TORRICEL™

The New Standard For Data Security

www.Torricel.com

Legal

Company Purpose

The company behind the new standard for data security.

Torricel exists to house our intellectual property relating to data security architecture and take advantage of it worldwide. We commercially exploit our IP through licensing agreements, and by offering a base product and implementation design book.

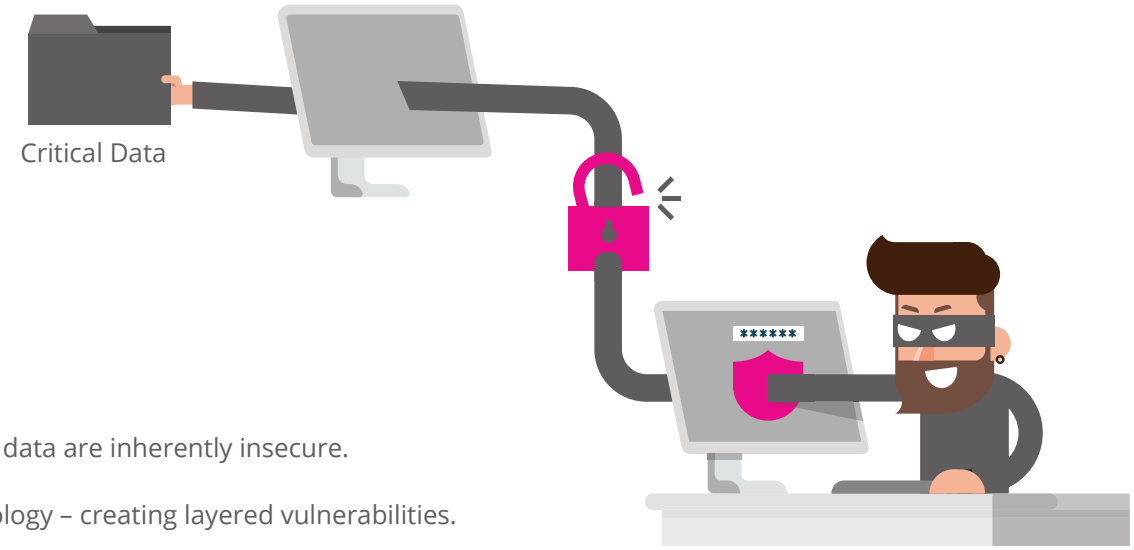
Torricel seeks to build a certifiable standard for data security and set benchmarks and certify technology as compliant under these.

Our team also brings the opportunity for consultancy, development and industry thought-leadership services based on our IP. Whilst we seek to exploit the property we currently hold, we never cease in innovating and expanding our product offering.

TORRICEL™

The Problem

Insecure and outdated data handling architecture.



- Storage and processing of sensitive and critical data are inherently insecure.
- Security is based on layering antiquated technology – creating layered vulnerabilities.
- Loss of trust due to well reported losses of the people's data and money protected.
- Current methods are a response to breaches – Torricel prevent breaches.
- Critical data is always connected to the internet, leaving doors open for hackers.

Your critical data is at the end of a hacker's wire!

facebook

87 million — Customer personal data stolen.

Google

52.5 million — Customer personal data stolen.

SingHealth
Defining Tomorrow's Medicine

1.5 million — Patients medical details.

BUNDESNACHRICHTENDIENST

Hundreds — German Politician: Contact details, Private Chats, Financial Information.

Adobe®

38 million — Customer usernames and passwords.

Uber

57 million — Customer usernames and passwords.

bitcoin

1 million — Bitcoin stolen from wallets and exchanges.

$4.2 billion — (Bitcoin Valuation Jan 2019)

Marriott

383 million — Customer details compromised.
8.6 million — Customer payment card details.
5.25 million — Unencrypted passport details.
20.3 million — Encrypted passport details.
And crytographic keys stolen to unencrypt data.

mastercard **VISA**

1.5m — Payment details compromised.

BRITISH AIRWAYS

380,000 — Payment details compromised.

AADHAAR

1.1 billion — Private details including bank, ID numbers, biometric data of all enrolled Indian citizens.

IBM

IBM Ponemon report estimates global average cost to a company of data breach is $3.62million.

T··Mobile·

2 million — Customer personal data.

