T H E E L E C T R O N

N E W S L E T T E R O F T H E I N S T I T U T I O N O F E L E C T R O N I C S

Issue 42: Summer 2019

DATA CENTRE WORLD

Data Centre World was the largest of seven co-located exhibitions that took place at London's ExCeL Exhibition Centre on 12th. and 13th. March, representing the UK's largest technology event for business with around 220 exhibitors and around 100 presentations in four dedicated theatres:

*DCW Keynote featuring Edge and Future Strategies

*Facilities and Critical Equipment

*Energy Efficiency, Cost Management and DCIM

*Data Centre Design and Build and Physical Security

Topics included panel sessions on 'Competing with Cloud: How Data Centres can deliver Efficiencies to rival Public Cloud', 'Are Fully Sensed Data Centres becoming the new Norm/Reality?', 'Smarter Energy Use in Data Centres: What can be done and what are the Challenges?', 'How can we help Companies to connect Corporate Environmental Strategies with Data Centre Growth?', 'Powering the Data Centre of the Future', and 'Does the Data Centre Industry need a Standardised Set of Security Regulations?'

Other more specific presentations included 'Digital Transformation of Data Centres', 'Data Protection in a Cyber-sensitive World', '+AI leading the Way in Smart Data Centre Facility Revolution', 'Fundamental Obstacles for Cloud Buyers', 'Data Centre Resilience and Hybrid IT Infrastructures', 'All clear: How a UPS operates to clear Faults', 'Critical IT Facilities at the Edge', 'Inside the Prototype Boden Type Data Centre: Opensource Monitoring of Opensource Hardware', 'How to build and manage Green Data Centres', 'Smart and clean Power Generation for Data Centres', 'How to use EN50600 to design an Energy Efficient Data Centre', 'Cybersecurity in UPS Communications', and 'Five Essentials to unlocking Smart Cities'.

A notable new feature for 2019 was the Sixth Generation Data Centre, an area dedicated to innovation that aimed to provide an 'eye-opener' into the data centre industry of the future. It had eighteen sponsors, including OPS, Contour, Nedstack, Flakt Group, Prism Power Group, Riello UPS, and Wave2Wave.

Contour and Nedstack stated jointly that 'The introduction of PEM Fuel Cell Technology enables smart DC grids as data centre power concepts', whilst Wave2Wave showed how their ROME system 'closes the automation gap by bringing the physical layer under full SDM control'.

Supporting Exhibitions

The other exhibitions running alongside Data Centre World were Cloud Expo Europe (96 exhibitors), DevOps Live (29 exhibitors), Smart IoT (40 exhibitors), Big Data World and AI Tech World (57 exhibitors) and Blockchain Tech World (14 exhibitors).

There were around 750 presentations attached to these exhibitions collectively with theatres devoted to:

*Future of Finance

*Cloud Innovation

*Connectivity

*Infrastructure, Storage and Virtualisation

*Multi-cloud Strategy and Management

*Digital Transformation

*DevOps, Containers and Cloud Native

*DevOps Innovation

*Cloud and Cyber Security Keynote

*Cyber Innovations and GRC

*Security Strategies and Service Providers

*Cyber Threats, Intelligence and Response

*Security of Things

*Big Data World Keynote

*Data Analytics BI

*Machine Learning and AI

*AI Keynote

*Data Management and Integration

*Digital Disruption Keynote

*Shared Cities Showcase

*Transformation in Industry

*Blockchain Keynote

*Realworld DLT

In addition there were featured streams across all events covering 'Diversity and Inclusion', 'Talent and Skills', 'Leadership and Culture', and 'Techerati for Good', plus dedicated Oracle and Accelerator stages.

There were 93 Panel Sessions across these exhibitions with topics such as 'Using Predictive Analytics to build a better Future for Displaced Children', 'Getting Business Value from Data Analytics, Business Intelligence and Robotic Process Automation', The Future of Telco', 'The Future of Multi-cloud', 'Multi and Hybrid Cloud: Pros and Cons', 'Security of Connectivity between Cloud Environments', 'Scaling DevOps Culture into the Organisation', 'Enterprise Security in a Complex Cloud Environment', 'Securing against Emerging Tech', 'Ransomware - Learning and Prevention', 'Next Steps - the Integration of IoT and Blockchain', 'Securing IoT in the Smart City', 'Taking Data Centricity to the Heart of the Organisation', 'The Power of converging Business Intelligence and Data Science', 'How Finance is leading the Way in AI',

'Smart Cities: The Good, the Bad and the Ugly', 'The Security Challenge for Smart Cities', 'Turning Data into Insights', 'Unlocking the Blockchain globally: Opportunities in Emerging Markets', and 'Attracting and retaining Blockchain Developers'.

Specialist presentations included 'Securing a Digital Workplace across Multiple Hybrid Clouds', 'Accelerating the Journey to AI', 'Cloud Native Journey while building a Digital Bank', 'Team Viewer - Securing Remote Access for the Digital Age', 'The Role of Fast Data in the Continuous Hybrid Cloud', 'Machine Learning and Artificial Intelligence Trends within Investment Management', 'How to make the right Connectivity Choices when moving to SD-WAN', 'How SD-WAN Intelligent Routing enables Network Recovery Improvements', 'Zen and the Art of Cloud Data Storage', 'Improving Digital Transformation with Enablement Pods', 'Leveraging Unsupervised Machine Learning with Continuous Delivery', 'How to survive in the Kubernetes Kingdom', 'Debugging Services in Kubernetes with Linkerd 2.0', 'Successful Multicloud Implementation using DevOps and Active Testing', 'Flying with Kubernetes', 'Enabling DevOps Practices within Legacy Environments', 'IP Strategies in the Cloud', 'Observing Enterprise Kubernetes Clusters at Scale', 'When the Cloud attacks', 'Incident Response in the Cloud in the GDPR World', 'How Capita is creating better Outcomes with Cloud Technologies', 'Using the Cloud to secure the Cloud: How Crowdstrike harnesses Cloud Infrastructure to combat Threat Factors', 'Reinventing Identity Management at the BBC', 'How to hack a Police Station', 'Building Photobox's Cloud Security Team', 'Using Deception Technology for Tailored Cyber Security Threat Intelligence', 'The Future Impact of AI on Cyber Crime', 'The Data Ethics Landscape in 2019', 'Putting your Data to work with AI', 'HomeServe's Journey towards Data-driven Decisioning', 'Lessons from the Field - Achieving Data Centricity', 'AI and Machine Learning Opportunities in the Insurance Industry', 'AI and Business Development at Stena Line', 'Flying High: Shaping the Future of Drones in UK Cities', 'How IoT and the Cloud are revolutionising Buildings and Cities of the Future', '5G Smart Tourism', 'Transforming Retail withIoT', 'Can Blockchain restore Trust in the Food Supply Chain?', and 'Securing the Blockchain with Multi-party Computation'.

