Deanonymising Households Trading on a Blockchain Smart Grid

ANDREW MATHER

Supervised by Professor Raja Jurdak and Dr Ali Dorri.
Science and Engineering Faculty, Queensland University of Technology, 2 George St. Brisbane City, QLD, 4000, Australia.

November 1, 2020

This project aims to contribute to the study of user anonymity in blockchain for the Internet of Things. The research explores machine learning methods to deanonymise users on a smart grid with blockchain. Data stored on decentralised blockchains is permanent and user privacy can be at risk. Research exists into anonymity concerns in blockchain but IoT and smart grid contexts warrant further research.

The project analysis includes stored blockchain transactions and off-chain solar exposure data. Section one and two will investigate the research topic and the surrounding literature. Followed by the third covering the project's methodology. It aims to determine how effective machine learning is to deanonymise smart grid blockchain users. This will highlight long-term blockchain anonymity risks due to permanent transaction data. Section four will report these results against the objectives.

The approach will first, source energy grid data and construct blockchain ledgers. Second, apply machine learning analysis on past blockchain transactions to identify households. Third, measure the benefit of adding off-chain solar exposure data as households also produce solar energy. Last, the project will investigate public key and ledger obfuscation methods to improve user privacy. Project outcomes include a better understanding of user privacy risks but also methods to mitigate these risks.

Results found machine learning models accurately link user transactions from past data without privacy steps. More frequent transactions aid attackers and the peak classification accuracy was 84% (customer ID) and 63% (postcode) with a convolutional network. Attacker success rates improve by including solar exposure data. Household energy usage and solar generation were reconstructed from net export at 85% R^2 accuracy with regression models. Smarter users can significantly reduce attack success by adding public keys. The lowest result became 4% (customer ID) and 11% (postcode). There are clear benefits in public keys up to about 20, where the benefit sharply tapers off thereafter and may not be worth the cost for a user. There is less notable but still a privacy benefit as public keys per ledger increase.

The results highlight concern for a user's privacy without appropriate obfuscation methods. If a grid participant uses a single public key, there are serious issues with maintaining privacy between transactions and their anonymity. While blockchain guarantees some level of anonymity, it is not absolute. Attackers can find creative ways of using stored blockchain data without even accessing a real-time network. A standard blockchain poses risks to users in this research's context and warrants more attention.

CONTENTS

1 Introduction **3**
1.1 Introduction . . . 3
1.2 Thesis Statement . . . 3
1.3 Context and Aim . . . 3
1.4 Objectives . . . 3
1.5 Significance . . . 4

2 Background and Literature Review **4**
2.1 Blockchain . . . 4
2.2 Blockchain for the Internet of Things . . . 5
2.3 Anonymity Concerns . . . 5
2.4 Related Works . . . 6
2.5 Time Series Classification . . . 7
2.6 Research Gap Identified . . . 7

3 Methods and Plan **8**
3.1 Research Overview . . . 8
3.2 Analysis Process . . . 9
3.3 Technical Frameworks . . . 10
3.4 Data Collection . . . 10
3.5 Data Analysis . . . 11
3.6 Project Management . . . 11
3.7 Project Timeline . . . 12

4 Research Results **13**
4.1 Populate Energy Grid Blockchain . . . 13
4.2 Transaction Classification Methods . . . 16
4.3 Adding Off-Chain Solar Data . . . 23
4.4 Obfuscation Techniques . . . 30

5 Conclusion **34**
5.1 Summary . . . 34
5.2 Limitations and Future Work . . . 34

6 References **35**

7 Appendix A - Additional Transaction Analysis Graphs **36**

8 Appendix B - Tabulated Results **38**

1. INTRODUCTION

1.1. Introduction

The massive growth in the Internet of Things (IoT) to collect, process, and send data via the Internet, requires a framework to handle all these devices. The IoT plays a role in many applications, for example, 'smart' devices in households, energy grids, and smart cities. Cost, efficiency, and security challenge centralised IoT systems as they grow. The IoT's large volume of information will need a decentralised approach [1], but user privacy and security challenges should be addressed.

Blockchain can handle this data as a decentralised ledger to record transactions carried out in a network. This is a developing field with wide potential uses. Applications include cryptocurrency, financial systems, smart contracts, and non-monetary areas such as IoT and smart grids. Blockchain creates a level of anonymity for users through cryptographic means using private and public keys (PK).

The level of user anonymity from a permanent ledger is not studied in-depth in an IoT setting, despite the growing use of blockchain. Studies on blockchain reveal malicious nodes can compromise user anonymity by classifying transactions using machine learning (ML) [2, 3] and off-chain data [3]. The project aims to contribute to the study of user anonymity in a smart grid using blockchain. It explores methods to deanonymise users using ML to analyse transactions [4] and include off-chain solar data [5].

1.2. Thesis Statement

The project will investigate user anonymity in blockchain transactions by using machine learning to classify households and their location. Off-chain solar exposure data will aid classification which can be compared to household energy production. The purpose is to link transactions to users and identify their 'ID' and location to deanonymise them. Obfuscation techniques to enhance a user's privacy are suggested and measured.

1.3. Context and Aim

Studies on blockchain reveal malicious nodes can compromise user anonymity. Such a node can link similar transactions and also use off-chain data, such as solar data. Research has not studied user anonymity in IoT blockchain in-depth, despite widespread use. Complexity is introduced by time-series data and linking transactions as unique public key use increases.

The project aims to determine how effective ML is in deanonymising users in a smart grid implementing blockchain. This should highlight long-term anonymity risks of blockchain by analysing permanent transaction and historic solar data. The research is limited to a smart grid setting and ML classification as the analysis method. It is also important to determine and measure methods to improve user anonymity.

1.4. Objectives

Objective 1: Populate blockchain ledgers from energy data.

- Source appropriate energy grid data.
- Convert to a blockchain format suitable for analysis.

Objective 2: Find the success rate of classifying blockchain transactions as specific users or locations.

- Measure the likelihood to link and classify a user's set of transactions.
- Investigate what classification models are effective.

Objective 3: Find the success rate when including off-chain solar data.

- Measure the likelihood to link and classify a user's set of transactions.
- Measure the likelihood a user's net energy export correlates with solar exposure data.

Objective 4: Investigate the effectiveness of techniques to improve user anonymity.

- Investigate methods to increase user privacy.
- Measure the effect of obfuscation techniques varying user public keys and ledger amounts.

1.5. Significance

Blockchain for IoT has attracted tremendous attention recently. A huge volume of personalised data will become permanently stored in blockchains. Thus, it is critical to study the anonymity of the users in IoT. Identifying users and linking them to transactions in a smart grid, not only reveals private information, but also information such as when a home is unoccupied.

This research is undertaken to achieve:

- A better understanding of risks in adopting blockchain for smart grids.
- Objective 2 will establish the likelihood an attacker can link and extract a user's blockchain data.
- Objective 3 will establish the likelihood an attacker's success increases using weather data.
- Objective 4 will analyse a range of privacy improving methods and measure their effectiveness.

The research is undertaken from an attacker's perspective on a smart grid using blockchain. The project involves trying to deanonymise households in the blockchain which a standard user would not attempt. The outcomes aim to benefit future users and ensure their privacy in an emerging technology.

2. BACKGROUND AND LITERATURE REVIEW

Literature from key areas of the project is reviewed to highlight key concepts, locate information required for analysis, and identify a research gap in section 2.6. First covered is background information about blockchain and its role in IoT and smart grids. Next discussed are similar prior works in user anonymity and privac. Last, relevant research is presented on machine learning classification techniques, particularly for time series data.

2.1. Blockchain

Blockchain is a framework to create a public and universal distributed ledger. Bitcoin introduced blockchain [6] as a transaction ledger to ensure auditability, immutability, and non-repudiation. Blockchain implements a method to reach consensus between unreliable parties. Whereas a standard process has a trusted third party (TTP), like a bank, responsible for transaction security. Blockchain properties remove the need for TTPs. Blockchains store ordered transactions in blocks linked to the previous block. Blocks contain a header, with a unique ID, and information [1]. Each block header stores the preceding block's hash to establish the links.

Network participants managing a blockchain are nodes or miners. They collate transactions into blocks to append to the blockchain. Networks use consensus algorithms to maintain trust and agreement to add a block. For example, Bitcoin uses a Proof of Work algorithm [6], and Ethereum Proof of Stake [7]. Transactions use encryption, hashes, and public key (PK) cryptography. Digital signatures encrypt a document hash, signed with private keys, and PKs prove who signed it [1]. Blockchain participants create anonymity with PKs concealing their identity. Changing PKs between transactions, as in Bitcoin [6], can improve user anonymity.

2.2. Blockchain for the Internet of Things

The IoT consists of physical devices connected to the internet which use communication networks to process data [1]. It makes devices 'smart' and gain computation and communication capabilities. Many devices cause large data traffic [8] and future applications could reach billions of devices [1]. Challenges for IoT devices include limited computing power, storage, bandwidth, and data bottlenecks. Blockchain can change how IoT networks operate with a decentralised framework [9, 10]. IoT networks could enjoy blockchain's lower costs, decentralised management, and inherent privacy [8]. A combination of IoT and blockchain looks to solve the challenges faced in IoT networks [10]. There are many IoT applications in daily life, businesses, and society, shown in Figure 1. Intelligent power distribution or smart grids are relevant to this project.

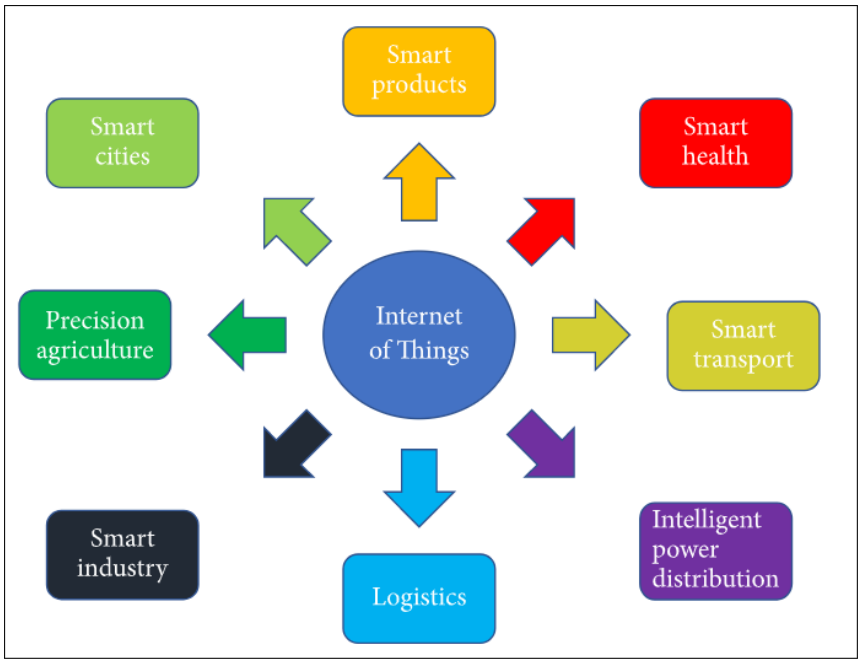

Fig. 1. IoT applications [1]

Energy systems and trading are developing with the benefits offered by the IoT [11]. Smart grids allow systems to communicate and optimise energy production, consumption [12], and thus utilisation [13]. They create the infrastructure to transfer energy between distributed producers and consumers. Some consumers can also be energy producers (prosumers) with solar energy [11]. Growing energy demand and supply has led to a desire for a decentralised energy system [14]. The authors at [11] highlight the challenges for such a system. First, managing transactions between users and the grid. Second, fluctuating supply from distributed renewable energy sources (e.g. rooftop solar). Third, TTPs lead to less efficient energy systems with more errors and operation costs. Blockchain is a likely path forwards to solve these issues in a smart grid [15].

Smart grids can decentralise behaviour using a blockchain framework. Blockchain and consensus algorithms can automate transactions and avoid TTPs. Other benefits can extend to real-time trading, anonymity features, and lower costs [16, 17]. The limits of IoT devices earlier are obstacles in implementing this system. The authors in [18] proposed a decentralised energy supply architecture which provided on-demand energy for miners in an IoT network using microgrids.

2.3. Anonymity Concerns

Using the IoT has many benefits but also increases exposure to new types of security and privacy threats. IoT issues go beyond standard information and privacy concerns as it can relate to people's physical lives and security. Privacy relates to the large amounts of personal data used by smart devices [1]. Likewise, smart grids will be complex networks, leading to privacy concerns [19] that need new approaches to solve [20]. Blockchains

can solve problems of centralised systems and increase resilience to failures and attacks [19]. This does not prevent new types of privacy risks. Blockchain anonymity research is primarily in digital currencies [21, 22]. Despite blockchain's attractive properties, further research is required into non-monetary IoT anonymity to create a trusted smart grid [19].

Blockchain users create auditability through PKs while maintaining anonymity. The purpose is to mask a user's transactions, purchases, or information [1]. Relevant to a smart grid would be a participant's energy purchasing amounts, and times. When a household is not consuming energy suggests the house is unoccupied. Privacy in blockchain should maintain transaction anonymity and have no ability to untie transactions [1]. Transaction anonymity means a transaction cannot be linked to a user, this is where different PKs are relevant. Untying transactions means transactions are not bound to user identities after routed through the network.

2.4. Related Works

We can apply ML approaches to a blockchain to investigate if user transactions are linkable. As noted earlier, blockchain users have PKs on transactions to achieve anonymity, with more public keys improving this. With supervised ML as suggested by [2], a malicious node could deanonymise a user by classifying transactions. An attacker can use the flow of inputs and outputs, to link user transactions. An attacker can attempt deanonymisation with real-time network traffic, but this research will focus on blockchain and historic solar data. IoT networks are subject to privacy risks around the exposure of user activity patterns from sensed data [2].

The authors of [2] concluded cryptocurrency studies show users can be deanonymised from transaction patterns stored on a blockchain. Their research analysed blockchain transactions in an IoT and smart home environment with ML to classify devices. They performed analysis as an informed and blind attacker on devices within a smart home. The attacker's aim was to link transactions to their type of smart device. For example, identifying which transactions belong to a smart lock, thus inferring when an owner leaves their home. They populated a blockchain from real-world smart home network traffic. The attack method monitored device transaction and used ML to compare with known patterns of potential devices. Results showed an informed attacker being up to 90% accurate, and a blind attacker around 30%. This indicates a serious risk in the privacy of devices using the blockchain. [2] also proposed methods to improve user privacy in the IoT blockchain. Three timestamp obfuscation methods reduced successful device classification by up to 30%. The techniques were combining several packets into one transaction, merging ledgers, and adding random transactions delays. We can draw parallels between [2] and this project where smart devices become smart homes and we investigate the pattern of energy over time, as opposed to frequency.

Authors at [22] suggest an attacker in a multiple PK scenario needs to create a one-to-many mapping between users and addresses. The analysis process suggested by [22] involves three stages. First, create a transaction graph of the blockchain transactions flow where PKs are the inputs and outputs. Second, create an address graph from the transaction graph to find the flow of payments between PKs. Last, show a user graph with the users and each PK that may belong to the same user; drawn from the previous information and blockchain heuristics. [23] used a full blockchain analysis to link users to public addresses.

For ML with unsupervised approaches, [3] is an example of clustering blockchain addresses. Clustering is a valuable method for ML problems [24], related to splitting data into groups. [3] takes a clustering approach to blockchain transactions and also off-chain data. Their scenario showed successful clustering of information, with off-chain data improving the accuracy. Clustering household energy patterns may show similarities between households located nearby.

[25] developed a method to deanonymise blockchain transactions using supervised machine learning to predict new entities. They perform multi-class classification to categorise a cluster of transactions. They use decision trees with random forest and gradient boosting algorithms. This paper has parallels with this project which

categorises transaction sets to households in a smart grid.

The authors of [26] desired an approach to compare weather data and power generation. They introduced linear and nonlinear time models for solar intensity prediction. This method will be useful for the project when comparing solar data to a user's energy production. Additionally, [27] explores techniques to convert daily solar data into hourly information by modelling a standard day's spread. This is important as the project's solar data was only available at daily resolution.

A work relevant for the obfuscation part of the project is [28]. The authors propose a privacy-preserving and data aggregation scheme. This will be useful for potential obfuscation techniques as they discuss dividing users into separate blockchains (ledgers) and using multiple PKs to protect a user's identity. There are similarities in the nature of these methods with [2].

2.5. Time Series Classification

Classification problems with orderable data can be treated as a time series classification (TSC) problem [29]. Researchers have investigated many methods to classify time series data [30]. Popular are nearest neighbour classifiers with a distance function if appropriate [31]. [31] shows an ensemble of classifier's outperforms the individual components. These approaches use either an ensemble of decision trees (random forest) [32] or an ensemble of different types of discriminant classifiers [33].

[29] gives an overview of potential deep learning applications for TSC. The authors found for univariate and multivariate data, the top three types of networks were residual (ResNet), fully convolutional (FCN), and multilayer perceptron (MLP) networks. The MLP is a traditional form of deep neural networks and was proposed in [34] as a baseline architecture for TSC.

Random forest is a decision tree machine learning approach used by [35] and [25] for TSC. The authors of [35] compared different decision tree approaches for TSC. They found support vector machines performed poorly and favoured ensembles for optimal accuracy. The better performing ensembles were MultiBoost and AdaBoost.M1. However, random forest performed similarly well and is favoured on larger datasets. This project will use neural network and decision trees options.

