techworld FROM IDG Insights

Issue: **February 2019**

THE COMPLETE GUIDE TO THE BIGGEST TECH TRENDS IN 2019

Credit: iStock

Produced by IDG

Credit: iStock

Looking forward to 2019

In this month's complete guide we've rounded up the very best of our industry trends and predictions pieces, which we ran over the festive period. This guide will provide you with a clear idea of what trends are set to shape the IT industry in 2019.

Our talented team of reporters each spoke to a huge number of industry experts and analysts to find out what trends were on people's minds as we round into 2019, from advancements in cloud computing and the Internet of Things, to the latest cybersecurity threats.

As well as technology predictions, we also have industry predictions for the public and banking sectors here in the UK, ahead of what should be another exciting year full of digital change. **Scott Carey**

Contents

Credit: iStock

Cloud computing trends

Our predictions for the biggest trends we can expect in 2019 for the cloud computing industry

Cloud computing is a fast moving beast, with new trends and technologies popping up all the time. Last year we predicted serverless and Kubernetes to maintain their strong momentum, and that the 'big three' vendors would maintain their stranglehold on the market.

Some of that held true, but serverless continues to be much talked about but little deployed, and Microsoft and Google did make some inroads into AWS's dominant market share over the course of the year. This year we don't expect serverless or Kubernetes to go anywhere, but they will continue

to evolve as adoption ramps up and enterprises look for ways to leverage these new ways of working.

In a blog post for its 2019 cloud predictions report, Forrester analyst Dave Bartoletti has pegged 2019 as the year of widespread enterprise adoption of cloud to power digital transformation efforts. In the report, by Bartoletti and Lauren Nelson, the analysts go on to state: "In 2019, cloud computing will be shorthand for the best way to turn disruptive ideas into amazing software."

That's a lot of industry jargon, but it does have the research to back it up, predicting the global cloud computing market to exceed $200 billion in 2019, which is up 20 per cent on 2018.

As we take stock of the year gone by, here are some predictions for where cloud is heading in the next 12 months, both in terms of the technology and the big vendors powering the industry.

Hybrid cloud momentum

With the release of Outposts in November, Amazon Web Services (AWS) finally admitted that it needs to be more hybrid cloud friendly for customers that will have applications hosted in their own data centres for some time to come.

It's a bit of a backward step for a vendor that has always been bullish (for obvious reasons) on the possibility of every app being ripe for cloud migration if needs be, but it seems like some customers have got their message through as AWS will now provide customers with a truly hybrid solution.

This brings AWS into better alignment with Azure, which has long been hybrid-friendly through Azure Stack, and Google claims to offer a bunch of tools to

allow customers to stretch their applications out to the cloud, such as Kubernetes Engine and Compute Engine, as well as Stackdriver for holistic monitoring and Apigee for API management.

Add to that the major hybrid cloud play inherent in IBM's $33bn acquisition of Red Hat in October.

"IBM will become the world's number one hybrid cloud provider, offering companies the only open cloud solution that will unlock the full value of the cloud for their businesses," IBM CEO Ginni Rometty said in a statement at the time.

Stephen Line, vice president EMEA at Cloudera sees that acquisition as part or a broader industry trend towards hybrid cloud and the need to provide customers with choice. He predicts: "The hybrid model is a challenge for public cloud as well as private cloud-only vendors. To prepare, vendors are making acquisitions for this scenario, most recently the acquisition of Red Hat by IBM. Expect more acquisitions and mergers among vendors to broaden their product offerings for hybrid cloud deployments."

Hybrid is certainly a significant market segment, according to Forrester's cloud predictions. "Nearly 60 per cent of North American enterprises now rely on public cloud platforms, five times the percentage that did just five years ago," analyst Bartoletti said. "Private clouds are growing fast, too, as companies not only move workloads to the top hyperscale public clouds but create powerful on-premises cloud platforms in their own data centres, using much of the same open-source software they can find in the public clouds.

"Success will be measured by developer satisfaction and time-to-market for new products and services, and

not by taking out cost. Firms will build private clouds on top of what they have, build them on top of cheaper open source platforms, or have private clouds built and run for them. Whichever they choose, enterprises will get real about on-premises and hybrid clouds."

Gartner predicts that by 2025, 80 per cent of organizations will have migrated away from on-premise data centres towards colocation, hosting and the cloud.

Stephan Fabel, director of product management, Canonical predicts: "Despite considerable uptake already, we expect multi-cloud's prominence to grow further still in 2019. Multi-cloud is almost becoming the default cloud strategy as organizations look to avoid vendor lock-in, granting themselves greater flexibility in deploying the most relevant cloud across different departments and functions."

Sean Fane, managing director, Spectrami UK believes: "Whilst the hybrid-cloud has been on the lips of CTOs for a couple of years, 2019 will be the year when we see organizations adopting true hybrid-cloud infrastructure, rather than multi-cloud environments.

"Concerns – whether justifiable or not – around data security and GDPR compliance will also drive adoption of hybrid environments – which not only give the chance to deliver the best performance at the best cost for each workload, but can ensure that data is always stored where it is most secure."

