. Renewables are those energy sources coming mainly from hydropower, wind, bioenergy and solar.

With the current energy market trading system, it is difficult to track the source of energy supplied to the customers to determine the percentage of renewables energy. This is due to a lack of an automated process to monitor transactional energy data during generation, transmission and distribution of electricity in real-time. For instance, having an automated process on tracking sources of energy could help envisaging the progress of Australia's Renewable Energy Target (RET). RET is a Federal Government policy designed to ensure that at least 33,000 gigawatt-hours (GWh) of Australia's electricity comes from renewable sources by 2020 [41].

A. DESCRIPTION OF ENERGY MARKET TERMS AND PARTICIPANTS

Energy market participants include generators, traders, retailers, brokers, customers and those involved in the regulatory and operational administration of the energy market. The market participants enter into contracts, including the placing of orders to trade, in one or more wholesale energy markets.

The electricity industry has many terms, abbreviations and acronyms used for generation, transmission, distribution and energy trade. Table 1 defines some of the terminology used in this paper.

Energy market participants relations is shown in Fig. 1, where electricity is generated (1) and recorded (2) at the power station and transported over long distances (3) through high and low voltage power lines before being distributed to customers (4). The retailers (5) and/or brokers (6) through the physical (7) and contract (8) market buy electricity at a wholesale price on the NEM (9) and sell it to customers. This wholesale and retail energy market is operated by AEMO (10) and regulated by AER (11). The role of the ACCC (12) is to enforce competition between energy market participants.

B. ENERGY MARKET TYPES AND PARTICIPANTS

The Australian wholesale electricity market, the NEM, is where generators sell electricity and retailers buy electricity. Retailers, who buy wholesale energy from generators then resell electricity to businesses and customers (households). Brokers provide competitive wholesale market brokerage services as they have market experience and access to generators.

In the Australian energy market, generators make energy offers to supply, and these are dispatched on a rolling five-minute dispatch interval basis while financial settlements (and the spot price) are based on a 30-minute trading interval.

Participants in national electricity market engage in energy trade through physical (spot) market trading and/or contract market trading. Generators, aside from the spot trading, sell a volume of energy through the contract markets. The retailers buy wholesale energy from the generators or through the broker and sell to residential, commercial and industrial customers. Fig. 2 shows the relationship between physical and contract energy trading markets.

1) PHYSICAL (SPOT) TRADING MARKET

In the physical trading market, traders sell energy on a day to day short-term basis as part of a process regulated by AEMO. Traders submit their bids in the NEM.

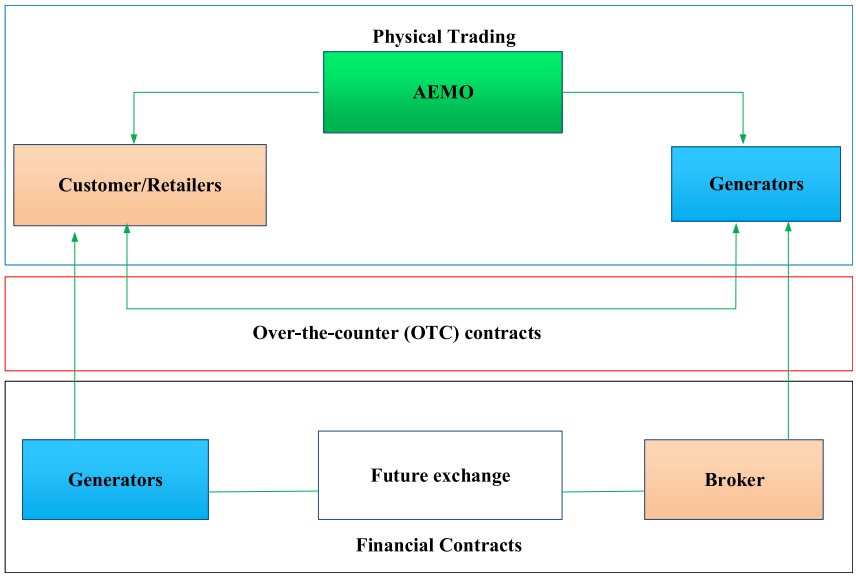

FIGURE 2. Current physical and contract trading market overview.

Fig. 3 shows interactions of key players in a physical (spot) market. In the physical (spot) market:

1) AEMO/retailers forecast the demand of electricity on how much energy to buy. Electricity demand is measured by metering supply to the network.
2) AEMO confirms supply of energy to retailers.
3) AEMO requests supply of energy from generators.
4) Generators (spot traders) are required to bid to supply electricity in five-minute blocks, while the AEMO dispatches electricity every five minutes.
5) Generators confirm offer from AEMO.
6) AEMO settles the bid and dispatch electricity to retailers.
7) Retailers sell electricity to customers.
8) Generators receive the spot price for the period that they were dispatched (financial settlement).

The physical trading market is performed on a short-term basis. However, electricity can also be sold on a longer-term agreement through the contract trading market as described below.

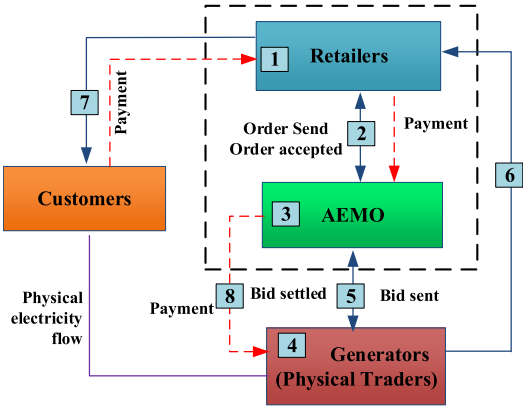

FIGURE 3. Current physical (spot) trading market model.

2) CONTRACT TRADING MARKET

Contract trading market is a trading market on a longer-term basis to supply or procure electricity at a more stable price and to secure certain levels of energy volumes. The supply or procurement of electricity is done over a particular period at a fixed price. The contracting market is done in two ways, over the counter (OTC) contract and through the future exchange.

The OTC markets allow wholesale electricity market participants to enter into a confidential contract between the two parties, generator and retailer.

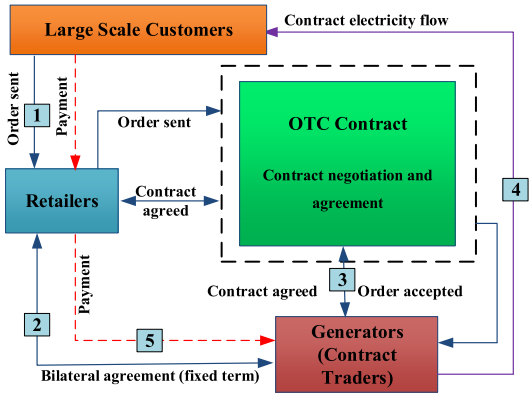

FIGURE 4. Current over-the-counter (OTC) trading market model.

Fig. 4 shows interactions of key players in an OTC market. In an OTC market:

1) Retailers or large customers request to buy electricity on a longer-term basis.
2) Generators (contract traders) make a deal with brokers or retailers, or directly to customers on a long-term energy sale agreement.
3) Agreement is made on how much energy to supply based on a long term contract.

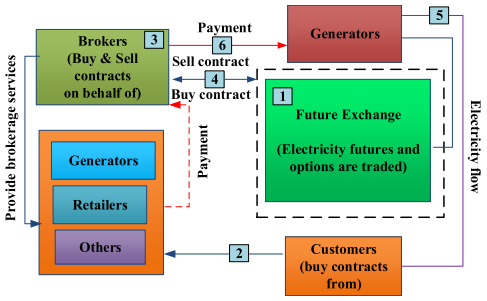

FIGURE 5. Current future exchange trading market model.

4) Generators dispatch electricity to customers through the power transmission and distribution network.
5) Generators settle on a price based on mutual energy sale agreement (financial settlement).

In a Futures exchange trading market, electricity futures and options are traded on the exchange. Participants (licensed brokers) buy and sell contracts on behalf of customers that include generators, retailers, speculators such as hedge funds, and banks and other financial intermediaries.

Fig. 5 shows interactions of key players in the Futures exchange market.

In the Futures exchange market:

1) Electricity Futures are traded on future (registered) exchanges.
2) Customers request to buy electricity.
3) Participants (licensed brokers) buy and sell contracts on behalf of clients that include generators, retailers, speculators such as hedge funds, and banks and other financial intermediaries.
4) Brokers negotiate prices with generators through the futures exchange mechanism and agreement is made between the generators and brokers on the sale of energy through the exchange market.
5) Generators dispatch electricity to customers through brokers.
6) Generators settlement price is based on mutual energy sale agreement (financial settlement).

Table 2 below summarizes the comparison between the physical and contract trading markets.

TABLE 2. Layers of Blockchain technology.

Blockchain Layers	Principal Components
Application layer	Cryptographic currency
Contract layer	Smart Contracts, Algorithmic mechanism
Incentive layer	Distribution mechanism, smart contract, script codes
Consensus layer	Proof-of-work (PoW), Proof-of-stake (PoS), Practical Byzantine fault tolerant (PBFT)
Network layer	Peer-to-peer network, Propagation mechanisms
Data layer	Data block, chain structure, time stamp, hash function

C. CHALLENGES OF THE CURRENT ENERGY MARKET TRADING SYSTEM

Energy market trading system is a trading system which energy market participants use for the buying and selling of electricity in the NEM.