Below a review is presented of some of the hot topics that have been making headlines at the event and in the media.

DIGITAL TRANSFORMATION: PRESSURE MAY LEAD TO WASTEFUL PROJECTS

A study by Couchbase has revealed that out of 450 heads of digital transformation in the UK, US, France and Germany over half (52 per cent) believe that an over-fixation on digital transformation is creating pressure to transform that could lead to rushing in to poorly conceived projects.

35 per cent stated that the primary driver for digital transformation is advances made by competitors, with 23 per cent citing changes in regulations and 19 per cent pressure from customers, leading to the conclusion that digital transformation is primarily being driven reactive needs rather than proactive ideas. 64 per cent believe that those that cannot keep up with digital innovations will go out of business or be absorbed by a competitor within four years, yet 95 per cent believe that digital transformation can appear to be an insurmountable task, suggesting that projects could prove to be unsuccessful.

Other findings were that 88 per cent of organisations had had a digital project fail, reduce in scope or suffer significant delays because their legacy database could not support it, whilst 87 per cent had needed to scale back ambitions for new applications and servicdes so that they will work with IoT or mobile devices, since these devices cannot match the data processing power of larger servers or guarantee a consistent connection.

Matt Cain, CEO of Couchbase is quoted in the September 2018 issue of *Digitalisation World* as follows:

"We are entering the era of the massively interactive enterprise where every part of an organisation, from sales and marketing to HR, finance and logistics, is built around engaging digital experiences. The revolutionary potential of digital transformation will have a hugely positive impact for those organisations that can do it well. However, the pressure to transform at speed means organisations have a higher risk of taking a rushed, reactive approach, driven by fear that the organisation will lose relevance, that results in substandard experiences and wasted investments. Transformation is not a destination. It is a continuous process that, at its best, is proactive, driven by the needs of the business as a whole and underpinned by the right data infrastructure. By adopting this approach and not letting the pressure face them, organisations can join the ranks of the leading 25 per cent."

SMART POWER GENERATION FOR DATA CENTRES

All data centres require a reliable and affordable power supply, which has traditionally been provided from a combination of grid electricity (for affordability) and diesel generators (for reliability). This method, however, has drawbacks such as dependency on increasingly unstable power prices and high local emissions from the generators that could potentially jeopardise the granting of environmental permits.

In the white paper with the above title Data Centre World exhibitor Wartsila Energy Business proposes the alternative of gas-fired engines to create the affordable and reliable power supply that is required, stating:

'State-of-the-art gas engines are capable of starting up just as fast as diesel engines, but unlike those, they are able to competitively generate power not only in emergencies, thus recouping their costs and even generating additional profits.'

It is argued that it makes sense to replace the engine-generator sets suitable only for emergencies with ones that can operate efficiently whenever it makes economic sense, even continuously if desirable.

Selection of a power generation technology for reliable emergency power supply applications is restricted by:

(i) Very rapid automatic start-up.

(ii) Modularity of capacity

(iii) Ability to run on locally stored fuel

(iv) Technological maturity

Until recently only water turbines and diesel engines could start up and reach full or nearly full power within one minute as required, and water turbines are only possible in a few geographically favourable locations. Furthermore, the modularity requirement combined with typical data centre power demands and the overnight costs of installation restricts this further to relatively small high-speed diesel engines that operate using light fuel oil stored on site.

These generators effectively serve as an 'insurance' that just covers emergency situations, but with 21st. century gas engine technology the economics of this solution are now being questioned. There has been, for example, a notable advancement in start-up time for gas engines:

'Recent development and testing has conclusively demonstrated that state-of-the-art gas engines may be started and brought to full power in considerably less than one minute of the starting order, which brings them within the world of emergency power supply.'

There has also been progress in the area of fuel storage with the emergence of small-scale affordable gas storage technologies, especially for liquefied natural gas (LNG), and dual-fuel technology that allows a power generation facility to operate using either gaseous or liquid fuel and to switch between them when running under load.

In addition the carbon footprint tends to be lower than that of grid electricity suggesting that 'operating the generating sets continuously instead of relying on grid would have a positive effect on the carbon footprint of the data centre'.

The paper states:

'If the data centre has a power generation facility that can be operated continuously, runs on an inexpensive fuel, and has a very low emission footprint, then it may very well be used as a primary source of power. Because of the way in which emergency power systems are normally designed - with capacity redundancy and concurrent maintainability that ensures that capacity sufficient to cover the data centre's critical load is always available - such a plant would be able to provide power supply without any interruptions, with the maintenance of individual pieces of equipment not interrupting operation. This approach would practically reverse the traditional way of operating a data centre - now the local power plant would become the primary source of electricity, while the grid would only be a back up.'

The paper concludes with a set of frequently asked questions, one of which is 'The quick start of a gas engine is very valuable, but what about output parameters? Are frequency and voltage stable enough for sensitive applications?'

The answer is given as follows:

'Tests of state-of-the-art gas engines reveal that voltage and frequency values are very stable and in line with typical data centre industry requirements. At this moment, it is combustion control that is the limiting factor for loading rates; whenever the engine can operate in a stable manner, the voltage and frequency parameters are well within typical limits.'

PATENT FOR INTEGRATED ELECTRONIC LOCKING ON INTELLIGENT PDUs

Chatsworth Products have been granted a patent for a new cost-effective simplified electronic access control product for data centre cabinets.

The new technology combines access control, intelligent power management and environmental monitoring into a single integrated platform.

Increasing migration toward remote edge compute sites and multitenant data centres has created a need for effective remote management of the data centre cabinet, whilst growing data privacy regulations such as the Payment Card Industry Data Security Standard (PCI-DSS) and GDPR have fuelled a need for improved cabinet access control.

The US Patent covers the integration of the functions of a rack power distribution unit (PDU), electronic access control and environmental monitoring into a single appliance within the cabinet. Through Chatsworth Products' intelligent eConnect® PDU, data centre managers can integrate environmental sensors and electronic locking capability as a single solution. Users can view and manage power at each outlet and cabinet, monitor the status of environmental conditions and control each cabinet access attempt within an audit trail report that is easily exportable via a user-friendly web interface.

In addition, these three systems can be linked through Secure Array™ IP Consolidation, allowing up to 32 PDUs, 32 EAC kits and 64 environmental probes to be networked under only one IP address, offering considerable savings in networking costs:

'A row of 16 cabinets with two PDUs each would only require two network connections with Secure Array, but would need up to 32 network connections in a standard deployment.'

Donald Conner, Electronics and Software Engineer Manager for Chatsworth Products states:

"The integration of EAC into the rack PDU continues our focus on simplification and efficiency for the CPI [Chatsworth Products] ecosystem. We wanted to bring a simple, cost-effective cabinet access solution to market without adding complexity to the data centre."