EQUIFAX®

143 million — Records stolen,
693,665 — UK consumers affected.
Stolen data included email address, password and secret question to reset password, driving license and payment card details, phone numbers.

timehop

21 million — Customer personal data.

TICKETFLY

27 million — Customer personal data.

EXACTIS

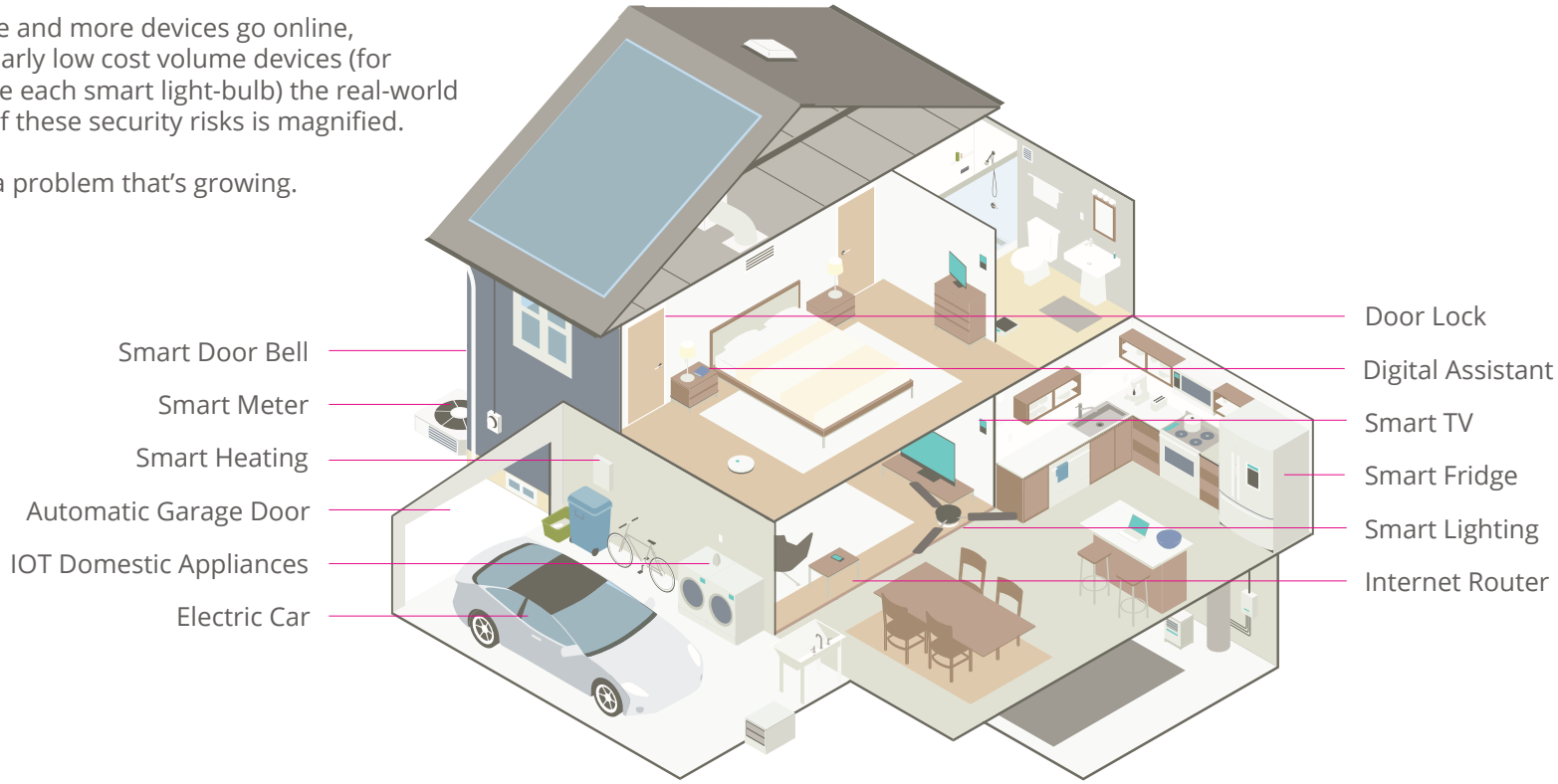
340 million — Consumer details, interests & characteristics.