In the current energy market trading system, transactional energy data are only available to energy generators and market participants for purposes of bidding for electricity. In addition, data recorded in the system do not differentiate the type (source) of energy generated (such as renewables or non-renewables). Once electricity is generated and mixed with the pool of electricity and dispatched through the transmission and distribution network, the energy market trading system cannot differentiate its sources. Similarly, customers are not able to identify if the source of energy supplied to them is from renewables or non-renewables. Energy market traders do not have verifiable and auditable technology to track and monitor sources of energy and this usually done through a manual process, which is time consuming and open to human error.

The current energy market trading system, which in some organizations is based on a Microsoft Office Excel®based trading mechanism, is also not providing the level of security required to trade energy. Sensitive transactional energy data are shared between energy market participants in a plain text format and phone conversations, and security is based on mutual human trust. There is no tamper resistant security provision built into it.

Energy supply becomes more efficient and sustainable if the sources of energy injected into the electricity macrogrid provide secure data visibility starting from power generation through the network to the end customers. In this regard, it is imperative to enhance the existing energy market trading system architecture to achieve this goal. The current energy market trading system architecture is shown in Fig. 6.

Fig. 6 is described as follows:

1) Electricity is generated through various sources, such as through burning fossil fuels (coal and natural gas), hydro, wind and solar. Electricity flows through a metered point at the power plant for a given period and is measured in megawatt-hours.
2) Transactional energy data are generated from the physical flow of electricity that the network traffic carries (such as data from sensors and smart readings). Information is passed through the power meter to the power recording system for use by the energy market trading system.
3) Traders trade electricity generated (produced) to the customers through physical (spot) trading or contract trading mechanism.
4) Electricity is traded (by making bids) between generators and market operators, usually through spot trading.
5) Electricity is traded between generators/market operators and third-party intermediaries (retailers or brokers), usually through contract markets.
6) Electricity is dispatched to customers.

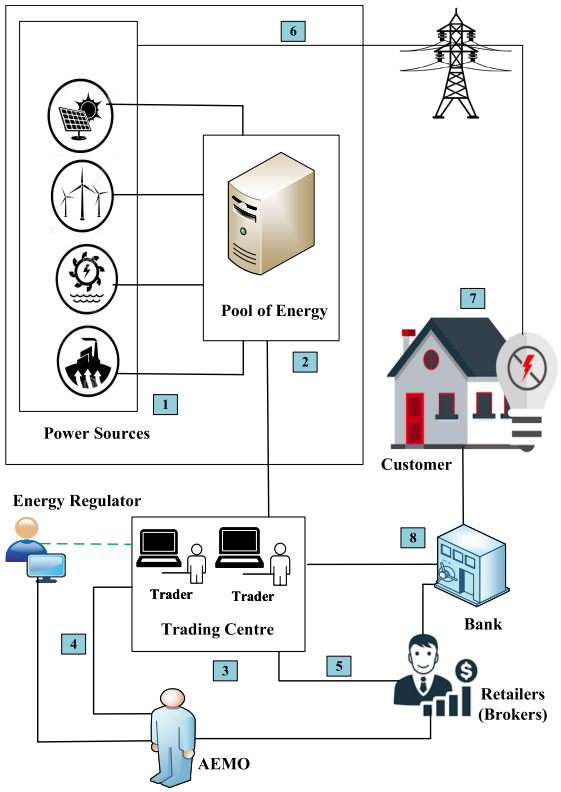

FIGURE 6. Current energy market trading architecture.

7) Electricity is provided (supplied) to customers.
8) Commercial (financial) transactions are settled via conventional payment system.

In the current energy market trading system sources of energy are not tagged or identified before they are mixed with the pool of energy. This has become a challenge for generators or AEMO to track and monitor sources of energy dispatched to customers in real time. As a result, it is not possible to know how much renewable energy is supplied to a customer. Customers are also unable to track and monitor the source and quantity of energy dispatched at their premises. Based on the shortfalls of the existing system, this research addresses issues of transactional data security and availability (visibility). We are proposing the design of a security mechanism to enhance the existing energy market trading system security. This will provide secure transactional energy data and transactional energy data visibility to end customers. This will be discussed in detail in our proposed solution below.

V. PROPOSED ENERGY MARKET TRADING SYSTEM AND ASSUMPTIONS

Our proposed energy market trading system is a trusted token-based trading system, which provides transactional data security to energy market participants. This system offers tools to help energy market participants to allow them to audit and verify the energy transactional data. Through this system they can verify actual energy generation, sales and payments.

In the proposed system design, it is assumed that power generation (and type) matches what the generators claim they are generating. This verifies that information about the power generation recorded by power metering and stored in power recording and monitoring system is correct.

The core components of the proposed system are described below followed by the solution design and architecture.

A. PROPOSED ENERGY MARKET TRADING SYSTEM COMPONENTS

Blockchain technology is used in this solution as a method to address the requirements of transactional data security discussed in Section II of this paper.

The core system components of our proposed design are cryptocurrency, smart contract and Public Key Infrastructure (PKI). The first two system components are part of the blockchain network (as described in Table 2 below). The PKI sits on the application layer of the Open Systems Interconnection (OSI) model.

Below we discuss each of our core system components and their application in this research.

1) BLOCKCHAIN TECHNOLOGY

Blockchain technology is a shared and distributed data structure (ledger) that is shared across a network. Its data structure is formed by a time sequence of digital blocks of transactions without a central control point. Blockchain is essentially an irreversible digital ledger on which decentralized applications can be built [26]. In a blockchain network there is no need for a trusted third-party (TTP) to process a transaction as this is replaced with a decentralized system. Each energy market participant's node in the blockchain network has a complete copy of the ledger, so one or two nodes going offline will not result in any data loss because each node owns a copy of the ledger.

Depending on the environment and the type of node, blockchain technology can be divided into three types, public blockchain, private blockchain and consortium blockchain. Each of these consists of six basic layers [1] and [6], data layer, network layer, consensus layer, incentive layer, contract layer and application layer, as listed in Table 2.

In the public blockchain, anyone can participate in the consensus process to write the data or block into it. Information is publicly available for everyone to read. However, in private blockchain, which this research is focused on, only authorized users can generate blocks and all permissions are kept centralized to an organization. In our case, authorized users are AEMO (in the case of physical trading) and generators (in the case of contract trading). Private blockchain is used by these users who want to create their own currencies. In the case of consortium blockchain it is controlled by a group of members. It has pre-defined set of nodes. Some users have write access and some, or all, read-only access.

The following subsections provide an overview of part of a blockchain technology utilizing smart contracts, cryptocurrency and consensus mechanisms.

a: SMART CONTRACT

A smart contract is a computer program that is capable of self-executing or enforcing a contract with terms of agreement between two or more energy market participants. It automatically fulfills the terms of the agreement once conditions are met without the need for intermediaries. For example, a smart contract can be used to implement an escrow that releases a fund after a cryptographic condition has been fulfilled. Escrow is a legal concept in which a fund is held by a trusted third party on behalf of two other parties that are processing a transaction. The fund is on hold until contractual obligations have been satisfied. In this case escrow is done between two parties that are not trusting each other and relaying on a TTP. This is a perfect use case for escrow smart contracts that operate in a no mutual trust manner and confidence in the contract.

There are different types of blockchain that provide smart contracts. One of the well-known smart contracts is provided by Ethereum. In our design proposal, we utilize the application of private blockchain with smart contracts. This is to allow energy trade between energy market participants without requiring a TTP once they are authenticated to join the blockchain network.

b: CONSENSUS MECHANISMS

In reaching consensus (agreement) in the blockchain technology, different consensus mechanisms may be used. PoW and PoS are the most used methods of reaching consensus in a permissionless public blockchain. In a permissioned blockchain a PBFT algorithm is used.

PoW is the mechanism that leverages the computational processing power to solve complex equations to confirm transactions and produce new blocks to the chain. A new block can only be created if the cryptographic hash value of the block that was last recorded is known through solving the complex equation. Random guesses must be made until the accurate combination is achieved. However, in PoS there is no competition required to determine the next transaction block, as the block created is chosen by an algorithm based on what the stake nodes have invested in the system, i.e. coin ownership.

With PBFT, each blockchain node needs to know the identity of every other blockchain node in the network. Consensus in the PBFT can be reached when the number of Byzantine faults (malicious nodes) is less than one-third of the total number of nodes. This is enabled by the fact that all honest nodes agree on the state of the system at that specific time as a result of their communication with each other.

PoS is an alternative consensus algorithm to PoW. PoS saves more energy and is more efficient. In PoW, miners (who create transactions) are required to solve a puzzle before any of their blocks is accepted by others. To add a malicious block, a computer more powerful than 51% of the network would be needed, which is high in system cost. While in PoS, it would be necessary for miners to have a high stake at the cryptocurrency to determine the next block. In order to add a malicious block, one would have to own 51% of all the cryptocurrency on the network.

In the PBFT algorithm, members of the blockchain are partially trusted and it is high in transactional speed and low in energy consumption and system cost. PBFT provides transaction finality without the need for multiple confirmations once approved and as it is not computationally intensive, a substantial reduction in power consumption is achievable. Additionally, permissioned blockchains are private and are by invitation with known identities, so trust between the parties already exists.