Google Cloud will make further inroads into the big three

It's very early days yet, but new Google Cloud CEO Thomas Kurian has a massive opportunity to earn Google a bigger piece of the global cloud computing market

share pie, by making the vendor a better enterprise selling machine. By investing in customer success and sales, Google will lose something of its traditional engineer-first reputation but will gain that all-important trust of enterprise customers that need consistency and reliability in their cloud vendors.

As Ray Wang, founder and principal analyst at Constellation Research, explains: “Enterprise customers need a different level of care, and Google hasn’t been able to deliver to date. So the resources available to Diane [Greene] may not have always been allocated in the right place, but the resource is there and she has to sit down and see what partners and customer are saying.”

If Kurian is able to better market Google as an enterprise vendor, rather than something of a machine learning specialist, you can expect the company to keep up its recent momentum and take more of the global market share from AWS and Microsoft, and make things more of a three-horse race.

In a more general overview of the market, Fabel from Canonical expects “to see Google focus on its AI credentials, Microsoft on its workload migration capabilities, and Amazon to continue pushing AWS hard in the public sector space”.

The rise of the service mesh

With the release of AWS App Mesh and Google’s open source Istio, 2018 saw the arrival of the ‘service mesh’. We expect to see this technology gain popularity as more organizations look for a way to manage complexity and unify traffic flow management, access policy enforcement and telemetry data aggregation across microservices into a shared management console.

Owen Garrett, senior director of product management at web server vendor NGINX says: “For organizations running large-scale, complex applications, and who reach the limitations of extending their microservices applications, a service mesh promises a solution.”

That being said there is still plenty of room for innovation, and uncertainty, around the technology.

“Time, then, will tell how it will develop as there is plenty of space for innovation,” Garrett adds. “Perhaps it will commoditize rapidly, and become a default, omnipresent feature of all major container runtime platforms. Perhaps new approaches, more efficient than the developing ‘sidecar proxy’ pattern, will emerge, offering better performance and lower resource usage. At this stage, there is no certainty as to how the technology will stabilize and who will be the leading providers.”

And of application networks

The likes of Forrester have been talking up the idea of an integrated enterprise application network for years now, but the vendors themselves now seem to be buying into the idea.

“Salesforce, Workday, SAP, Oracle, and other app leaders are opening up their platforms and adding new development tooling, integrations, and deployment options, with an eye to which specific industries they can target to accelerate adoption. SaaS apps are becoming development platforms, and that shift will start to bear fruit in 2019,” Bartoletti at Forrester writes, doubling down on a prediction he made in 2018. He has good reason though, as Salesforce’s record $6.5bn acquisition of Mulesoft was a clear integration play.

Devang Sachdev, director of product marketing and solutions at SaaS vendor Twilio naturally agrees. “Application platforms will usher in an entirely new way for developers to consume and customize enterprise software,” he tells us.

“Application platforms deploy like a SaaS application, integrate like an on-premises-based solution and iterate at the pace of API-based platforms. With application platforms, developers benefit from the low cost and scalability of the cloud are no longer limited like they are with SaaS which cannot be customized for specific business needs.”

Serverless momentum

During AWS re:Invent in November we saw Amazon CTO Werner Vogels naturally focus on serverless computing, alongside a raft of granular announcements to help developers go serverless.

This included Firecracker, an open source virtual machine monitor for spinning up MicroVMs, Ruby support for Lambda and an AWS toolkit for popular integrated development environments (IDEs).

As technical evangelist at AWS Abby Fuller said at the time: “I like seeing all the focus on developer quality of life improvement, so supporting the additional languages for Lambda, supporting Ruby outright, but also custom runtimes to code in whatever language I want. It’s really just being able to enable whatever use case developers want and letting them focus not on managing and provisioning infrastructure, but what makes my application my application and what differentiates me.”

We also saw our first (almost) full serverless deployment in the wild, with Danish web company

Trustpilot speaking about their shift to serverless during AWS re:Invent.

The latest Cloud Foundry Foundation global cloud trends survey found: “In just the past six months, awareness has swelled to the point that it is now in its next phase of adoption, with a plurality evaluating the technology.” Across the EU specifically 17 per cent said they are already using serverless, with 31 per cent evaluating the technology.

What will be interesting in 2019 will be how this model, and the terminology ‘serverless’ itself, extends into the rest of the industry. Google and Microsoft Azure have cloud functions, so serverless deployments are a technical possibility, but neither vendor appears to have fully bought into the architecture yet.

Fabel from Canonical also expects “to see the beginnings of open source serverless solutions start to compete for broad acceptance in the developer community, which will shape the future of that technology ecosystem for years to come”.

Ross Winser, senior research director at Gartner, for one predicts: “More than 20 per cent of global organizations will have deployed serverless computing technologies by 2020, which is an increase from less than five per cent today.”

Stephen Long, managing director for enterprise at KCOM predicts that “we will see much greater use of serverless design patterns in 2019”.

“The major cloud providers all offer serverless runtimes,” he says. “Of course, SaaS products are serverless to the consumer, but it is the ability to connect the SaaS and PaaS together without having to provision physical or virtual servers that is really the liberating idea.”