Further Information

Chatsworth Products were an exhibitor at Data Centre World and may be contacted at Chatsworth Products Europe, Cavendish House, Bourne End Business Park, Cores End Road, Bourne End, Buckinghamshire SL8 5AS. Telephone: 01628 524 834. www.chatsworth.com

NEXT GENERATION HIGH POWER MODULAR UPS

Data Centre World exhibitor Borri SpA has unveiled its next generation High Power Modular UPS for data centre power protection solutions, the UPSaver 3vo, a modular, scalable and flexible UPS that offers 'an adaptable approach to changing data centre demands, scaling or adding redundancy at any time'.

The UPSaver 3vo integrates with Borri 3-L Green Conversion technology based on a patented control algorithm that manages the 3-level battery-inverter subsystem to enhance system efficiency and extend battery life with lower costs.

The system features four flexible operating modes to optimise efficiency and maintain total system reliability:

* Double High Efficiency mode (all the online double conversion protection - VFI-Voltage frequency independent mode - at 97 per cent efficiency with Borri-patented 3-L Green Conversion technology).

* Very High Efficiency mode (maximum efficiency in unstable mains conditions with Active Filtering, the Borri Voltage Independent mode offering 97.5 per cent efficiency).

* ECO mode (for stable mains in Voltage Frequency Dependent mode offering 98 per cent efficiency).

* Ultra High Efficiency (the most innovative technology for data centre equipment total protection with 99.5 per cent efficiency and minimum cost of ownership).

Commenting on the launch Enrico Simone, Chief Technical Officer for Borri, said:

"With the UPSaver 3vo we are proving our customer with the superior technology, great ease of use and an extremely flexible layout that can be designed around new or existing data centres. Saving energy is one of the main focuses in the data centre industry due to rising energy bills and environmental constraints. This is one of the reasons why we've integrated UPSaver 3vo with the 3-level Green Conversion technology. This patented algorithm helps improve a data centre Power Usage Effectiveness and reach 97 per cent VFI efficiency at any load."

Further Information

Borri Group is a global provider of power electronics systems and solutions for harsh industrial and demanding commercial and ICT secure power requirements merging over eighty years of experience in developing, manufacturing and supplying uninterruptable power systems and solutions. The company is comprised of three business units: Industrial Power, Critical Power and Renewable Power, and has its headquarters in Bibbiena, Italy. They may be contacted on +39 0575 5351 or at www.borri.it

FIRST THERMAL MONITORING SOLUTION TO TRACK DATA CENTRE COOLING LOADS IN REAL-TIME

Data Centre World exhibitors EkkoSense have launched EkkoAir Wireless, the world's first thermal monitoring solution to track data centre cooling loads in real-time, using standard temperature and current measuring sensors that can be installed in any chilled water or direct expansion cooling system.

As part of the EkkoSense Critical Things® family, EkkoAir Wireless sensors continually monitor air inlet and outlet temperatures, along with fan motor current, so as to detect subtle changes in airflow that can may be indicative of problems with fan performance, as well as identify when filters are dirty and provide alerts on potential CRAC/AHU blockages.

The company states:

'Combining EkkoAir Wireless cooling duty data with distributed temperature measurements from EkkoSensor wireless temperature and humidity sensors provides true, real-time insight into overall data centre cooling duty performance. Using EkkoAir Wireless data with EkkoSoft® Critical thermal modelling, monitoring and visualisation software also offers an intuitive, 3D real-time view of cooling performance across entire data centre estates, providing insight into any cooling resources that are not being used efficiently.

EkkoAir Wireless uses the same wireless infrastructure as EkkoSensors, and all measurement data is encrypted with 128-bit AES encryption before transmission to an EkkoHub wireless data receiver for forwarding to our cloud-based EkkoSoft visualisation and analysis software. Each sensor is uniquely identified at manufacture and associated with a specific CRAC/AHU at installation. EkkoAir Wireless devices can be powered from an existing low voltage supply, from the monitored equipment or from an internal battery.

EkkoAir Wireless is housed in a standard DIN rail mount enclosure with two compact temperature and humidity sensors that connect via small cables. Sensors can be fixed in position using screws, cable ties or an integrated magnetic mount. The humidity sensing element is protected with a PTFE membrane to avoid measurement errors caused by dust build-up. Single or three-phase fan current measurements are made using standard millivolt output current transformers. An opto-isolated 12V-24V AC input is provided. This can be used to monitor the operating status of the CRAC/AHU.

EkkoAir Wireless transmits data at intervals of between 30 seconds and 10 minutes. Data can either be transmitted as an instantaneous value, or as the average from multiple measurements spaced evenly through the transmit interval. This ensures that changes in AHU/CRAC operative conditions between transmissions are captured.'

Further Information

Further information may be obtained from EkkoSense, Sir Colin Campbell Building, University of Nottingham Innovation Park, Triumph Road, Nottingham NG7 2TU. Telephone: 0115 823 2664. Email: info@ekkosense.com

YELLOWFIN PUBLISHES GUIDE TO AUTOMATED ANALYTICS

Yellowfin, a global business intelligence and analytics software vendor, and exhibitor at Big Data World, has recently published a Guide to Automated Analytics that aims to assist businesses to reduce their dependency on accidental data discovery.

It is argued that the accidental nature of data discovery combined with the sheer volume of data to search through frequently means that it takes more than one business person to notice that something feels "off" before issues are investigated. Even when someone does voice a concern, it takes critical KPIs to be affected before investigations begin. This can take weeks or months and it can be 'a disaster for the business bottom line'.

The Guide highlights three specific problems that hamper access to data insights, namely:

1. Dashboards (set up for monitoring KPIs and good for that, but not good for data discovery).

2. Constraints on the analytics team (the analytics team's capacity cannot match the influx of data or the demand for their skills).

3. The 'Christopher Columbus' approach to data discovery (days and weeks of mostly educated guessing to find statistically significant deviations in data that matter to the business - analysts cannot know what to look for unless there has already been an indicator of data change uncovered).

Yellowfin proposes automation of data discovery to remove the accidental component of uncovering insights and end what it calls 'dashboard data discovery':

'Automated analytics should not be limited by the dashboard interface or its in-built interactions; it should trawl your live, dimensional data at its source. If it finds a statistically significant anomaly, trend change, spike, dip etc. it should notify you so that you can act instantly. This means that you are not glued to your dashboard trying to slice and dice for more information. Automation will tell you about a change the moment it happens.'

Yellowfin's solution is the automated data discovery tool Yellowfin Signals:

'Signals is a platform agnostic and automatically and continuously discovers and surfaces the most important changes in your live data as they happen. There's no need to manually upload data into workbooks. Signals ensures that discovery is instant and predictable instead of accidental'.