In our case, the energy market participants who participate in a blockchain network to trade energy, operate under known energy market identities. Those identities are authenticated using a certificate-based authentication method (as discussed in Section 1.3 below) before their participation in the blockchain network is allowed. For these reasons we consider PBFT consensus algorithm to be the most suitable candidate for our use as it meets our proposed system requirements due to its high speed and low energy consumption.

c: PUBLIC-KEY CRYPTOGRAPHY

Asymmetric-key cryptography is commonly referred to as ''public-key cryptography''. It uses a mathematically associated key pair – a public key and a private key, for encryption and authentication purposes [25]. A digital certificate is used to attest to the binding between a particular entity and its public key by a trusted third party, known as a Certification Authority (CA), under the Public Key Infrastructure (PKI) scheme.

In our zero-trust proposed system model anyone attempting to access the trading system must be authenticated first. Zero-trust security concept, which is applied to this research, is centered on not trusting any internal or external market participants of the network. In this research, we utilize the application of a X.509 v3 digital certificate which contains extension fields that allow additional fields to be added to the certificate. The certificate itself is used for the authentication of the market participants to access the energy market trading system and the additional attributes are used for the authorization purposes to access the trading system. This digital certificate allows us to verify that energy market participants are authenticated before they attempt to access the energy market trading system and their participation in the blockchain network.

B. PROPOSED ENERGY MARKET TRADING SYSTEM DESIGN AND ARCHITECTURE

Section A above discussed core components of our design solution and demonstrated how these core components can provide secure energy market transactional data through the application of cryptocurrency, smart contracts and PKI. This section elucidates the proposed architecture.

Our proposed trading system utilizes the application of blockchain technology to replace the TTP trading model with

a decentralized blockchain system model. PKI is also used for market participants' authentication before their permission to join the blockchain network is allowed.

The proposed system provides the mechanism that allows AEMO (in the case of physical trading) and generators (in the case of contract trading) to audit what they have sold. The proposed energy market trading system allows for auditing through the escrow model and the recording of all sales. Information provided to AEMO and to generator facilitates a mechanism for payments and penalties. AEMO and generators, through this system, can verify actual energy generation, sales and payments. The advantage of such a system is that AEMO and generators do not have to manually monitor every single transaction. The system is able to provide reliable transactions and allows them to audit the system as required.

The information that this proposed system provides and the mechanism we have through the escrow system can support AEMO's role. This ensures that the energy and the information in the system about the energy in fact correspond. This means that all market participants still fulfil their roles as they do currently. What we have proposed in this system is a mechanism for mutual trust in the system, rather than human trust when trading energy using a Microsoft Office Excel®based trading mechanism, over the phone, email or other means. In a fully trusted third-party model, AEMO (in the case of physical trading) and generators (in the case of contract trading) controls and manages energy data transactions. The system is able to automate the auditing of sales and facilitate payment process for both AEMO and generators and transferring that responsibility to cryptocurrency with the support of smart contracts. Double spending is also addressed by tracking where the money goes, through the digital tokens we create that represent electricity. Once energy data transaction are validated, they become irreversible and data are saved to blockchain.

1) ROLES AND RESPONSIBILITIES OF ACTORS IN OUR BLOCKCHAIN SOLUTION

The four main roles in the blockchain network for the physical trading model, as shown in Table 3, are AEMO, generator, retailer (broker) and customer. In the case of the contract trading model only the generators and customers are involved in the blockchain network, as described in Table 4. All these roles interact with the blockchain by creating transactions. The actors can also provide PBFT consensus to support trust between those that are involved in the blockchain transaction process. Once the trading participants have been authenticated to access the trading system, they have different roles to play. In the blockchain solution as listed in Tables 4 and 5, and illustrated in Fig. 7. Each participant has its own role(s) and responsibilities when they interact with the blockchain. How the smart contract is created and executed with the support of an escrow is also described in Table 5 and the process is shown in Fig. 8 and Fig. 10. When a digital token is exchanged between energy market participants, the smart contract acts an as escrow to ensure all parties get the result of the expected transaction before the actual financial transaction is made.

2) BLOCKCHAIN AND SMART CONTRACT DESIGN SOLUTION

A blockchain interaction and sequence model of both the physical and contract trading model is described below. These models are derived based on the roles, responsibilities and interactions of the market participants described in Table 3, Table 4 and Table 5.

a: BLOCKCHAIN AND SMART CONTRACT DESIGN – FOR PHYSICAL TRADING

Fig. 7 shows the proposed physical trading model with three layers: actor and role, service and processes.

Actors and roles layer display blockchain node and market participants' accounts/roles. Services layer are for the actors and roles to make transactions based on their permission on the blockchain, while the processes layer looks at the discovery of nodes in the network, checking on permissions and consensus mechanisms, and block creation processes.

All the roles of the market participants in the physical trading model interact with the blockchain network by creating transactions. They can also provide a PBFT consensus mechanism to support trust between those involved in the blockchain transaction process. Services such as create transaction, create contract, sell digital tokens, issue digital tokens, send messages and smart contract are used by actors and roles to interact with the blockchain to make transactions. The proposed model also includes four processes: network discovery, transaction, consensus and block creation processes. The network discovery process acquires the Internet Protocol (IP) address of the participant node. If the system identifies and recognizes the IP address of the participant node then the participant node is allowed to join the blockchain network. Permissions will be checked on the transaction process on who is permitted to create transactions, issue or sell digital tokens, transfer funds etc. A consensus is reached by each node when a new block has been distributed. In the block creation process, when a new block is created, it will be linked to the previous block. Every node on the network updates its block-chain to reflect the change.

In the physical trading model AEMO requests a transaction to issue digital tokens and schedule bids. Generators make transactions which triggers the creation of a smart contract that implements an escrow with retailers or brokers. Transactions are broadcast to the blockchain network consisting of market trader nodes that are involved in the market transactions. These nodes communicate to reach a consensus after the cryptocurrency and a smart contract processes are completed. The new block is then added to the existing block, which is a time-stamped series of immutable records of data.

Fig. 8 shows the trading interactions for the physical trading model between the trading participants. Fig. 7 indicates the roles of participants with the involved services and processes in the blockchain network.

TABLE 3. Roles of market participants in the blockchain solution: the case of physical trading.

Entities				
Name	Roles	Capabilities	Action Taken	Resources
AEMO	Handles the day-to-day operations of the electricity market Receives money	Predict electricity demand Create transactions Send messages Audit transactions and payments Create digital tokens Issue digital tokens to generators Participate in the consensus mechanism	Issue digital tokens to generators Schedule/award/reject bids Make transactions Accept money from retailers (brokers) Pay money to generators Impose penalties to generators	Rules and regulations
Generator	Produces and sells electricity Receives money	Create transactions Receive digital tokens from AEMO Sell digital tokens to retailers/brokers Submit bids to sell electricity Create contract Participate in the consensus mechanism	Make transactions Accept bids Sell digital tokens Create smart contract with brokers/retailers	Power generators
Retail/broker	Buys electricity on behalf of the customers Pays money to AEMO Receives money from customers	Create transactions Buy digital tokens from generators Sell digital tokens to customers Participate in the consensus mechanism Create contract	Make transactions Sell tokens Create smart contract with customers	Retailing and brokering
Customer	Buys electricity Pays money to retailer/broker	Buy digital tokens from retail/broker Submit to buy electricity	Accept/reject contract	Smart meter

TABLE 4. Roles of market participants in blockchain solution: the case of contract trading.

Entities				
Name	Roles	Capabilities	Action Taken	Resources
Generator	Produces and sells electricity Receives money	Create transactions Create digital tokens Sell digital token to customers Submit bids to sell electricity Create contract	Make transactions Accept/reject bids Sell digital tokens Create smart contract with customers	Power generators
Customer	Buys electricity Pays money to generator	Buy digital tokens from generator Submit to buy electricity	Accept/reject bids Accept/reject contract	Smart meter

TABLE 5. Interaction of market participants with blockchain solution.

Interaction	
AEMO and generators	AEMO interacts with generators on bidding, scheduling, supply and sale of energy, on payments and penalties, and on issuing digital tokens.
Generators and retailers	Generators and retailers interact between each other when creating smart contracts and selling/buying digital tokens.
Retailer (broker) and customers	Retailers (brokers) interact with customers on energy supply, on creating a semi smart contract between them and selling/buying digital tokens.
AEMO and customer	AEMO interacts with customers through the smart meter to verify the supply of energy to customers.

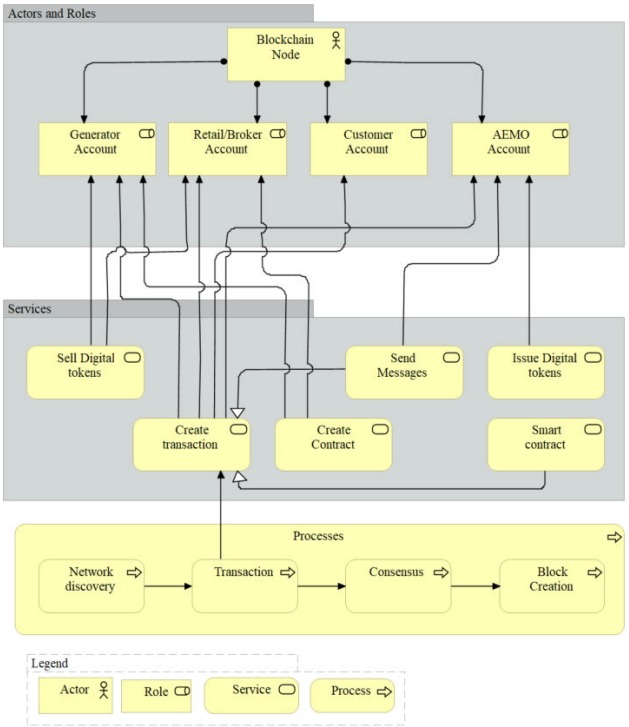

FIGURE 7. A Model for our proposed blockchain network: The case of physical trading.