The ‘Smart’ Problem

Smart Devices and devices with an internet connection are quickly becoming the mainstay of all new products. The weakness in software design and in current computing data handling architectures means that now more than ever before, we are vulnerable to targeted and group attacks.

As more and more devices go online, particularly low cost volume devices (for example each smart light-bulb) the real-world effect of these security risks is magnified.

This is a problem that’s growing.



Your Vulnerable Data

Trade Secrets

Preferences, Habits, Living Profile
Consumption Habits

Health Records

Personal Biometric Data

Smart Watch

Other Private Information

IDs, Passport & Driving Licence
Internet Banking & Crypto Wallets

Calendar & House Occupancy

Methods of Attack

Human Weakness

Easy to guess passwords, being 'duped' into clicking on emails, visiting websites posing as well-known brands, or being convinced to contact fake call centres - there are many ways a hacker can trick innocent users into giving away access to their own or even an organisation's computer.

Trusted Persons

Attacks don't just come from 'the internet'. They may be employees, contractors, blackmailers, trespassers and visitors. They can run their own programs, or manually copy critical data.

Brute Force, Artificial Intelligence and Distributed Denial of Services (DDoS) Attacks

Hackers are becoming more advanced with every moment that passes. Furthermore, computers are becoming more powerful. When combined together, hackers are able to continually attempt system penetration until one of two things occurs - the a genuine user account is discovered, or the system security fails.

AI and Quantum Computing will further increase the quantity and intelligence of these attacks.

Trojans, Viruses, Spyware, Ransomware

These software programs allow a hacker access to your computer, leak data from your computer, or make data and systems inaccessible. All data is compromised. It is further possible for those infections to spread to other computers on the network or in the user's contact lists.

System Flaws

From direct attacks on computing system architectures to specific weaknesses in component combinations, hackers have discovered ways into computer systems beyond the operating system.

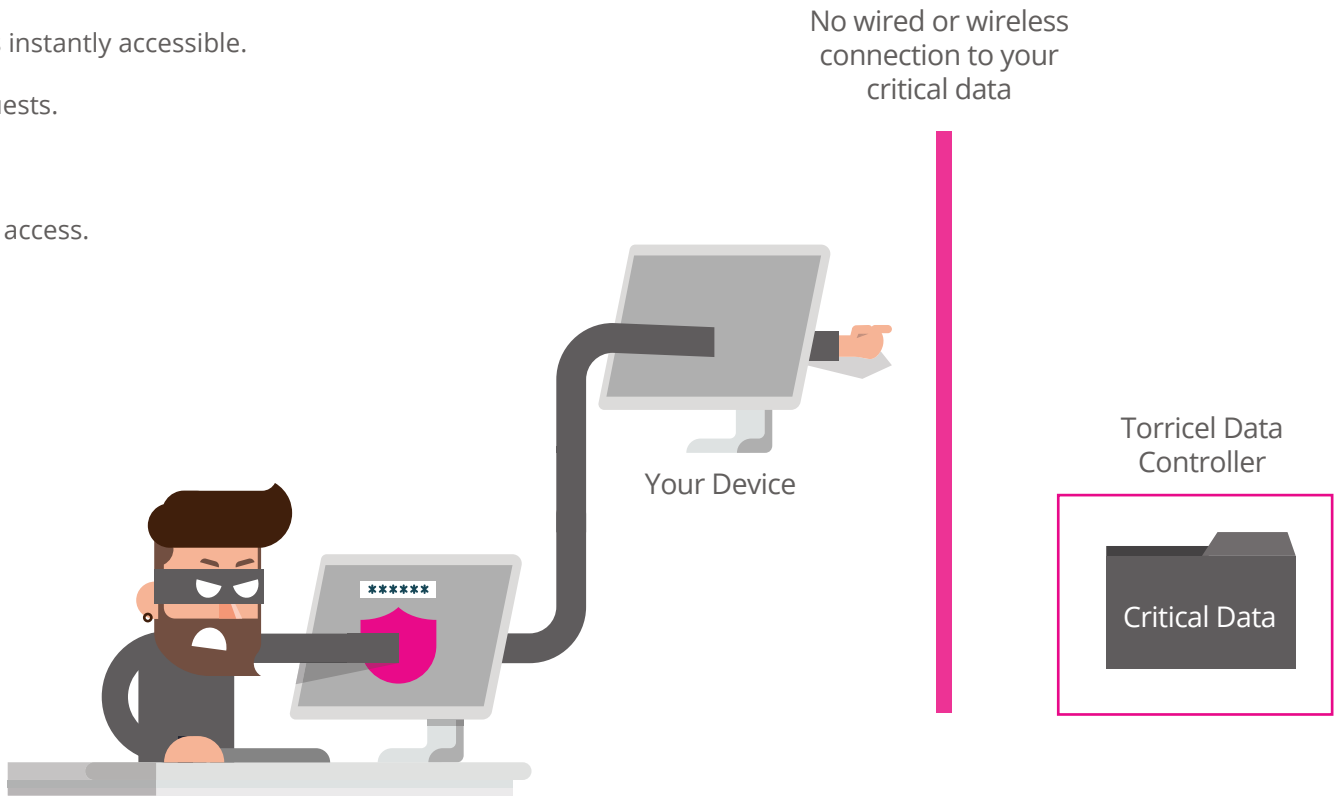
Heartbleed, an attack on OpenSSL software compromised the secret keys used to identify service providers and to encrypt traffic. Names and passwords of users and their content were compromised. It went further – attackers could eavesdrop on communications, steal data directly and impersonate services and users.