Further Information

Yellowfin is ranked among the top five analytics platforms across all 15 Gartner Critical Capabilities for Analytics and BI Platforms. Copies of 'A Guide to Automated Analytics: How to stop running your Business on Accidental Data Discovery' may be obtained from Yellowfin EMEA, Unit 10, Whittle Court, Knowlhill, Milton Keynes MK5 8FT. Telephone: 01908 887 225.

CASE STUDY: GATESHEAD HEALTH NHS TRUST

Gateshead Health NHS Foundation Trust runs the Queen Elizabeth Hospital, Dunston Hill Hospital, QE Metro Riverside and some services at Bensham Hospital within Gateshead, Tyne and Wear. It also runs services from Blaydon Primary Care Centre. With approximately 4,500 employees, its primary function is to deliver acute services in hospital, emergency care services and pathology.

It is a digitally mature Trust that has been linked to Newcastle University Hospital as a fast follower, as part of the Global Digital Exemplar programme. It used Cognos and QlikView, but these were not being used to their full potential:

'QlikView was used exclusively for financial information, so it was impossible to add in additional data sources. Cognos was difficult to use and any new reports had to be built by BI developers'.

As part of the NHS the Trust has to work towards nationally mandated performance and KPI metrics, which requires a huge amount of focus due to the risk of financial and reputational damage if they are not met:

'An analyst would spend two days a week on a Refer to Treatment Time (RTT) report - aggregating data, visually checking it and applying business rules within Excel before distributing the report to a wide number of Waiting List Managers, Service Line Managers and Directors who would then validate the numbers and review any poorly performing patients'.

This situation was reviewed by David Thompson, Information and Development Manager, who identified a potential for Yellowfin:

'Yellowfin is accessed by over 100 people within the Trust: The Finance Team, Service Line Managers, Clinicians - medical staff and surgical staff who are responsible for clinical care, Waiting List Managers, Directors and Executives, and various others. Using Yellowfin's API functionality, Yellowfin-driven content is consumed by hundreds of people beyond those with a licence.

Waiting List Managers can track patients on various patient waiting list bandings. Yellowfin allows them to review their current position and pinpoint those at risk through a high-risk report and an early warning report.

The Chief Clinical Information Officer is now able to track and manage clinical metrics like "Patient Flow" to ensure patients are being seen as quickly as possible, and that any ancillary services like nutrition or physiotherapy are being delivered effectively so that patients can be discharged as quickly and as safely as possible'.

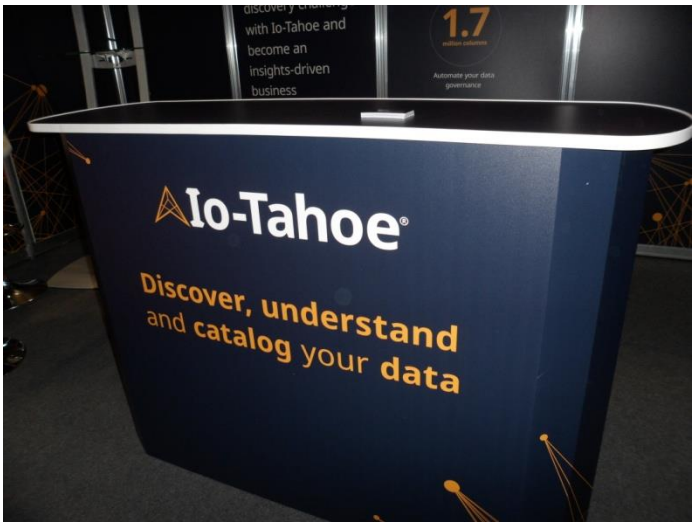
David Thompson states:

"By decentralising reporting a far greater number of people can now create content, so it's reduced the pressure on training and retraining technical staff. Our analysts used to spend a disproportionate amount of time data processing rather than data analytics. Yellowfin cuts a lot of that out. I would say that so far Yellowfin has saved us approximately six to eight days of data preparation a month and improved our visibility across the business into our KPIs and performance metrics.

The financial element of reporting is very complex within the NHS with different levels that impact income, coding and how long a patient is in hospital. As a result it's not always easy to identify drops in income. I'm keen to see if Yellowfin Signals can help us to identify the reasons for these drops and spikes in income".

Contact details as above.

CASE STUDY: CENTRICA



Also exhibiting at Big Data World was Io-Tahoe, whose smart data discovery tool has recently been deployed at Centrica, the multinational energy and services company with its headquarters in Windsor, Berkshire.

Centrica had an enormous amount of information about its customers globally resulting in a substantial amount of accumulated data, as well as confidential corporate information. With GDPR there was a considerable amount of pressure to determine exactly what information the company had and where it resided. This meant that implementing a data discovery strategy became a key focus.

In September 2017 Centrica investigated the concept of smart data discovery, which led to Io-Tahoe's advanced platform. A pilot project was initiated across four data sources. Io-Tahoe's sensitive data discovery capability enabled 30 billion records and 1.07 million columns to be processed in a fraction of the time that was first envisaged. The results were fed back to the architecture team, who then endorsed it for data discovery.

Even the initial project was large in scope with Io-Tahoe being deployed across 16 HP servers, each holding petabyte-sized loads. One data source alone was 40TB, and the team

worked with over 1,200 databases and 1,500 applications covering millions of customers and associates.

Team Leader Daljit Rehal stated:

"Using Io-Tahoe enabled us to connect to each data source and scan each source. It certainly validated a whole heap of assumptions, such as duplicated data across multiple sources. We knew that would be the case, but Io-Tahoe allowed us to quickly articulate what and where it was".

This provided a solid picture of what sensitive data resides where, which enabled the ranking or classification of apps by potential risk. To put things into perspective the company had a side-project that took personal information residing in non-production systems that was examined by a third party that spent eight months cataloguing four data sources as against 22 data sources in one month using Io-Tahoe.

Implementing Io-Tahoe as part of Centrica's smart discovery platform enabled the team to know where to look for any given data, as well as establishing who has access to it and for what purpose. Another key advantage has been the ability of Io-Tahoe to work with the data itself, rather than having to rely on metadata.

Daljit Rehal concludes:

"Our customers have a right to know what data we hold about them. Our work has enabled the team to narrow that search. We know where that personal data resides exactly, so that when someone contacts us we know exactly where to look. We've developed a more automated approach to subject access requests. Previously we had to go logging on from app to app, and it was very much a manual process. Io-Tahoe has enabled us to develop a streamlined solution that's sharply reduced both our time and our legal exposure".

