SAND2019-10786C

Designing a Physical Security System Using Blockchain

Ashley Mayle[1], Gabriel Birch[2], Jaclynn Stubbs[3], and Marie Vasek[4]

[1] University of New Mexico amayle@unm.edu
[2] Sandia National Laboratories gcbirch@sandia.gov
[3] Sandia National Laboratories jstubbs@sandia.gov
[4] University College of London firstname.lastname@gmail.com

Abstract. Physical security network architectures are typically highly centralized. This is an issue because it makes the network more susceptible to insider attacks and means that external threats would need fewer resources to disrupt the network architecture. We discuss a network implementation that addresses these issues utilizing a proof of work based blockchain implementation employing MultiChain software. This network contains two types of data input; microwave sensors and visual imagers. These data types were selected due to their ubiquity in perimeter intrusion detection security systems, and enables a realistic representation of a network architecture that supported these common data inputs. The cameras in this system are utilizing the You Only Look Once (YOLO) object detection to find important targets in the scene. The data from the camera and the outputs from YOLO were placed on the same transaction and sorted based on the outputs from YOLO. The described implementation provides the resiliency increase that is expected from a distributed ledger protocol. Simulation results indicate that the properties of blockchain that we expected to work in the system do hold true showing the potential for blockchain based security network structure. Based on these results we theorize that security systems in general could use this type of system in a meaningful way.

Keywords: Physical Security, MultiChain, Communication Network, Private Blockchain

1 Introduction

Blockchains are often thought to be synonymous with cryptocurrencies such as Bitcoin and Ethereum, but the applications for blockchains are much larger than the financial sector. Many companies are currently utilizing private blockchains for tracking their supply chains in a more accurate and secure manner[4]. Others are using blockchain to track the movements of employees in secure areas[4]. These use cases point to a broader use of private blockchains for increasing transparency, resiliency, and providing operational value. In this analysis, we evaluate the feasibility of a private blockchain communication network within the

domain of physical security systems, as there are similar issues shared between a physical security system and the current applications.

Current physical security architectures are large complex systems which contain several different parts performing a multitude of tasks. This large architecture can be inefficient and unable to keep up with fast paced changes in technology because it is hard to implement new applications quickly on such a complex system built on implicit trust in components. There are issues with protecting against insider threats to data history, assessments, and to the components themselves. There are also challenges involving the correctness of historical data, with the speed that data can be sent to an operator, and with accuracy of data moving through the system. Because of these issues there is an obvious need for updates to current security architectures. In this work we discuss the application of distributed ledger technologies in the form of a blockchain to the current physical security system.

This work will explore the application of a private blockchain implementation using MultiChain. MultiChain is a private blockchain that is built on the bitcoin core [3]. MultiChain currently uses a proof of work model but is investigating other models of consensus for future versions of this system meaning that as MultiChain updates the system would gain any advancements in security with the updates. The MultiChain implementation of blockchain has smart filters which check if transactions meet certain rules before adding them to the block. This is useful because it means code can be created to keep data of similar types in the same parts of the network without large overlap of different data types which could cause problems with assessment. This is also useful because it allows the system to perform checks on aspects of a transaction autonomously without an operator which will add additional resiliency without additional human interaction with the system.

We used MultiChain to create a decentralized network of cameras and sensors that are capable of communicating data with with increase resiliency and security prioritization to human operator. Prioritization implies that human interfaces into the security system can easily differentiate between relevant and irrelevant security information. This would possibly allow operators to be more alert as they work because there would be less information presented to them for processing. The camera data that was added to the blockchain included outputs from the You Only Look Once real time object detection algorithm. By using YOLO, images can be sorted by a computer depending on whether an object of importance was in the scene or not.

This work involved the use of admin nodes, regular nodes, and smart filters on multiple blockchains that are loosely connected with each other. The admin nodes add permissions to the network as well as make and approve changes to smart filters to control the network. The regular nodes act as validators for the system as well as being the nodes where data is generated and added to the system. Both of these nodes are important because the admin nodes control the structure of the system but the regular nodes add more bulk to the system and

allow for nodes with less privileges to be on the edges of the system completely unprotected while having admin nodes be in more secure locations.