Attacks on the core hardware such as 'Meltdown' and 'Spectre' have been labelled 'catastrophic' in severity. Meltdown exploited well know processors by Intel, AMD and ARM. Spectre hit microprocessors that perform branch-prediction. Both of which have relied on the 'patching with software' response seen time and time again, some of which are not completely effective resolutions.

Our Solution

Secure by Design

- Physically disconnected so cannot be accessed by hackers.
- Creates an offline data storage that's instantly accessible.
- Only works with legitimate data requests.
- High security at fast speeds.
- Protect critical data and control user access.



TORRICEL™

An Illustration of Our Solution: The Coin Slot

Remember coin slots? A physical mechanism that would only accept certain specific kinds of coin. The most secure coin slots used a combination of internal traps, weight triggers, and electromagnets that could detect alloys that didn't match the precise mix used by official currency mints.

Even the most visually exact, and correctly weighted counterfeit coins would be rejected because they couldn't precisely match a valid coin's electromagnetic signature. Additionally, in some machines, valid coins were deposited into a secure vault built into the wall behind the machine, so even if a thief stole the whole unit, there wasn't a single coin stored inside it.

Torricel recreates that level of mechanical security and asset protection using a unique data architecture and network protocol that even the most determined hacker organisation couldn't exploit. Not because it's complex, but because, like the coin slot, it is simple and segregated by design.

We have created a system that only allows legitimate transactions to pass through it, and isolates each step in the process using multiple single-task systems.

This means anyone trying to access the system through the internet can never gain access to the system that verifies the data requests, or that holds your digital assets and private data.

TORRICEL™

How can you hack something that's never connected to the internet?

You can't.

How existing system architecture handles data requests

How existing system architecture handles data requests

1. A user / hacker sends a request to a server.
2. The request is sent over a network of connected systems to the destination.
3. “Firewalls” - a primative software based data compliance devices intercept and pass data to the destination.
4. The destination computer receives the request and retrieves the data from its storage.
5. The data passes back over the network of wires and systems to the user / hacker.

Unsafe

A physical link between the user / hacker and critical data is always maintained, allowing for repeated attacks.

How Torricel architecture handles data requests

1. A user / hacker sends a request to a server.
2. The request is sent over a network of connected systems to the destination.
3. “Firewalls” - a primative software based data compliance devices intercept and pass data to the destination.
4. A Torricel ‘access slot’ receives the data request, and then physically disconnects from the internet.
5. The isolated access slot connects to a Torricel Autonomous Cold Clearing system. This system holds the critical data, and is never online.
6. Data is only processed and returned to the user if explicitly authorised.

Safe

A physical connection never exists between the user / hacker, protecting critical data.

Torricel's Architecture in Detail

The Torricel ASCC architecture combines the flexibility of an always connected data system with the security of cold storage.