Further Information

The report 'Io-Tahoe's Smart Data Discovery accelerates Insights from Centrica's Sensitive Data Landscape' was published in February 2019 and may be obtained from Io-Tahoe LLC, 111 Broadway, Suite 601, New York NY 10006, U.S.A. www.io-tahoe.com

ROBOTS TO REVOLUTIONISE TRANSFORMER INSPECTION

Transformers are critical elements of power networks and when they fail unexpectedly the impact on critical infrastructure such as hospitals and industry can be catastrophic. With the average age of installed large power transformers in the US now around 40 years, and the situation little better in the UK, many experts are of the opinion that more needs to be done to mitigate failure risks through early detection and improved inspection. Invasive onsite surveys, however, have traditionally been both costly and dangerous to undertake.

Now, Data Centre World exhibitors and sponsors of the Energy Efficiency, Cost Management and DCIM Theatre, ABB, have developed a robotic solution that is set to revolutionise the internal inspection of transformers, improving safety, avoiding extensive downtimes and reducing maintenance costs.

The article 'Transformers: Robots to the Rescue?' by Louise Frampton in *Mission Critical Power* , Issue 20, February 2019, explains more:

'The conventional approach to inspecting transformers requires taking a unit out of service before draining it down; a technician will then enter the transformer to visually check the condition of components such as the windings, tap changer, insulation and seals. This is a complex process that requires a risk assessment and a confined space entry, as well as time for cooling, draining down and oil handling. It can require an outage with a total duration of three or more days.

Not only does this approach involve a great deal of complexity and time, it carries with it a potential risk to human life and the risk of damage to the asset'.

ABB's solution is the submersible TXplore, which is designed to enhance safety by eliminating the confined space risk to the technician, the risk of the technician causing damage whilst inside the transformer, and the environmental and safety risks associated with oil spillage (because the oil stays in place throughout the inspection). A full inspection can be completed in less than a day:

'The submersible robot is designed to balance ease of navigation with robustness, allowing the inspection of all areas of interest, such as bushings, leads, tap changer, core tap, core support and insulation etc. With the preservation of mineral oil quality of primary importance, the robot construction is optimised to leave no detectable footprint - either chemical or physical - as it operates within the transformer. The outer shell is also made of a high-performance plastic, which minimises the risk of electric coupling and structural damage to the transformer.

As the robot enters the unit instead of a human, no medical or environmental safety team is required during inspection. Only two employees, a robot pilot and top-side equipment operator are needed on site, which results in a dramatic reduction in personnel, time and costs, compared with human inspection. This would normally require a large team and downtime of three or more days'.

Ability Power Transformer

In addition to the above, in April 2018 ABB also launched the Ability Power Transformer, which connects through a set of diagnostic tools to deliver real-time performance data and insight into operations.

The same article states:

'The build-up of heat, dissolved hydrogen gas and moisture in the insulating mineral oil in transformers can all lead to premature failure or significant damage. These types of contamination reduce the dielectric strength of the oil as well as the cellulose paper insulation wrapped around the windings in some models.

Therefore, in the new digitally enabled transformer, sensors can measure not only the temperature of the oil, but also key components inside the transformer, while monitoring oil quality and the accumulation of gas'.

Further Information

More information on this subject and other ABB innovations may be obtained from David Watton on 0115 964 3725. Email: david.walton@gb.abb.com

QUBE CINEMA REVOLUTIONISES DIGITAL CINEMA DISTRIBUTION

Qube Cinema is a leading manufacturer of servers, projectors, mastering and distribution technology for digital cinema, which has taken over from the traditional, more expensive more expensive method of physically transporting multiple reels of film prints. In addition, digital films do not degrade over time and can be projected using less-skilled labour. Security, however, has been an issue, causing the film industry to tend to lag behind other industry sectors when it comes to making the transition from analogue to digital.

Content owners (companies producing films) have been especially concerned about piracy, but theatre owners and distributors did not want the burden of cost and complexity associated with providing security against it. Qube Cinema therefore sought to provide a pioneering solution that enabled the efficient management of digital cinema keys online combining the highest levels of security with ease of operation.

For this Qube Cinema turned to nCipher Hardware Security Modules (HSMs). With digital cinema, movies are encoded and encrypted into a Digital Cinema Package, or DCP, and distributed via hard drive or satellite feed from which they can be decrypted at the theatre or cinema using information contained in a unique Key Delivery Message, or KDM. This unlocks the film for a specific theatre or cinema for a specific timeframe and number of showings. Content owners, however, were uneasy about the software-based in-house encryption measures typically used by distributors, and particularly the possibility of losing the encryption keys and becoming locked out of their own content.

The new solution, called KeySmith, effectively cures this problem. With it, a studio or independent film maker submits a movie for distribution, which then gets converted into a DCP, within which a set of AES keys are used to encrypt individual files. A Distribution KDM, or DKDM, that securely carries these keys is then made available to the distributor's KeySmith account. This DKDM enables KeySmith to generate KDMs for individual theatres and cinemas. The nCipher HSMs create a unique RSA public/private key pair and associated digital certificate for each company within KeySmith. These HCMs encrypt the AES keys with the recipient theatre/cinema's public key using an application that runs inside the certified security boundary of the HSM. Only the intended recipient can decrypt the package with the associated private key, which is unique and securely installed at manufacture.

The nCipher HSMs provide a hardened, tamper resistant environment for performing secure cryptographic processing, key protection and key management. They are certified by independent authorities, establishing quantifiable security benchmarks.

Further Information

nCipher Security was an exhibitor at Cloud and Cyber Security Expo and may be contacted at www.ncipher.com

CLOUD AND HEAT TECHNOLOGIES LAUNCH WORLD'S FIRST ENERGY EFFICIENT SUPERCOMPUTER

At Cloud Expo Europe Cloud and Heat Technologies, a specialist in the planning, building and operation of energy and cost-efficient data centres, launched 'The Beast', the world's most energy efficient supercomputer.

Its impressive technical specification incorporates a total output of up to 500kW, with the ability to be equipped with up to 17,280 CPU cores or up to 1,056 GPU nodes. It is housed in a durable 20-foot container and, utilising Cloud and Heat's waste heat recovery system, it can be operated across a wide variety of climate zones.

The company states:

'Energy consumption in the global data centre market continues to grow rapidly, because of the huge volumes of data now being created, stored and processed. With investment support from ETF, this new system enables customers to make the most energy efficient use of virtual servers. It will also allow users to capture and then re-use the waste heat generated which can lower the overall energy consumption as it is recycled for use in heating buildings and water'.

Cloud and Heat Technologies Chairman, Bill Joss, added:

"We believe this new system can help the UK industry reduce its electricity costs by up to £111 million annually and reduce the equivalent amount of carbon emissions produced by the UK as 127 wind turbines.

We are delighted to be working with air conditioning specialists STULTZ as we launch into the UK market. This means we can offer their customers access to a combination of cloud-based computing power and decentralised heat generation as a proven solution satisfying a broad range of applications".