Once the initial network was built we also tested whether the network could continue working if some nodes were taken offline, both admin and regular nodes. We did this by turning off the virtual machines that ran the nodes and trying to perform vital functions in the system such as adding new nodes and making transactions. This was useful to test because while we know metrics of how blockchains work in cryptocurrencies, it is important to validate that those properties remain the same in a security system because if they do not then teh positives we would gain out of the system would be minimal.

This work is organized as follows; a discsusion of the backgtound and motivation is presented, followed by the methodology describing the communication network architecture and resiliency tests. The results evaluating the resiliency and robustness of the network are presented. We conclude with a summary and discussion of future work.

2 Background and Motivation

Blockchain technology has mostly been used as the technological backbone of cryptocurrencies. Blockchain is currently used to solve problems in systems that have existed for many years but those problems are only now coming to the forefront of the fields that blockchains are being used in. Many of these applications are changing the status quo in their fields and leading to new opportunities for applications of blockchain technology. These applications include supply chain management, immutable audit logs, production systems, as well as many other types of applications[4]. Each type of application can give us interesting insights as to the feasibility of the use of distributed ledger technology in a physical security system. The best applications of blockchain have strongly motivated problems that require redundancy, resiliency, and strong controls on data.

One of the main non-cryptocurrency applications utilizing blockchain currently is supply chain management. Blockchain based supply chains are being used or researched by several different companies including Walmart and De Beers[4]. Saberi et al. [6] describes the relationship of blockchain to supply chain management. They state utilizing blockchain would fundamentally change the way that supply chain is thought of, as supply chains have historically been a trust based centralized system. By incorporating blockchain supply chains can move away from these problems and move towards a trustless decentralized system. Historically security systems have similarly had a centralized architecture built on trust in the components of the system. This is one of the problems with the security architecture, much as it has been with supply chains, and blockchain could potentially aid in alleviating these problems in the same way.

Another area where blockchain could be useful is in production systems as production has many disjointed moving parts in the same way that a supply chain or security system does. In their paper Afanasev et al. [1] discuss a cyber-physical production system based on a private Ethereum network. Each node

on the network was given a certain amount of ether to pay for the transactions. The amount given was based on the priority of the node. This idea is relevant as a security system can have nodes that need to be more secure than others. For example, nodes closer to a target would need to be evaluated by system administrators more often so giving them less of an asset to make transactions with would ensure that those components were being more closely watched.

Blockchain has also been applied to identity management systems. Polyswarm demonstrated this concept in an application for the U.S. Department of Homeland Security (DHS) [4]. This project tracks the movement of employees through DHS facilities to accurately reflect access and authentication in their system. The immutable data logging features of distributed ledger technology ensures that the data will be accurate for audits in the DHS facilities. This work is focused on the application of blockchain to the perimeter intrusion detection aspect of a physical protection system rather than the application to access control.

There are many other examples of blockchain applications outside of cryptocurrencies, however, a system designer must assure that the problem being solved is appropriate for a blockchain implementation. In a paper by Wüst and Gervais [7] they discuss what type of blockchain one should use for different types of needs.The authors outline the difference between public and private blockchains as well as blockchains difference to a database. Oftentimes an application will try to use blockchain when a database would suffice. A database does not address all problems in a security system as while the nodes in the system are known they should not be trusted. Accordingly, we hypothesis that a security system would benefit from the use of a private blockchain as it will keep data from the public but does not require trust in the system. This work will investigate the use of the MultiChain private blockchain as the communication network for a security system.

A common challenge in security systems is the amount of centralization. Often data from various sensors and imagers is sent to a central location for processing and assessment which allows for insider attacks to be completed without many resources. Centralization is also a problem due to few points of failure (e.g., power or hardware failures). These limited processing points then become critical elements within the larger security system. Existing security systems additionally suffer from a variety of degrees of database mutability control, potentially opening a system to insider attacks that can be completed quickly with limited traces being left by the attacker action. Lastly, the current architecture could have problems protecting against future threats because of the speed of an attack. the current system might have problems processing and assessing data quickly enough to protect against an extremely fast threat.