Open source convergence

The back end of 2018 showed a new trend towards enterprise giants going after open source communities. As we've seen, IBM acquired Red Hat for $33bn and Microsoft bought GitHub for $7.5bn, despite confirmed interest from rival vendor Google Cloud. Not to mention the high-profile merger of open source data platforms Hortonworks and Cloudera.

So why the pricey acquisitions? And is this the signal towards a wider industry trend? What it really marks is a drastic change of heart from previously renowned closed shops Microsoft and IBM that contributing to open source and developing proprietary intellectual property need not be conflicting interests, and that some of the most interesting developments are coming from that open source community. Google Cloud is also consistently outspoken about its commitment to open source.

The long-term goal is to leverage these communities to stay ahead of the competition, but there is, of course, a short-term business benefit, too. As Docker CEO Steve Singh explains: "From building Concur, to being on the executive team of SAP, whenever you do an acquisition there's always a business reason behind it. The business reason might be I want great technology, the business reason might be I need to be able to monetize a particular thing.

"If you look at why SAP bought Concur, Ariba, or Fieldglass, or SuccessFactors or Qualtrics," the former SAP executive says, "they did it because they wanted to deliver that functionality to their customers, and they have this economic or sales engine or distribution engine that's just bigger." **Scott Carey**

Credit: iStock

Cybersecurity trends

Our pick of the biggest cybersecurity trends that need to be on your radar for 2019 according to a wide range of industry experts

With the cybersecurity industrial complex in full swing and good business for all the major players, from governments and state sponsored groups, to criminal attackers and the vendors as well as their shareholders, we wonder what horrors this dystopian hell world will spew forth next.

It was arguably 2017's devastating WannaCry and NotPetya ransomware variants that brought cybersecurity into mainstream focus, taking it from the idea of banking scams and into the realm of hobbling hospitals and businesses that depended on critical systems with real-world physical consequences.

Then 2018, just as GDPR came into effect, brought with it data breach after data breach, affecting millions of customers across industries, including customers of household names like Reddit, Facebook, Uber, British Airways and the Marriott hotel chain. But it won't be just consumers that pay the price of these incidents. When GDPR was implemented in May 2018, the regulation meant companies that were found to have allowed a breach due to malpractice would face hefty fines.

State-sponsored breaches or attacks continued throughout the year, and it will be intriguing to see where these 'advanced persistent threat' groups head next – perhaps further underground, according to some commentators. And while the majority of attackers are still going for the low-hanging fruit, there are methods of attack that are becoming increasingly more sophisticated.

Here's what 2019 might hold in cybersecurity.

Better, smarter IoT botnets

The first truly global case of a powerful Internet of Things (IoT) botnet was Mirai in 2016. It was achieved with a few lines of simple code, but was so effective because it targeted objects like IP cameras that were connected to the Internet but rarely secured or updated, and managed to bring down a decent chunk of the web.

The Internet providers and DNS companies have buffeted their defences since Mirai, but the IoT market – which could reach $6.5 trillion by 2024 – is only going to increase dramatically. Some manufacturers may have sharpened up their products to be updatable, but certainly not all will have, especially when these things become interwoven into the fabric of everyday life.

Malwarebytes' lead malware analyst Chris Boyd notes that in 2018 several thousand MikroTik routers were compromised to quietly be transformed into crypto coin miners. "This is only the beginning of what we will likely see in the new year, with more and more hardware devices being compromised to serve up everything from coin miners to malware," he warns.

"Large-scale compromises of routers and IoT devices are going to take place and they are a lot harder to patch than computers. Even just patching does not fix the problem if the device is infected."

Kaspersky adds that IoT botnets will keep growing at an "unstoppable" pace, in what is becoming a recurring warning that shouldn't be underestimated.

Mike O'Malley, VP for carrier strategy and business development at Radware, adds that hackers will attempt to turn IoT devices into a 'swarm' network of self-sufficient bots that can make semi-autonomous decisions, pool their collective intelligence together to solve problems, or "opportunistically and simultaneously target vulnerable points in a network".

"'Hivenets' take this a step further and are self-learning clusters of compromised devices that simultaneously identify and tackle different attack vectors," he continues. "The devices in the hive can talk to each other and can use swarm intelligence to act together, and recruit and train new members to the hive."

A 'hivenet' that can identify and compromise more devices would, O'Malley warns, be able to grow "exponentially" and "thereby widen its ability to simultaneously attack multiple victims". "This is especially dangerous as we roll out 5G," he adds, "as hivenets

could take advantage of the improved latency and become even more effective."

According to VP of IoT at Sectigo, Damon Kachur, it's important to consider the role of digital certificates. "From an end user perspective, the slow uptake of security in IoT devices has prompted governments to regulate," he says. "Nations and more US states will follow California's lead and enact legislation requiring security for IoT networks. This is particularly important for healthcare, transportation, energy, and manufacturing sectors, which face the highest risk.

"The legislation stops short of prescribing strong forms of authentication, but thankfully consortium groups such as the Open Connectivity Foundation and AeroMACS have championed the use of strong certificate-based authentication in their best practice standards for IoT.

"The attack vectors and threat actors to the IoT are constantly evolving, warranting best practice device provisioning, and the ability to quickly and proactively manage current cryptographic algorithms with those that will supersede them in the future. This will be vital within the lifespan of the devices being deployed to customers," he adds.