Correlation and cointegration are statistical approaches to compare time series. This is relevant for the project's comparison of household energy transactions to solar data. The authors in [36] investigated how to optimise wireless sensor networks in environmental monitoring. They used a statistical approach to cointegrate sets of time series data to select the optimal number of sensors. This was successful showing only 25% of the original sensors were not cointegrated. In particular, [36] describes an analytical framework to analyse multivariate time series data as required in this project.

2.6. Research Gap Identified

Research in blockchain user anonymity is developing and uses both transaction and off-chain analysis. Despite widespread usage of blockchain in IoT, user anonymity level is not yet studied thoroughly. The literature investigated shows research into IoT implementations of blockchain and some into the privacy, usually Bitcoin focused. The combination of machine learning analysis on stored data in the smart grid context is a new contribution. Privacy concerns abound as smart grids develop and it is important to understand the risks before storing user data on a permanent and public ledger.

3. METHODS AND PLAN

3.1. Research Overview

Figure 2's flow diagram provides an overview of the starting smart grid blockchain context, high-level research process, and desired outcomes. The analysis stages are further detailed in the following sections.

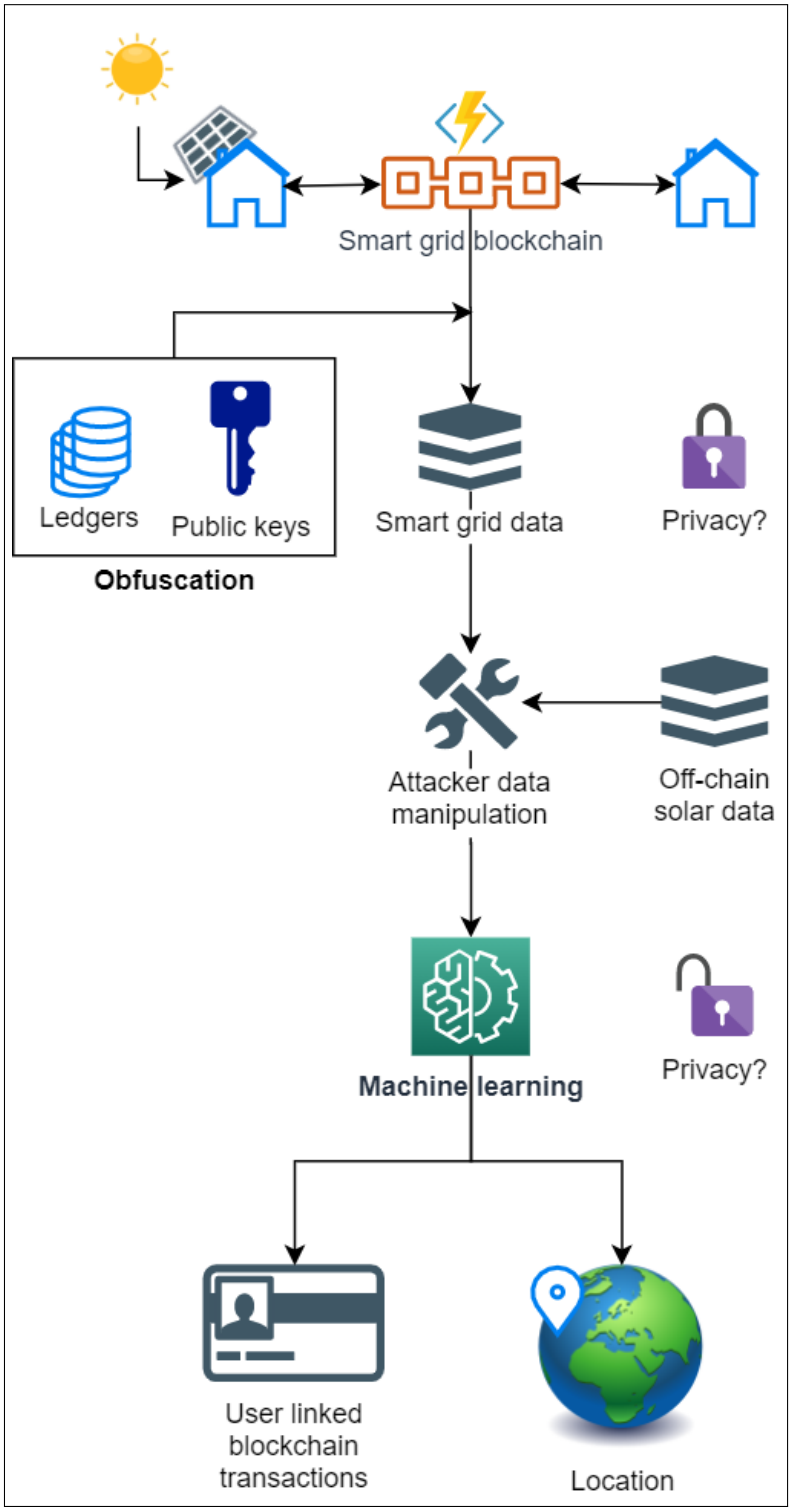

Fig. 2. Research context and overview

3.2. Analysis Process

Figure 3 breaks down the analysis process into five stages. It covers the objectives required to address the thesis statement from section 1.4. The figure is followed by a more detailed approach.

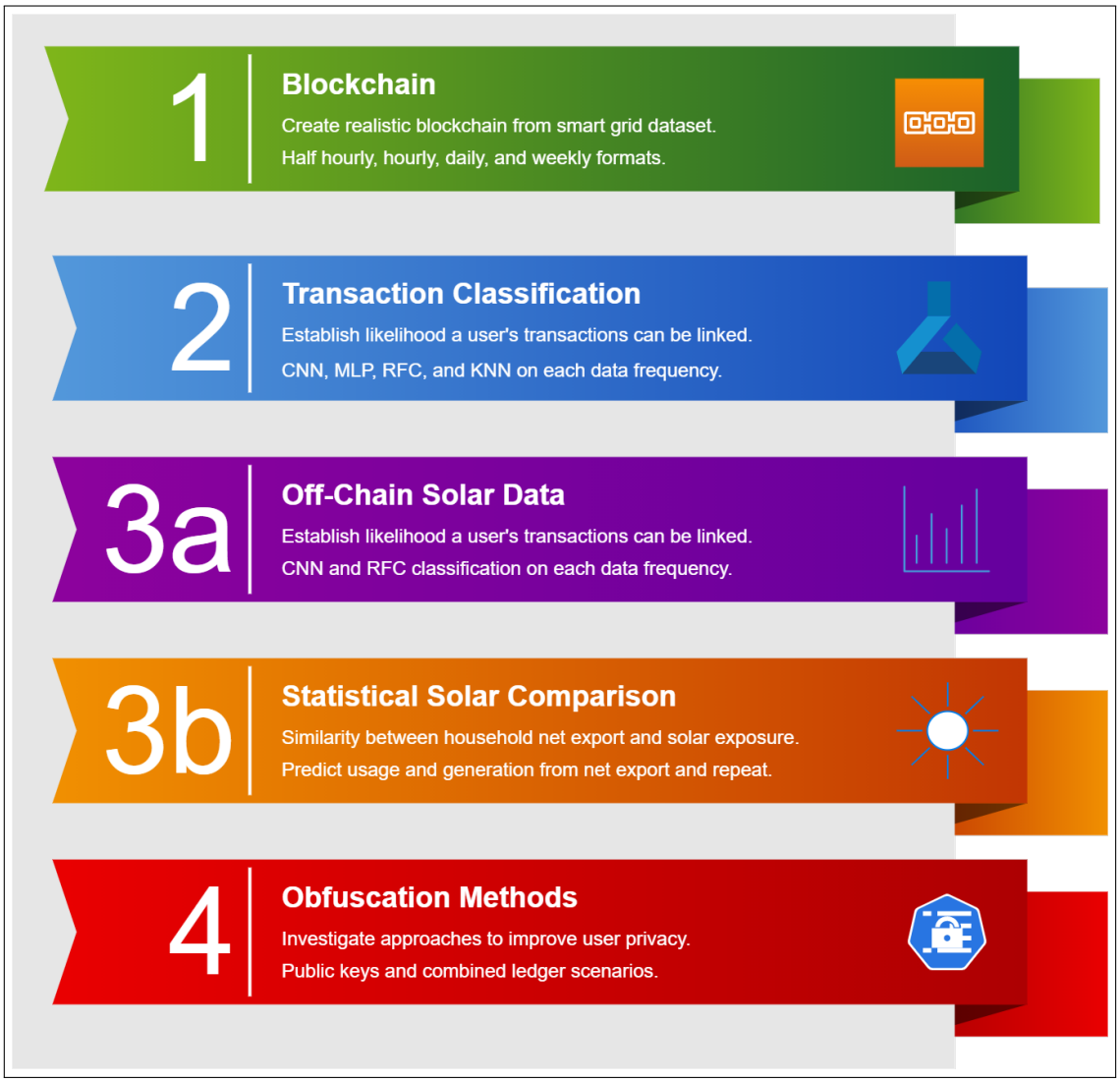

Fig. 3. Key phases

1. Background information and literature review on relevant papers for:
   (a) Blockchain-based IoT, smart grid and energy trading.
   (b) Privacy concerns in IoT blockchain contexts.
   (c) Machine learning classification techniques.
2. Source an appropriate energy dataset. It should contain a reasonable number of customers with energy use and solar energy production. As well as information that distinguishes user locations.
3. Convert energy data into blockchain ledgers for objective one.
4. Perform machine learning analysis on blockchain transaction data for objective two.
   (a) Test a variety of classification models.

(b) Apply to classifying transactions by customer or location.

(c) Measure with respect to transaction frequency.

5. Investigate attacker benefits from including off-chain solar exposure data for objective three.

   (a) Combine user datasets with historic solar exposure data to increase attacker accuracy.

   (b) Apply machine learning classification as in objective two to measure an attacker's benefit (3a).

   (c) Perform statistical comparisons between user net energy export and solar data directly (3b). Also, predict user energy usage and generation from net export and measure improvement.

6. Suggest and evaluate methods to improve user anonymity for objective four.

   (a) Measure improvements in privacy as consumers use additional public keys.

   (b) Measure improvements in privacy as additional ledgers are mixed.

7. Deliver progress and final project reports.

3.3. Technical Frameworks

- Analysis techniques:
  - Classification with decision trees and neural networks.
  - Correlation and cointegration.
- Python (3.8):
  - Data manipulation: Pandas (1.1.0) and NumPy (1.18.5).
  - ML: Scikit-learn (0.23.1) and Keras (2.4.3) with TensorFlow back end (2.3.0).
  - Graphing: Matplotlib (3.3.0) and Seaborn 0.10.1.

3.4. Data Collection

Past energy use and generation data is sourced from Ausgrid solar home electricity data [4]. It contains Australian household data where households are prosumers. The data set has half-hour data from 1 July 2010 until 30 June 2013 for 300 households across New South Wales. It includes energy consumption (on and off-peak) and generation. All households have a full data set and Ausgrid performed quality checking. Other datasets found such as [37] include fewer households making anonymity hard to study and are not situated in Australia with available solar data from the Bureau of Meteorology.

A blockchain will be populated with transactions corresponding to the energy use and generation of households in the dataset. Different blockchains were made with transaction frequencies of per week, day, hour, and half-hour. The highest frequency is half-hour periods the data provides. Each energy use period will be treated as a communication between a smart meter and the grid. Thus, the process will generate a transaction for each period per household. Assumptions for this process will include:

- Real-time network traffic is abstracted out. The focus is on attackers with access to permanently stored transaction information.

- Blockchain algorithms such as consensus algorithm are not required and will assume to pass each transaction. Patterns of transactions are not reliant upon these blockchain steps.

A single node will act as a miner collecting all transactions until reaching the blocksize. Then the miner creates a new block appended to the ledger. ML models analyse the datasets to deanonymise households to achieve objective two. Relevant off-chain data is added for the third research objective. Ausgrid data provides postcodes for each household and therefore historical data from the Bureau of Meteorology at [5] is easy to source and is accurate.

3.5. Data Analysis

Each phase of the project will perform a similar ML analysis on the acquired data. The project will use Python frameworks to perform mainly classification. Python and the required libraries listed in 3.3 are freely available and suitable.

The method will have an 'attacker' training machine learning models locally and measuring the ability of these models to predict users and their location. The next stage will use further classification and statistical approaches to link a user to the most similar solar data set. The last stage investigates obfuscation methods to increase resilience against ML attacks used. Likely suitable will be increasing public key counts and mixing ledgers.

3.6. Project Management

To prepare this project, the key research questions, objectives, and outcomes were detailed to highlight the focus of the project. A literature review was completed to reinforce the project direction and goals. This was extended to develop reasoning behind the selected classification methods implemented. A break-down of the phases of the project defines the necessary order of work in Figure 3 earlier. These processes will aid to ensure the project is completed in manageable sections and with appropriate quality control and testing. Each step shows the main research and investigation activities required.

3.7. Project Timeline

Figure 4 provides an overview of the project timeline with all planned progress complete.

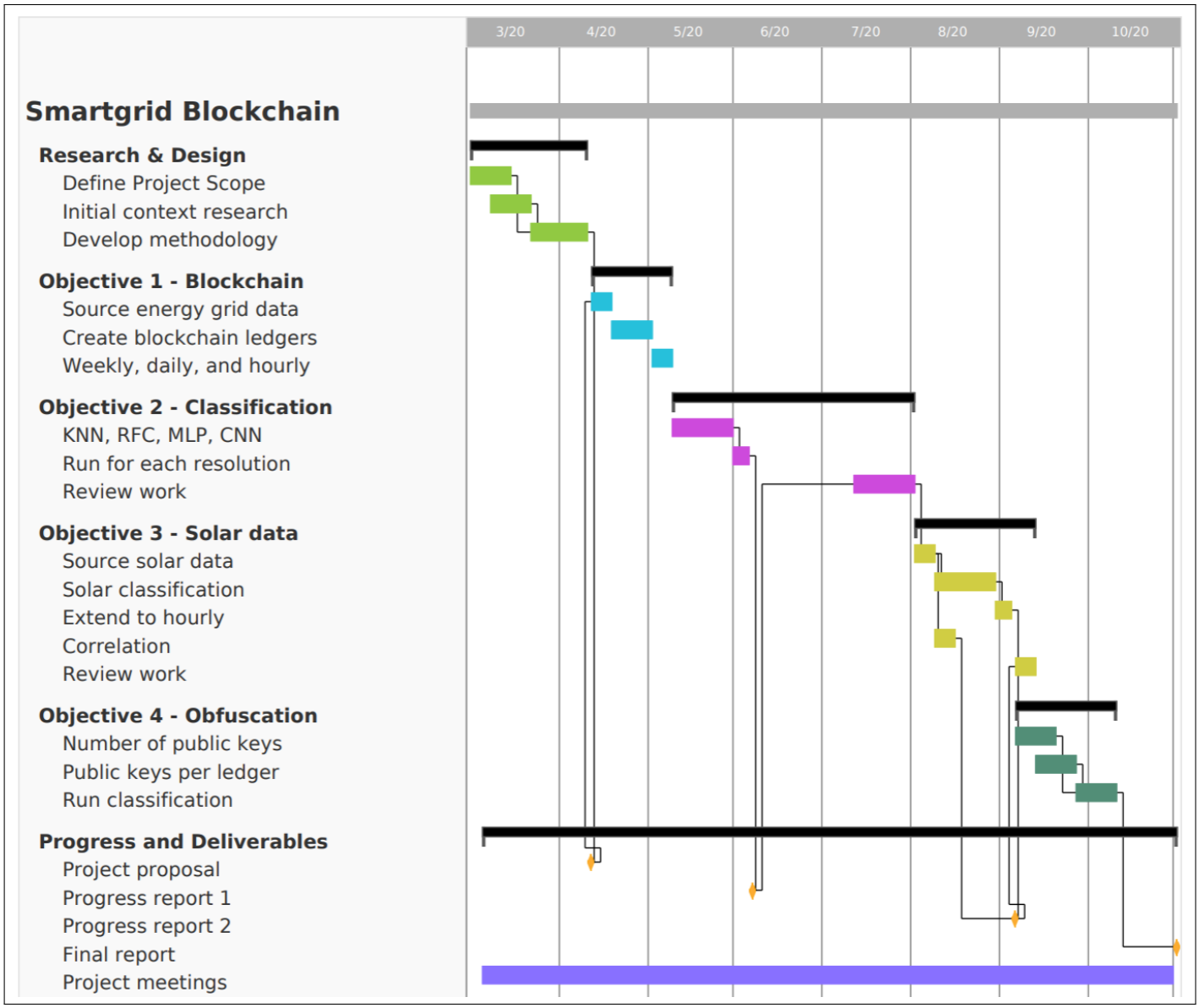

Fig. 4. Project timeline and progress

4. RESEARCH RESULTS

4.1. Populate Energy Grid Blockchain

Energy grid data

The first objective was to source appropriate energy data and prepare appropriate blockchains. Ausgrid energy data [4] was found and evaluated to suit the project. It contains all the information desired to complete the research. The following Table 1 shows a sample of the dataset.