We propose that the use of Blockchain in a security system can help mitigate the issues facing the security architectures. Challenges and limitations in many security systems ultimately stem from a high level of centralization, which could be solved using a DLT-like data communication architecture. This would be used to distribute the processing and assessment across different nodes so that if one processing location goes down the overall impact to the system is reduced. The

second problem could be corrected by blockchain because data is immutable once it is placed on the blockchain and so it would extremely difficult for an insider to change or remove events from the data log once they were written to the chain. The last problem could possibly be solved by adding a blockchain to the system because it would allow for quicker autonomous assessment of the data and would put less load at a centralized point by spreading the processing to the edge of the system.

3 Methodology

3.1 Network

MultiChain, a private blockchain, was used for the notional decentralized security data communication network. The notional network is shown in Figure 1.

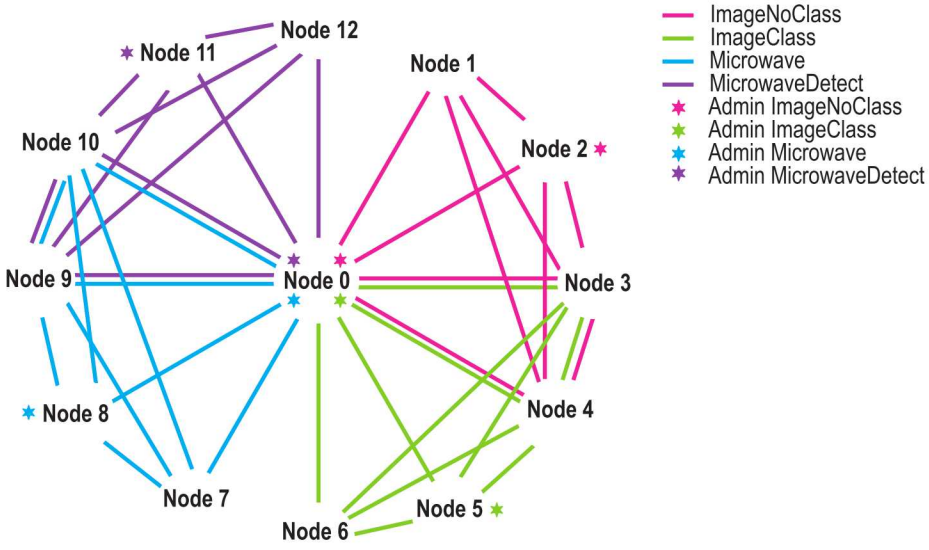


Fig. 1. Network Diagram for a 12 nodes with two types of data input

The MultiChain network has two types of nodes; admin nodes and member nodes. The nodes are defined by what permissions they have. Admin nodes have permissions to create and approve filters and add new nodes to the chain while member nodes do not. The chain starts with a single admin node and is built out of that node. The MultiChain network for this project was setup to have five admin nodes and eight member nodes. These nodes represent the imagers, sensors, validators, and network admins in the system.

This setup was designed to take advantage of having a decentralized architecture; new nodes can still connect to the network and new filters can still be approved as long as some subset of admin node(s) are present. MultiChain has the advantage that no nodes in the system need to be trusted for the network to continue operations. If an admin node is taken over, the other admin or admins can start a stream or even a new chain with the non-compromised nodes. Showing that it would be difficult to perform an attack on this system by shutting off nodes without a large amount of resources.

This network contains four different types of data inputs occurring at nodes three, four, nine and ten. Each color in figure 1 refers to a different set of data that is communicated between that sub-network. The pink sub-network contains all data that originates from a camera and has no classification data attached to it. The green sub-network contains all data that originates from a camera which has a classification for an object in the scene. These types of data are on two different sub-networks so that people processing this data can focus their attention on the most relevant and security critical information.

The blue and purple sub-networks handle microwave data, the blue sub-network handles the data from the microwave with no intrusion and the purple sub-network handles the data from the microwave when there is an intrusion. These sub-networks are connected so that data can flow to either network depending on whether the input had a detection or had no detection.

This network can be expanded upon either by adding more inputs for the current types of data or by adding new types of data to be stored in the distributed ledger. This means that one could add data about employee movements, movement of materials, or data from other intrusion sensors like infrared sensors. Adding this information would make the system more complex but could add even more decentralization meaning it would take more resources to hijack the system.