There are separate cryptocurrencies (i.e. digital tokens) for the different types of power source that enable the cryptocurrency scheme to make the required separate totals that maintain integrity without trusting the retailers (brokers). This is to sum up and verify its integrity on how much renewable energy the retailer (broker) bought from the generators. In this manner, it can be checked if the sum of all the renewable energy sold to customers exceeds the sum of the renewable energy bought by retailers (brokers).

b: BLOCKCHAIN AND SMART CONTRACT DESIGN – FOR CONTRACT TRADING

In the case of the contract trading, it is similar to the concept of the physical trading. Fig. 9 shows the proposed model with three layers: actor and role, service and processes for contract trading. Actors and roles layer display blockchain node and market participants' accounts/roles. Services layer are for the actors and roles to make transactions based on their permission on the blockchain, while the processes layer looks at the discovery of nodes in the network, checking on permissions and consensus mechanisms, and block creation processes.

The market participants including generators and customers, interact with each other on the blockchain network. The consensus mechanism of PBFT is also adopted in this model to ensure that at least two-thirds of the nodes are honest. Services displayed in Fig. 9, create transaction, create contract, sell digital tokens, send messages and smart contract are used by actors and roles to interact with the blockchain. The model also includes four processes, which is similar to the concept of the physical trading model. In this model, generators request a transaction to issue digital tokens and schedule bids. A generator initiates a transaction which triggers the establishment of a smart contract that implements an escrow with customers. The transaction is distributed to a blockchain network consisting generator and customer nodes that are involved in the transaction. These nodes communicate to establish consensus and verify with cryptocurrency and a smart contact. The new block is then added to the existing block, which is a time-stamped series of immutable records of data.

Fig. 10 shows the trading interactions for the contract trading model between the trading participants.

The key differences in the proposed design between the physical and contract trading as shown in Table 6 are that the design of the physical trading is more complex (as it involves various stakeholders including energy generators, regulators, energy traders, wholesalers, retailers, brokers and customers that play a role in the blockchain system), and the existence of operational dispatch and the five-minute settlement rule. However, in the contract trading design, only generators, retailers and customers are involved and there is no five-minute settlement rule. As such, the design consideration in terms of the number of nodes required in the blockchain system that participate in the consensus mechanism and the size of the system is different

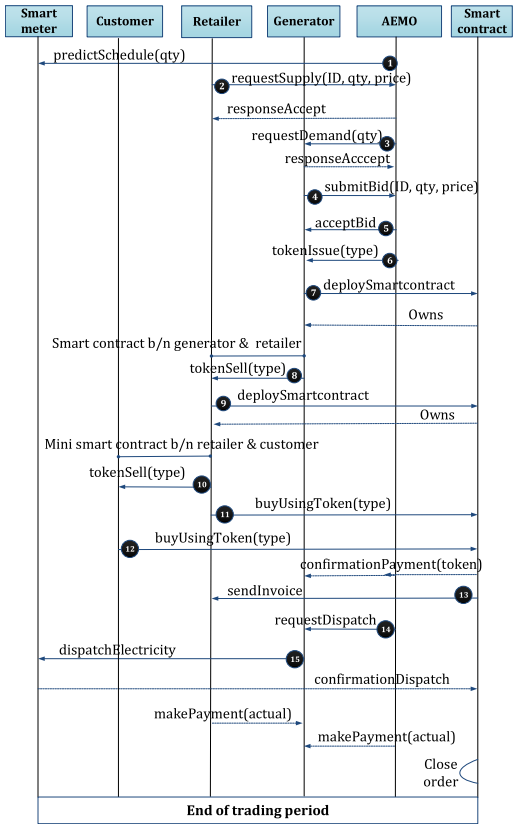

FIGURE 8. The proposed blockchain network that uses a smart contract for physical trading.

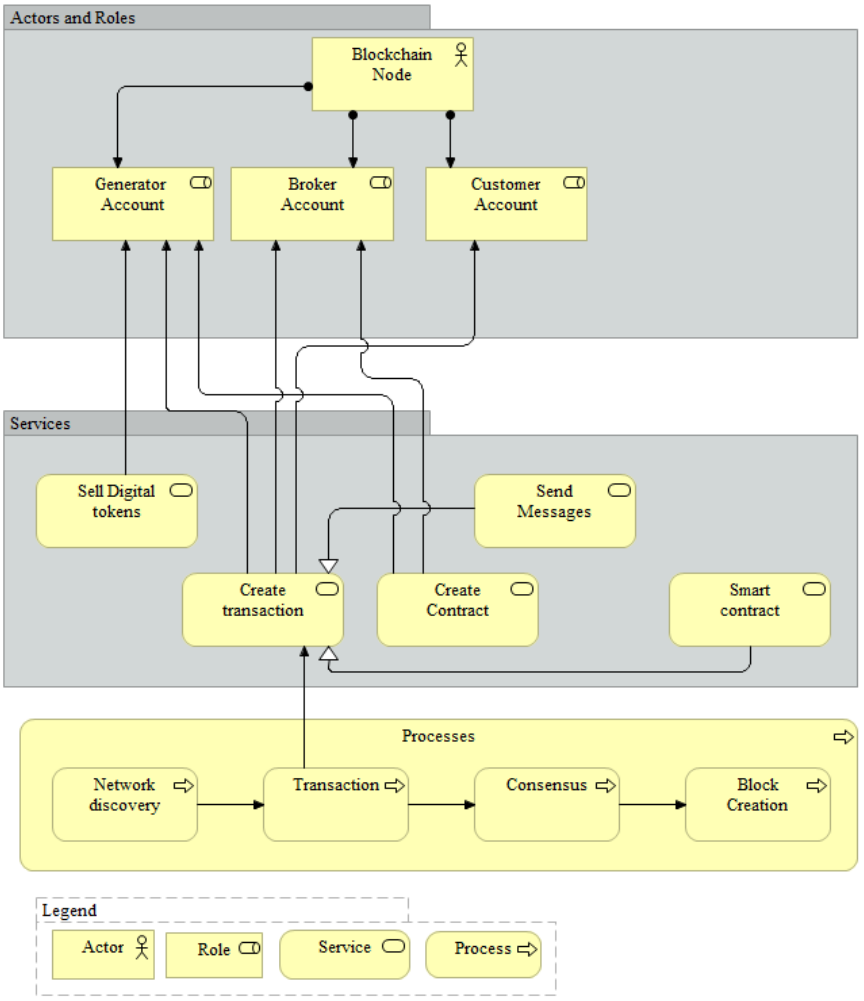

FIGURE 9. A Model for our proposed blockchain network: The case of contract trading.

TABLE 6. Differences between physical and contract trading design requirements.

Capability	Physical trading	Contract trading
Settlement	Short term electricity sale in NEM (5minutes settlement on spot price)	Long term electricity sale (contract on firm price)
Operator	AEMO	Generator
Stakeholders	Generator, retailer/broker, AEMO, customers and other regulatory bodies	Generator, retailer and customer
Contract type	Between generator and AEMO on spot pricing	Between generator and retailers on fixed pricing
Digital token	For tracking source of energy	For tracking source of energy
Energy supply	The balancing of energy supply and demand (no battery storage)	The balancing of energy supply and demand (no battery storage)

between these two designs. The token structure and the smart contract mechanisms also vary between these two designs.

c: DIGITAL TOKEN AND MARKET PARTICIPANTS CONTRACT DESIGN

This section discusses the design concept of different types of digital tokens and market participants' contracts. In this paper, digital tokens represent electricity generated from different types of sources of energy including coal, hydro, wind and solar. Three market participants involve in a smart contract including, generator, retailer and customer. The first two market participants' smart contracts are for the physical trading model and the third one is for the contract trading model. Fig. 11 and 12 show our two examples related to a digital token smart contract and retailer smart contract written in Solidity programming language to demonstrate the programing side of the proposed smart contract. Solidity is a programming language used for implementing smart contracts on various blockchain platforms.

1) Digital token contracts

There are four digital token contracts including coalToken, hydroToken, windToken and solarToken. These digital tokens are created for every five-minute trading period.