Table 1. Example original energy data

Customer	Generator	Postcode	Type	Date	0:00	0:30	1:00	...	23:30
1	3.78	2076	CL	01/07/2013	1.250	1.244	1.256	...	1.081
1	3.78	2076	GC	01/07/2013	0.303	0.471	0.083	...	0.068
1	3.78	2076	GG	01/07/2013	0	0	0	...	0

This dataset contains the energy use and solar production of 300 households over three years. The data frequency is in half-hour blocks which is nice from the perspective of creating blockchain transactions of a reasonable resolution. Each day a household's data is split into off-peak consumption (CL), general consumption (GC), and gross solar generation (GG). Additional features are the household generator size and postcode. Generator sizes range from 1kWh to 10kWh systems, but average low in this range at 1.68kWh. This is a key driver of energy production and useful to have available. Important are the user ID and postcode attributes allowing classification analysis from data to predict user or location (aided by off-chain data). Solar exposure data by area, in the time period of the energy data is available at [5] and discussed in section 4.3.

Wrangle energy data

Sourced energy data needs to first, be wrangled into a suitable format for time series classification, and second, have the required features of blockchain ledgers added. This section describes the process to populate a blockchain from the energy data with various options. Visualisations of the dataset are provided and used to explain how a household can be 'fingerprinted'. An attacker is able to use transaction timestamps, values, and PK information to link data for each and possibly between PKs in the blockchain.

The data was manipulated into a time series format with a date-time column removing the separate attributes for each time period. This allows each blockchain ledger row to represent one transaction. Blockchains were produced with different transaction time frequencies; half-hourly, hourly, daily, and weekly. Larger transaction periods may more distinctly identify users, and work against overfitting, however, there is far less data to identify a user. At this stage, the three years were left separate and 0 amount values kept. Table 2 shows a sample of the rearranged data.

Table 2. Example wrangled energy data

Customer	Postcode	Type	Datetime	Amount
1	2076	CL	01/07/2013 0:00	1.250
1	2076	GC	01/07/2013 0:00	0.303
1	2076	GG	01/07/2013 0:00	0
1	2076	CL	01/07/2013 0:30	1.244
1	2076	GC	01/07/2013 0:30	0.471

Create blockchain ledgers
The energy data is now suitable for creating blockchain ledgers. There will be four transaction types:

- Genesis transaction → First transaction for a ledger or public key.
- On-peak consumption (CL).
- Off-peak consumption (GC).
- Solar energy export (GG).

Adding several features is required to populate the blockchain. Each transaction has a hash (of its content) included as an identifier, and the previous transaction's hash to create a chain. Also each household signs transactions they generate with a PK. This produces the following structure of a transaction:
Hash | Previous Hash | Public Key | Timestamp | Transaction Type | Amount

In the initial stages of the investigation, three classification ledger scenarios are considered:

- One ledger per customer (LPC).
- One ledger per postcode (LPP).
- All one mixed ledger (AOL) with unique public keys per transaction.

First, ledger per customer allocates each customer's transactions to a separate ledger. Second, ledger per postcode groups households in the same postcode to a ledger but are still differentiated by their PKs. These two scenarios will have one PK per customer, representing limited security measures for a user. Last, with one fully mixed ledger and unique PKs per transaction is a difficult case for an attacker. Neither of these are realistic but will produce a bound of expectations. Realistic and privacy increasing (compared to best case) variations of ledgers and public keys will be analysed under objective four, obfuscation techniques. Households using a single public key is possible, but has a drastic reduction in privacy and is unlikely. On the other hand, new public keys require genesis transactions which cost the PK holder, thus a new PK per transaction is unlikely.

Table 3 shows a sample format of a created blockchain ledger. Note, customer ID and postcode are removed from the classifier training and test sets.

Table 3. Example blockchain ledger

Hash	PHash	PK	Customer	Postcode	Type	Datetime	Amount
Genesis		PK_1	1	2076	CL	01/07/2013 0:00	1.250
a	Genesis	PK_1	1	2076	GC	01/07/2013 0:00	0.303
b	a	PK_1	1	2076	GG	01/07/2013 0:00	0
c	b	PK_1	1	2076	CL	01/07/2013 0:30	1.244
d	c	PK_1	1	2076	GC	01/07/2013 0:30	0.471
e	d	PK_1	1	2076	GG	01/07/2013 0:30	0

Data Visualisation
It is important to understand trends in the household energy patterns. Figure 5 shows the pattern of energy use and generation of four customers over an example day. Figure 5 brings two key insights. User consumption more clearly distinguishes users, and all customers have a similar solar generation trend (expected from day/night cycles) but magnitude depends on generator capacity. Customers shown, 37, 59, 102, 226 have solar

capacities of 1.5, 2.8, 2.0, and 1.5kWh respectively. This explains why customer 59's production is greater.

Figure 6 shows the same household's consumption by day across the data. It is observed again consumption is a much better 'fingerprint' of a user's transactions. Trends, peaks, and troughs provide distinguishing features amongst these consumers. The generation is also more distinct in this view than the single day in Figure 5.

Figure 7 shows the consumption of the same consumers by week across the data. This view is quite similar to Figure 6 sharing many features, but with less fine variations and noise. While this visually looks to distinguish users easier, lost detail and reduced data is important, as section 4.2 will show.

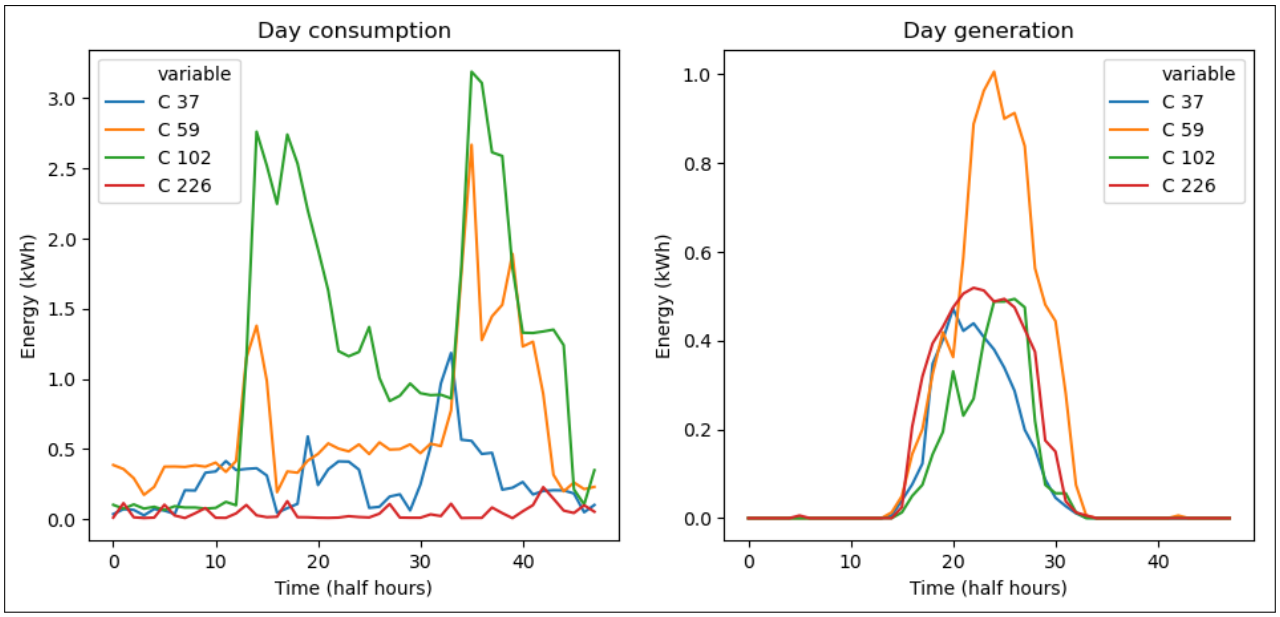

Fig. 5. Energy pattern of four customers over a random single day

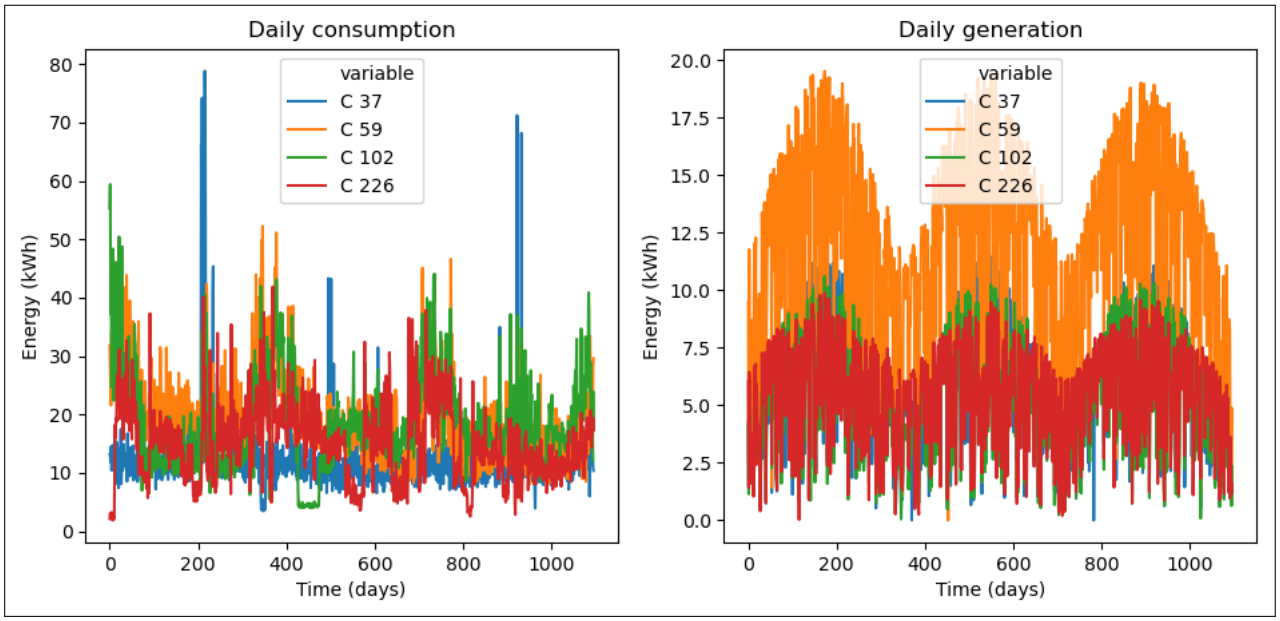

Fig. 6. Energy pattern of four customers by day over three years

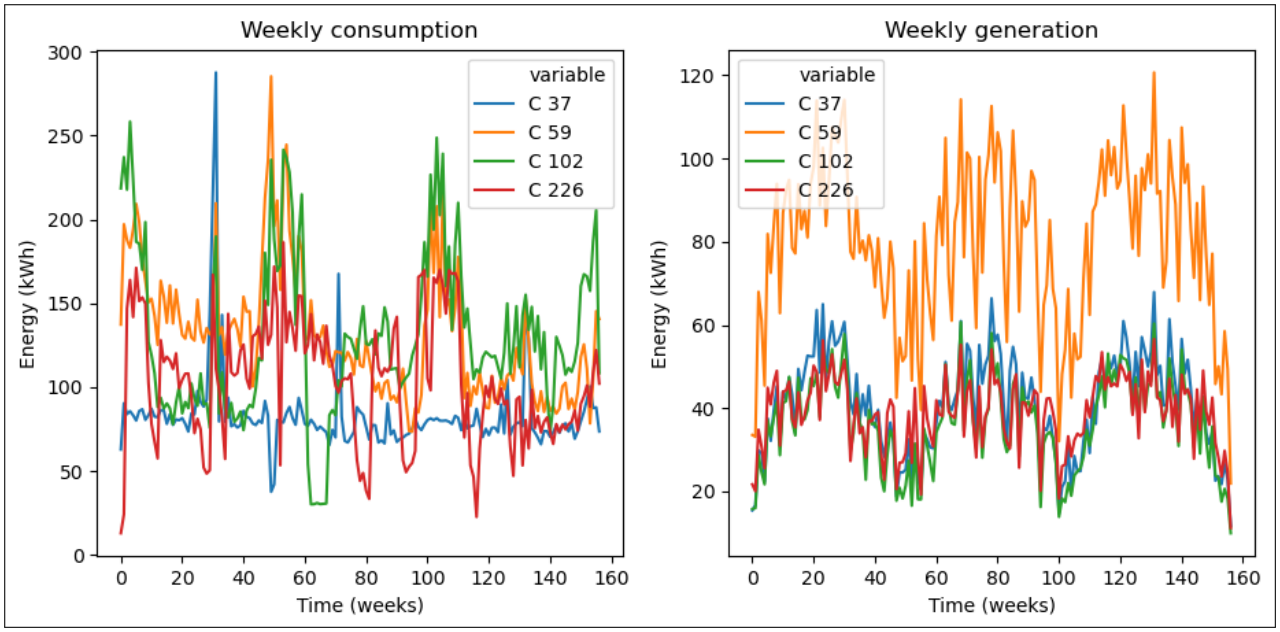

Fig. 7. Energy pattern of four customers by week over three years

4.2. Transaction Classification Methods

Objective two aims to show an attacker's classification attempts on the blockchain before including off-chain solar data. Attackers can construct a set of a user's energy transactions by linking transactions emerging from the same PK and those with statistical similarity. This provides a time series which can fingerprint a user's energy consumption and generation. The visualisations indicate consumption is likely more important than production to classify users in this stage. Solar generation, however, will matter more for objective three in section 4.3 when off-chain solar data is added. With a set of user transactions, an attacker may be able to first, continue to link transactions to a user as an ongoing privacy risk, and second, potentially reveal household location with off-chain solar data.

Selection of classifiers

The classification methods implemented include two decision trees and two neural networks:

- K-nearest neighbours (KNN).
- Random forest classifier (RFC).
- Multilayer perceptron neural network (MLP).
- Convolutional neural network (CNN).

The goal is to predict a category and the dataset has labelled data, thus classification is used over clustering. The dataset is not text based and a Stochastic Gradient Descent (SGD) or KNN classifier is suitable. A KNN classifier was selected as a simple baseline approach, initial testing easily outperforming a SGD model.

Section 2.5 discussed decision trees for time series classification (TSC). Random forest was an effective option, especially for large multivariate data like this project. Section 2.5 also covered suitable deep learning networks for TSC. CNN models were reported best in the main paper discussed, and MLP networks also suggested effective and may generalise larger multivariate data well.

Analysis approach

An overview of this section's analysis process is laid out in Figure 8 and is followed by additional provided.

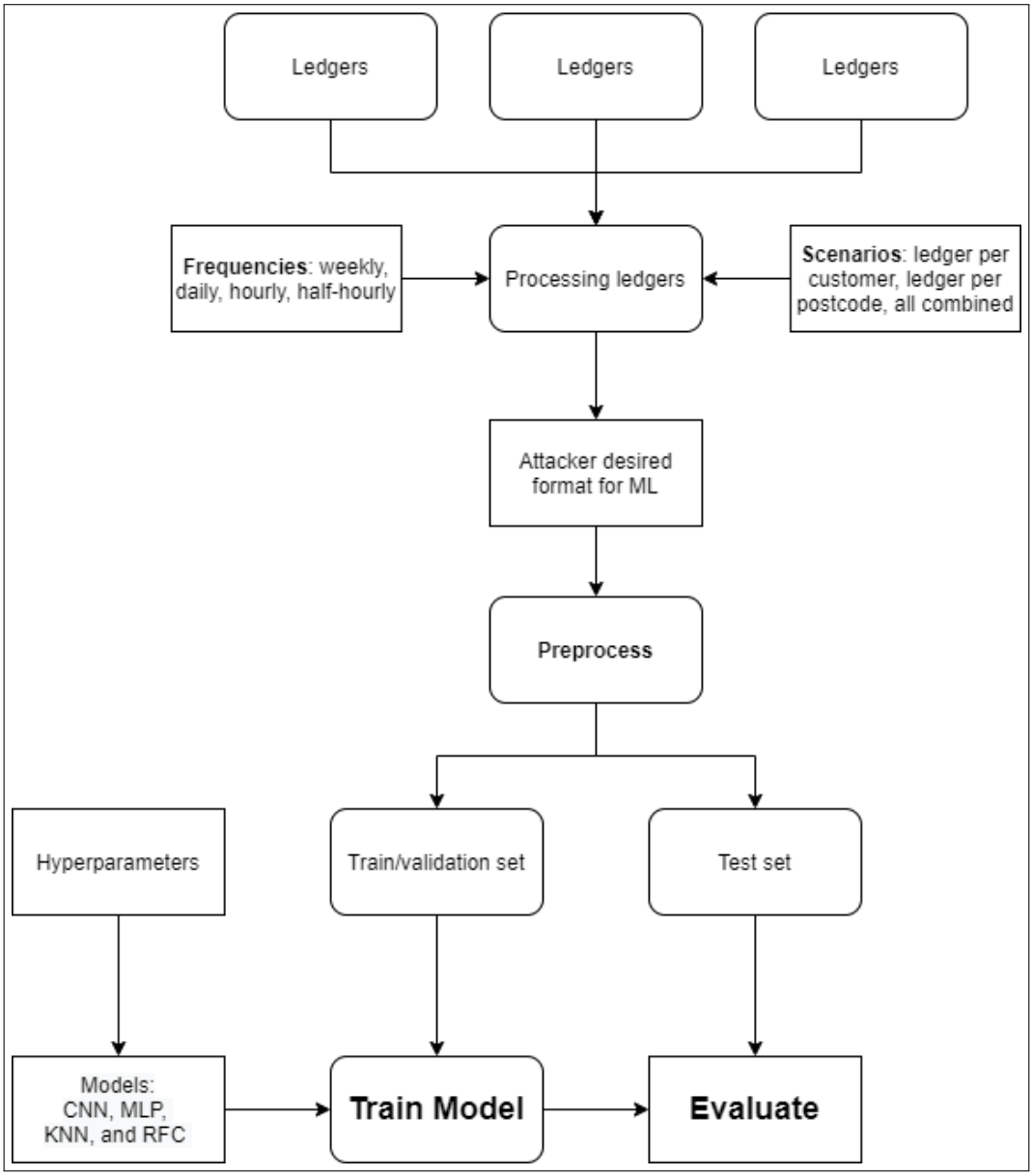

Fig. 8. Classification analysis approach

1. Preprocess data:
   (a) Categorical data made numerical and scaled.
   (b) Random train (includes validation) and test sets (80/20) constructed. Customer, postcode, and generator dropped from train and test sets to leave only the blockchain data.
   (c) Zero energy amount transactions removed as these would not create transactions.
   (d) For the one ledger case PKs are made unique and ledgers combined.
2. Run each classifier for weekly, daily, hourly, and half-hourly transaction time frequencies to predict:
   (a) Customer: i) Ledger per customer (LPC), ii) Ledger per postcode (LPP), iii) All one ledger (AOL)
   (b) Postcode: i) Ledger per customer (LPC), ii) Ledger per postcode (LPP), iii) All one ledger (AOL)

3. Evaluate overall classifier accuracy. For the best model, top-5 accuracy will be measured.

4. Iterate model performance to tune hyperparameters for greater accuracy.

Transaction Classification Results

This section presents the results of the analysis outlined above. The best results were achieved by the CNN classifier, as suggested by literature. The results are presented in Figures 9, 10, and 11 separated by ledger scenarios previously listed. This allows easy comparisons of the classifiers and a discussion of each will follow. Appendix A contains graphs which separate the results by classifier and Appendix B has tabulated results.