This network will connect physical pieces of the system digitally. An example of the physical system is shown in figure 2. The cameras in this architecture are indicated by squares. There are two cameras in this system each connected to both imager blockchains, the microwaves are displayed as triangles there are similarly two of them each connected to both microwave blockchains, and the validator and admin nodes which are not data inputs are represented as circles. The validator and admin nodes are spread through different buildings so that an adversary would need to break into multiple buildings in the system to fully interrupt the communication in the system.

3.2 Data Sorting

Figure 3 shows how the data is sorted in this security system. The data is sorted by using smart filters. A smart filter in MultiChain is code that is added to the chain and approved by the admin nodes. This code affects which transactions will be accepted by the chain and therefore allows the data to be sorted to the appropriate channels depending on the values in the transaction. There are two different types of transactions in this system, there are camera transactions and

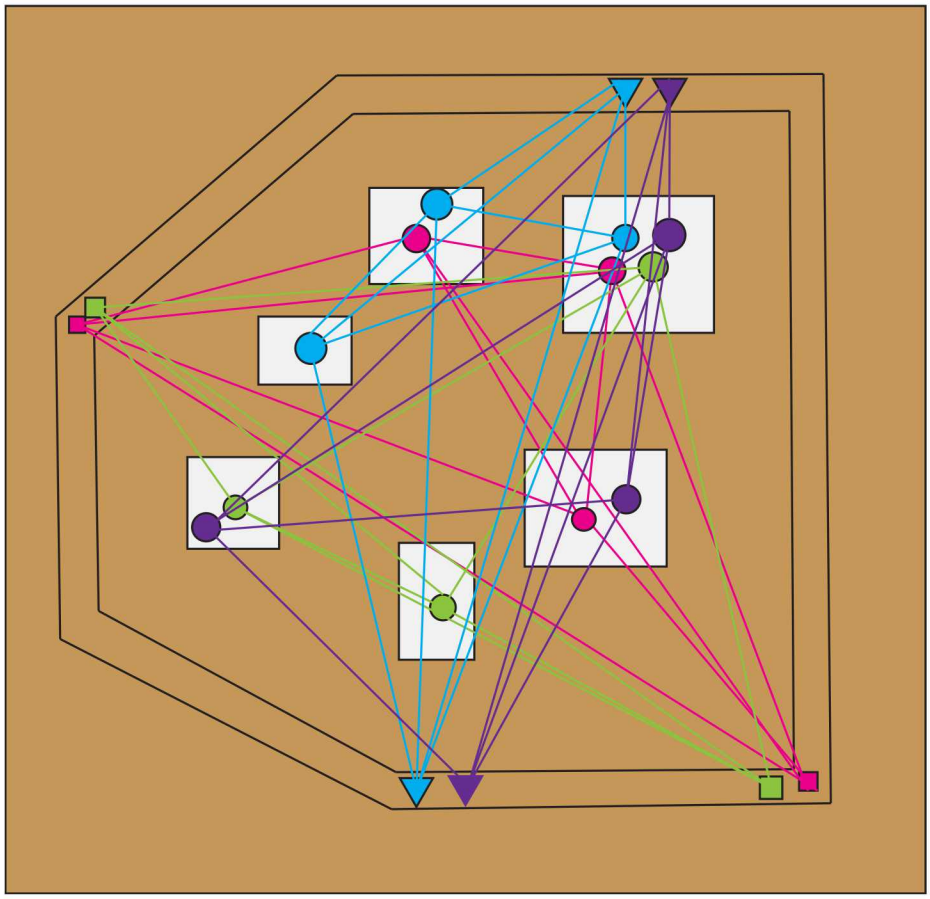
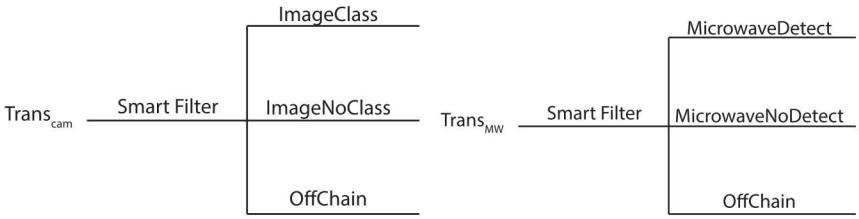


Fig. 2. Diagram of blockchain connections in the physical system



(a) Camera Sorter (b) Microwave Sorter

Fig. 3. Diagram of how data is sorted in the system

microwave transactions. An example of a transaction is listed below. Other types of transactions are listed in Appendix A.

