**First Slide (20/780)**

Hello X, Y, Z , my name is James O’Connor and you are very welcome to my dissertation research presentation.

The main goal of my dissertation is to examining a new Distributed Ledger Technology called IOTA for V2X communication applications.

This will be examined through building a proof-of-concept application around a simple use case scenario.

If there are any questions or clarifications needed along the way please feel free to ask

**Presentation Summary (60/780 – 7%)**

A quick summary of the presentation, it is broken into 6 sections. We will start with a quick introduction into the research. The next three sections, we will break apart the different technologies that are involved in this exploratory research. They are:

1. Distributed ledger technologies
2. The IOTA Framework (which is the distributed ledger technology I am exploring)

And then

1. An overview of V2X communications and how it pertains to this research

Section 5 will deal with the conclusions of the literature review, and finally section 6 will conver the research objectives, scope and plan going forward

So section 1-4 is dealing with the what, what are these technologies, section 5 deals with why do this research and then section 6 and 7 will deal with how I am going to do it

**Introduction (100/780 – 12%)**

So to reiterate, I am exploring the potential of DLTs in the autonomous vehicle (AV) industry through the development and testing of a V2X communication application.

…and the research focus here will be on security and scalability – by that I mean data and device security and application/ platform scalability

I thought it would be good to begin with the hypothesis and we can work back from there. The research hypothesis is as follows:

***The IOTA framework*** *can be used as a* ***secure*** *and* ***scalable V2X communication protocol*** *for* ***OBU data transmission among autonomous vehicles*** *to* ***share data and identify dangerous road conditions***

There’s a lot to unpack here, so the next few sections will discuss the components of this hypothesis in detail

Distributed Ledger Technology (DLT)- Definitions - **(140/780 – 17%)**

In order to understand the IOTA framework is, we have to first discuss DLTs. There are many ways that distributed ledger technology can be defined, 1 defines it as

In general it is a paradigm shift in application development, moving away from centralised hub-and-spoke architecture. Core principles are rooted in consensus and cryptography which promotes security, integrity, and transparency of data and applications.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Blockchain: A DLT Example (1) (200/780 – 25%)**

TO go a little deeper, I will quickly talk through an example of a DLT

Blockchain is the most popular form of DLT used in the industry today.

Three main components to any DLT :

* 1. Transactions – Data or value transfer between two parties
  2. Nodes – network of computers organised in a peer-to-peer architecture, that provide the network computing power.
  3. Ledger – An authoritative order of valid transactions stored and shared on all nodes

I’m going to walk through how a typical blockchain works. THis is the bitcoin protocol, which is the most popular DLT built in 2008 using blockchain technology and really brought DLTs to centre stage.

Here is a high level of how the network operates

1) Transactions, signed with a public key, get sent to all of the nodes for approval

2) Network of computers solve an equation to confirm validity

3) Once the puzzle is solved, these transactions are added to the cryptographically chained link of logical units called blocks and the transaction is complete

Explaining Bitcoin: A Blockchain Example (2) - **(300/780 – 38%)**

In my opinion, the best way to start understanding how blockchain works is to understand what a hash function is. A hash function is a function that takes a number of inputs produces an output of fixed length. For example, the SHA256 hash function takes an arbitrary set of input data and maps it to a unique 256 bit signature output.

The bitcoin network uses this exact hash function to validate blocks of transactions. In order to add a block of about 500 valid transactions to the shared ledger, nodes have to first find a valid hash function output. This is also known as “mining”.

The static input values to this hash function are the block number, the block id, the hash value from the previous block, valid signed transactions to be confirmed, (about 500) and a timestamp. There is only one input value that is variable and this is called a nonce. With all the other input values static, the nodes loop through different nonce values until it outputs a valid hash value.

These are set by the bitcoin source code, they change periodically, and at any given time there are very few of them. There’s about a 1.5\*10-22 chance of calculating this, or about ten minutes for a computer.

Once the block cracks the code, it gets to add the block to the ledger, and gets rewarded, typically in cryptocurrency.

What we end up with is a chain of transaction data, called a ledger, broken into logical units, all dependently linked using hash values. This makes the data immutable because you can’t change the data. If you changed it you would produce a different hash value. Because they’re all linked, If any hash value changed along the chain, this would invalidate the entire chain of blocks. It’s like trying to unbake a cake. The network operates on a “longest-chain-wins” system so only way to out-run the chain is if you had the majority of computational power in the network.

So that’s how a typical blockchain works. There are many different kinds with their own nuances but this is a popular approach.

With this approach we get data transparency, data immutability and security. Sounds great, so what’s the catch? blockchains are not a silver-bullet solution.– It has a slow throughput and can have a huge environmental impact, and high transaction fees. To use our same example, the bitcoin network can only confirm 500 transactions every ten minutes and uses about 0.5% of the global energy consumption to run the network and cost more based on the network congestion.

The IOTA Framework – Title

I fundamentally believe in DLT, but the current blockchain format does not scale well and consumes a vast amount of energy. If you can imagine, if the bitcoin protocol only confirms 500 transactions per 10 minutes, then the use cases in terms of connected devices is limited. What if we could get the benefits of DLT, with a higher throughput of feeles transactions using less computational energy? This is where the IOTA framework comes in

The IOTA Framework – (1)

The IOTA framework is a DLT that was created in 2017 by the IOTA Foundation specifically for IoT devices to deal with these two issues.

The biggest difference between IOTA DLT and other blockchains is that it does not use blocks or mining. This makes the network feeless (as there is nobody to pay), it speeds up the transaction confirmation process and reduces the computational power required. This enables fast micro-transactions in a m-2-m economy.