Further Information

Cloud and Heat Technologies was founded in 2011 and is based in Dresden, Germany. Its stated mission is to make sustainability the driver of innovation. The company builds and operates energy-efficient, green, reliable and scalable data centres that meet the demands of the cloud future. It offers private and public OpenStack-based cloud solutions in customised IT infrastructure solutions and large IT infrastructures with a holistic combination of cloud and heat solutions. In both of these fields Cloud and Heat Technologies uses the latest generation of the hot water direct cooling system that they developed and patented.

Cloud and Heat Technologies' systems have been successfully deployed across the globe in the areas of high-performance computing and on-premise cloud. The company also supports data centre operators and project developers in their drive toward green building initiatives and consumer solutions, particularly in edge computing architectures, IoT and digitisation projects.

In addition to IT cooling, efficient heat recovery is at the heart of the company's solution. Its patented technology enables the company to manage the heat produced by the IT equipment to a constant temperature of 60 degrees Centigrade and export it to heat buildings and water. This technique both lowers the cost of cooling the data centre and recycles heat and hot water so as to reduce the carbon footprint of IT systems.

More information may be obtained from www.cloudandheat.com

FIRST SERVERLESS FUNCTION ASSURANCE FOR SECURING SERVERLESS ENVIRONMENTS

Also exhibiting at Cloud Expo Europe was Aqua Security, the leading platform provider for securing container-based and cloud native applications, who have recently launched version

4.0 of the Aqua cloud native security platform, which introduces new security and compliance controls for serverless functions and Linux hosts.

Aqua's comprehensive serverless security solution now includes a full chain of controls to discover functions across multiple cloud accounts, scan them for vulnerabilities, detect excessive permissions and configuration issues, and provide function assurance - preventing the execution of untrusted or high-risk functions based on defined policies.

The key controls for serverless environments include:

* Functions discovery (creating an inventory of functions stored across cloud accounts).

* Vulnerability scanning (deep scanning of functions packages and dependencies for known vulnerabilities, known as CVEs, based on multiple sources and supporting multiple programming languages).

* CI/CD integration (so-called 'shifting left' beyond scanning functions by providing development teams with plug-ins for Continuous Integration environments to detect security issues as functions are being built).

* Permissions Assessment (identifying use of excessive or over-provisioned permissions specific to the serverless cloud environment, and monitoring for unused permissions - reducing the possible attack surface of a function).

* Sensitive Data Assessment (detecting secrets and hard-coded keys within the functions themselves, or within environment variables, specific to the cloud environment - for instance AWS credentials or Azure Authentication keys).

* Function Assurance (ability of security teams to set policies to determine the risk threshold to allow or disallow function execution, based on a variety of factors including CVE severity, CVSS score, sensitive data and permissions).

* Function Anomaly Detection (monitoring of function usage patterns and alerting on sudden spikes in the frequency or duration of function execution).

Aqua 4.0 incorporates:

* Malware scanning (detecting malware in the host OS or any of its components).

* Vulnerability scanning (scanning for CVEs found in the host operating system or any of its components).

* Whitelisted or Blacklisted users and OS packages (so teams can specify which types of users or OS packages are either allowed or forbidden from being used on a host).

* User Activity Monitoring (Aqua now logs all user commands on the host OS for security and compliance tracking, in addition to the previously available user logins and login attempts tracking).

* Centre for Internet Security Benchmarks Testing (having achieved CIS certification for its Kubernetes benchmark, Aqua now provides detailed information on each benchmark test success/failure to provide teams with remediation information).

* Custom Benchmark Scripts (enabling the upload of scripts that customise benchmarking to account for configurations that are not supported in the standard CIS benchmarks, including Kubernetes clusters on Red Hat OpenShift).

* Host Assurance (allowing setting of policies that will determine a threshold for host compliance and security risk based on the results of the above scans and checks and generate alerts and audit events upon policy violations).

Commenting on the launch on March 4th., Amir Jerbi, Chief Technical Officer and Co-Founder of Aqua Security, said:

"The new technologies supporting cloud native applications require a holistic approach to security and compliance across the application lifecycle as well as up and down the stack, and this has become more evident in recent months with significant vulnerabilities discovered in Kubernetes and runc [a component used in most container runtimes which is part of Linux OS distributions]. With this new release from Aqua, our customers can protect their applications against those as well as yet undiscovered vulnerabilities, by implementing tight compliance and whitelisting-based zero-trust security".

Further Information

Aqua was founded in 2015 and is backed by Lightspeed Venture Partners, Microsoft Ventures, TLV Partners, and IT security leaders. It is based in Boston, Massachusetts, U.S.A. and Israel.

Aqua Security enables enterprises to secure their container and cloud native applications from development to production, accelerating application deployment and bridging the gap between DevOps and IT security. Aqua's Cloud Native Security Platform provides full visibility into container activity, allowing organisations to detect and prevent suspicious activity and attacks in real-time. Integrated with container lifecycle and orchestration tools, the Aqua Platform provides transparent automated security while helping to enforce policy and simplify regulatory compliance.

Aqua 4.0 builds on previous Aqua host protections that already included testing hosts according to CIS benchmarks, scanning hosts for known vulnerabilities and monitoring user logins.

More information is available from www.aquasec.com

DIGITAL CATAPULT LAUNCHES IoT MANUFACTURING TRIAL

Two UK businesses have been selected to take part in an 'industry first' £230,000 national digital pilot project to demonstrate the power of IoT in manufacturing.

Digital Catapult will run the project, known as The Connected Factory Demonstrator, in which Dyer Engineering Group and Special Metals Wiggin will explore how IoT and LPWAN can improve productivity, streamline processes, improve yield and enhance quality control.

Jonathan Silk, Quality and Technical Director for Hereford-based Special Metals Wiggin, which manufactures a range of nickel alloys for the aerospace, energy, marine, automotive and nuclear industries, is quoted in the February 2019 issue of *Networking* as follows:

"We anticipate that by introducing state-of-the-art wireless technology we will make significant advancements in process control and asset tracking. This will enhance our position in a highly competitive worldwide market for the supply of nickel alloys. We look forward to the opportunity of working with Digital Catapult and the solution providers".

Also quoted is Jeremy Silver, Chief Executive Officer of Digital Catapult, who says:

"The impact of advanced digital technologies cannot be underestimated, and we're looking forward and we're looking forward to working with Dyer Engineering and Special Metals Wiggin to demonstrate the full potential of future networks technologies in a working manufacturing environment".

ON-CHIP OPTICAL CONNECTION BREAKTHROUGH

Researchers at the University of Twente in The Netherlands claim to have successfully connected two parts of an electronic chip using an on-chip optical link.