Transactions

```
sendwithdata 1WfiQNZirYMwVqVgdKvaboupEpz3FWHzcAEzec
'{"tamperAsset":10, "classifyAsset":10}'
'{"json":
    {
    "filename":"/media/TA-V_FFMPEG_DATA/210/2019-05-07_14-53-09.png",
    "classify":"person",
    "percent":0.5402294993400574,
    "center x":1024.7264404296875,
    "center y":180.95614624023438,
    "width":16.506134033203125,
    "height":33.79193878173828
    }
}'
```

This transaction is sent through the camera blockchains. This transaction has an image with an object detected in it. It is being sent to another address in this case "1WfiQNZirYMwVqVgdKvaboupEpz3FWHzcAEzec" which is the location of another node on this blockchain. The assets being sent are the tamper asset which represents the value of whether the system has been tampered with or not. It also contains the classify asset which is the asset that this particular code is based off of. This asset needs to be sent anytime the code is run. These values are both set to 10 he tamper asset is 10 so that the tamper smart filter will approve this as a valid transaction.

The data passed through in this transaction is a json object. It contains a link to the image being passed as well as the classification made by YOLO along with the percentage and location value. This is useful information for the operator to have as it will allow them to find object in the image being referenced more easily making for a quicker assessment of the data. This transaction will be added to the ImageClass blockchain because the JSON object contains a value for classification, if it did not it would be sent to the ImageNoClass chain.

Smart Filters Each transaction is added to a specific blockchain based on the code written in the smart filters for that chain. Each smart filter affects transactions made on the blockchain that it is approved for. A transaction can be sent to multiple blockchains which will sort the data accordingly. An example of a smart filter is shown below all other smart filters for this system are in Appendix B.

```
Classify Filter function filtertransaction()
{
     var meta=getfiltertransaction();
```

```
    s=String(meta.vout[1].data[0].json.classify);
    if (s.valueOf() == " ".valueOf())
    {
        return "Classify not found"
    }
}
```

This is a smart filter that checks to see if there is an object detected in an image. This code is written in JavaScript and checks that the classify value in the JSON object of the transaction contains a value from YOLO. This filter is placed on the Image Class chain. If the transaction fails this code check, the image will not be added to the Image Class chain and will need to go through another smart filter to be added on a different chain matching the data type and detection status.

With the smart filters and transactions set up the network ran with data being placed on the chain correctly and securely. This shows that the network can support a data load that is common in physical security systems. This means that it will be valuable to make some initial measurements of the system for quantitative analysis. This will allow us to determine if there are actually added security measures from the use of blockchain in the system.

3.3 Resiliency

This system utilized the MultiChain network framework which contained admin nodes as well as regular nodes. These nodes were connected together based on the framework described in section 3.1. This framework allowed the system to communicate data effectively and securely. It is important to have quantitative analysis for new security architectures so that there can be proof that the system will work under specific threat models. This ensures that the system will perform as we expect it to during the worst circumstances.To make preliminary steps toward providing quantitative measurements for a blockchain based security system, we performed three tests on the system described above.

The first test was taking down different combinations of admin nodes. We wanted to run this test because an admin node provides a multitude of important features for the system. Admins control connection to the network, the control of the creation of code, the approval of code, and the permissions of each node in the system. If taking an admin node offline could take away any of these features then the network would be susceptible to an easy attack. With more resources being required for every admin node simultaneously taken down, being able to successfully run with fewer admins effectively increases the robustness of the system. We performed this test by shutting down the virtual machines that hosted the admin nodes for each sub-network. This simulated the plug being pulled or a power issue occurring which would turn the node off and disconnect it from the network architecture.

The second test was taking down a regular node. This test was important to show that a partial outage of the system would not remove vital capabilities

from the entire system. For example if one half of the system shown in figure 2 were to be taken off line the consequences for the other half of the network should be kept to a minimum; if half the system can be disabled in an attack the other half must still function. We will test this by taking down a node one at a time and checking each time that the system continues to add transactions to the blockchain.