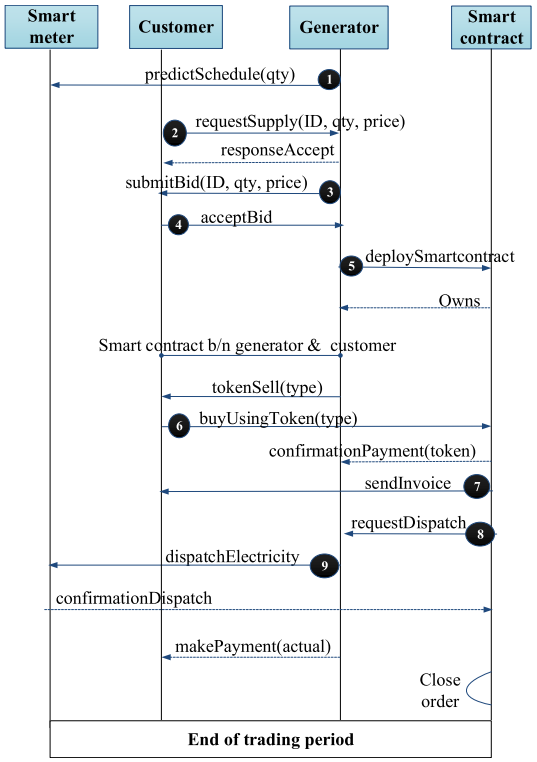

FIGURE 10. The proposed blockchain network that uses a smart contract for contract trading.

```
1  //A basic retailer contract using Ethereum
2  //blockchain example.
3  //The same applies for other contracts such as,
4  //generator, AEMO and customer
5  pragma solidity ^0.5.1;
6  contract retailerContract {
7        //A mapping to track the retailer token balances
8        mapping(address => uint256) public balances;
9        //a wallet where the funds will be sent whenever
10       //an account (retailer) buys token
11       address payable wallet;
12       constructor(address payable _wallet) public {
13       wallet = _wallet;
14       }
15        //buyToken() function that increment the balances.
16        //Funds can be transferred to the wallet whenever
17        //the buyToken() function is called
18       function buyToken() public payable {
19       balances[msg.sender] += 1;
20       //send digital token to the wallet
21       wallet.transfer(msg.value);
22       }
23 }
```

FIGURE 11. Example of retailer smart contract program.

2) Contracts between the generator and retailer
Generator and retailer have their own blockchain address. These addresses are used to send and receive digital tokens between them. AEMO initially issues digital tokens (coalToken, hydroToken, windToken and solarToken) to the generator that match what a generator says they will generate as part of the bid process. Retailers can request to buy digital token from the generator. The payment by the retailer for the digital token is held in the contract escrow. AEMO can transfer the payment from the escrow account when the consensus is reached through the PBFT mechanism that the energy is supplied to the customer.

```
1  // A basic coalToken contract using Ethereum blockchain example.
2  // The same applies for other type of tokens, such as hydroToken,
3  //windToken and solarToken
4  pragma solidity ^0.5.1;
5  // The keyword "public" makes those variables easily readable from
6  //outside.
7  contract coalToken {
8        string  public symbol = "Coal";
9        string  public standard = "DApp Token v1.0";
10       uint256 public totalSupply;
11 // Events allow light clients to react to changes efficiently.
12 //256-bit integer typically used to store token balances.
13       event Transfer(address indexed _from,
14       address indexed _to, uint256 _value);
15       event Approval(address indexed _generator,
16       address indexed _retailer, uint256 _value);
17 //The first mapping object, balanceOf, will hold the token balance
18 //of each owner account. The second mapping object, allowance, will
19 //include all of the accounts approved to withdraw from a given
20 //account together with the withdrawal sum allowed for each.
21       mapping(address => uint256) public balanceOf;
22       mapping(address => mapping(address => uint256)) public allowance;
23       function coalToken (uint256 _initialSupply) public {
24            balanceOf[msg.sender] = _initialSupply;
25            totalSupply = _initialSupply;
26 }
27 //The transfer function transfers the value amount of the coalToken
28 //to retailer address _to. It requires the address of the retailer
29 //that is transferring the amount to and the number of tokens that is
30 //transferred. The visibility of the token transfer on the blockchain
31 //can be public or private.
32       function transfer(address _to, uint256 _value)
33       public returns (bool success) {
34            require(balanceOf[msg.sender] >= _value);
35       balanceOf[msg.sender] -= _value;
36       balanceOf[_to] += _value;
37       Transfer(msg.sender, _to, _value);
38       return true;
39 }
40 function approve(address _spender, uint256 _value)
41 public returns (bool success) {
42       allowance[msg.sender][_spender] = _value;
43       Approval(msg.sender, _spender, _value);
44       return true;
45 }
46 //Transfer tokens from generator address to the retailer address
47     function transferFrom(address _from, address _to, uint256 _value)
48     public returns (bool success) {
49          require(_value <= balanceOf[_from]);
50          require(_value <= allowance[_from][msg.sender]);
51          balanceOf[_from] -= _value;
52          balanceOf[_to] += _value;
53          allowance[_from][msg.sender] -= _value;
54         Transfer(_from, _to, _value);
55         return true;
56 }
57 }
```

FIGURE 12. Example of digital token smart contract program.

3) Contract between a retailer and a customer
Retailers have their own blockchain address, the same as in the other contracts. These addresses are used to

send and receive digital tokens between them. When a retailer buys digital tokens from the generator they acquire ownership of the bought token. Customers can initiate a purchase request from retailers at any time. The payment paid by the customers for the digital token is held in contract escrow, where retailers can withdraw the total escrow amount to their account when the consensus is reached through the PBFT mechanism that the energy is supplied to the customer. A successful purchase of a digital token by a customer will add the customer in the list who is receiving power and trigger event.

4) Contract trading between a generator and a customer. This contract is in regard to the contract trading model. Generators have their own blockchain addresses and the customers can be anyone from the public. As generators have the power digital token, customers can initiate a buy request from generators at any time. The payment paid by the customers for the digital token is held in contract escrow, where generators can withdraw the total escrow amount to their account when the consensus is reached through the PBFT mechanism that the energy has been supplied to the customer.
Smart contracts programs in Fig. 11 and Fig. 12 have been verified using a Ganache Ethereum blockchain testing environment. Ganache is a blockchain for Ethereum platform that is used for deploying blockchain and running tests.

d: AN OVERVIEW OF THE PROPOSED ARCHITECTURE

The proposed physical and contract trading smart contracts architectures are shown in Fig. 13 and 14. The architecture of the end state of our solution is shown in Fig. 15. For physical trading, as shown in Fig. 13, AEMO have special addresses (accounts) to allow them to create digital tokens and they generate separate digital tokens for every type of energy and timestamped every five minutes. AEMO dispatches electricity every five minutes, so generators are required to bid to supply electricity at five-minute intervals. This also allows retailers to buy and sell electricity from generators and for customers to buy electricity from retailers using those digital tokens for transaction and payment verification purposes. AEMO forecasts on how much energy to generate during a particular time slot and then create digital tokens with unique identification numbers, date/time, the energy volume and other relate information.

In the physical trading smart contract model, as shown in Fig. 13, the proposed smart contract is performed as follows:

1) AEMO, the operator of the national electricity market, issues a digital token to the generator for each source (type) of energy the generator produces.
2) The generator trades digital tokens to the retailer. The retailer re-trades the digital tokens when selling electricity to the customer.

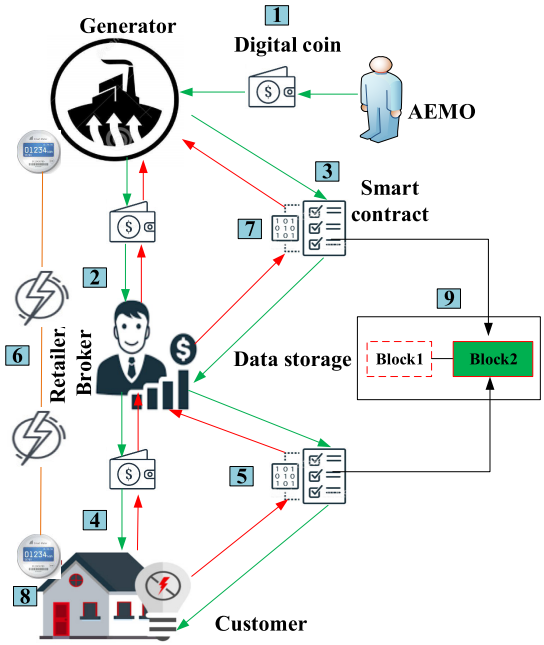

FIGURE 13. Proposed physical trading smart contract architecture.

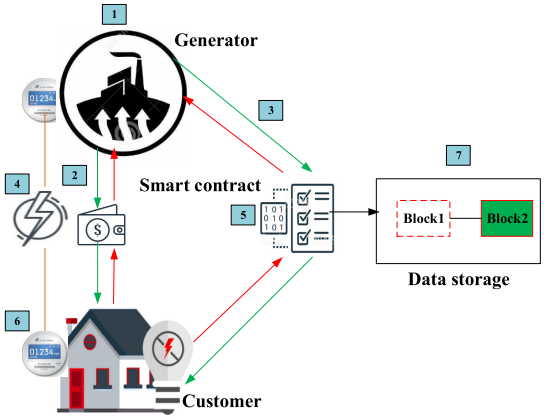

FIGURE 14. Proposed architecture for contract trading with smart contract.

3) The payment is held in escrow (smart contract) until all obligations in the contract are fulfilled.
4) The retailer re-trades the digital token to the customer. This allows the customer to buy electricity from the retailer.
5) The payment is transferred to the retailer (in a mini smart contract between retailers and customers).
6) Power is generated by the generator and consumed by the customer.
7) The payment held in escrow is released after it is confirmed that electricity is dispatched to the customer.
8) Smart meter is checked and approved.
9) Smart contract is executed and added to the blockchain network.
10) Money is transferred to generators through a conventional payment system.