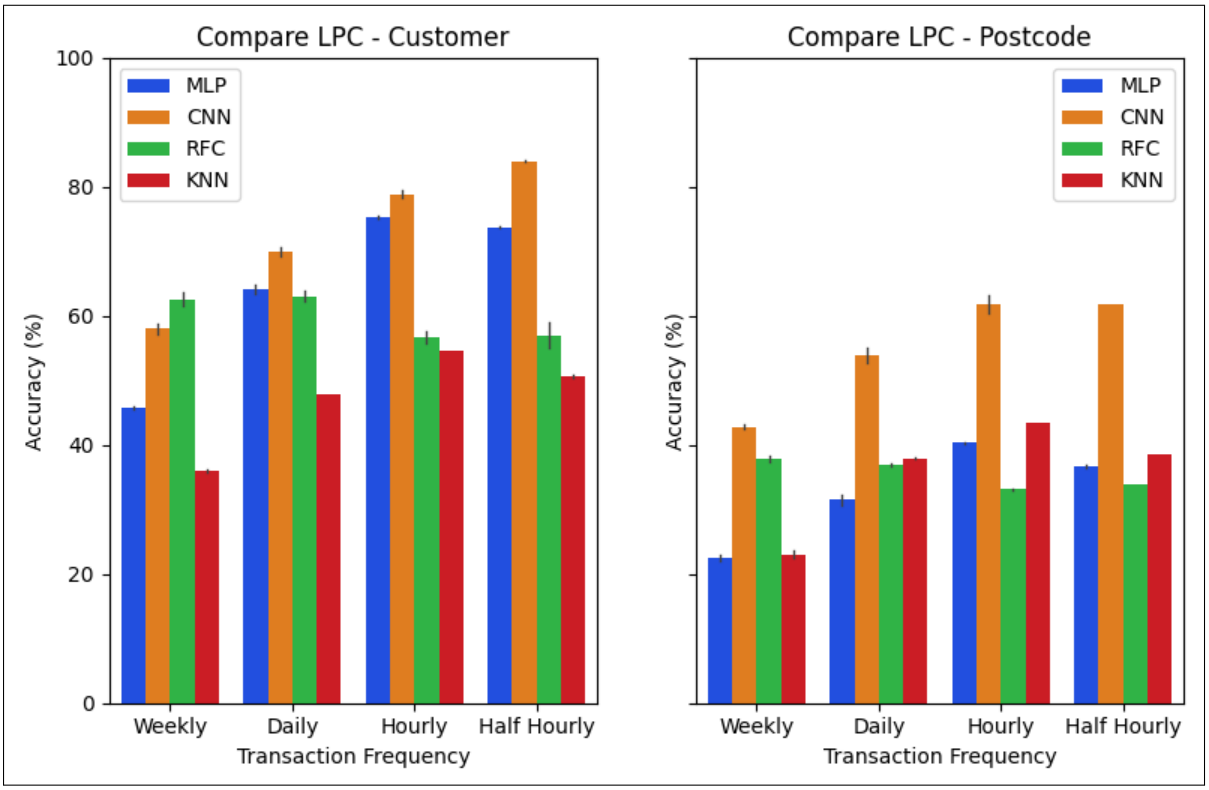

Fig. 9. Comparison of classification models on ledger per customer (LPC)

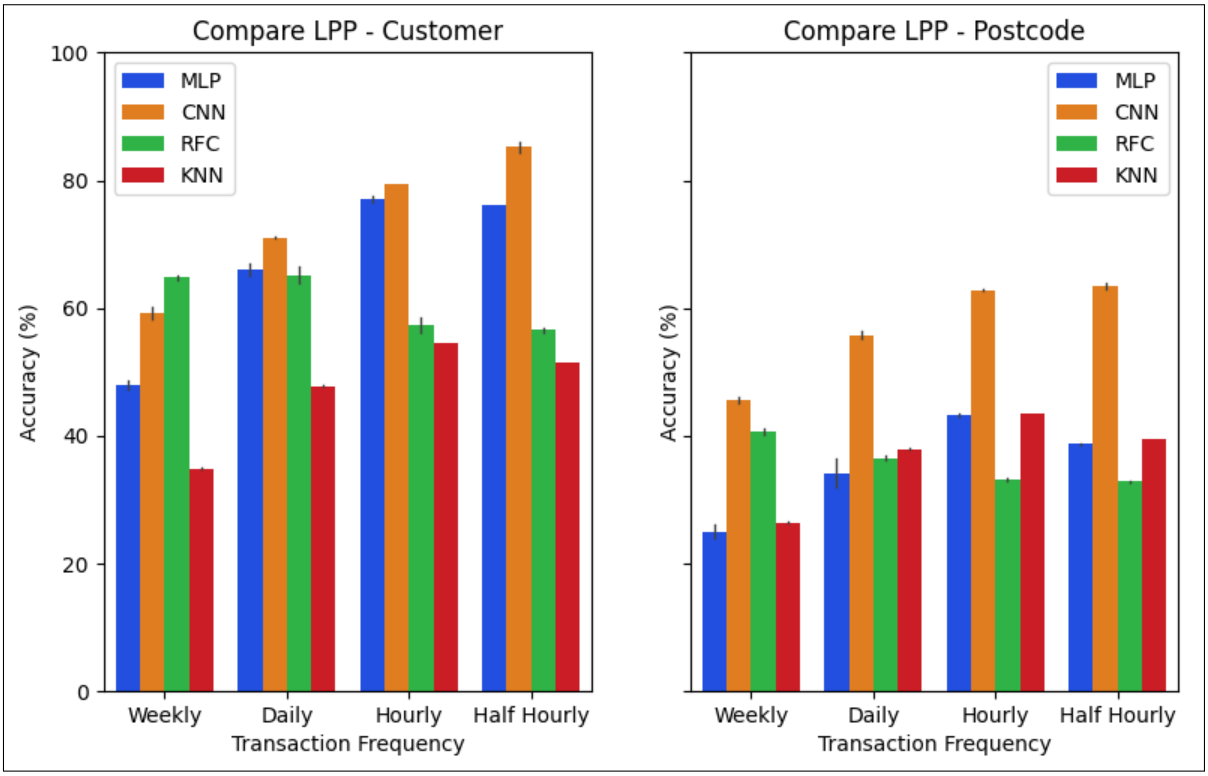

Fig. 10. Comparison of classification models on ledger per postcode (LPP)

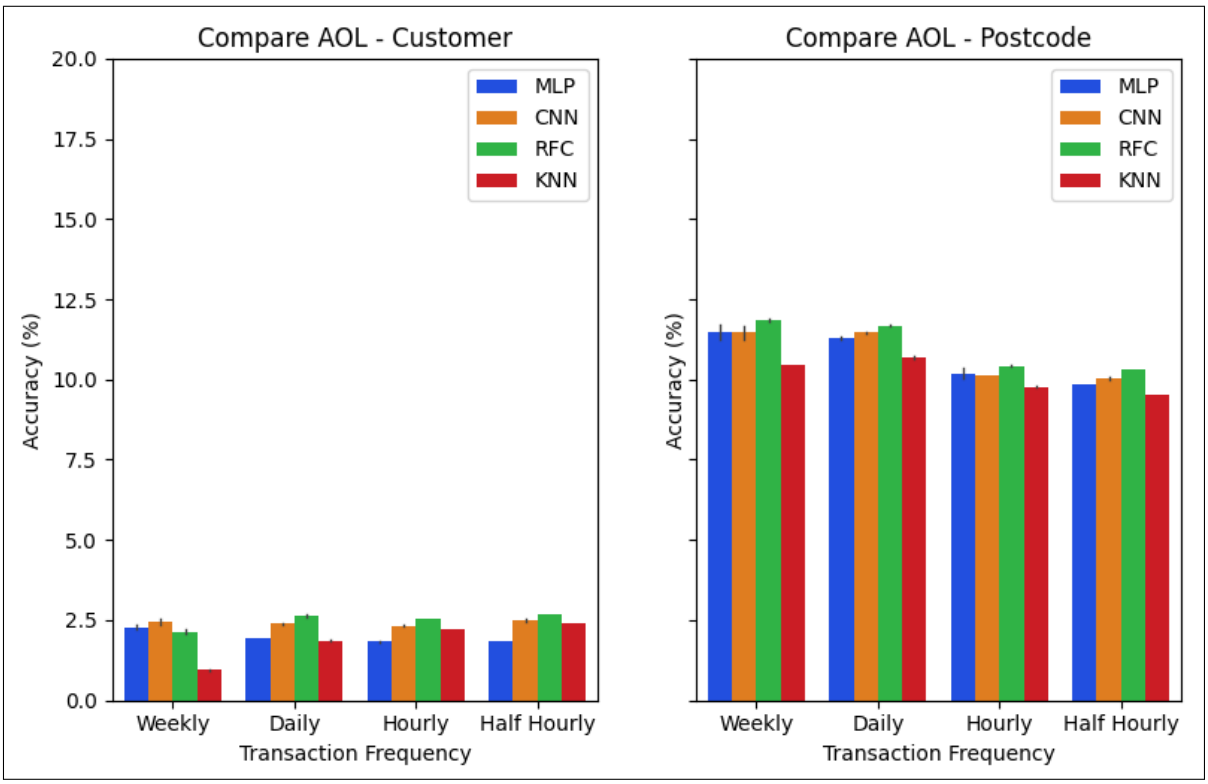

Fig. 11. Comparison of classification models on all one ledger (AOL)

K-Nearest Neighbours
A KNN was implemented first as a baseline classifier and had the least accurate predictions. The results show a maximum accuracy of 54% for customer and 43% for postcode classification on hourly transactions. This is an average and for example was 95% for predicting customer 138 but also 0% for a several users. These results are a promising starting point and were achieved after tuning the model 'k' value. Initial tests using $k = [1, 50]$ found the best results for customer classification with $k = 3$ and postcode classification $k = 2$.

There was no notable difference in performance between the LPC and LPP scenarios for the KNN model. In the mixed ledger case, customer and postcode predictions dropped to at best, about 2% and 11% respectively. A large decrease in accuracy is expected, however, the KNN model also performed worst here. An important trend in the results is the increase in accuracy as the time frequency increases to hourly, but drops at half-hourly. This smallest transaction frequency perhaps begins to mask consumer patterns, and overfitting occurs.

Random Forest Classifier
Next a RFC was implemented and the results are slightly better than the KNN as expected for an ensemble classifier. The best accuracies are 65% (customer) and 41% (postcode) on weekly data. The performance pattern is quite different as the model performs better with larger transaction frequencies. Weekly is the most accurate with it decreasing with each reduction in time period. Performance is better in the LPP scenario, which is reasonable as this ledger setup actually provides additional information. Users remain distinct by their PK but some grouping of users that share postcodes is known. The RFC mixed ledger case results are the best of all the models which may be important in later obfuscation tests.

An RFC classifier can provide the feature weights used by the model. The weights were similar in all tests and are 70% reliant on PK/ledger information, 20% on transaction amount, and 10% on transaction type. This seems reasonable as once a group of transactions is identified as a user, the remainder can be classified by sharing a PK. Changes in these weights will be interesting when PK numbers are varied.

Hyperparameters were tuned over test runs to establish better performance. The parameters considered were the number of trees, maximum tree depth, and the maximum features to consider when splitting. 100 trees were allowed to run till pure, unless memory limits were reached, with the square root of data attributes used for maximum feature splitting. The RFC results are a promising improvement as the neural networks are favoured by literature to perform best.

Multilayer Perceptron
The MLP classification results improve upon the RFC model significantly in the separate ledger scenarios. The results have a maximum accuracy of 77% (customer) and 43% (postcode) on hourly data. The LPP scenario slightly outperforms the LPC as similarly explained for the RFC model. Also the KNN pattern of accuracy loss at half-hourly data has occurred but to a lesser extent. The model struggles with the one ledger case and performs worse than both decision trees.

The results are averages and for example, 72 customers were classified with 100% accuracy, but also ten with 0%. This large range of outcomes is described by large standard deviations. For example for customer classification average standard deviations are 35%, 30%, and 10%, respective to LPP, LPC, and AOL scenarios. The spreads were slightly lower in more accurate transaction frequency tests.

The MLP model generally ran until convergence, but was limited to 1000 iterations. Hyperparameters tuned for the MLP model were the number of hidden layers and neurons per layer. Testing found best performance with three hidden layers of 10 neurons. Overall the MLP results are accurate and trend towards better accuracy with higher transaction frequency (until overfitting).

Convolutional Neural Network
The CNN classification model achieved the best results of all the methods by significant margin, except for the mixed ledger where the RFC outperformed it slightly. The results have a maximum accuracy of 85% (customer) and 62% (postcode) on half-hourly data. The CNN is the only model which improves with every increase in transaction frequency, including the half-hourly data. In particular, the CNN significantly outperforms other models in predicting postcodes, while only somewhat for customer outperforming the MLP. The one ledger case is handled similarly to the other models, perhaps signifying the neural network advantages, clear in the LPC and LPP scenarios, will lessen when more PKs and other obfuscation techniques are used.

Hyperparameters tuned for the CNN model were the filter size, batch size, and number of epochs. 128 was used for the filter and batch sizes, while 100 epochs were run for each test. Additionally, the CNN construction uses two 1D convolutional filters, and tested several optimisers and measures of loss for the best performance.

Top-5 accuracy tests were run for the CNN, as an attacker could rank several likely options to aid deanonymisation attempts. For the daily and hourly time frequencies the top-5 accuracy results are in table 4. This will be compared to a similar table after adding solar data in section 4.3. The results show almost perfect predictive power in the single PK (LPC and LPP) scenarios, and accuracy three-five times greater than overall accuracy for the mixed single ledger. These levels of accuracy show an attacker's chances at linking a user's transactions far above acceptable without obfuscation techniques. The top-5 accuracy is quite high even for the mixed ledger scenario and more sophisticated obfuscation may be required.

Table 4. Top-5 CNN accuracy

Frequency	Predictor	LPC	LPP	AOL
Daily	Customer	>99%	>99%	9.0%
	Postcode	97.7%	96.7%	30.2%
Hourly	Customer	>99%	>99%	9.4%
	Postcode	98.5%	>99%	30.5%

Accuracy Measures
The provided results are the average of three experiments. They include error bars to indicate one standard deviation of spread for each bar. This points out the decision tree results are far more stable than the neural networks. Their error bars are shorter and sometimes not visible. The error bars are still small for the neural networks results. Therefore, the variability in results is not an important factor.

The results are measured by accuracy, a measure of all correct classifications. Alternative measurements are precision, recall, and the F1-score. The F1 score is the harmonic mean of precision and recall and gives a measure of incorrectly classified cases. Measuring true positives and negatives favours accuracy, whereas measuring false positives and negatives favours the F1 score. This F1 score penalises extreme values across the classes. Accuracy is also chosen when the class distribution is similar while F1-score is a better metric for imbalanced classes. The accuracy measure is used as all classes are of equal importance and size in the dataset. Plus this analysis does not false positives and negatives higher than true. Experiments were run to measure F1 score alongside accuracy, however, the results were highly similar. F1 accuracy was always within several percentage points of the accuracy measure, as expected with equally balanced classes.

Overall Comparison
The CNN model performs the best on the data, especially for postcode prediction, and handles the more frequent data well. However, the RFC handles the low information single ledger scenario best and should

continue to be considered. Most models trend towards better accuracy at more frequent transaction data, except can overfit at half-hourly. Throughout, LPP results outperform LPC as PKs still separate customers but additional postcode grouping information is provided. This will be interesting to see how it varies as PK numbers are changed.

Guesswork should expect average accuracies of 0.33% for customer and 1% for postcode (approximate as not evenly distributed). This is relevant for the low accuracy predictions in the AOL scenario. However, when the models perform well above this accuracy it does not follow predicting postcode should outperform user ID.