Previously an optical link was not possible using standard silicon chip technology, but PhD student Vishal Agarwal evaluated how to develop a very small optocoupler circuit that delivers a data rate measured in megabits per second and in a very energy-efficient way.

The article 'Light connects Two Worlds on Single Chip' in Issue 16, Q1 2019, of *Optical Connections*, explains the development as follows:

'Using light, it is possible to isolate one part of a single chip from another - the two different worlds will be able to communicate, but there is no electrical connection. In "smart power" chips, for example, the high-power part can be isolated from the digital control circuits. Such isolation ensures safe operation in applications like medical electronics and automotive systems.

A so-called "optocoupler" is demanded by such situations, but until now this has always been a relatively bulky device, and separated from the actual electronic chip'.

The new pioneering optocoupler can be integrated with the electronics using standard chip technology (CMOS) and measures 0.008 square millimetres.

NANOSIZED AMPLIFIER HELPS LIGHT SIGNALS PROPAGATE THROUGH MICROCHIPS

Researchers at Aalto University in Finland have developed a nanosized amplifier that helps light signals propagate through microchips.

The researchers made their breakthrough with the help of a Finnish invention known as the atomic layer deposition method, which is seen as being a promising method for developing microchip photonic processes, and ideal for processing various kinds of microcircuits as it plays an important role in manufacturing the latest microprocessors.

The above journal in the article 'Data-transmitting Light Signal boosted by Nanosized Amplifier' (p.5) quotes doctoral candidate John Ronn as follows:

"Photonics, or light transfer, that is already widely used in Internet connections, is increasingly being used by microcircuit systems because light is a more energy efficient and faster way of transferring data than electricity. The increase in information also requires an increase in performance. Boosting performance through electronic methods is getting to be very difficult, which is why we're looking towards photonics for answers."

In the development of photonics, however, new components will also have to work cooperatively with electronics-based systems:

"Silicon is a key material in electronics, and that's why it is also included in our light amplifier along with the amplification element erbium.

Today's compound semiconductors, which are used, for instance in LED technology, can also be used effectively in light amplification. That being said, most compound semiconductors are not compatible with silicon, which is a problem for mass production".

Professor Zhipei Sun is also quoted:

"Our international collaboration made a breakthrough with one component: a nanosized amplifier. The amplification that we got was very significant. But we'll still need more components before light can completely replace electricity in data transfer systems. The first possible applications are in nanolasers, and in sending and amplifying data".

APPLIED OPTOELECTRONICS PROVES OBO FEASIBILITY AND SAMPLES 400G SILICON-PHOTONICS OPTICAL MODULE

Applied Optoelectronics is demonstrating the feasibility of its silicon photonics platform for the requirements of on-board optics (OBO) by sampling 400G optical modules based on silicon-photonics technology.

The modules are designed to meet these requirements, as outlined in specifications such as the recently released version 1.1 of the onboard optical module specification published by the Consortium for Onboard Optics (COBO).

OBO modules can be used in higher-speed data switches, with interface speeds ranging from 400Gb/s to 1.6Tb/s. By designing these modules to be mated directly to a circuit board in such a switch, an increase in the density of optical interfaces to the switch is enabled.

The sample modules are designed for customers developing next-generation switches for large data centres, as these switches gradually evolve from 100Gb/s interconnects to 400Gb/s and higher. They leverage new silicon-based optical technology to support 16 optical channels with a total throughput of 400Gb/s.

Future versions of the device are expected to use the same technology, but increase the bandwidth to 100Gb/s per optical channel, ultimately enabling 1.6Tb/s of data throughput over a single OBO module.

[Reference: *Fibre Systems*, Issue 23, Spring 2019, p5]

BLOCKCHAIN: SOME RECENT DEVELOPMENTS

Blockchain and Distributed Ledger Technology are very much emerging disciplines of electronics and this year the world's first 'Scholars in Blockchain' International Scientific Conference was held alongside Blockchain Technology World.

Major participants included, notably, The British Blockchain Association, which was established in 2017 as a not-for-profit membership-funded organisation that promotes the comprehensive adoption of Blockchain and Distributed Ledger Technology across the public and private sectors of the UK and around the world.

Volume 1, Issue 2 of *The Journal of The British Blockchain Association (JBBA)* was published in December 2018, and in order to provide an insight into the subject to electronics professionals and students, this issue of *The Electron* concludes with a review of just a few of the articles in this publication.

In his Editorial, Editor-in-Chief Dr. Naseem Naqvi notably thanked Her Majesty The Queen and HRH Prince Charles for their positive feedback on the inaugural issue.

What is Blockchain?

The article 'Why Blockchain will disrupt Corporate Organisations - What can be learnt from the "Digital Transformation"?' by Eric P.M. Vermeulen et al (p.93-94) introduces blockchain technology as follows:

'To understand Blockchain Technology, it makes sense first to consider the Internet. The Internet enabled a free, fast and global exchange of information and ideas. The blockchain adds another dimension by making it possible to transfer and exchange value and assets without the involvement of traditional (centralised and authoritative) intermediaries. Blockchain technology achieves this by storing personal and other information in a decentralised accessible and secure online environment.

Stated simply, a blockchain is a shared and distributed digital "ledger" or "database" that maintains a continuously growing list of "blocks". A block can contain a record of transactions involving digital assets, but could also include "facts" or other information . Once the record is verified and validated, a block is added to the chain with previous records in linear and chronological order.

What makes the blockchain such a revolutionary technology is that the ledger or database is distributed to a countless number of participants ("nodes") around the world in public peer-to-peer networks (similar to the Internet) or private (or permissioned) peer-to-peer networks (similar to an intranet). It is the decentralised character of the blockchain that makes it so potentially disruptive. Participants hosting a copy of the blockchain can be individuals or organisations (and even things). The only condition is that they have a smartphone or Internet connection. Everybody with a smartphone can create a real digital ID and interact with other people in the blockchain network.

Network connectivity is vital because it allows for multiple identical copies of the blockchain to be available simultaneously across the network. This makes it practically impossible to alter or erase information in the blockchain. The use of cryptographic hashes makes tampering with blockchain records even more difficult, if not impossible. Cryptographic hashes compromise complex algorithms. The result of this combination of technologies is that even a miniscule change to the blockchain will result in a different hash value, making manipulation instantly and readily detectable by other participants.

Digital signatures help establish the identity and authenticity of the parties involved in the transaction. These security measures make blockchain validation technologies more transparent and less prone to error and corruption. Even if they are not 100 per cent secure, they are indeed more reliable than existing methods of verifying and validating transactions via third party intermediaries.

In short, blockchain technology creates an independent and transparent platform for establishing truth and building trust. Intermediaries, bureaucracy and old-fashioned procedures are replaced by the "4Cs" of code, connectivity, crowd and collaboration. The technology increases openness and speed, while at the same time significantly reducing costs'.