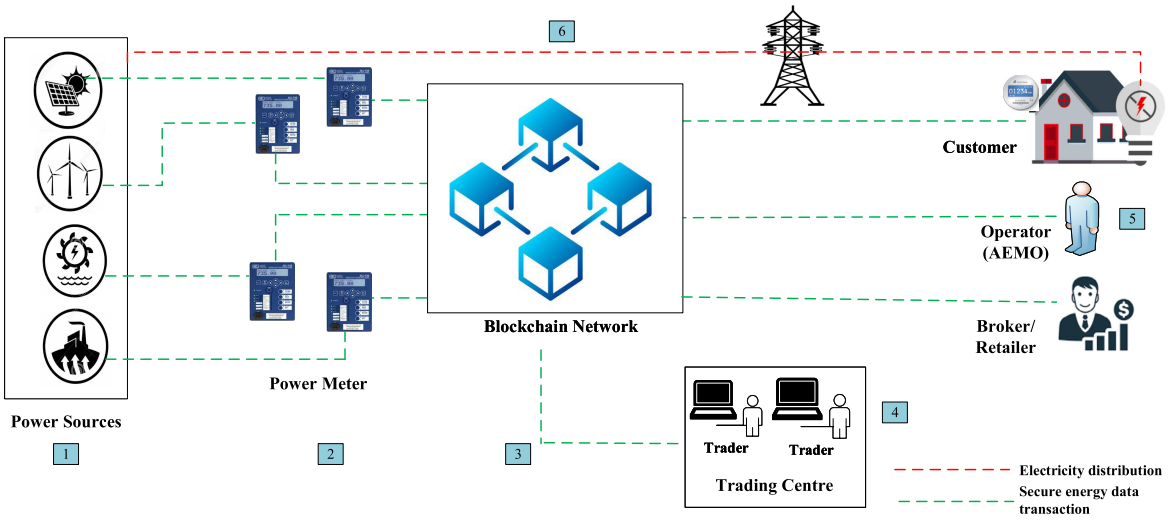

FIGURE 15. Proposed architecture for a macrogrid energy trading system design.

In the case of contract trading, as shown in Fig. 14, generators can employ multiple accounts to generate digital tokens to sell to brokers or directly to customers.

The process of the proposed smart contract includes:

1) Generators issue new digital tokens for each type of energy source they generate.
2) Generators sell tokens to customers. This allows customers to buy electricity from the generators based on their demand.
3) Money is kept in escrow (smart contract) until electricity is dispatched to customers.
4) Power is generated by the generators and consumed by customers.
5) Escrow is released after it is confirmed that electricity is consumed by the customer.
6) Smart meter is checked and issues approval.
7) Smart contract is executed and saved to the blockchain.
8) Money is transferred to generators through a conventional payment system.

Fig. 15 shows an overview on the proposed architecture for a macrogrid energy trading design. Energy market participants operate under known energy market identities and those identities are authenticated using a certificate-based authentication method before they participate in the proposed blockchain-based trade process model (3).

The operator (trader) in the blockchain network (3) fetches data from power meter (2) to provide energy market transactional data for market participants (5). With the use of digital token and blockchain that increases transparency and allows customers to verify the renewable energy dispatched to them is not oversold. The electrical transmission and distribution network (6) provides electricity from the power generation stations to customers.

The above proposed design has no real-time requirement. The main purpose of this project is to design a framework for the trading system so that transactional data are auditable, verifiable and trackable when needed after the trading period is complete. Payments from retailers and customers do not occur instantaneously, as retailers and wholesale customers disburse to AEMO on a weekly basis, and AEMO subsequently disburses to generators. The payment mechanism we are proposing through the digital tokens assist AEMO to verify actual energy generation and sale before actual payment is authorized.

VI. SIMULATION DESIGN

This section discusses the key assumptions used in developing the proof-of-concept design.

A. ESTIMATED VOLUME OF TRADING TRANSACTIONS IN THE NATIONAL ELECTRICITY MARKETS

To assist in the assessment of a practical feasibility of the proposed design and architecture we first estimated the maximum number of transactions (and the size of data) that could be processed in the national wholesale electricity markets in the five-minute dispatch periods. Generators who are registered in NEM make bids (offers) into the electricity market to generate and sell electricity at various prices for each of the five-minute dispatch periods in a day. Market participants system submit and receive confirmations of five-minute bid and offer data in five-minute blocks [48]. Currently there are 100 generators and 30 retailers that participate in the national electricity market in Australia. Generators submit bids on a daily basis with potentially many subsequent rebids with the five-minute period. We assume that the maximum number of transactions can occur is if:

1) All generators and retailers participate in the bid and re-bid process in a five-minute trading period.
2) All generators and retailers access the dispatch and trading data during the bid and re-bid process in a five-minute trading period.

Based on the above assumptions we summarize the maximum number of transactions and amount of data that could be processed in the national wholesale electricity market in Table 7.

TABLE 7. Number of transactions and amount of data in NEM.

	Five-minutes	Trading day
Maximum number of transactions	230	66,240
Maximum amount of data	26 megabyte	130 megabyte

B. SELECTED SIMULATION TOOL

To evaluate the feasibility of the proposed trading system this research investigated numerous platforms. One of the platform deems suitable for the proposed design and architecture is the Kaleido's enterprise blockchain platform [44]. Kaleido can support the configuration of permissioned blockchain based on the hyperledger fabric mechanism.

This simulation is based on the permissioned blockchain as per the proposed design and architecture. Following are key requirements to get the simulation system up and running..

1) Initiate a consortium account and location that the blockchain network to be hosted. In our simulation a group of energy market participants ''market operator'' is initiated for the permissioned blockchain-based trading network.
2) Establish a new environment (a blockchain network that the organizations will participate in), the type of blockchain and the consensus algorithm to be used. In our simulation we established a ''energy trading'' permissioned blockchain network for a market participants to participate in. We used the Istanbul Byzantine Fault Tolerant (IBFT) consensus algorithm on the hyperledger Besu technology as per our proposed consensus mechanism.
3) Establish key market participant accounts in the blockchain network that participate in energy market trading processes and the assignment of a consensus mechanism to the accounts. In our simulation platform we set up four market participant accounts with generator, AEMO and retailer as signer role in the consensus (they can propose and vote on blocks) and a customer as a non signer role (not allowed to propose and vote on blocks).
4) Import a smart contract to the respective market participant accounts setup in step 3 above. In our simulation platform we deployed smart contracts in the blockchain network for use by market participant accounts during the energy trading processes.
5) Establish digital tokens in the blockchain platform for use by the market participant accounts. In our simulation platform we deployed digital tokens for use by market participant accounts during the energy trading processes. Tokens are used for auditing and verification of sources of energy purposes.

VII. PROPOSED SYSTEM DESIGN ANALYSIS

This section analyses and evaluates the proposed trading system.

The main difference between the current energy market trading system (Fig. 6) and the proposed energy market trading system (Fig. 13) is that in the current energy market trading system, when electricity is generated, it is directly transmitted and distributed to customers without tagging or monitoring the sources of energy. This has limits on the transparency and authenticity for energy market participants to verify and audit energy transactional data for each source of energy dispatched to customers. It is also difficult for customers to know the percent of energy sources dispatched to them. In the proposed energy trading system, the source of energy is recorded and tagged prior to the electricity dispatch to customers so that customers can verify the authenticity of provisioning renewable energy. The other main difference between the current and proposed energy trading systems is that the current energy market trading system is not designed to provide energy market transaction data. It is mainly based on mutual human trust and trading is done through insecure means of communication. This research proposes the use of blockchain technology with a token-based cryptocurrency and smart contract mechanism to achieve transactional data confidentiality and integrity.

A. THE DESIGN MEETS THE SYSTEM REQUIREMENTS

This section contends that the proposed scheme meets the three requirements mentioned previously in Section I.

1) REQUIREMENT 1: ENERGY MARKET TRADING SYSTEM MUST PROVIDE THE CONFIDENTIALITY AND INTEGRITY FOR ENERGY TRADING. THIS IS TO SUSTAIN CONTINUED ENERGY SUPPLY AND SALES

In the proposed trading system, market participants' identities are authenticated using a certificate-based PKI authentication method before the participant is allowed to join in the blockchain-based trading system. The ledgers in the proposed blockchain technology are immutable and the energy market transactional data cannot be edited or deleted unless an agreement reached in a PBFT consensus method. During the trading process on the transmission and distribution of energy, all the energy transactional data are encrypted.

Our proposed blockchain solution is based on a permissioned blockchain which requires specific authorization to read, access, and write information to it. Access is restricted to authorized market participants and information is encrypted to protect confidentiality. During the trading period, those market participants interact in the permissioned blockchain technology using their roles. Those roles have been assigned specific permissions for each market participants and those permissions are checked on the blockchain network during the transaction process to verify who is

permitted to create transactions, issue or sell digital tokens and/or transfer funds. This means that only authorized market participants can access market related data during a particular trading period until AEMO discloses the market information after the trading process is completed. This ensures the confidentiality and integrity of accessing trading data for each trading process.

2) REQUIREMENT 2: ENERGY SOURCES MUST BE TRACKED DURING ENERGY GENERATION AND ENERGY DISPATCH SO THAT RENEWABLE ENERGIES ARE SEPARATELY IDENTIFIED FROM NON-RENEWABLES

In the proposed design we introduced the metering systems at the energy plant that are directly connected to each source of energy (coal, hydro, wind, solar etc) to identify and tag the source (type) of energy prior to energy transmission and dispatch. That information is passed to blockchain technology as shown in Fig. 15. Using token-based cryptocurrency and a smart contract on the blockchain network enables the tracking of those energy market transactions.