Overall machine learning models can quite accurately link user transactions from past blockchain data when users take limited steps to protect their privacy. More frequent transactions aid an attacker, as does using separated ledgers, whether by users or postcodes. The next section will highlight attackers can do even better by including off-chain solar data before considering user privacy enhancing measures.

4.3. Adding Off-Chain Solar Data

Section 4.2 highlighted the high risk attackers can classify and link a user's energy transactions. Users can take measures to reduce this likelihood, but first we will consider an attacker adds off-chain solar data to increase their success rate. The physical nature of solar generation means off-chain solar exposure (or other weather) data may have similarity to household production and help distinguish users. Solar exposure data can be split into areas over a smart grid and added as a feature to classification analysis. It can also be be statistically compared to user energy transactions directly. The following outlines the analysis approach, sourcing and processing the solar data, and then discusses the results. Solar classification tests use the CNN and RFC models established previously as performing well in the scenarios.

Analysis approach

An overview of this section's analysis process is laid out in Figure 12 and is followed by additional detail.

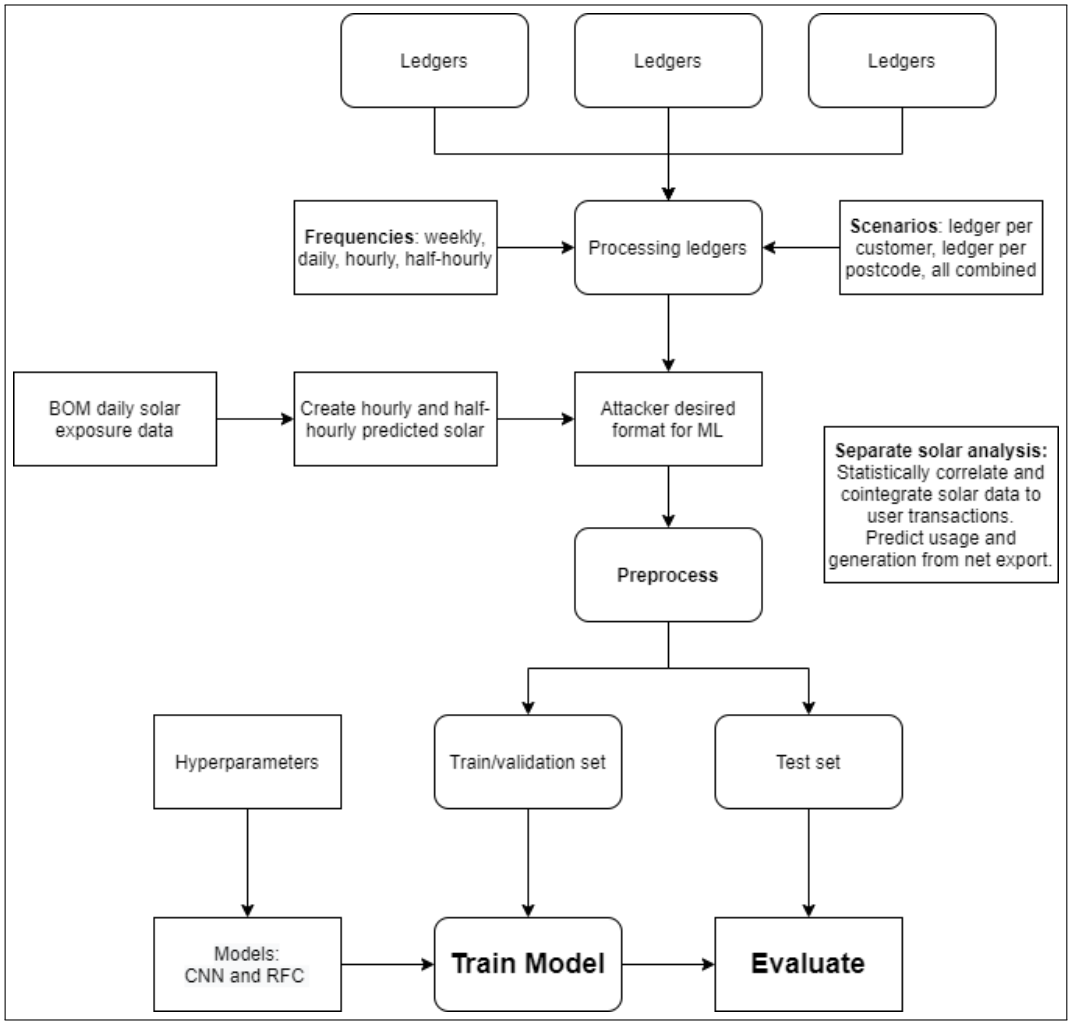

Fig. 12. Solar analysis approach

1. Source solar exposure data for each postcode from the Bureau of Meteorology at [5]. This provided daily data available at a high frequency of locations.
2. Generate approximate hourly and half-hourly frequency data from the daily solar data.
3. Add time series solar exposure as a new feature to the dataset.
4. Run classification tests with CNN and RFC models:

(a) Preprocess data as described by section 4.2's analysis approach.

(b) Run each classifier for weekly, daily, hourly, and half-hourly transaction frequencies to predict:

i. Customer: i) Ledger per customer, ii) Ledger per postcode, iii) All one ledger

ii. Postcode: i) Ledger per customer, ii) Ledger per postcode, iii) All one ledger

(c) Evaluate overall classifier accuracy using the same hyperparameters as section 4.2. For the CNN model, top-5 accuracy will be measured.

5. Statistically compare household data sets to each region of solar data. This helps show support for whether solar data should be beneficial to the previous analysis.

(a) Correlate and cointegrate each household's net export to all solar data sets.

(b) Use regression analysis to predict a household's solar generation from usage.

(c) Correlate and cointegrate each household's gross solar generation to all solar data sets.

Solar data

Historic solar exposure data was sourced from the BOM at [5] for each postcode in the original energy data. Other weather data is available but the analysis is limited to the most relevant for solar energy production. The original data contains 100 unique postcodes across the 300 households and one set of off-chain data was collected for each. This process required determining the closest weather station to the centre of each postcode. All except three regional postcodes had a weather station within 5km but they are also larger areas far from others. Several inner city postcodes do share the same closest weather station but this should have limited impact. All weather stations have solar data for the 2010-2013 time period required and Table 5 shows an example of the solar data format.

Table 5. Example solar data

Year	Month	Day	Daily global solar exposure (MJ/m*m)
2010	7	1	9.9
2010	7	2	4.4
2010	7	3	10.6

The solar data was only available in a daily format as more frequent data is only available at limited locations. Therefore, a polynomial estimation approach discussed in [27] mentioned in section 2.4 was implemented. This uses a day's total solar exposure from the datasets and splits it into hourly or half-hourly pieces. Daily analysis can directly use the data sourced and weekly sum up the preceding seven days.

Solar Classification Results

This section presents the results of analysis with added solar data outlined above. The best results achieved were in line with section 4.2. The CNN model performs best in the LPC and LPP cases, with solar data slightly improving accuracy as expected. While the RFC model again achieved the best results in the AOL scenario also improved by the solar data. The results are presented in Figures 13, 14, and 15 separated by ledger scenarios. This allows comparison of the classifiers and a discussion of each will follow. Appendix B contains tabulated results of the presented graphs.

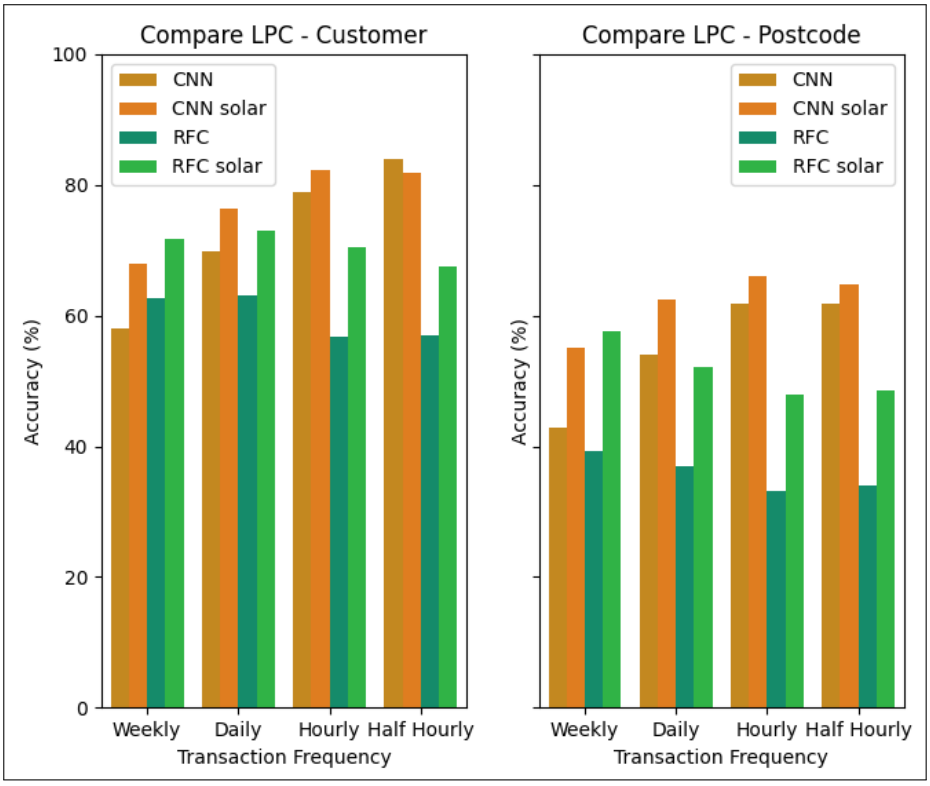

Fig. 13. Comparison of solar classification models on ledger per customer (LPC)

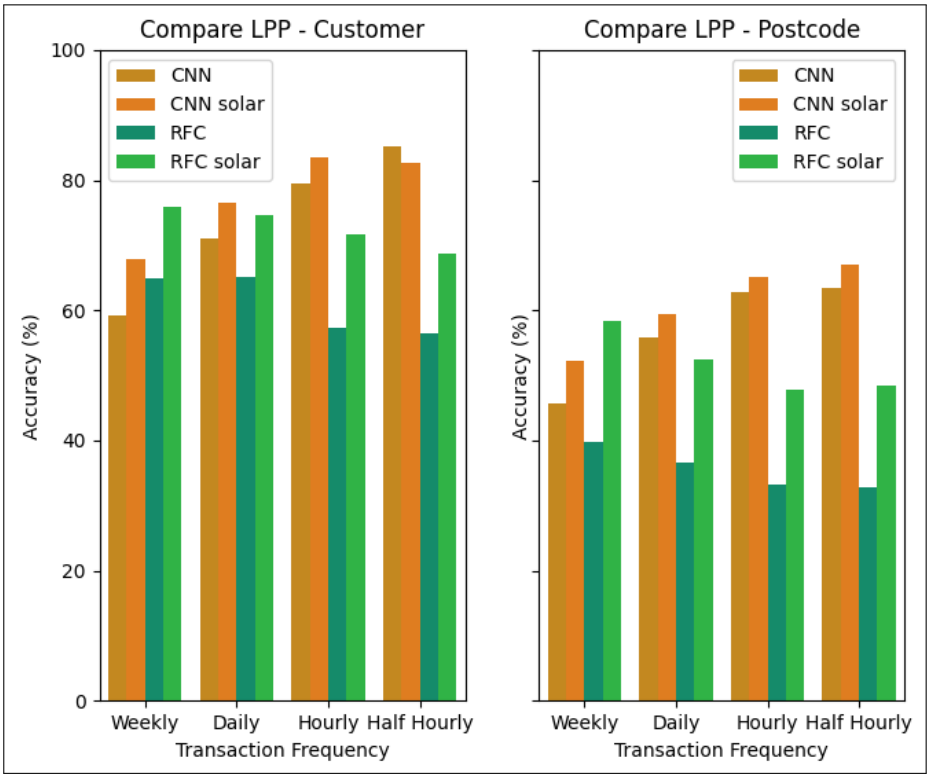

Fig. 14. Comparison of solar classification models on ledger per postcode (LPP)

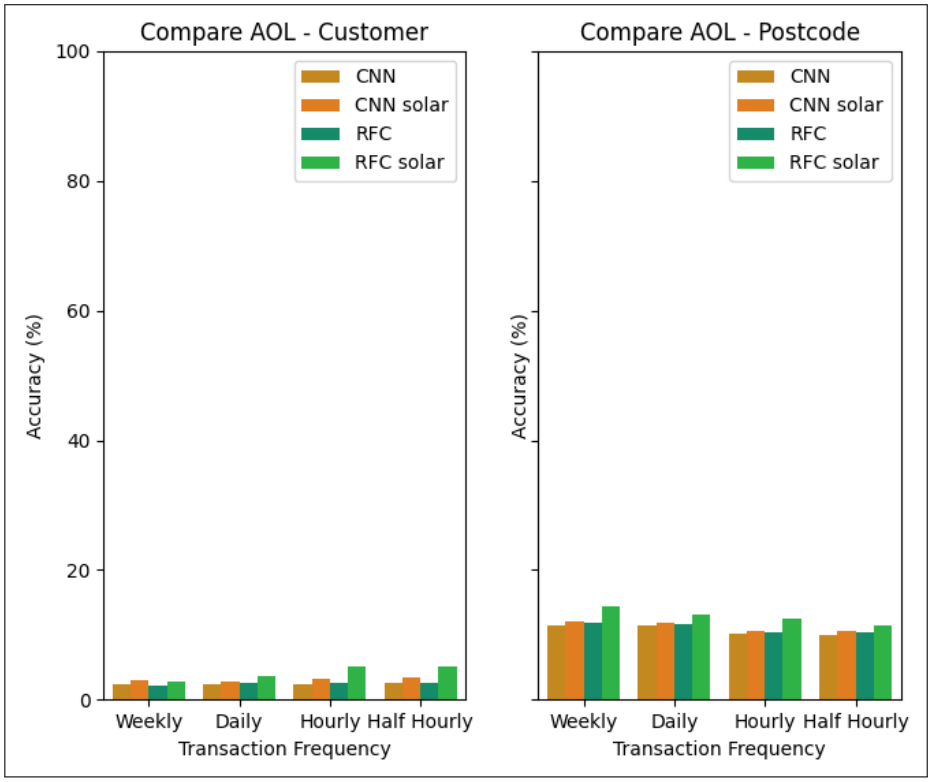

Fig. 15. Comparison of solar classification models on all one ledger (AOL)

Random Forest Classifier

The RFC was run first and the best accuracies are 76% (customer) and 58% (postcode). The results show an improvement in all cases and frequencies. The downward trend as frequency increases for LPC and LPP remains. The improvement on postcode prediction is greater than for customer in all scenarios. This is expected as the solar data supports location prediction better. The model placed a 5% weighting on the solar data and used the same parameters as section 4.2.

Convolutional Neural Network

The CNN accuracy also increased in all cases and frequencies with the inclusion of solar data. The best results of the tests run are 84% (customer) and 66% (postcode). The increasing trend as frequency increases for LPC and LPP remains. The improvement on customer and postcode predictions are even, unlike the RFC which benefited more in postcode prediction. The CNN handles the one ledger case similarly to the RFC, perhaps signifying the neural network advantages, clear in the LPC and LPP scenarios, lessen when using more PKs and obfuscation techniques. Table 6 shows the top-5 accuracy predictions and the deltas to the equivalent table in section 4.2. Improvements here can only be seen in the one ledger scenario and these were small.

Table 6. Top-5 CNN daily data with solar accuracy

Frequency	Predictor	LPC	LPP	AOL
Daily	Customer	>99% (0%)	>99% (0%)	11.0% (+2.0%)
	Postcode	97.7% (0%)	>97.6% (+0.9%)	31.7% (+1.2%)
Hourly	Customer	>99% (0%)	>99% (0%)	11.5% (+2.1%)
	Postcode	>98.7% (+0.2%)	>99% (0%)	30.5% (0%)

The energy data set provides gross generation measured by the solar meter. However, in a blockchain energy trading environment, sale transactions would contain energy exported. Energy exported would be gross generation less household use of their own production. Classification results would likely benefit from energy export (over generation) as it would better uniquely identify users and avoid the daily generation for same kWh system sizes being highly similar. The following section will investigate statistical similarity between net export and solar data but also how this can be improved by predicting solar generation from net export.

Solar Statistical Comparison

To support the solar data providing the classifiers helpful information, correlation and cointegration statistical tests were run. This will first compare household net exports statistically with daily solar data. Second, predict with regressors a household's energy usage (and thus also solar generation as the difference) from their net export. Third, perform the statistical analysis again with the new predicted values.

For each household, energy production transactions are taken and compared against all 100 solar data sets with correlation and cointegration. The time series are of the same length across the three year period of the original energy data. After a household's production is compared to each region's solar data, they are ranked using the correlation coefficient or cointegration t-statistic. The rank of the correct postcode of the household under analysis is taken as the score for each measure.

Analysis on household net exports produced the following values in Table 7. The average ranks are out of 100 and show limited correlation and no cointegration predictive power. Figure 16 shows the distribution of correlation ranks and seem random with a slight favouring of higher ranks. At first, this simple correlation of solar data to user net energy export does not seem to aid classification. However, if a user's energy usage and thus solar generation could be reconstructed from their net export, this should increase.