What makes our approach uniquely secure is the fact we have baked-in security which means:

1. Torricel is physically unhackable, because if one network connection is open, the others are forced shut by the Smart Switch because they are built on one-way physical relay switches (exclusive OR switches). Even if it was possible to gain control of the Smart Switch (which it isn't) it's not possible to connect the stages together simultaneously.

2. The system uses Whalesong - our bespoke communication protocol language that can only process a limited set of commands.

   This means that unless the data parsing through the system is legitimate, validated transaction data, the system has no way of parsing it. It is impossible to embed codes, exploits, buffer overruns, platform attacks, viruses or malware that can pass through the Cashier Gateway, because it physically cannot transmit anything other than valid data.

3. The "input / output" Access Slot is never connected to the Autonomous Cold Clearing system, and the Cashier Gateway can only be physically connected to one or the other, not both, because of independent enforcement by the Smart Switch. This means nothing from the internet can access the secure data in Cold Clearing, even if the Cashier Gateway could be forced to pass it over, which it can't because it can only communicate a strictly limited set of data formats.

Autonomous Secure Cold Clearing (ASCC)

ASCC stands for “Autonomous Security Cold Clearing”, comprised of self-contained, isolated computing and storage systems that form the Torricel architecture. Unlike the isolated processes of commonly used virtualised security solutions, Torricel uses a genuinely isolated, dedicated hardware and software architecture.

How ASCC Works

1: Smart Switch

At the heart of the Torricel architecture is the Smart Switch, normally deployed as a physical series of relays or physical data line controls, triggered using a strict sequence of primitive logic-flag signalling.

This is a dataless system that continuously ensures each element within the architecture is isolated from each other. It effectively un-plugs our systems from all network connections before any requests are processed, critical data is accessed, or during the data transaction approval process.

It’s like a series of digital air locks, where only one airlock can be open at any one time. This ensures that nothing can pass through the system without being intercepted and validated multiple times on systems that are physically disconnected from one another.

2: Access Slot

Like its physical namesake, the Access Slot is the part of the system that’s accessible to the outside world.

If a user wants to transact, the transaction request enters the Torricel architecture here. The Access Slot is the connection layer that is accessed by at the beginning and completion of the data transaction.

When a data request comes in, if the Access Slot validates it, it asks the Smart Switch to connect it to the Cashier Gateway.

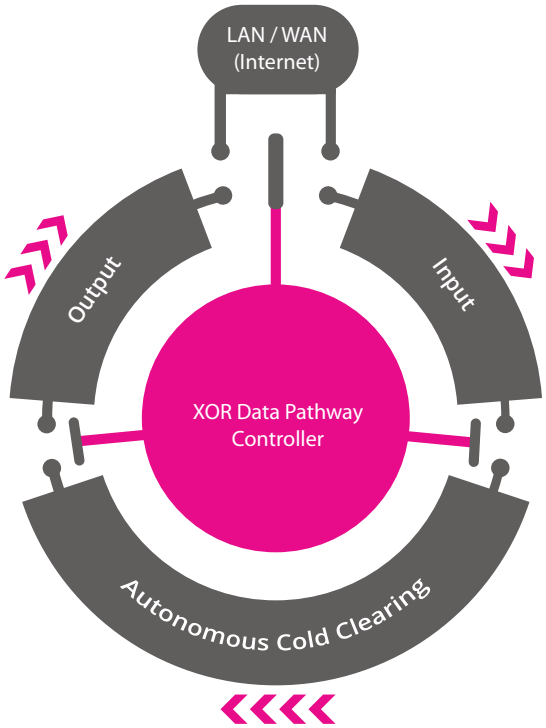
3: Cashier Gateway

Like a cashier with a one-way security tray at a bank counter service, when a request comes in from the Access Slot, the Cashier Gateway system is disconnected from the rest of the system. This means any hacking activity coming from the internet access point cannot physically progress beyond the Cashier Gateway.

The Cashier Gateway uses our unique communication protocol - named Whalesong - that is limited to only communicate legitimate - and correctly formatted - data requests. It cannot process commands, because the Whalesong communication protocol doesn’t contain any. Nor can it attack the commonly found UART (universal asynchronous receive and transmit) communications system; a security weak point in serial communications.