3) REQUIREMENT 3: CUSTOMERS SHOULD HAVE ACCESS TO ENERGY DATA TRANSACTION DETAILS SO THAT THE TYPE OF ENERGY PROVISIONED TO THEIR PREMISES IS KNOWN

Customers buy a specific type of digital token that represent the source of energy. Digital tokens are traded using cryptocurrency and the security properties of cryptocurrency are assured. Generators and AEMO ensure that those digital tokens are created appropriately. The blockchain network records, stores, and tracks those sources of energy data. In this manner customers are able to view their overall energy usage and identify provisioning renewable energy. The automated process on tracking sources of energy could help envisaging the progress of Australia's Renewable Energy Target (RET) and customers to verify the authenticity of provisioning renewable energy.

Below we discuss the feasibility of our proposed design and architecture based on the volume and amount of data transaction in NEM (as specified in Table 7), the blockchain system simulation we setup in Section VI and the prior work on performance of the permissioned blockchain.

a: AVAILABILITY

As demonstrated in the simulation setup, cloud-based blockchain platforms are readily available that meet our proposed design and architecture. The simulation platform we set up is based on a free starter subscription and this demonstrates the commitment of availability of the platform in a concept stage leading to production deployment.

b: SCALABILITY

In the context of energy markets, scalability refers to the ability for a system to handle increasing number of transactions per second and the amount of data that is processed through the system. The blockchain platform we assessed as a proof-of-concept is capable of sanctioning on-demand availability of computer system resources, pertaining primarily with computing power and data storage.

c: PERFORMANCE

Our proposed design and architecture propose a permissioned blockchain. Performance on a permissioned blockchain, such as the hyperledger fabric, is different from that of Bitcoin. Hyperledger fabric has a concurrency controller that help increase throughput when processing transactions. Recent research [45] has also demonstrated the re-engineering of a hyperledger fabric to increase transaction throughput from 300 to nearly 20,000 transactions per second. Similar work has also been conducted in [46] and [47] to attest the better performance of the permissioned blockchain based on the hyperledger fabric than that of the permission less blockchain.

B. COMPARISON BETWEEN CURRENT AND PROPOSED TRADING SYSTEM

This section analyzes security functions provided from the proposed trading system against the existing trading system, as listed in Table 8.

TABLE 8. Comparison between current and proposed energy market trading systems

Functionality	Current energy market trading system	Proposed energy market trading system
Confidentiality	Data is transferred between parties in a plain text format	Data is encrypted and confidentiality preserved
Integrity	It requires human mutual trust in the trading process, which can pose security risks of unauthorized access and/or disclosure of trading data intentionally and unintentionally	The ledgers that holds trading transactions are immutable unless agreement reached in a consensus method
Authentication	No authentication method exists	Certificate-based authentication method
Tracking and monitoring	Manual process	Sources of energy are recorded and tagged Customer can identify provisioning renewable energy

The proposed solution is based on a mega power generation macrogrid that involves numerous market participants and regulatory bodies. It provides confidentiality and integrity for energy trading data. However, the proposed trading system also relies on other systems to collect data, such as the power recording system, the supervisory control and data acquisition (SCADA) and frequency control ancillary services (FCAS). The protection of data from these systems and their physical infrastructure security is also vital in maintaining

confidentiality of energy transactional data from generation to transmission and distribution of energy.

C. COMPARISON BETWEEN THE PROPOSED TRADING SYSTEM IN THE NATIONAL ELECTRICITY MARKET AND THE PEER-TO-PEER TRADING SYSTEM IN LOCAL MARKETS

The proposed blockchain based trading system in the national electricity market is more complex than in local markets as it involves various stakeholders including energy generators, regulators, energy traders, wholesalers, retailers, brokers and customers. All the aforementioned stakeholders have a role to play in the blockchain system. The existence of operational dispatch and a five-minute settlement rule also makes the system design more complex. In the blockchain based peer-to-peer trading system only prosumers (local energy generators) and customers are involved and there is no five-minute settlement rule. As such, the design consideration in terms of the number of nodes required in the blockchain system that participate in the consensus mechanism and the size of the system is different between these designs. The token structure and the smart contract mechanisms also vary between these designs. The digital token proposed in the national electricity market represent transaction for auditing and verification purposes while in the peer-to-peer the digital token represent the actual financial currency. Electricity in peer-to-peer is mainly generated from a rooftop solar energy and is traded in microgrid while electricity in NEM is generated from different sources of energy by mega generators and traded in macrogrid. Table 9 compares the national electricity trading markets and the peer-to-peer electricity trading markets.

TABLE 9. Comparison between national electricity trading markets and peer-to-peer electricity trading markets.

Capability	National electricity markets	Peer-to-peer electricity markets
Energy supplier	Macro generators (energy produced by powerplants)	Prosumers (energy produced through solar rooftop)
Electricity grid	Macrogrid	Microgrid
Commitment	Short term spot price and long term fixed price electricity sale	Short term electricity sale (contract)
Operated by	AEMO (physical trading) and mega generators (contract trading)	Prosumers
Stakeholders	Generators, retailers, brokers, customers and government authorities	Prosumer, customer and retailer
Contract type	Between generator and AEMO in physical trading Between generator and retailers in contract trading	Between prosumers and customers
Digital token	Represent transaction for auditing and verifications purposes	Represent financial currency

VIII. CONCLUSION AND FUTURE WORK

This research addressed required security architectures for the energy trading system. A digital token-based structure supported by smart contracts is proposed to not only enhance overall energy transactional data security but provide additional capabilities in the operation of the scheme so that sources of energy dispatched to customer premises are known. It clearly identifies the separate needs of the electrical power distribution management and the associated financial and payment systems needed to enable efficient and timely operation of the structure. This proposed energy market trading system architecture not only enhances the security management of energy market trading but provides incentives for prompt and efficient settlement. In addition, potentially human operator error has been removed from the system. In summary, the application of blockchain technology in the mega power generation macrogrid energy trading, investigated in this research, presents a higher transactional data security compared to the existing trading system.

The design and architecture proposed for the permissioned blockchain based trading system in this paper, supported by experiment, is a model that can be used in real-world deployments for secure trading in a national wholesale electricity market. The future work (with the support of a state-owned power generator) is to develop a complete prototype to demonstrate the feasibility of our proposed design and architecture. This paper forms a foundation for the creation of a prototype for trusted national energy trading system. This will form a base of future requests for research funding. The proposed design and architecture will be developed as a complete proof-of-concept which may be used when tendering for supply and installation. It is suggested that the government will issue the development and testing of this proposal. Upon the successful bidder testing, this proposal suggests that the government would issue tenders for the production and installation of the proposed trading system. This is based upon the successful experience in the energy sector, in particular, the successful structure and deployment of energy related network and systems over many years.

ACKNOWLEDGMENT

The authors would like to thank Dr. Bob Maczkowiack for taking the time to review the manuscript. They would also like to thank his invaluable comments and editing work on this study.

REFERENCES

[1] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.

[2] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep. 2018.

[3] T. Dimitriou and G. Karame, "Privacy-friendly tasking and trading of energy in smart grids," in *Proc. 28th Annu. ACM Symp. Appl. Comput. (SAC)*, Coimbra, Portugal, 2013, pp. 652–659.