Table 7. Solar exposure correlation and cointegration to net export

Measure	Mean Rank	Stdev	Median	Mode
Correlation	42.87	29.59%	39	3
Cointegration	53.28	30.35%	55	22

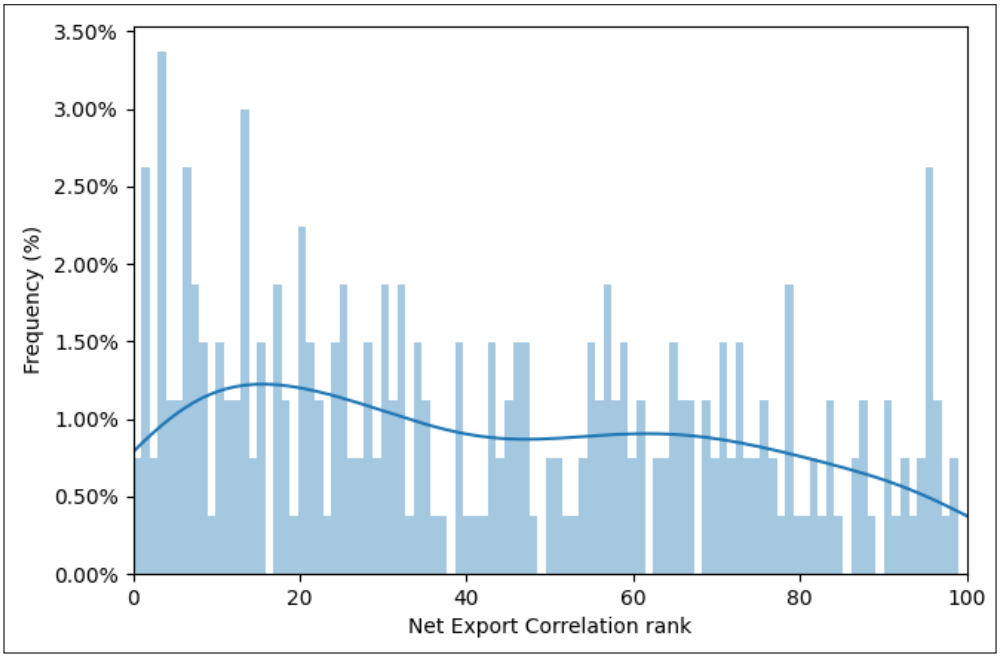

Fig. 16. Correlation distribution

The next stage of the statistical comparison is to improve the results by predicting energy usage and solar generation from net export. This is done with three regressors trained on past data. This process involved removing any transaction without any solar production, otherwise accuracy is misleading as net export equals the inverse of usage when no production occurs. The chosen regressors were a linear, random forest and multilayer perceptron (similar to those used in section 4.2). Table 8 shows the analysis accuracy results.

Table 8. Regression results

Regressor	RMSE	R2
Linear	0.1571	70.53%
Random Forest	0.1240	81.66%
MLP Regressor	0.1113	85.07%

The regression models establish there is strong predictive power in splitting a user's usage and generation from net export with some history. The MLP regressor performed best as the most complex model, achieving 85% R^2 accuracy. Now the earlier statistical comparison will be performed again with the predicted split data from the MLP regressor.

Table 7 shows the analysis results from analysing the predicted household energy production . The average ranks are out of 100 and show some correlation and no cointegration predictive power. The distribution of correlation ranks are in Figure 17 and show a strong skew towards highly ranking the correct postcode of a household. However, the distribution has a large spread of results, making it less useful in many cases. Overall this simple correlation of solar data to user energy production shows solar data should be expected to aid the earlier classification.

Table 9. Solar exposure correlation and cointegration to gross generation

Measure	Mean Rank	Stdev	Median	Mode
Correlation	26.18	27.17%	17	1
Cointegration	56.09	33.90%	64	-

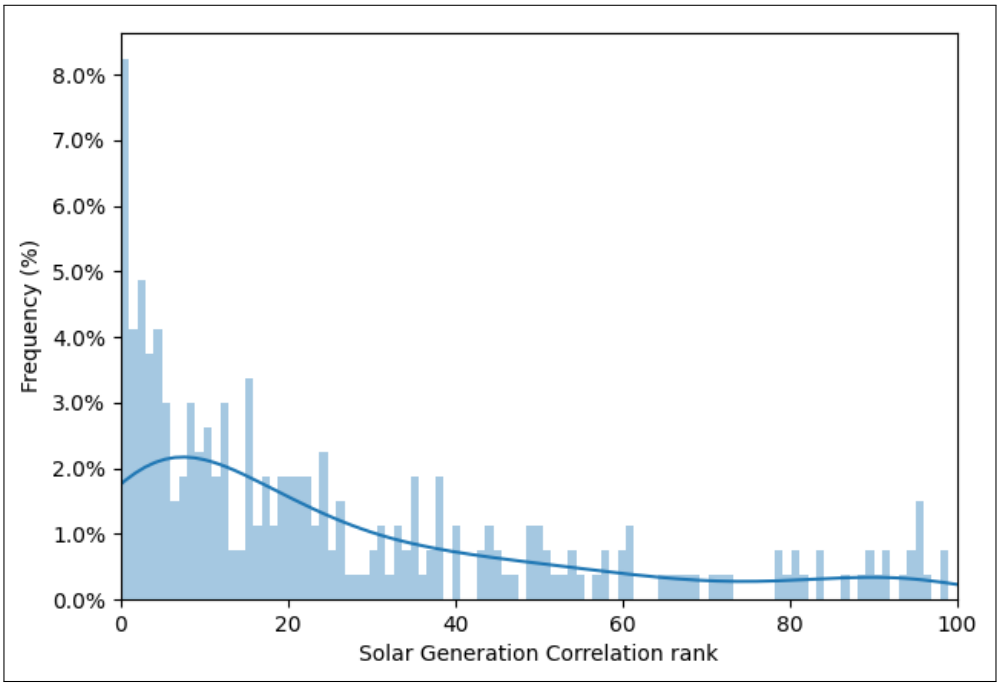

Fig. 17. Correlation distribution

The machine learning models are consistently improved by including additional solar data which has some correlation to a household's energy production. This aids in both cases where users take limited steps to protect their privacy and also the mixed ledger scenario. The next section will suggest and measure approaches for users to reduce these success rates, without requiring the expensive process of a new PK every transaction.

4.4. Obfuscation Techniques

Section 4.3 highlighted attackers can enhance their classification attempts by adding off-chain solar data. Users can take measures to reduce this likelihood as the previous sections involved only three scenarios. Two of which a user took no additional privacy steps, and the third (AOL) an excessive amount. First, users can split up their linked transactions with extra public keys. However, these come at a cost to balance with benefit. Second, the blockchain itself can mix public keys together on ledgers instead of leaving them separate. The following outlines the analysis approach, generating new obfuscated blockchains, and then discusses the results. The same previous classification models will be used, however, focused on half-hourly data, where an attacker performs best.

Analysis approach

An overview of this section's analysis process is laid out in Figure 18 and is followed by additional detail.

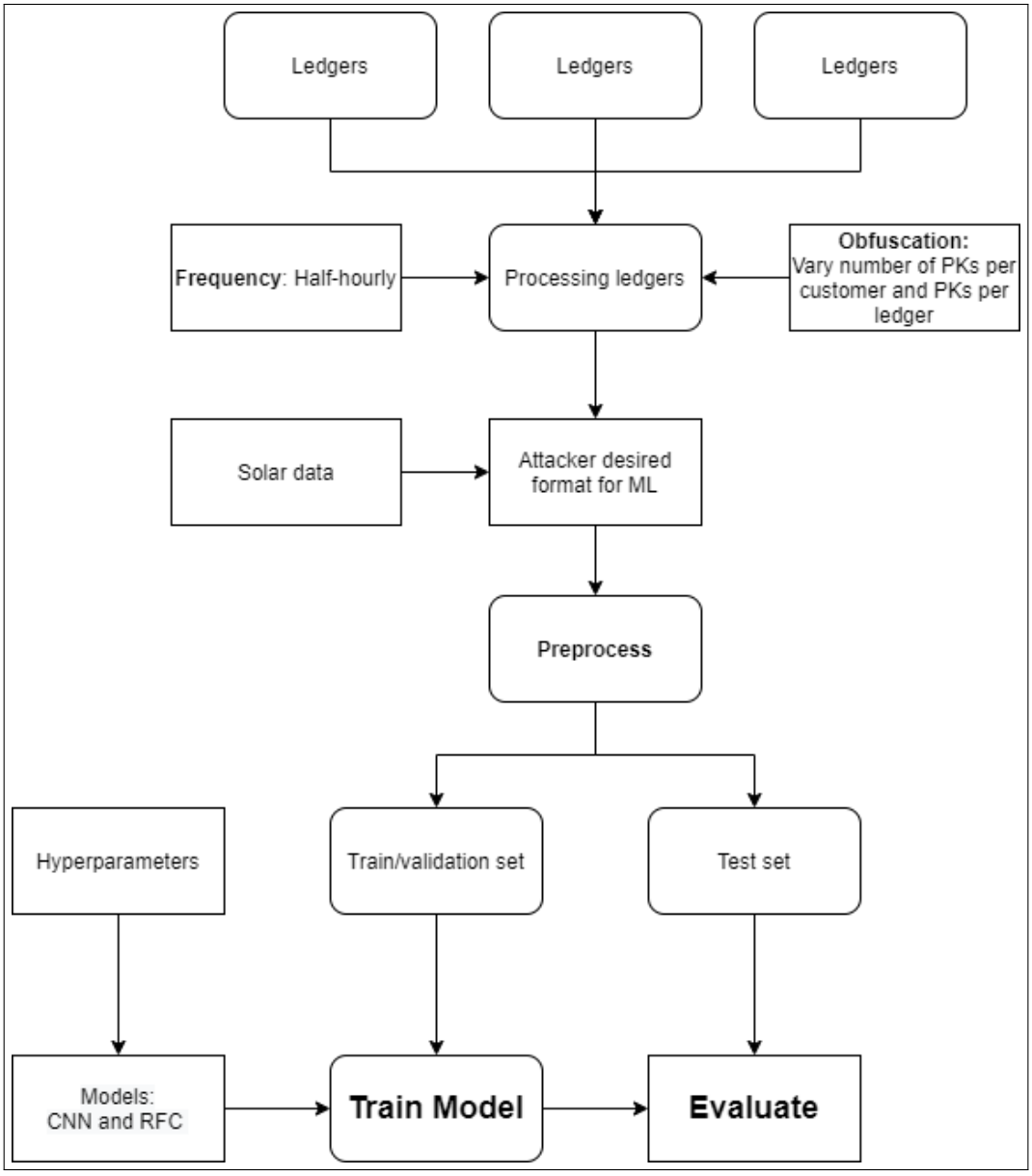

Fig. 18. Obfuscation analysis approach

1. Generate obfuscated blockchain ledgers with desired variations.
2. Vary number of PKs per customer: 1, 2, 5, 10, 20, 50, and n. Where n is unique PK per transaction.
3. Vary number of PKs per ledger. 1, 2, 5, 10, and 20.
4. Run classification tests with CNN and RFC models:
   (a) Preprocess data as described by section 4.2's analysis approach.
   (b) Run each classifier for half-hourly transaction frequency to predict:
      i. Customer
      ii. Postcode
   (c) Evaluate overall classifier accuracy using the same hyperparameters as section 4.2.

Obfuscation Results

New blockchain datasets were generated for each combination of PKs per customer and PKs per ledger listed above on half-hourly data. Scenarios with one PK are already analysed by the LPC case as combining ledgers is irrelevant when customers have only one PK. The same classification analysis from section 4.3 is applied which includes the solar exposure data. The next four figures 19-22 display the results. These include the overall picture from 1 to n (but charting stopped at 100), and zoomed versions from 2 to 50 to highlight differences.