The Cashier Gateway also checks the request against a series of security policies to detect request pattern anomalies, and past activity such as unusual amounts or payees. If the transaction doesn’t pass policy requirements, the Cashier Gateway rejects the transaction and the smart switch isolates it from the Access Slot, making it impossible for anything to pass further into the system, or back out into the network.

Any additional sent data such as malware probes, or serial comms attacks (like buffer overrun attempts), triggers the Cashier Gateway to shut down and reject the transaction, even mid-way through a data send process. If the data is valid, the cashier instructs the Smart Switch to physically isolate it from the Access Slot, before it opens a connection to the Clearing system.



Secure Data Storage and Processing Architecture

How ASCC Works

4: Autonomous Cold Clearing

The Cashier Gateway can only transmit valid data to the Autonomous Cold Clearing system once it is isolated from the network by the Smart Switch.

Additionally, the Cashier Gateway communication protocol language - Whalesong - is only capable of transmitting validated data.

Once the data is received by the Autonomous Cold Clearing system, it is isolated from the Cashier Gateway by the Smart Switch, while it processes the transaction.

The Autonomous Cold Clearing system performs additional policy checks to spot unusual or suspicious requests, and if the data request meets the standard, it processes the request (e.g. cryptographic signing with the private key). This ensures the critical data (e.g. private key) is only ever accessed on a machine that is physically disconnected from all other systems, providing unhackable cold storage security.

5: Completion

Once the data request has cleared, the Smart Switch isolates the Cashier Gateway from the network, and allows the Cold Clearing system to transmit the completed transaction data to the outgoing Cashier Gateway.

The Smart Switch then isolates the Cold Clearing system, before reconnecting the outgoing Cashier Gateway to the Access Slot. This is done using a one-way communication system that means no data can be received by the outgoing Cashier Gateway at this point,

The Smart Switch then isolates the outgoing Cashier Gateway from the Access Slot, before the Access Slot can transmit the requested data to the required destination.

Torricel ASCC Proof Of Concept : TorriWallet

TorriWallet is a functioning Minimum Viable Product (MVP) and proof of concept of Torricel's ASCC architecture. This server-type cryptocurrency wallet has been self-funded and developed in-house by the team. We have patent pending, prototyped, software scripted and tested the system.

Benefits

- Secure – The first online 'cold storage'.
- Platform Agnostic – seamlessly integrates with any technology.
- Multi-sig ready.
- Trust – A brand synonymous with proven and repeatedly tested security.
- Accessibility – Mobile app, web app and API.

How it Works

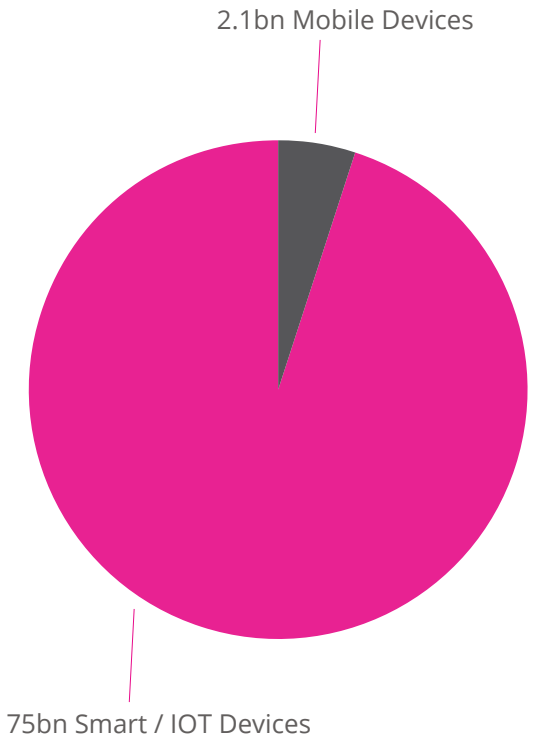
1. A payment request is received by a server / database.
2. The Access Slot is connected to the server and pulls the request.
3. The controller physically disconnects the network connection.
4. Cashier Gateway AI checks the request against wallet policies and looks for anomalies in the request.
5. The request is translated into Whalesong, our comms protocol language.
6. The controller physically connects the Cashier Gateway system to Autonomous Cold Clearing, allowing the request to be sent to it. The controller then disconnects all data lines.
7. The Autonomous Cold Clearing AI undertakes a further policy / anomaly check before performing its function (e.g. signing a transaction with the encrypted private key)
8. The controller then opens a connection to the access slot, again passing the data using the Whalesong protocol. Once sent, the systems are disconnected.
9. The Cashier Gateway conducts a final set of checks and converts the request back to normal language.
10. Finally the controller connects the Cashier Gateway to the network and the data is securely sent.
11. All this is done in a matter of moments and the system is ready to process the next transaction.