[4] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, Oct. 2010, pp. 238–243.
[5] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, Oct. 2010, pp. 327–332.
[6] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proc. 10th Annu. ACM Workshop Privacy Electron. Soc. (WPES)*, Chicago, IL, USA, 2011, pp. 49–60.
[7] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Manubot2019. Accessed: Sep. 6, 2019. [Online]. Available: http://bitcoin.org/bitcoin.pdf
[8] G. Kappos, H. Yousaf, M. Maller, and S. Meiklejohn, "An empirical analysis of anonymity in Zcash," in *Proc. USENIX Secur. Symp.*, Baltimore, MD, USA, 2018, pp. 463–477.
[9] M. Spagnuolo, F. Maggi, and S. Zanero, "BitIodine: Extracting intelligence from the Bitcoin network," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Christ Church, Barbados, 2014, pp. 457–468.
[10] D. Ron and A. Shamir, "Quantitative analysis of the full Bitcoin transaction graph," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Okinawa, Japan, 2013, pp. 6–24.
[11] E. Androulaki, G. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in Bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Okinawa, Japan, 2013, pp. 34–51.
[12] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Proc. IEEE 3rd Int. Conf. Privacy, Secur., Risk Trust IEEE 3rd Int. Conf. Social Comput.*, NY, USA, Oct. 2011, pp. 197–223.
[13] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. Mc-Coy, G. M. Voelker, and S. Savage, "A fistful of Bitcoins: Characterizing payments among men with no names," in *Proc. Conf. Internet Meas. Conf.*, Barcelona, Spain, 2013, pp. 127–140.
[14] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed E-Cash from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, Berkeley, CA, USA, May 2013, pp. 397–411.
[15] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, Berkeley, CA, USA, May 2014, pp. 459–474.
[16] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Christ Church, Barbados, 2014, pp. 486–504.
[17] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for Bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, San Juan, Puerto Rico, 2015, pp. 112–126.
[18] E. Heilman, L. AlShenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "TumbleBit: An untrusted Bitcoin-compatible anonymous payment hub," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, 2017, pp. 1–36.
[19] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical decentralized coin mixing for Bitcoin," in *Proc. Eur. Symp. Res. Comput. Secur.*, Wroclaw, Poland, 2014, pp. 345–364.
[20] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-resistant mixing for bitcoin," in *Proc. 13th Workshop Privacy Electron. Soc. (WPES)*, Scottsdale, AZ, USA, 2014, pp. 149–158.
[21] A. E. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Jose, CA, USA, May 2016, pp. 839–858.
[22] S. Meiklejohn and R. Mercer, "Möbius: Trustless tumbling for transaction privacy," in *Proc. Privacy Enhancing Technol. Symp.*, Barcelona, Spain, 2018, pp. 105–121.
[23] M. Mihaylov, S. Jurado, K. Van Moffaert, N. Avellana, and A. Nowé, "NRG-X-Change: A novel mechanism for trading of renewable energy in smart grids," in *Proc. 3rd Int. Conf. Smart Grids Green IT Syst.*, Barcelona, Spain, 2014, pp. 101–106.
[24] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Nowe, "NRGcoin: Virtual currency for trading of renewable energy in smart grids," in *Proc. 11th Int. Conf. Eur. Energy Market (EEM)*, Krakow, Poland, May 2014, pp. 1–6.
[25] D. R. Kuhn, V. C. Hu, W. T. Polk, and S.-J. Chang, "Introduction to public key technology and the federal PKI infrastructure," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-32, 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf
[26] H.-Y. Paik, X. Xu, H. M. N. D. Bandara, S. U. Lee, and S. K. Lo, "Analysis of data management in blockchain-based systems: From architecture to governance," *IEEE Access*, vol. 7, pp. 186091–186107, 2019.
[27] I. Karamitsos, M. Papadaki, and N. B. A. Barghuthi, "Design of the blockchain smart contract: A use case for real estate," *J. Inf. Secur.*, vol. 9, no. 3, pp. 177–190, 2018.
[28] C. Fromknecht, D. Velicanu, and S. Yakoubov, "A decentralized public key infrastructure with identity retention," IACR Cryptol. ePrint Arch., Las Vegas, NV, USA, Tech. Rep. 803, 2014. [Online]. Available: https://www.iacr.org/docs/
[29] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, "A privacy-preserving thin-client scheme in blockchain-based PKI," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6.
[30] S. Misra, S. Goswami, C. Taneja, A. Mukherjee, and M. S. Obaidat, "A PKI adapted model for secure information dissemination in industrial control and automation 6LoWPANs," *IEEE Access*, vol. 3, pp. 875–889, 2015.
[31] A. L. R. Gómez-Arevalillo and P. Papadimitratos, "Blockchain-based public key infrastructure for inter-domain secure routing," in *Proc. Int. Workshop Open Problems Netw. Secur.*, Rome, Italy, 2017, pp. 20–38.
[32] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, "Cecoin: A decentralized PKI mitigating MitM attacks," *Future Gener. Comput. Syst.*, vol. 107, pp. 805–815, Jun. 2020.
[33] S. Matsumoto and R. M. Reischuk, "IKP: Turning a PKI around with decentralized automated incentives," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Jose, CA, USA, May 2017, pp. 410–426.
[34] L. Axon and M. Goldsmith, "PB-PKI: A privacy-aware blockchain-based PKI," in *Proc. 14th Int. Joint Conf. e-Bus. Telecommun.*, Madrid, Spain, 2017, pp. 311–318.
[35] M. Al-Bassam, "SCPKI: A smart contract-based PKI and identity system," in *Proc. ACM Workshop Blockchain, Cryptocurrencies Contracts*, Abu Dhabi, United Arab Emirates, 2017, pp. 35–40.
[36] X. He, J. Lin, K. Li, and X. Chen, "A novel cryptocurrency wallet management scheme based on decentralized multi-constrained derangement," *IEEE Access*, vol. 7, pp. 185250–185263, 2019.
[37] A. Rondelet and M. Zajac, "ZETH: On integrating zerocash on ethereum," 2019, *arXiv:1904.00905*. [Online]. Available: http://arxiv.org/abs/1904.00905
[38] B. Bünz, S. Agrawal, M. Zamani, and D. Boneh, "Zether: Towards privacy in a smart contract world," IACR Cryptol. ePrint Arch., Las Vegas, NV, USA, Tech. Rep. 191, 2019. [Online]. Available: https://www.iacr.org/docs/
[39] S. Somin, G. Gordon, and Y. Altshuler, "Network analysis of ERC20 tokens trading on ethereum blockchain," in *Proc. 9th Int. Conf. Complex Syst.*, Cambridge, MA, USA, 2018, pp. 439–450.
[40] S.-F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, "RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero," in *Proc. Eur. Symp. Res. Comput. Secur.*, Oslo, Norway, 2017, pp. 456–474.
[41] (2019). *The Renewable Energy Target (RET) scheme, Australia Clean Energy Council*. [Online]. Available: https://www.cleanenergycouncil.org.au/advocacy-initiatives/renewable-energy-target
[42] *Current Electricity Industry Structure, Energy Futures Australia*. Accessed: Nov. 9, 2019. [Online]. Available: http://www.efa.com.au/Page.aspx?intPageID=6
[43] *Basics, Geoscience Australia*. Accessed: Nov. 9, 2019. [Online]. Available: https://www.ga.gov.au/scientific-topics/energy/basics
[44] *Enterprise Blockchain for Modern Business Networks*. Accessed: Nov. 9, 2019. [Online]. Available: https://kaleido.io/
[45] C. Gorenflo, S. Lee, L. Golab, and S. Keshav, "Fastfabric: Scaling hyperledger fabric to 20,000 transactions per second," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, Seoul, South Korea, May 2019, pp. 455–463.
[46] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Vancouver, BC, Canada, Jul. 2017, pp. 1–6.
[47] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," in *Proc. IEEE 26th Int. Symp. Modeling, Anal., Simulation Comput. Telecommun. Syst. (MASCOTS)*, Milwaukee, WI, USA, Sep. 2018, pp. 264–276.
[48] *Dispatch*. Accessed: Jun. 20, 2020. [Online]. Available: http://nemweb.com.au/reports/current

AKLILU DANIEL TESFAMICAEL received the B.S. degree in mathematics from the University of Asmara, Asmara, Eritrea, in 1997, and the M.S. degree in information technology from the University of South Australia, Adelaide, Australia, in 2003. He is currently pursuing the Ph.D. degree in information security with the Queensland University of Technology (QUT), Brisbane, Australia.

He is currently a Senior Network Engineer at CS Energy, Queensland Energy Company, which generates and sells electricity in the National Electricity Market. He has previously worked in the energy sectors and government departments for over 15 years, attaining the position of Solutions Architect and Senior Network Engineer. His research interest includes network and security architectures for critical infrastructure.

VICKY LIU received the Ph.D. degree in information security from the Queensland University of Technology, Australia, in 2011. Her Ph.D. dissertation proposed an information system architecture to facilitate the enforcement of privacy and security. She is currently a Lecturer with the Science and Engineering Faculty, Queensland University of Technology. Her research interest includes network and security, in particular focusing on the Internet of Things (IoT) technologies and security aspects as well as network performance optimization. Recently, she actively involves in a number of government-funded research projects in addressing solutions for designing appropriate IoT architectures and balancing performance and security for IoT ecosystems.

MATTHEW MCKAGUE received the B.Sc. degree (Hons.) in mathematics from the University of Regina, Regina, Canada, in 2004, and the M.Math. and Ph.D. degrees in combinatorics and optimization from the University of Waterloo, Waterloo, Canada, in 2005 and 2010, respectively.

He is currently a Lecturer in cryptography with the Queensland University of Technology, Brisbane, Australia. He was a Research Fellow with the Centre for Quantum Technologies, Singapore, and a Lecturer with the Computer Science Department, University of Otago, Dunedin, New Zealand.

WILLIAM CAELLI received the B.Sc. degree (Hons.) from The University of Newcastle, NSW, Australia, in 1966, and the Ph.D. degree in nuclear physics from The Australian National University (ANU), Canberra, Australia, in 1972.

He was a Co-Founder of ERACOM Pty Ltd. (originally Electronics Research Australia Pty Ltd.), in 1979, the Foundation Director of the Information Security Research Centre (ISRC), QIT/QUT, in 1988, and later the Founding Head of the School of Data Communications. He was the Director/Founder of International Information Security Consultants Pty Ltd. (IISEC). He is an Emeritus Professor and an Officer in the Order of Australia (AO). He is currently an Emeritus Professor with the Queensland University of Technology, an Adjunct Professor with Griffith University, and an Honorary Fellow in cybersecurity at TAFE, QLD. He has 50 years of involvement, experience, teaching, and research/publication in all aspects of information/cybersecurity, including public policy and related matters, having first investigation experience of a cyber-attack, in late 1968. He has over 55 years of professional experience in ICT overall.

Dr. Caelli is a member of the National Cybersecurity Committee and the Cyber Resilience Task Force of the Australian Computer Society (ACS). This has included some eight years as a Member of the Board of the USA's Colloquium for Information Systems Security Education (CISSE).

ERNEST FOO (Member, IEEE) received the B.E. degree (Hons.) and the Ph.D. degree from the University of Queensland, Brisbane, Australia, in 1992 and 2000, respectively.

He is currently an Associate Professor with Griffith University. He has published over 110 refereed articles, including 20 journal articles. He has extensive experience with computer networking having worked and taught in this area for over 15 years. He has also been responsible for the design and development of the QUT SCADA Security Research Laboratory. The SCADA Laboratory consists of multiple vendor system miniatures that are run from industrial PLCs. His research interest includes secure cryptographic protocols with an active interest in network security applications. These include specific applications in the areas of industrial control system security and cyber-physical systems, such as SCADA and the smart grid.