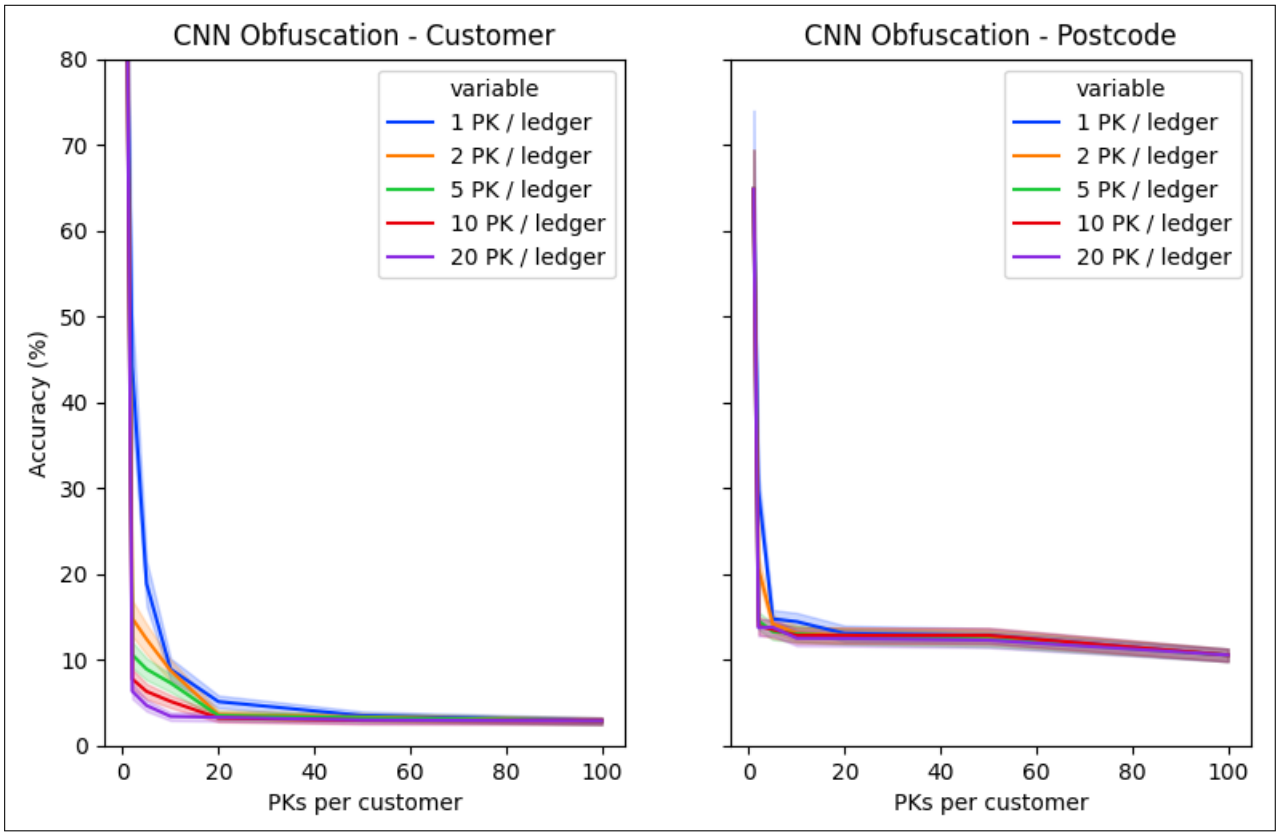

Fig. 19. Obfuscation results - CNN model

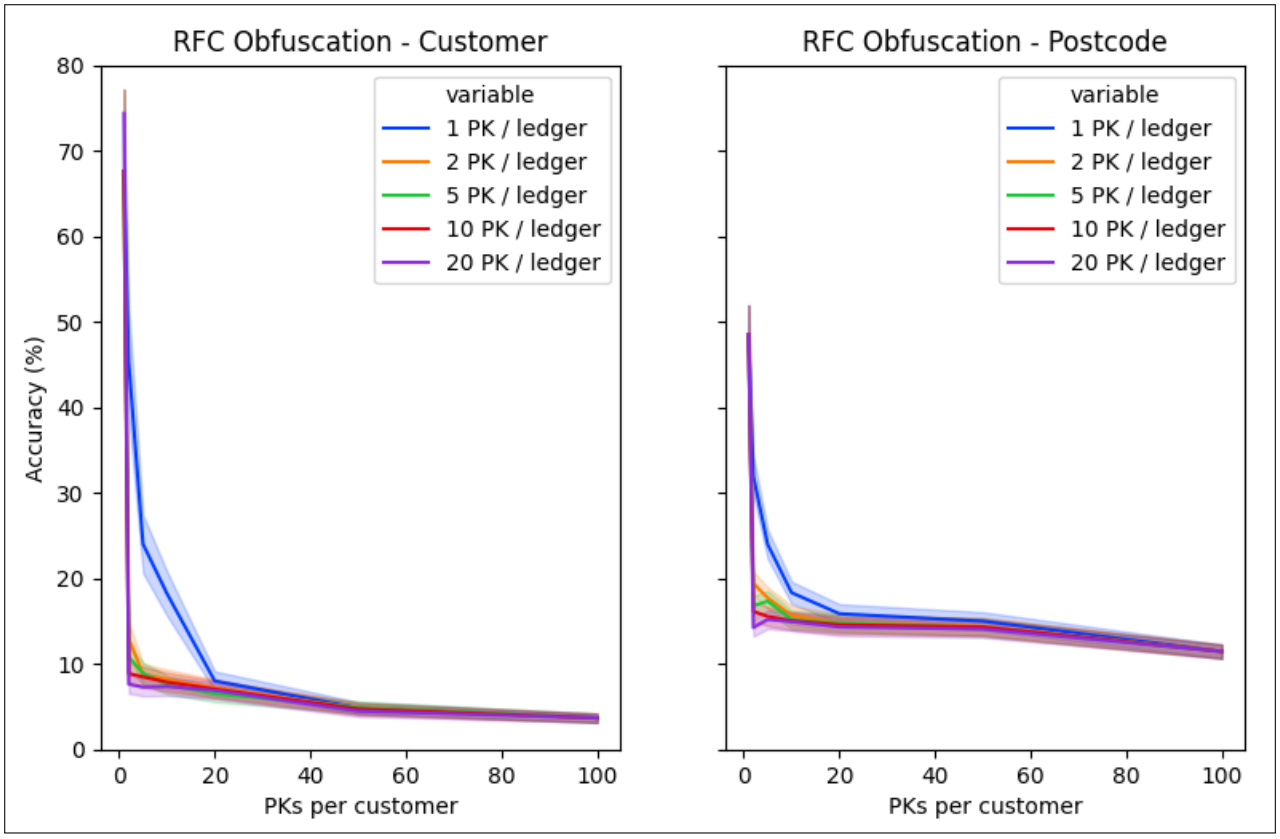

Fig. 20. Obfuscation results - RFC model

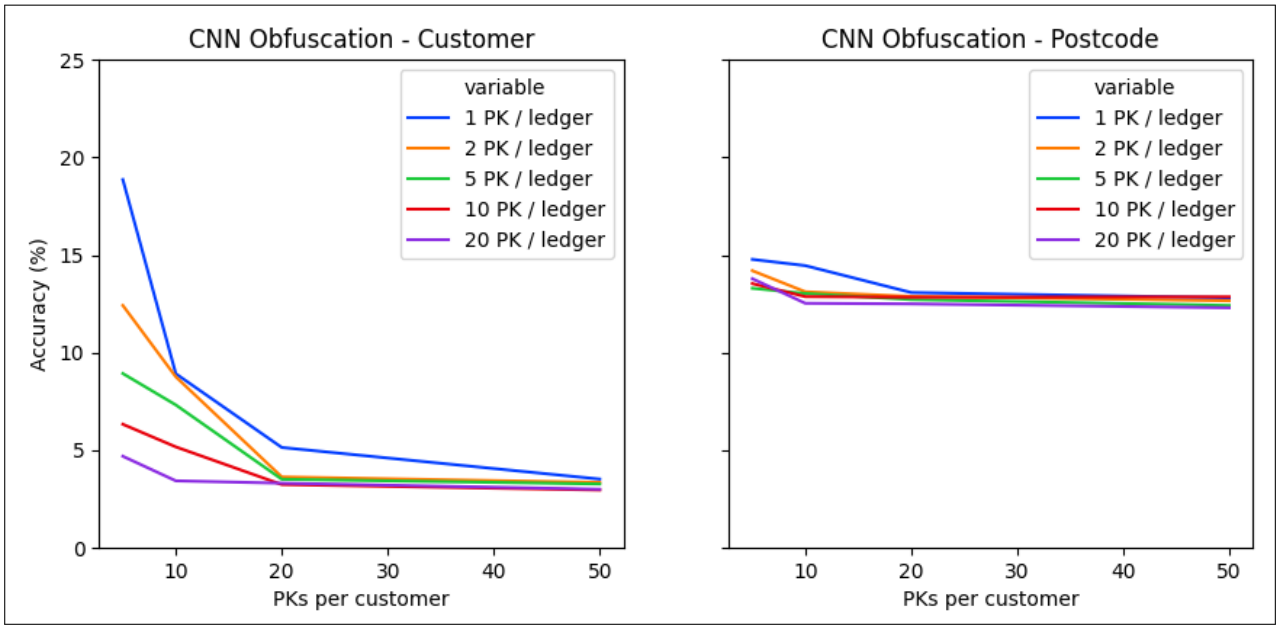

Fig. 21. Obfuscation results - CNN model zoomed

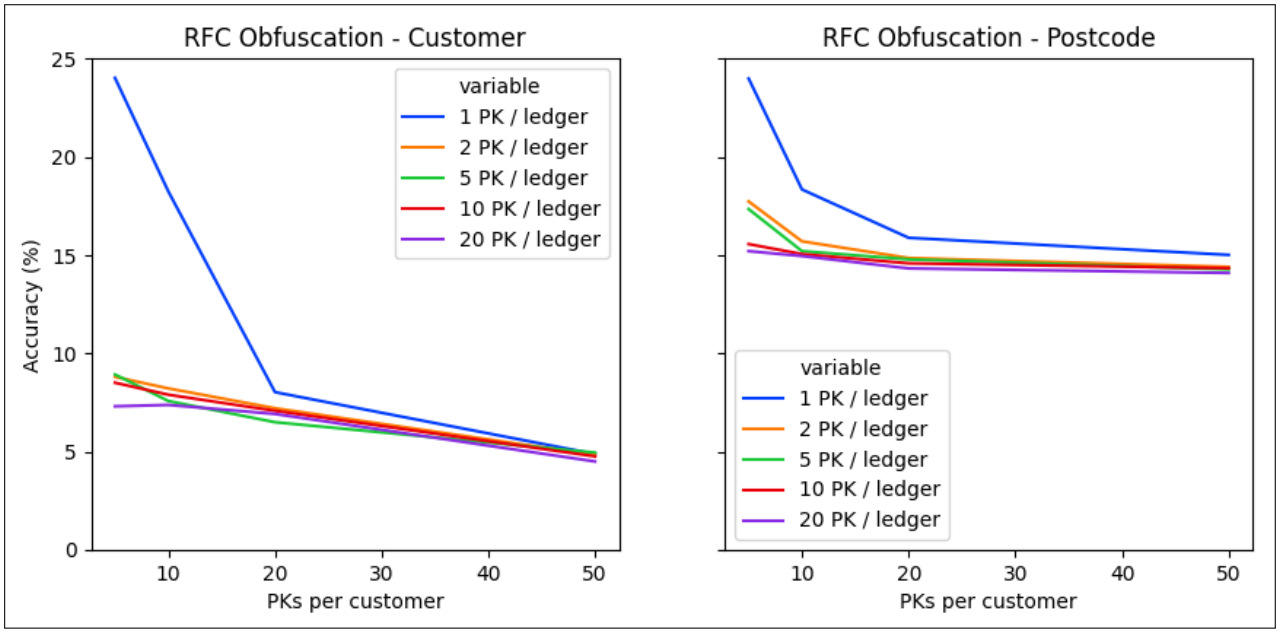

Fig. 22. Obfuscation results - RFC model zoomed

The RFC performs better in both customer and postcode predictions in the obfuscation results. This is consistent with expectation from previous sections. Decision trees handled the AOL scenario better. Both classifiers lose more accuracy predicting customer. The results start from a higher level and finish lower than postcode prediction. Previous sections showed customer transaction linking being more effective than predicting their location. At low accuracy, however, the dataset has far less postcodes (as expected in a real grid) and performs better likely because of this. As in 4.2 the F1 score was highly similar to the accuracy measures provided in these results as all classes are of equal size.

There is significant and clear reduction in accuracy across all figures as PKs per customer increase. Accuracy rapidly decreases for the first few additional PKs and then diminishing returns occur. Looking at Figure 21 and 22, once PK counts reach 20 (or sooner) limited improvement is gained even from many more PKs. There is less notable but still a reduction in accuracy as PKs per ledger increase. This is seen as the lines shift downwards as the amount of ledger mixing increases. This is quite clear in Figure 21 customer, and also the case for postcode prediction, although less clear. Figure 22 shows a similar outcome for RFC model.

There are clear benefits in PKs up to about 20, where the benefit sharply tapers off thereafter and may not be worth the cost for a user. Ledgers are a feature of the blockchain itself and combining would only be limited by the technical implementation.

5. CONCLUSION

5.1. Summary

The emergence of blockchain in IoT emphasises the importance of research into user privacy in potential uses. This thesis has begun investigating user privacy in smart grids if they removed TTPs in favour of a blockchain energy trading solution. The research completed covered the four planned main objectives. First, formed blockchain ledgers from sourced energy grid data. Second, analysed the likelihood an attacker can link user transactions or predict their location in initial scenarios. Third, measured an attacker's benefit by adding off-chain solar exposure data. Last, applied obfuscation techniques to improve user privacy from the attacks.

Machine learning models could quite accurately link user transactions from past blockchain data when users take limited steps to protect their privacy. More frequent transactions aid an attacker, as does separating ledgers whether by users or postcodes. A peak classification accuracy of 85% (customer ID) and 63% (postcode) was achieved with a convolutional neural network. Whereas a random forest classifier achieved 65% and 40%.

Attacker success rates are slightly but consistently improved by including solar data. Regression analysis found household energy usage or solar generation could be reconstructed from net export with 85% R^2 accuracy. This showed notable statistical correlation in predicting which area a household resides by comparing the predicted user energy figures to each region's solar exposure data.

There is a significant and clear reduction in accuracy as PKs per customer increase. Accuracy rapidly decreases for the first few added PKs and then suffers diminishing returns. There is less notable but still a reduction in accuracy from combining ledgers. The PK benefits are clear up to about 20, where the benefit sharply tapers off thereafter and may not be worth the extra cost for a user. Ledgers are a feature of the blockchain itself and combining would only be limited by the technical implementation.

These results highlight concern for just how private is a blockchain without appropriate obfuscation methods. If a grid participant uses a single PK, they could have serious issues maintaining privacy. While a blockchain does guarantee some level of anonymity, it is not absolute. Attackers can find creative ways of using data stored on a permanent blockchain without having access to real-time network traffic. A standard blockchain implementation poses risks to users in this research's context and warrants attention.

5.2. Limitations and Future Work

- The Ausgrid dataset contains 300 prosumers. This was suitable for this research, but several aspects limit deeper research. The dataset is limited to a (reasonable) portion of NSW. On a larger or smaller grid area the conclusions could differ especially for example, smaller and more densely populated countries.
- Machine learning models were not this research's focus. Care was taken in selecting recommended models. However, further computation resources and deep learning knowledge could be beneficial.
- Solar exposure data was available per day for the desired period and areas. This was a limitation when applied to hourly and half-hourly transaction sets. To split the daily data, polynomial distributions were used. More sophisticated research exists, or better resolution data could be found.
- More obfuscation techniques could be applied to further reduce attacker success rates. In particular, obfuscation applied by the blockchain on transactions. Such as, applying random adjustments to timestamps or combining transactions.
- Investigate how obfuscation results change with larger datasets. Larger data will increase the transactions per PK may alter the number of PKs that balance privacy and cost best.
- Data from a real smart energy grid. The ultimate goal of research into this area would include such data. It could also consider the feasibility of real-time network information abstracted out in this thesis.

6. REFERENCES

1. E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. de A. Rocha, “A survey of how to use blockchain to secure internet of things and the stalker attack,” Secur. Commun. Networks pp. 1–27 (2018).
2. A. Dorri, C. Roulin, R. Jurdak, and S. S. Kanhere, “On the activity privacy of blockchain for iot,” (2019), pp. 258–261.
3. D. Ermilov, M. Panov, and Y. Yanovich, “Automatic bitcoin address clustering,” (2017), p. 461–466.
4. Ausgrid, “Solar home electricity data,” https://www.ausgrid.com.au/Industry/Our-Research/Data-to-share/Solar-home-electricity-data (2014).
5. Bureau of Meteorology, “Climate data online,” http://www.bom.gov.au/climate/data/ (2020).
6. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” (2008).
7. G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” https://www.ausgrid.com.au/Industry/Our-Research/Data-to-share/Past-outage-data (2014).
8. M. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, “Blockchain technologies for the internet of things: Research issues and challenges,” IEEE Internet Things J. **6**, 2188–2204 (2019).
9. D. Puthal, N. Malik, S. Mohanty, E. Kougianos, and G. Das, “Everything you wanted to know about the blockchain: Its promise, components, processes, and problems,” IEEE Consumer Electron. Mag. **7**, 6–14 (2018).
10. M. Swan, *Blockchain: Blueprint for a New Economy* (O’Reilly, Sebastopol, CA, USA, 2015), 1st ed.
11. T. Alladi, V. Chamola, J. Rodrigues, , and S. Kozlov, “Blockchain in smart grids: A review on different use cases,” Sensors (Switzerland) **19** (2019).
12. R. Bayindir, I. Colak, G. Fulli, and K. Demirtas, “Smart grid technologies and applications,” Renew. Sustain. Energy Rev. **66**, 499–516 (2016).
13. U. Ahsan and A. Bais, “Distributed big data management in smart grid,” 26th Wirel. Opt. Commun. Conf. pp. 1–6 (2017).
14. L. Cheng, N. Qi, F. Zhang, H. Kong, and X. Huang, “Energy internet: Concept and practice exploration,” (2017), p. 1–5.
15. 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. **100**, 143–174 (2019).
16. V. Hassija, G. Bansal, V. Chamola, V. Saxena, and B. Sikdar, “Blockcom: A blockchain based commerce model for smart communities using auction mechanism,” (2019), p. 1–6.
17. G. Bansal, V. Hassija, V. Chamola, N. Kumar, and M. Guizani, “Smart stock exchange market: A secure predictive decentralised model,” (2019), p. 1–6.
18. J. Li, Z. Zhou, J. Wu, J. Li, S. Mumtaz, X. Lin, H. Gacanin, and S. Alotaibi, “Decentralized on-demand energy supply for blockchain in internet of things: A microgrids approach,” IEEE Transactions on Comput. Soc. Syst. **6**, 1395–1406 (2019).
19. B. Muhammad, J. Zhao, D. Niyato, L. Kwok-Yan, and X. Zhang, “Blockchain for future smart grid: A comprehensive survey,” IEEE Transactions on Comput. Soc. Syst. (2019).
20. P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, “Smart grid metering networks: A survey on security, privacy and open research issues,” IEEE Commun. Surv. & Tutorials **21**, 2886–2927 (2019).
21. M. K. Khalilov and A. Levi, “A survey on anonymity and privacy in bitcoin-like digital cash systems,” IEEE Commun. Surv. & Tutorials **20**, 2543–2585 (2018).
22. M. Conti, S. Kumar, C. Lal, and S. Ruj, “A survey on security and privacy issues of bitcoin,” IEEE Commun. Surv. & Tutorials **20**, 2543–2585 (2018).
23. D. Ron and A. Shamir, “Quantitative analysis of the full bitcoin transaction graph,” (2013), pp. 6–24.
24. Z. Ghahramani, “Unsupervised learning,” Adv. lectures on machine learning **20**, 72–112 (2003).
25. H. H. S. Yin, K. Langenheldt, M. Harlev, R. R. Mukkamala, and R. Vatrapu, “Regulating cryptocurrencies: A supervised machine learning approach to de-anonymizing the bitcoin blockchain,” J. Manag. Inf. Syst. **36**, 37–73 (2019).
26. Y. Wang, G. Cao, S. Mao, and R. M. Nelms, “Analysis of solar generation and weather data in smart grid with simultaneous inference of nonlinear time series,” in *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS),* (2015), pp. 600–605.
27. T. Khatib and W. Elmenreich, “A model for hourly solar radiation data generation from daily solar radiation data using a generalized regression artificial neural network,” Int. J. Photoenergy **2015**, 1–13 (2015).
28. Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, “Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities,” IEEE Commun. Mag. **56**, 82–88 (2018).
29. H. I. Fawaz, G. Forestier, J. Weber, L. Idoumghar, and P.-A. Muller, “Deep learning for time series classification: a review,” Data Min Knowl Disc **33**, 917–963 (2019).
30. B. A, L. J, B. A, L. J, and K. E, “The great time series classification bake off: a review and experimental evaluation of recent algorithmic advances,” Data Min. Knowl. Discov. **31**, 606–660 (2017).
31. J. Lines and A. Bagnall, “Time series classification with ensembles of elastic distance measures,” Data Min. Knowl. Discov. **29**, 565–592 (2015).
32. M. G. Baydogan, G. Runger, and E. Tuv, “A bag-of-features framework to classify time series,” IEEE Transactions on Pattern Analysis Mach. Intell. **35**, 2796–2802 (2013).
33. A. Bagnall, J. Lines, J. Hills, and A. Bostrom, “Time-series classification with cote: The collective of transformation-based ensembles,” IEEE Transactions on Knowl. Data Eng. **27**, 2522–2535 (2015).
34. Z. Wang, W. Yan, and T. Oates, “Time-series classification with cote: The collective of transformation-based ensembles,” Int. joint conference on neural networks p. 1578–1585 (2017).
35. A. Jović, K. Brkić, and N. Bogunović, “Decision tree ensembles in biomedical time-series classification,” (Springer, Berlin, Heidelberg, 2012), p. 917–963.
36. S. Bhandari, N. Bergmann, R. Jurdak, and B. Kusy, “Time series analysis for spatial node selection in environment monitoring sensor networks,” Sensors **18**, 11–27 (2017).
37. Open Power System Data, “Household data,” (2017).