Attacks on critical national infrastructure

A recent parliamentary committee warned that critical national infrastructure is at risk from cyberattackers. The National Cyber Security Centre (NCSC) also recently warned that states hostile to Britain would likely target the country's infrastructure.

While high profile real-world examples of these sorts of attacks have been relatively scarce (especially

in Britain – with only WannaCry and NotPetya coming close to date) some experts are warning that 2019 could see intra-state rivalries become more realized in the cyber realm. Even taking hostile states out of the equation, attackers motivated by money might see weakness in the country's current approach to critical national infrastructure and hit it for financial reasons before it's fixed.

James Wickes, CEO and co-founder of Cloudview, says that attacks on infrastructure could also be linked to the increase in Internet-connected devices.

"Many of these devices are poorly secured, posing serious risks to individuals, businesses, utilities, and ultimately national security," Wickes says. "Experts have already identified that new smart energy meters, which the government wants installed in millions of homes, will leave householders vulnerable to cyberattacks.

"Cybercriminals could artificially inflate meter readings, making bills higher, but ultimately this could lead to a catastrophic attack on our electricity grid. The National Grid was put on alert in March 2018 by officials from the NCSC amid fears of a Russian cyberattack, and given advice on how to boost its defences to prevent power cuts."

Former DHS Under Secretary and Nozomi Networks adviser Suzanne Spaulding reveals that the electric grid in America has a "fair amount of physical redundancy" to back cyber controls, but as virtual infrastructure becomes embraced, those physical redundancies are abandoned, which would make it easier for an attacker to have "cascading impacts that can cause real damage".

"With fewer physical controls in place it will be harder to regain control of systems, minimize damage,

and stop an attack from progressing," she adds. "Given the benefits of the networked world the move to digitalization isn't going to slow down. It's important we realistically asses our dependence upon cyber and the potential consequences of a disruptive attack.

"Maintaining physical backups or other redundancies, changing operational processes, and even keeping less data can reduce the impact of a successful attack."

Crypto-jacking

If 2017 saw the Tulip-mania style boom and bust of cryptocurrencies, 2018 saw a significant uptick in crypto-jacking, the process of taking control of a device or network of devices to use the additional compute for crypto mining.

Webroot went as far as to claim in its mid-year threat report that crypto-jacking accounted for as much as 35 per cent of all threats – and that its customers attempted to visit websites running crypto-jacking scripts 3 per cent of the time. The most popular crypto mining domain was Xxgasm.com for 31 per cent of traffic, while Coinhive.com accounted for 38 per cent of traffic.

Check Point, meanwhile, says that the global impact of crypto miners had doubled in the first half of 2018.

Rich Campagna, CMO for Bitglass says that we can expect to see "a lot more of this in 2019 and beyond".

"This technique combines two commonly used types of attacks: crypto-jacking, when malicious individuals appropriate devices' compute power in order to mine for cryptocurrency; and cloud-jacking, when illegitimate third-parties hijack enterprise cloud resources. Together, the two hacking methods can be used to mine cryptocurrency at a highly-accelerated rate."

More ransomware

Ransomware has persisted for so long both because it can be used to such devastating effect and for its relative simplicity. Indeed, scripts are available to buy on the dark web for mere pennies in many cases, just point and shoot.

According to John Fokker, head of cyber investigations at McAfee, the ransomware underworld will "consolidate", creating "fewer but stronger malware-as-a-service families that will actively work together".

"We also predict a continuation of the strongest ransomware 'brands' using affiliate structures to increase their threat," he adds.

Good old blackmail

According to enterprise architect at Carbon Black's threat analysis unit, Paul Drapeau, compromised data sets could very easily enable a new path to traditional blackmail. "Breaches in Facebook and other social media platforms represent a wealth of data to be mined by bad actors," he reveals. "This data could be used to correlate activities between people to find illegal, scandalous or compromising behaviour, and then leverage that for traditional blackmail at scale."

What could that look look? "'Pay me the bitcoins or your spouse/employer gets copies of these direct messages' an example note might read," he explains. "We can fight ransomware with anti-malware tools or backups, but we depend on giant companies to protect our more personal details.

"The breach doesn't even have to be real to result in extortion attempts, as was seen in 2018 with the mass email scam purporting to have compromising video and

passwords of the victims. Imagine an attacker building on data from a breach and fabricating message contents, and then demanding ransom be paid. This type of attack is definitely more work, more targeted and difficult, but the payoff could be there. Victims may be willing to pay more money and pay up more readily when it is their real lives and reputations at stake versus their digital lives."

That could look like a 'spearphishing' attempt, but rather than tricking a high-worth individual like a CFO into transferring money – it's a lot more personal.

APT groups, nation states, and state-sponsored attacks

Kaspersky believes that the advanced persistent threat groups (think Fancy Bear, Shadow Brokers) might do more to cover their tracks – less outspoken branding or signature attacks, in short, which would make detection and attribution "extremely difficult". The vendor adds that one of the most likely scenarios in this new approach would be building tools catered to highly specific targets.