Opportunities

Whilst the uses of Torricel are vast, we believe the following markets hold the most immediate opportunities:

- Internet of Things (IOT): **75 billion** estimated devices by 2025
- Mobile smart devices: **2.1billion** in circulation
- Database and Data Security: Spend **$5 billion** currently.
- Cryptocurrency custodial services (exchange, wallet, commercial deployments). **$184 billion** market capitalisation currently.
- Artificial Intelligence: estimated at **$3 trillion** spend in defence industry alone.

IOT / Smart Device market is set to dwarf the Mobile Market



Mobile Devices & IOT

Securing Mobile Devices

Security is currently software automated, or virtualised in CPU design.

From mobile devices to the IOT, Torricel protected devices would safeguard the interests of the consumer, the provider and the dependant ecosystems.

Our security architecture can be built into CPU hardware, building security in as standard.

Smart Homes

Securing Home and Work Environments

Smart Homes are the future, with added convenience for consumers. The big data they generate allows for more informed supply chains. Weaknesses in the security of Smart Home technology however are potentially dangerous.

For instance, it is not only digital financial assets that need to be secured. Private information about consumption from your Smart Fridge that could (for example) be used by the dairy industry to increase / decrease production and delivery, can also be used by criminals to predict inoccupancy of homes.

Torricel Technology will underpin these local data storage and communication requirements, rendering this critical data secure and accessible only by those with explicit authority.

Cryptocurrency Wallets

Securing Retail and High Value Investors

We are seeking to further develop TorriWallet for deployment directly into commercial hardware wallets for the retail, trade and industry and consumer spaces.

By improving the security, we dramatically improve the viability of using Blockchain and cryptocurrencies for millions of people and institutions worldwide.

Commercial grade – Racked hardware for deployment as localised wallets for branches, regions and business providers, either onsite or in data centres, exchanges and other services.

Consumer grade – Small format deployments for permanently connected devices within the home and portable devices.

Digital Asset Exchanges

Securing Exchanges

Torricel security lends itself perfectly to the heart of instant-access custodial storage of cryptocurrency exchanges.

Our technology is platform agnostic and optimised for multiple entry - app, web and API.

Our solution offers exchanges improved security not only to Private key and signing processes, but also to the critical digital information stored for Know Your Customer (KYC) compliance.

An API will provide developers with the means to build our Torricel ASCC security architecture in to their third party apps, products and services as standard.

TORRICEL™

The 4th Industrial Revolution

Securing Infrastructure and the Economy

The 4th Industrial Revolution is here, from Artificial Intelligence to the growth of the subscription economy, ‘Industry 4.0’ spans or will affect most manufacturing markets.

The data required to ensure the 4th IR becomes reality is vast, as is the potential to hack and steal proprietary information or the funds that flow between each part.

Torricel is a product of, and a solution for the 4th IR – allowing this constant flow, whilst providing security.

Database

Securing Big Data systems

Large databases are relied upon worldwide by governments, the military, institutions, blue-chips and SMEs alike.

They house a large mix of data types, spanning general mass data of low importance to highly sensitive and critical data.

Torricel protects sensitive data, ensuring access only to authorised personnel and systems - in specified volumes.

The Addressable Market

Torricel intellectual property is of core interest to businesses operating in the design and distribution of any technology based solution.

Silicon Chip Design, License and Manufacturing

Torricel ASCC Data Security Architecture can be integrated into multi-core silicon chips, including system on chip (SOC) designs.

Potential licensees include major processor designers and manufacturers, reaching markets as far and wide as mobile/smart devices, IOT products, home computing, industry workstations and servers.