7. APPENDIX A - ADDITIONAL TRANSACTION ANALYSIS GRAPHS

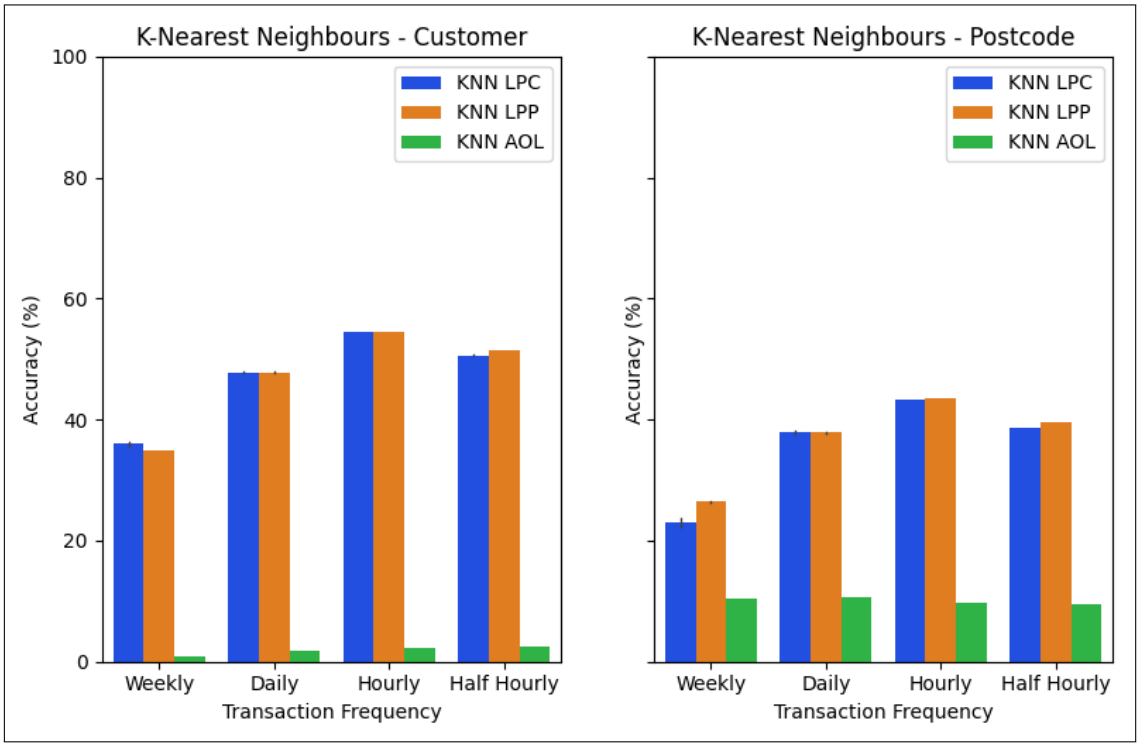

Fig. 23. Overall accuracy of KNN classification by transaction resolution and scenarios

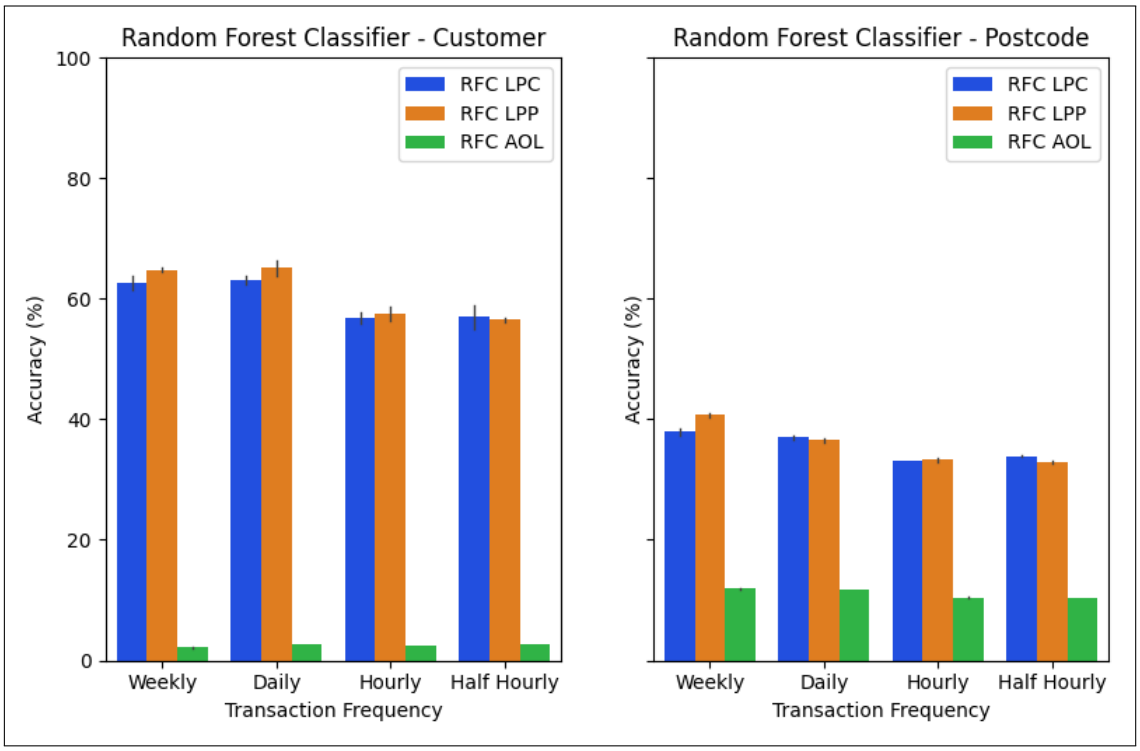

Fig. 24. Overall accuracy of RF classification by transaction resolution and scenarios

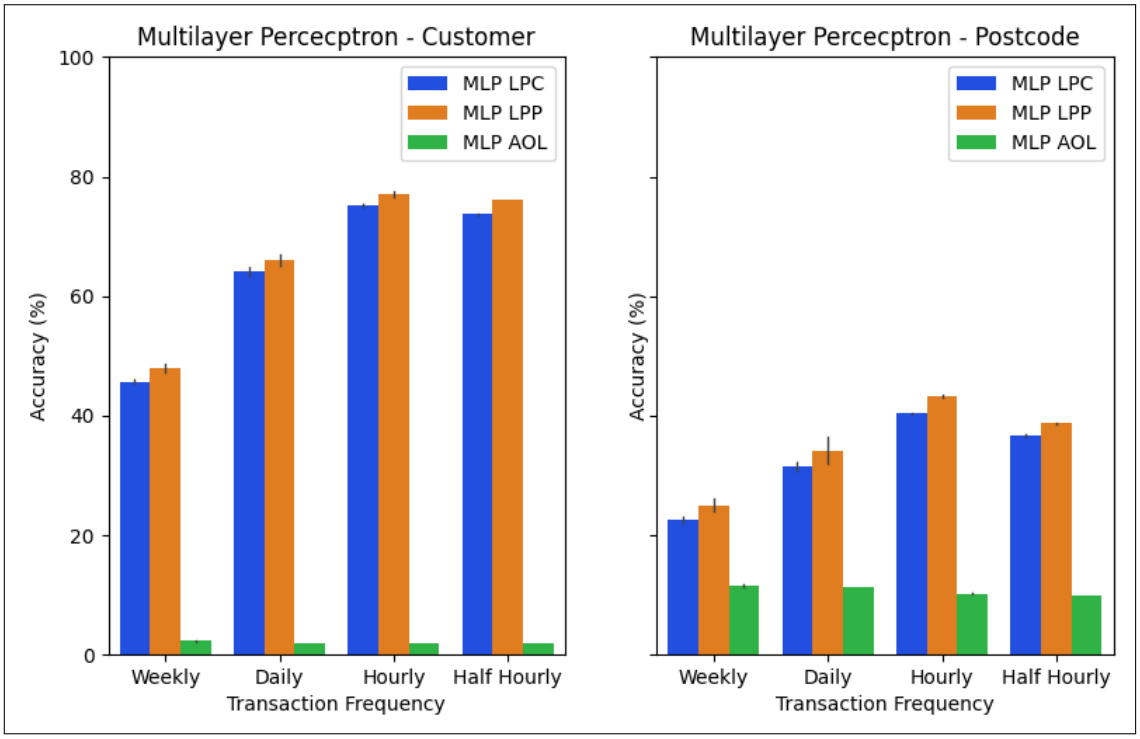

Fig. 25. Overall accuracy of MLP classification by transaction resolution and scenarios

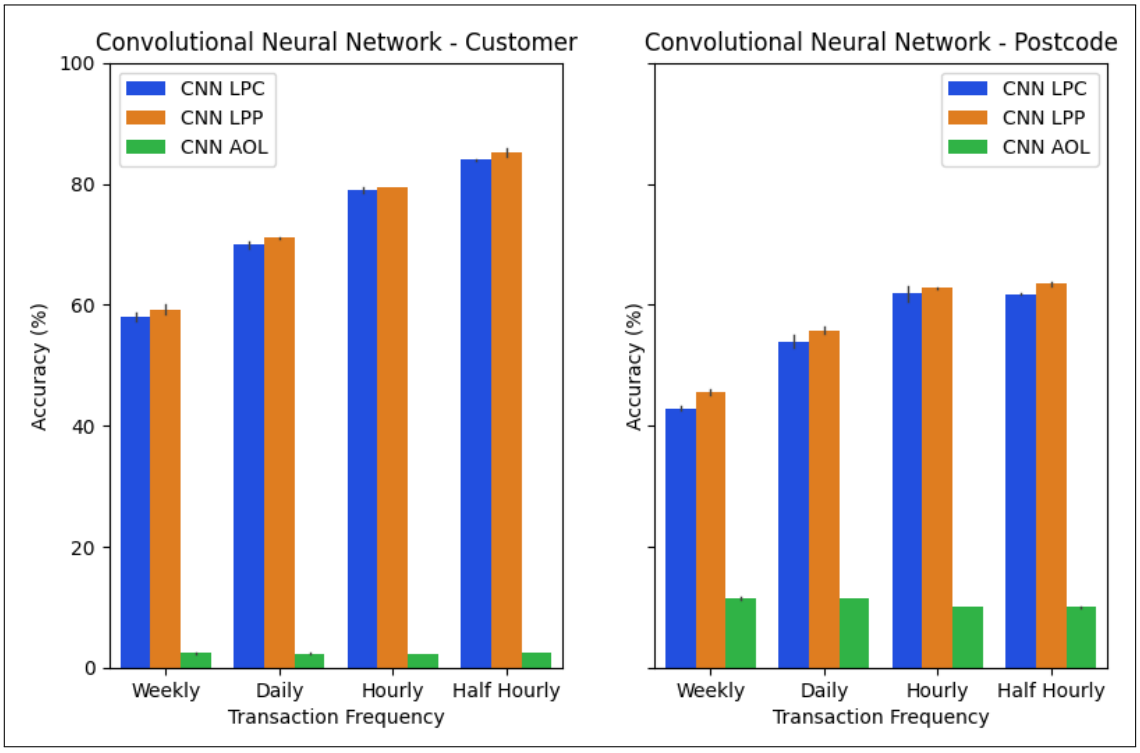

Fig. 26. Overall accuracy of CNN classification by transaction resolution and scenarios

8. APPENDIX B - TABULATED RESULTS

Section 4.2 Objective 2 Tabulated Results

Classification		Weekly			Daily		
Method	Case	LPC	LPP	AOL	LPC	LPP	AOL
MLP	Customer	45.72%	47.88%	2.28%	64.18%	66.11%	1.93%
	Postcode	22.52%	25.00%	11.48%	31.45%	34.13%	11.31%
CNN	Customer	58.03%	59.21%	2.47%	69.91%	71.05%	2.39%
	Postcode	42.85%	45.65%	11.46%	53.96%	55.77%	11.47%
RFC	Customer	62.63%	64.81%	2.14%	63.10%	65.14%	2.63%
	Postcode	37.89%	40.69%	11.86%	36.94%	36.52%	11.67%
KNN	Customer	35.97%	34.91%	0.95%	47.82%	47.83%	1.86%
	Postcode	23.06%	26.44%	10.47%	37.94%	37.92%	10.69%

Fig. 27. Weekly and daily results for transaction classification

Classification		Hourly			Half Hourly		
Method	Case	LPC	LPP	AOL	LPC	LPP	AOL
MLP	Customer	75.26%	77.03%	1.83%	73.73%	76.10%	1.86%
	Postcode	40.33%	43.21%	10.20%	36.68%	38.70%	9.86%
CNN	Customer	78.92%	79.40%	2.33%	83.98%	85.21%	2.48%
	Postcode	61.84%	62.79%	10.12%	61.78%	63.44%	10.03%
RFC	Customer	56.74%	57.39%	2.55%	56.98%	56.54%	2.68%
	Postcode	33.10%	33.23%	10.43%	33.90%	32.89%	10.30%
KNN	Customer	54.52%	54.54%	2.22%	50.61%	51.46%	2.39%
	Postcode	43.39%	43.46%	9.77%	38.56%	39.57%	9.52%

Fig. 28. Hourly and half hourly results for transaction classification

Section 4.3 Objective 3 Tabulated Results

Classification		Weekly			Daily		
Method	Case	LPC	LPP	AOL	LPC	LPP	AOL
CNN	Customer	67.98%	67.87%	3.05%	76.36%	76.58%	2.84%
	Postcode	55.06%	52.27%	12.04%	62.49%	59.47%	11.94%
RFC	Customer	71.77%	75.89%	2.84%	72.90%	74.55%	3.70%
	Postcode	57.69%	58.38%	14.43%	52.11%	52.45%	13.03%

Fig. 29. Weekly and daily results for solar classification

Classification		Hourly			Half Hourly		
Method	Case	LPC	LPP	AOL	LPC	LPP	AOL
CNN	Customer	82.33%	83.49%	3.31%	81.81%	82.68%	3.50%
	Postcode	66.14%	65.06%	10.55%	64.85%	66.98%	10.57%
RFC	Customer	66.56%	67.61%	5.08%	67.62%	68.81%	5.17%
	Postcode	47.90%	47.77%	12.55%	48.52%	48.51%	11.48%

Fig. 30. Hourly and half-hourly results for solar classification

DELTA		Weekly			Daily		
Method	Case	LPC	LPP	AOL	LPC	LPP	AOL
CNN	Customer	9.95%	8.66%	0.58%	6.45%	5.53%	0.45%
	Postcode	12.21%	6.62%	0.58%	8.53%	3.70%	0.47%
RFC	Customer	9.14%	11.08%	0.70%	9.80%	9.41%	1.07%
	Postcode	19.80%	17.68%	2.57%	15.17%	15.92%	1.36%

Fig. 31. Weekly and daily delta of initial against solar results

DELTA		Hourly			Half Hourly		
Method	Case	LPC	LPP	AOL	LPC	LPP	AOL
CNN	Customer	3.42%	4.09%	0.98%	-2.17%	-2.53%	1.02%
	Postcode	4.30%	2.28%	0.44%	3.07%	3.54%	0.54%
RFC	Customer	9.83%	10.22%	2.54%	10.64%	12.27%	2.50%
	Postcode	14.81%	14.54%	2.12%	14.62%	15.62%	1.18%

Fig. 32. Hourly and half hourly delta of initial against solar results

Section 4.4 Objective 4 Tabulated Results

Obfuscation PK		Half Hourly Data, PKs Per Ledger = 1						
Method	PKs	1	2	5	10	20	50	n
CNN	Customer	81.81%	44.22%	18.87%	8.92%	5.14%	3.52%	2.89%
	Postcode	64.85%	29.71%	14.78%	14.46%	13.08%	12.81%	10.57%
RFC	Customer	67.62%	45.31%	24.03%	18.25%	8.03%	4.88%	3.70%
	Postcode	48.52%	32.00%	24.00%	18.35%	15.89%	15.02%	11.48%

Obfuscation Ledger		Half Hourly Data, PKs Per Ledger = 2						
Method	PKs	1	2	5	10	20	50	n
CNN	Customer	81.81%	14.86%	12.42%	8.76%	3.63%	3.35%	2.89%
	Postcode	64.85%	20.71%	14.20%	13.12%	12.88%	12.66%	10.57%
RFC	Customer	67.62%	13.00%	8.81%	8.22%	7.21%	4.83%	3.70%
	Postcode	48.52%	19.44%	17.74%	15.71%	14.86%	14.41%	11.48%

Obfuscation Ledger		Half Hourly Data, PKs Per Ledger = 5						
Method	PKs	1	2	5	10	20	50	n
CNN	Customer	81.81%	10.61%	8.93%	7.32%	3.51%	3.27%	2.89%
	Postcode	64.85%	14.56%	13.30%	13.03%	12.72%	12.42%	10.57%
RFC	Customer	67.62%	10.84%	8.93%	7.58%	6.50%	4.95%	3.70%
	Postcode	48.52%	16.82%	17.35%	15.21%	14.79%	14.28%	11.48%

Obfuscation Ledger		Half Hourly Data, PKs Per Ledger = 10						
Method	PKs	1	2	5	10	20	50	n
CNN	Customer	81.81%	7.79%	6.33%	5.17%	3.24%	2.96%	2.89%
	Postcode	64.85%	13.95%	13.54%	12.87%	12.84%	12.86%	10.57%
RFC	Customer	67.62%	8.89%	8.51%	7.90%	7.08%	4.76%	3.70%
	Postcode	48.52%	16.16%	15.57%	15.06%	14.59%	14.34%	11.48%

Obfuscation Ledger		Half Hourly Data, PKs Per Ledger = 20						
Method	PKs	1	2	5	10	20	50	n
CNN	Customer	81.81%	6.37%	4.69%	3.43%	3.31%	3.00%	2.89%
	Postcode	64.85%	13.76%	13.79%	12.53%	12.50%	12.30%	10.57%
RFC	Customer	67.62%	7.66%	7.31%	7.38%	6.92%	4.50%	3.70%
	Postcode	48.52%	14.27%	15.21%	14.96%	14.33%	14.10%	11.48%

Fig. 33. Obfuscation by varying public key and ledgers results