According to Priscilla Moriuchi, director of strategic threat development at Recorded Future, state-sponsored groups are likely to place an increasing focus on telecommunications companies and ISPs.

"Telecoms and ISPs are woven into the fabric of the Internet and provide threat actors with access to trusted infrastructure to enable secondary attacks or intrusions," she says. "They also are the midpoints for global telecommunications and intrusions into these types of companies can expose not just user data, but phone calls, text messages, geolocational history, contacts, and more. Telecommunications companies and ISPs are the crown jewels for hostile foreign intelligence

services, and I expect to see a proliferation of operations targeting these companies from a wider variety of nation-state actors in 2019."

She adds that non-traditional attacks and access points are also likely to become more widely used, including attacking the supply chain, hardware vulnerabilities and such, while state-directed influence campaigns that use social media will expand.

According to the former Department of Homeland Security Under Secretary Suzanne Spaulding, and current Nozomi Networks adviser, the USA will become more aggressive in naming hackers.

"Until recently, the US did not publicly attribute various cyber incidents to specific nations, despite public pressure to do so," she says. "It can be difficult to attribute cyber activity with 100 per cent certainty, but US officials were also concerned about public demands to respond if they were to attribute an attack."

The US is "already less afraid of attribution," she adds, pointing towards sanctions against Russia in response to perceived threats on American infrastructure.

Encrypted traffic malware

The increased understanding of the importance of encryption could well be exploited by groups that hide malware itself within encrypted traffic.

Omar Yaacoubi, founder and CEO of Barac, points out Google research that suggests 80 per cent of all traffic will be encrypted in 2019, and a PwC study that says 60 per cent of attacks will occur on encrypted traffic.

"The downside of encryption is that security tools can't inspect encrypted traffic for malware, making it the perfect place for a threat actor to hide any kind of

malicious traffic," he warns. "A recent Vanson Bourne survey of 500 CIOs found that 90 per cent of firms had experienced or expected to experience a network attack using SSL/TLS, and 87 per cent believe their defences were less effective because of this emerging trend to bury malware in encrypted traffic.

"The challenge for organizations is how to detect this malware without decrypting the traffic, which opens a whole new can of worms about privacy and also has a massive impact on network performance.

"One solution is to look at the metadata associated with these traffic flows, using AI and machine learning to accurately detect the difference between bad and good flows. This allows businesses to identify and block bad traffic without going through the pain of decrypting and examining the contents of each and every data packet, and to be compliant with data privacy laws."

AI-assisted imposters

In January 2019, Nvidia unveiled extremely lifelike human face rendering, and there's no reason that this technology won't end up in the hands of bad actors, whether they're hacking groups or nation states.

Could facial rendering technologies like these be used to create entirely new personas, perhaps for the spreading of disinformation – in a country like the USA that under the Obama administration made propaganda against its own population entirely legal? That might sound paranoid, but 15 years ago you'd be paranoid for suggesting people were watching you through your webcam, until that, well, happened. **Tamlin Magee**

Credit: iStock

Internet of Things in 2019

We examine some of the biggest trends we're expecting in IoT, from security to edge computing, and Robotic Process Automation

The Internet of Things (IoT) market didn't explode in 2018 as it had the year before, rather it seems vendors are preparing to make a big impact in 2019. Gartner still holds onto its prediction that there will be over 20 billion IoT devices by 2020, though as we get closer to that date, consumers remain concerned about the performance and security of IoT deployments.

Here we examine some of the major trends shaping IoT today, and what we can expect in 2019.

Adoption

Unsurprisingly, the IoT market will continue its upward trajectory. 2018 was a year of increased IoT focus from vendors such as Splunk and Google Cloud, and we expect 2019 to bring more of the same.

Analyst firm Forrester predicts that business-to-business (B2B) IoT applications will take off in a big way this year, while business-to-consumer (B2C) will continue to find its footing. It believes that 85 per cent of companies will implement or plan to implement IoT solutions in 2019.

"B2B IoT will take a play from the mobile rollouts in 2000 that went beyond the buzz of what was possible, focusing on field assets, distributed management, and remote control. In that same way, B2B IoT will focus on driving efficiencies, connecting the enterprise, expanding the edge, and in some cases, providing personalized customer experiences," it says in a blog post.

Adoption is particularly expected to surge across the manufacturing, healthcare, retail and utilities industries.

Industrial IoT

According to research firm IndustryARC, the Industrial IoT (IIoT) market is expected to reach over $123 billion by 2021. As the race to deliver becomes heated among vendors, more industrial and manufacturing firms are expected to adopt IoT in 2019 than ever before.

"The potential of IoT within industrial sectors will be high, but this new world still isn't properly understood. The big institutions have not seen the benefits as they already believe they have solutions which are sound," Jamie Bennett, VP of engineering IoT and devices at Canonical argues. "IoT within

connected cars, smart building and in farming will accelerate as the ROI is more clear-cut."

A report from Statista shows that manufacturing, transportation, logistics and utilities industries are expected to spend $40bn each on IoT platforms and services by 2020.

2018 saw a number of logistics and delivery vendors start to reap the benefits of IoT, but as connectivity becomes of greater importance we should expect to see more connected solutions in 2019. In fact, research from GE Digital found that 22 per cent of organizations believe an IIoT-ready platform is the most important technology to invest in.