Electronic Designers, Computer Builders and Integration

The big names in IT will all need a way to protect the systems they produce and install. From large scale datacentres and workstation deployments, down to local IP telephony and network switches, Torricel provides an affordable solution to large scale security integration.

Domestic Appliance & Smart / IOT Brands

From the smart fridge to the smart bulb, the number of devices in this space is increasing exponentially.

Major domestic appliance brands have a critical interest in protecting their end-user data (and in turn their brand). Aside from general product quality and user experience, the value the public will place on the security used within their appliance is growing and will continue to grow significantly, forcing the subject to be a core design requirement.

Furthermore, the UK government's 'Secure by design' public strategy will make low-cost architectural security (which Torricel offers) the go-to solution with all smart / IOT appliances.

Organisations and Institutions

These markets may not directly design or build the technology which they use, but they do influence, through specifying the capability and compliance of such systems.

Governments, military, banking / financial institutions, healthcare and other organisation types have protection of critical data as their current and ongoing core objectives.

Industry 4.0 Manufacturers

From hand-held manufacturing tools to large industrial plant and machinery, the manufacturers behind intelligent manufacturing have a significant obligation to secure their, and their customers' manufacturing data, in turn protecting new revenue models.

The Torricel Roadmap

Concept and Patent

- Initial Torricel concept : Jan 2018
- Keltie patent lawyers appointed : Feb 2018
- Patent process submitted : May 2018

Prototype, Demo & Realisation

- Jun 2018 : PCB Prototypes
- Aug 2018 : Software development for Bitcoin wallet proof of concept
- Sep 2018 : Fully working Bitcoin wallet prototype
- Oct 2018 : Top-tier custodial integration research
- Nov/Dec 2018: Investment sourcing / Customer research

Fundraise

- Jan/Mar 2019 : Seed investment

Full-Scale Monetisation

- Aug 2019 : Revenue from IOT / Smar Device / Crypto Licensing & Consultancy
- Feb 2020 : Revenue from silicon IP Block licensing

Founders & Advisors

Del Thomas
Business Director

Del has started, as well as driven the growth and success of multiple start-ups over the last 15 years. He has a proven track record of building highly-tuned organisations in the technology sector and an in-depth knowledge of the authoring, registration and delivery of patents and IP.

Paul Emerton
Inventor and Technology Director

Paul is a natural born tech geek starting in the '80s with a BBC Micro. He wrote his first data security system in the early '90s. In his working life he designed one of the first and most comprehensive TV Advertising algorithm-based analytics systems. He was recently contracted by an international aerospace and defence company for forensic data recovery and system repair. Most recently, his work on data security sparked the idea that became Torricel.

David Angell
Marketing, Communication and Engagement Coordinator

David for 15 years has been at the forefront of digital change, with expertise across the disciplines of digital marketing, SEO and communications. His career has seen him work at Google's EMEA HQ advising companies from SME to multi-national in digital advertising and analytics. He ran Online Communications for former Deputy Prime Minister Nick Clegg prior to and through the 2010 election, realising one of the first, and most successful UK digital political campaigns.

Keith Emerton
Technical Engineering Consultant

Keith's knowledge of strict military grade compliance and innovative efficient engineering led to him advising on the development of some of the core principals of the Torricel data movement architecture. His primary focus is on the highly controlled, audit-ready development of Torricel Data Control Standards and the co-design of the exclusive-OR network of data switches.

Paul Lucraft
Financial Compliance and Payments Consultant

Paul is an experienced Banking and Financial Services Expert. He initially qualified as a Chartered Accountant with what is now Deloittes and then worked for TSB and Lloyds TSB for 12 years in finance, credit risk and fraud prevention. Paul worked for MasterCard for 9 years, rising from regional Risk Manager to General Manager. Paul has since launched his own specialist payments and risk consultancy business and now works as a leading industry expert providing support to payments organisations, retailers and other businesses.

The Feedback So Far

"If you have what you say you have, it's a game changer."

CEO of Major Crypto

"Sounds amazing, how can we get custodial services?"

Leading Financial Institution

"This should be written in as a European standard."

Senior Committee Member
European Cyber Security, OBE

"On initial briefing, I couldn't believe it would work. In fact it's so counter-intuitive for today's approach to development, it's quite brilliant..."

Lead Programmer