Blockchain enabled Healthcare

The Featured Article in the publication is entitled 'Innovation to Transformation: Consumer-directed Healthcare on the Blockchain' (p.51-53) and consists of an interview with Chrissa McFarlane, President of The Patientory Association, on the subject of the future of blockchain enabled healthcare.

Healthcare, including medical education, is an area where blockchain technology is viewed as having quite considerable potential, and The Patientory Association has been formed as a global not-for-profit healthcare member organisation consortium that governs the PTOYNetTM Blockchain. The article explains the workings of this particular Blockchain as follows:

'The PTOYNetTM securely stores and manages healthcare information in real-time, and such storage and management is facilitated by a blockchain-based token (called "PTOY"). The PTOY token regulates the PTOYNetTM for the healthcare ecosystem through "smart contracts". The goal is to provide a secure, private permissioned blockchain network for healthcare organisations to collaborate and innovate in a completely decentralised fashion. Currently, the foundation connects healthcare industry adopters of the PTOYNetTM, which members of the Association can join as "nodes" on the network. The Patientory Association facilitates the development of standards that are essential to the implementation and

adoption of the PTOYNetTM - such standards are necessary for interoperability, auditability and for transparency purposes.

These frameworks will help ensure the safety, reliability and usability of the PTOYNetTM platform by its members and the general public; a prerequisite to the wide acceptance of the PTOYNetTM platform as a viable means of transacting business by the industry and the general public'.

The article then describes how Patientory Inc., as the industry leader for blockchain solutions, has developed the first version of its Distributed Application, or DApp, which offers unique solutions that interconnect with most EHR systems enabling doctors, administrators and consumers to communicate via a single easy-to-use platform:

'The solution will work with almost any healthcare EMR, thereby bringing together many previously inaccessible data silos. These range from EHRs to patient monitors, wearable devices, and various other ambulatory applications. Connecting this data together enables a more complete view of a person's health information. The Patientory Inc. Dashboard is currently testing for large healthcare organisations, with current EPIC, Cerner, MediTech or Allscripts installation. This dashboard is a population health management software solution that regulates and safeguards against patient data in the blockchain, while providing convenient secure access to actionable health information and clinical administrative decision support, enabling physician-coordinated care enhanced by peer-to-peer patient support.

Patientory's DApp leverages blockchain technology that captures patient healthcare transaction records real-time, on an encoded, distributed ledger (blockchain). This has incredible security benefits as the records are spread across a replicated database in which all data is synchronised across the entire network. The users can only access the "blocks" (pockets of information relevant to themselves) to which they have permission to, and all transactions are date and time stamped. The data is not stored or controlled by a single entity or in a single location. This means that any single healthcare provider does not have the sole control over an individual's Electronic Health Records. This allows for more efficient and secure sharing of healthcare data among different providers and EHR platforms.

The main goal of the DApp is to help users track their health history and combat related rising health issues. The DApp will provide a complete view of a person's health by leveraging information from wearable devices and other apps, enabling instant access to personal health data. In time it will connect to the hospitals and GPs that adopt the PTOYNetwork Blockchain (currently hosting over 30 PTOYNetTM nodes around the world) to create a seamless system for tracking and monitoring patient health records and clinical outcomes'.

E-Voting on the Blockchain

Another area for which blockchain technology has been recognised as having potential is that of electronic voting and the article with the above title by Kevin Curran of the School of Computing, Engineering and Intelligent Systems at the University of Ulster (p.103-109) explains how this could be feasible:

'The blockchain serves as a public ledger of transactions which cannot be reversed. The all-important consensus of transaction (i.e. legitimate votes) is achieved through "miners" agreeing to validate new records being added. Whenever a new insertion is to be made e.g. votes, then a new transaction record is created by a voter adding details of their cast vote to the blockchain. Should it be deemed a valid transaction then the new vote is added to the end of the blockchain and remains there forever. What is neat about this solution is the fact that no centralised authority is needed to approve the votes, but rather a majority consensus. Here everyone agrees on the final tally as they can count the votes themselves, and because of the blockchain audit trail, anyone can verify that no votes were tampered with and no illegitimate votes were inserted'.

In the past, building a secure electronic voting system has proved to be a difficult task, but the creation of a decentralised platform that is capable of addressing previous weaknesses is now envisaged by the author to offer "a new hope":

'Blockchain distributes individual voting information across thousands of computers globally making it impossible to alter or delete votes once they have been cast. This approach promotes greater trust between voters and governments by protecting their data and privacy. Trust is inherently created by having the user in control over their data. Platforms like this now allow citizens to cast their votes on smartphone apps, rather than having to

queue up at polling stations. Implementing a blockchain does not require governments to completely rebuild their systems, but rather their existing platforms can be re-modelled to fit. All signs point toward a shift towards decentralised remote participation as opposed to traditional centralised gatherings at public polling stations.

A blockchain architecture specifically addresses one of the most difficult factors challenging electoral integrity - trust. Blockchain ensures trust is distributed amongst a set of mutually distrusted parties, all of whom are potentially adversarial, that participate in jointly managing and maintaining the cryptographically secure digital trail of an election. By distributing trust in this way, blockchains create a trustless environment whereby the amount of trust required from those participating in an election is minimised'.

As a working practical example the author highlights the case of the city of Zug in Switzerland where the Luxoft Holding, a global IT service provider of technology solutions, is piloting an e-voting platform that is set to enable the first consultative vote to be undertaken using blockchain:

'As one of the founding members of The Crypto Valley Association, which aims to build the world's leading blockchain and cryptographic technology ecosystem, Luxoft partner with organisations working on government-based blockchain service solutions and invite them to jointly create Blockchain for Government Alliance. In pursuit of driving the adoption of blockchain-based services in government, Luxoft is striving to establish a blockchain for government alliance and hence promote blockchain use-cases in public institutions. Zug already accepts cryptocurrency for services and has digitised the blockchain-based solution e-Vote, including the platform itself. Software and algorithms are built on Hyperledger Fabric. Integrated with Zug's Ethereum-based digital ID registration application, residents are hereby allowed to cast votes on the blockchain.

The solution claims to use an innovative encryption technology that anonymises the votes and allows tamper-proof tally and secure audit. With the help of the Lucerne University of Applied Sciences and Arts, Amazon AWS and n'cloud.swiss, the platform is deployed on three different data centre in the cloud. Two of these are in Switzerland and one in Ireland. By distributing the data into three different data centres, security and data loss risks are distributed geographically for robustness'.

Further Information

Further information on the above, and other subjects related to blockchain, as well as subscription information for the journal, may be obtained from The British Blockchain Association, Kemp House, 152-160 City Road, London EC1V 2NX.
www.britishblockchainassociation.org