Emerging IoT projects

During the early years of IoT, it was difficult to identify exactly what the technology would be used for other than the theory of 'connected things', but that is no longer the case.

2018 saw numerous emerging projects. According to research by IoT Analytics, the smart city topped the list of the most common IoT projects, with 45 per cent of such projects in Europe alone. Connected devices and industrial applications followed closely behind.

In 2019, smart city applications and infrastructure projects are expected to see exceptional growth.

"As we enter 2019, the number of connected devices will only increase as more organizations begin to realize the benefits of IoT technologies. Consequently, next year [2019] will see the birth of a smarter IoT – whereby fully connected businesses will begin to pull data for more predictive use," Martin Hodgson, head of UK and Ireland at Paessler argues.

Although the consumer market has been predicted to remain in the early stages, the smart home and connected devices markets should continue to grow to meet customer demand. According to software firm Arm, 2019 is expected to see a growth in the availability of IoT smart home products as the expansion of consumer products will surpass the usual lighting, heating, and other smart home areas. It will instead deliver increased automation and efficiency to everyday tasks.

Security remains a concern

Despite this, IoT security will be a huge concern. The past 12 months saw a rise in IoT security appearing in the headlines, all for the wrong reasons. From self-driving car accidents to connected devices and security glitches, the need for vendors and manufacturers to put security and data privacy at the core in 2019 is paramount. As B2B takes hold of IoT there is concern that vulnerabilities will impact trust in the connected world. In fact, 92 per cent of IoT developers believe security will continue to be an issue in the future, according to Evans Data.

"Security must take precedence over innovation if confidence in IoT is to grow and severe security issues are to be avoided," Canonical's Bennett says. "If we get this right though, adoption will continue at an exponential rate, greater consolidation will drive developers to edge computing, while connected applications will unlock multipurpose robots, leading to far greater capability and functionality."

Although concern has reduced since the government's IoT Code of Practice was released in October 2018, this still stands as an initial guideline to IoT manufacturers and vendors.

"Next year [2019] we hope to see binding agreements to strengthen this security initiative. However, the question of who is responsible for this standardization across the IoT is yet to be answered," Bennett adds.

Edge computing

Edge computing will have a huge impact for IoT devices as data volumes and the need for low-latency applications grows.

"We're going towards edge computing, which is gaining momentum continuously as we realize that volumes are just too large to be pushed to the cloud," argues Markus Noga, head of machine learning at SAP.

As long as organizations demand immediate action based on real-time data analysis, particularly in manufacturing and logistics, edge will continue to be a buzzword in the industry.

"In 2019, 5G deployments and the increasing proliferation of the IoT will be the key drivers behind the edge gaining significant awareness and traction," Andrew Fray, managing director at Interxion says. Businesses will look to data centre providers to lead the charge when it comes to developing intelligent edge-focused systems. In terms of technological developments, a simplified, smarter version of the edge will emerge."

Robotic Process Automation

Last year saw a massive uptake in the adoption rate for Robotic Process Automation (RPA) software, and this growth shows no signs of slowing down anytime soon.

According to Chris Huff, CSO at RPA software vendor Kofax, 2019 will see large software companies

acquire RPA capabilities. This will follow in the footsteps of SAP's acquisition of Contextor in 2018.

Furthermore, Gartner predicts that 85 per cent of large organizations will have deployed some form of RPA by the end of 2022.

"RPA has a very important part to play as organizations are increasingly searching how to improve and modify their applications on a continuous basis, so everything that is repetitive and reoccurring in nature, and is a sequence of simple steps, RPA is very well-positioned to address," says Noga. "The evolution that we're going to see is going to be towards more and more intelligence, going into the direction of a wider spread adoption in terms of the use of a number of bots in digital workspace is what I would are the two main trends."

According to Blue Prism, as vendors make attempts to scale more desktop automation tools all design limitations will become more apparent. This is also backed by the increasing competition in the market.

"For RPA to deliver value, longevity and resilience at scale, automations should be carefully planned, modelled and designed. Shortcuts to building a process will increasingly introduce risks, such as 'Grey IT', which is potentially very damaging for an organization," argues Pat Geary, chief evangelist at Blue Prism. "Therefore, 2019 will be the year where more rigour is applied to RPA vendor selection. Higher numbers of organizations will adopt a more strategic approach when selecting RPA products, and greater proof will be demanded that a RPA product is really designed for the enterprise.

"Throughout 2019, we'll see further evolutions with a shift from rule-based decision-making automation,

to a more advanced intelligent automation. Importantly, these will increasingly deliver the thinking and analytical capability to make operations smarter and autonomous, to ensure that digital workers more closely replicate human decision-making" Geary adds.

What to expect

Overall, 2019 will be an interesting year for stakeholders in the IoT ecosystem. From the increase in connected devices to a rise in intelligent automation, there will be several deployments of note to keep an eye on. Security and privacy will become of greater importance as systems and devices become increasingly powerful, too.

Gartner predicts that IoT will continue to deliver new opportunities, with a number of new and improved technologies over the next decade.