The final test was detecting tampering of the physical system. This test is important because not all attacks target taking the system offline some threats are an attack on the physical components of the system to change their direction or to change how the sensor actually communicates the data. In the current system there is a message sent to the human operator that a tamper has been detected. This system will need to show the capability to perform a similar task. This test was simulated by changing the tamper values for the transactions to represent the change in value from the sensor.

These preliminary tests should show a quantitative result for how the system performs under a few stressors. If these tests prove positive then more testing will be required of the system to prove resiliency.

4 Results

The first test showed that the network would continue to allow new regular and admin nodes to be created as well as the creation of new contracts and the approval and falsification of older smart contracts. This was true for each sub network when any one admin node was taken down in the network and true for the whole network when up to four of the five admin nodes were taken down depending on which set of nodes were taken down simultaneously. In a larger system more admin nodes would be able to be taken down as the system would be distributed across more actors that could maintain functionality.

The second test showed that taking regular nodes offline still yielded a network that was able to support the transactions required for the system to communicate data. We found that as long as 2 nodes in the sub network remained on the network could still communicate the data as expected. This is important because if only one node needed to be taken down to cut communication then the failure of a single sensor would compromise the operation of the entire network, an obvious failure for a secure system. Similarly in a larger system more nodes could be taken offline and this functionality would still work because there is more decentralization and simply more nodes to take offline in general.

The final test was to see if the system could detect a tamper in the physical space. When a physical security element such as a microwave is tampered with it will change its signal to a value separate of intrusion or secure. This value is represented in the system as the tamper asset. Code was written in this architecture to detect a change in this value from the expected value of 10 seen in Appendix B. If there is a change in the tamper asset for a transaction that transaction will be ignored by the system to prevent misinformation from making its way to a human for assessment. This simulated tamper assessment is similar to a real life

tamper but would need to be tested further on a physical test bed to confirm the results given by the simulation.

Overall the results from this work indicate that a blockchain based communication network would be a reasonable step forward for researchers in physical security. It brings many important advancements, such as decentralization and immutable data logs, to this test system without introducing any known defects that were not already present in the original system

5 Conclusion and Future Work

The results discussed above show that this type of network has promise to be a future communication network for a new physical security architecture. These tests indicate that the network is resistant to power failures and attacks which take down parts of the system as one would need to take down many nodes to shut off communication to the human operator. The results for taking down admin nodes show promise for the network being able to adapt to an attack with more work put into the system as an admin node can add new nodes and change code such that an attacker may not be able to maintain control of enough of the network to perform an attack. The last aspect of the system which was tested was the ability to detect tampers. This test showed that the system was able to correctly detect when a tamper was happening and disregard the data being sent in as it might be false. This will allow a human to assess the component of the system which has been tampered with before adding that information back into the network.

There are other benefits to the system which we believe to be true but have not been tested yet such that it will be hard to destroy or change historical data in the system so that when an audit occurs accurate data is represented and so that if an insider tries to attack the system it will be recorded accurately without being changed by said insider. A final benefit that this system appears to provide is that the physical security system no longer needs to rely on trust of the components and of the human in the loop. This will allow the system to be secure and resilient because components could break or fault and it would not affect the system as a whole.

There are many avenues to expand on this work all of which would be valuable to proving that blockchain can be used as the communication network of a physical security system. Firstly it would be useful to build a physical test bed to more accurately test the physical threats to the system such as tampering. This would help to show that the system works outside of the digital space and can truly meet the needs of this type of system. The second avenue would be testing different types of private blockchain implementation such as private Ethereum, Hyperledger fabric, R3 Corda, etc. to see if these results hold true across multiple types of blockchain implementations or if there is added benefits to the from other types that have not been seen in MultiChain to this point.

A final avenue to expand on is testing more resiliency metrics, while this work shows that it would be feasible to use blockchain as the communication network

of the system it is important to take a solid quantitative approach when making changes to security systems. This means that metrics need to be fleshed out and tested on both the old security system and a new security system. The current metrics in preliminary testing are focused heavily on how a blockchain would operate in the system. The metrics that will be created should focus on creating a system with absorptive, adaptive, and recoverable capacity [2]. If these metrics can be met by the system, then the system will prove suitable to be deployed as a security system communication network.