"As the IoT continues to expand, the need for a governance framework that ensures appropriate behaviour in the creation, storage, use and deletion of information related to IoT projects will become increasingly important," argues Nick Jones, research vice president at Gartner. **Hannah Williams**

Credit: iStock

Banking technology trends

What technology trends can we expect to see across the UK banking sector in 2019? Here are some predictions from industry experts

While 2018 promised to bring in a new era of digital banking with the introduction of open banking and PSD2 regulations, the reality is a landscape that looks much the same, with very few needle-moving developments.

It is still early days though, and the major banks have all made moves of varying degrees to become more open and digitally competitive in the face of challenger banks and fintech disruption.

In her foreword to the latest *MoneyLive Future of Retail Banking* report, Juliet Knight, director at

Marketforce, sums up the current industry mood: “Of all the forces weighing on the banking industry, from open banking to Brexit, there is perhaps none as fundamental as the change in consumer behaviour. For decades, banks have relied on customer inertia as a valuable component in the business model; even mis-selling scandals and the launch in the UK of the seven-day switching service have failed to prick customer apathy.”

So what can we expect in the year ahead? With no major new regulations on the horizon we hope to see banks continue to innovate and learn from their nimble fintech siblings, with more open banking-enabled features and products hitting the market and perhaps even some innovative ideas that aren’t simply borrowed from the fintech sector.

Here’s what to expect in banking technology in 2019.

The banks hit back

Whether the average person on the street knows what open banking is or not is less relevant when the big banks are releasing new digital products that make regular interactions simpler.

In 2018 both Barclays and HSBC made it possible for customers to see multiple accounts from their mobile apps, regardless of if that account is held with a rival bank, just in slightly different ways. While HSBC created a whole new app, first as a Beta, then as the Connected Money app, Barclays has baked the feature into its core banking app for all customers.

On the business lending side, NatWest launched a standalone digital business current account under a new brand called Mettle. Meanwhile, Lloyds earmarked 2,000 new digital roles to speed up its innovation curve.

"We've seen the bar continuously raised on what you can do with a truly digital proposition," says David Brear, CEO of financial services consultancy. "I think we'll increasingly see banks copycatting of fintech features, possibly to incumbents detriment if they don't get their underlying core technology sorted out to deliver digital, not digitised experiences."

Elsewhere, Nationwide didn't launch anything of note in 2018, but did announce its technology strategy, including more than £4 billion in investment. We also wait with baited breath to see if rumours on a standalone digital bank materializes from the corridors of RBS in 2019.

"It seems this work is already making an impact: two out of three of our respondents believe the gap in the quality of the digital experience between traditional banks and fintechs has narrowed over the last two years," as the *MoneyLive Future of Retail Banking* report for 2018/19 outlines.

Less patience with digital failures

Last year saw an unprecedented number of major IT failures at UK banks, with Barclays, HSBC, NatWest, RBS and TSB all hit with significant outages, something both the government and consumers are clearly losing patience with.

The Treasury Select Committee announced in November that it will investigate whether banks are sufficiently prepared for outages, and if regulators such as the Financial Conduct Authority and the Bank of England are equipped to hold them to account.

Nicky Morgan MP, chair of the Treasury Committee, said at the time: "The number of IT failures at banks

and other financial institutions in recent years is astonishing. Millions of customers have been affected by the uncertainty and disruption caused by failures of banking IT systems. Measly apologies and hollow words from financial services institutions will not suffice when consumers aren't able to access their own money and face delays in paying bills.

"The committee has launched this inquiry to consider the causes and consequences of these failures, and will examine what industry and regulators are doing to promote operational resilience."

Add to that the fact that recent figures from the Current Account Switch Service showed TSB had the sharpest decline in net customers following its most recent IT failures and it would seem that customers also have little patience for IT issues.

Chris Huggett, senior vice president for Europe and India at Sungard Availability Services puts these issues down to pressures on banks with legacy systems to adapt to digital disruption.

"As the trend of technology becoming ever more focused on the end-user continues into 2019, so too will the trend of legacy IT systems burdening the digital transformation efforts of high street banks with downtime and disruption," he argues.

"This year, botched efforts to both migrate legacy systems from 50-year-old COBOL-run IT infrastructures to the cloud, and to embed new applications into a tangled web of new and old software were exacerbated by protracted periods of downtime for customers whilst the high street banks have scrambled to bring services back online. With customer-centred digital transformation efforts high on the agenda in 2019,

disruption to banking services will be inevitable given the complex web of new and old in the IT systems of traditional banks. Having the resilience to recover from inevitable IT fiascos without customers being affected will be vital to ensuring operational continuity and services for customers, helping to stem the flow of customers moving to digital native challenger banks."

What will happen with open banking?

The much-lauded open banking 'revolution' will enter its second year in 2019, and while YouGov research from August showed that 72 per cent of adults in the country had still never heard of it, that sort of statistic is overblown. Open banking is an inherently difficult thing to market, and its success is far less reliant on name recognition than it is on adoption, but concerns over data security still need to be met for the regulation to be considered a success.

Jed Murphy, UK head of strategy and innovation at Cardlytics put it best when he said: "Most people knew there wouldn't be a 'big bang' moment with open banking. But even as we approach the end of 2018, it is some way off from effecting real consumer change. Old habits die hard when it comes to your personal finances, particularly around privacy. If entrenched customer behaviour is going to change, concerns must be tackled head-on, with industry-wide changes and truly compelling propositions."