6 Acknowledgment

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

A Transactions

```
sendwithdata 1FdqTN7c8XXkSbh9s262kKyLRMNZHgz92svNYL
'{"tamperAsset":10,"detectAsset":10}'
'{"json":
   {
       "Microwave":"2.5"
   }
}'
```

The above transaction is a microwave transaction that shows a microwave in an alarm state. This transaction is valid because the tamper value in the system was set to 10. This means that it will be added to the Microwave Detect chain.

```
sendwithdata 1FdqTN7c8XXkSbh9s262kKyLRMNZHgz92svNYL
'{"tamperAsset":10,"detectAsset":10}'
'{"json":
    {
        "Microwave":"5"
    }
}'
```

The above transaction is similar to the one above, the only difference is that this transaction has a microwave in a secure state so it will be added to the Microwave No Detect chain.

```
sendwithdata 1WfiQNZirYMwVqVgdKvaboupEpz3FWHzcAEzec
'{"tamperAsset":10, "classifyAsset":10}'
'{"json":
   {
```

```
    "filename":"/media/TA-V_FFMPEG_DATA/210/2019-05-08_15-00-59.png",
    "classify":"", "percent":0
   }
}'
```

The above transaction is a camera transaction that shows an image from a video feed which has not detected a target. This transaction is valid because the tamper value in the system was set to 10. This means it will be added to the Image No Class chain.

B Smart Filters

```
No Classify Filter function filtertransaction()
{
var meta=getfiltertransaction();
s=String(meta.vout[1].data[0].json.classify);
if (s.valueOf() != " ".valueOf())
{
return "Classify found"
}
}
```

This is a smart filter that checks if there is no object detected in an image. This filter is run on the Image No Class chain. If a transaction fails this check, the transaction will not be added to the Image No Class chain and will need to go to another chain to check if the transaction follows the rules set by that chain.

```
Tamper Filter function filtertransaction()
{
var meta=getfiltertransaction();
s=String(meta.vout[0].assets[0].qty);
if(s.valueOf() != "10".valueOf())
{
return "Tamper Detected"
}
}
```

This is a smart filter detects tampering in the system by checking the value of a tamper asset and comparing it against a predetermined value. This value can be changed periodically to make sure that an attacker does not have time to test the system enough to figure it out. This smart filter is placed on every chain to detect tampering on all sensors in the system.

```
MicrowaveDetect Filter function filtertransaction()
{
    varmeta=getfiltertransaction();
```

```
    s=String(meta.vout[1].data[0].json.Microwave);
    if (s.valueOf() !="2.5".valueOf())
    {
        return "No intrusion found"
    }
}
```

This smart filter checks to see if the data sent by the microwave indicates there was an intrusion. If a transaction fails this check it will not be added to the Microwave Detect chain and will need to be sent on another chain to check if the transaction follows the rules set by that chain.

```
Microwave Filter function filtertransaction()
{
    var meta=getfiltertransaction();
    s=String(meta.vout[1].data[0].json.Microwave);
    if (s.valueOf() !="5".valueOf())
    {
        return "Intrusion found"
    }
}
```

This code checks to see if the data sent by the microwave indicates that the microwave is in secure mode. If a transaction fails this check it will not be added to the Microwave No Detect chain and will need to be sent to another chain and checked by its filters.

References

1. Maxim Ya Afanasev, Anastasiya A Krylova, Sergey A Shorokhov, Yuri V Fedosov, and Anastasiia S Sidorenko. A design of cyber-physical production system prototype based on an ethereum private network. In *2018 22nd Conference of Open Innovations Association (FRUCT)*, pages 3–11. IEEE, 2018.
2. Royce Francis and Behailu Bekera. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, 121:90–103, 2014.
3. Gideon Greenspan. Multichain private blockchain—white paper. *URl: http://www. multichain. com/download/MultiChain-White-Paper. pdf*, 2015.
4. Paul Makowski. Blockchain-security symbiosis, 2019.
5. MultiChain. Working with smart filters. `https://www.multichain.com/developers/smart-filters/`, 2019.
6. Sara Saberi, Mahtab Kouhizadeh, Joseph Sarkis, and Lejia Shen. Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7):2117–2135, 2019.
7. Karl Wüst and Arthur Gervais. Do you need a blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 45–54. IEEE, 2018.