Jake Ranson, CMO at Equifax UK, added: "January 2019 marks the first anniversary of open banking, and we can expect it to play a central role in the banking sector for the year ahead. As more companies evolve the new technology into live customer journeys, consumers

will really begin to experience the full benefits of the proposition and demand for open banking will increase.

"Of course, challenges remain – there is still an educational deficit regarding how open banking can improve consumers' financial lives, as well as understanding data's positive predicative capabilities."

Nick Caley, VP of financial services and regulatory at ForgeRock says "there's plenty to celebrate", though. "We're only 11 months into building a new financial ecosystem and there are already 86 Third-Party Providers (TPPs) registered with the FCA to provide either Payment Initiation or Account Information services based on the UK Open Banking Standard," he adds.

Imran Gulamhuseinwala, the implementation trustee for open banking also, naturally, took an optimistic spin on the first 10 months of open banking, telling us: "Some really exciting products have been introduced into the market, which are beginning to show how – powered by open banking – people are having the opportunity to more easily and securely move, manage and make more of their money. But with the line of sight we have into the open banking 'pipeline', this is going to considerably ramp up in 2019. We expect the ecosystem to develop with even greater momentum and pace not least as we see greater conformance with the implementation of the standards as well as greater innovation in the market."

Take the UK fintech Iwoca as a success story, which announced new open banking connections to Barclays and HSBC in December, adding to an existing connection with Lloyds Bank. This allows small businesses that bank with those lenders to apply for loans or a credit facility quickly and easily by giving them direct access to five years of transaction history instantly.

Senthil Ravindran, executive vice president and global head of xLabs at Virtusa adds: “Open banking has been ‘in the wild’ for almost a year now, and though we’ve seen a handful of consumer apps, it’s largely failed to spark the promised revolution, mostly down to banks’ reluctance to give away data to fintech rivals.” He predicts that this will change in 2019, “with competition giving way to collaboration”.

Finally, Frank Jan Risseeuw, CEO at Yolt believes that “the combination of innovative technology and legislation is generating a growing openness to cross-industry partnerships and a more established sharing economy”.

Voice

It has been hailed as the next big banking channel for years now, but voice services could see a spike in adoption in 2019 if the *MoneyLive Future of Retail Banking* report is anything to go by.

The report reads: “More than four out of five (84 per cent) of our bankers believe that voice-activated digital assistants will become the next major consumer channel and 78 per cent think the majority of digital natives, those who have grown up with Internet-related technology, will embrace voice as a banking channel within the next two years.”

This sort of adoption hinges on security and reliability however: “For more serious situations involving money, such as shopping or payments, consumers prefer more traditional channels, with almost half not trusting the voice assistant to correctly interpret and process their order or feeling uncomfortable sending payment through a voice assistant.

Martin Ewings, director of specialist markets at Experis added: “Voice technology risks becoming the next big IT skills gap and a real barrier to innovation. The value of the market is forecast to reach $8.3 billion by 2023, but this rising demand is set to have an impact as early as next year. While voice technology has been around in the consumer world for the past few years, enterprise adoption is the next major focus for organizations.”

That adoption curve isn’t just for customer service queries either, with the bankers surveyed expecting almost half of balance checks and a third of payments to be activated via voice within five years.

Hilda Jenkins, digital product director at Barclays also sees voice as an increasingly important channel.

“With advances in user experience and user interfaces, I suspect we’ll start to see more complex customer needs surfaced on mobile platforms, such as investments, trading and mortgages,” she says. “I expect conversational UI will bring smoother experiences for customers completing these complex actions on mobile, and help them manage their finances more effectively.”

American banks are ahead of the curve on voice, with US Bank offering voice services on all three major voice platforms (Amazon, Google and Apple) and Capital One has had Alexa skills available for over a year now.

Brexit

Of course Brexit is set to continue to cause turmoil for one of the UK’s largest industries.

Charlotte Crosswell, CEO of Innovate Finance made a statement on the current state of negotiations after PM Theresa May pushed back the key vote in December:

"The turmoil in the Brexit process means confusion continues for companies across the fintech ecosystem. Our own membership reflects this, with a split variety of views as to which would be the best option.

"Whatever the outcome, we will be working to protect the interests of fintech businesses and the people that work within our community, so we can provide practical help and advice going forward to make sure the UK fintech sector continues to thrive."

In more positive news, the banks performed well under the Bank of England's stress test ahead of what is widely expected to be a chaotic period in March.

Lee Thorpe, head of risk business solutions at the UK and Ireland office of analytics vendor SAS says: "Following the UK banks' poor performance in the European Banking Authority's stress tests earlier this year, their showing in the Bank of England's tests paints a more encouraging picture ahead of next year's increasingly likely post-Brexit chaos.

"Banks must make a greater effort to automate and industrialize their risk analysis capabilities to ensure they have sufficient technical capabilities and capital to survive during rapidly changing and potentially extreme economic circumstances."

AI

AI has been hailed as a potentially transformative technology across industries, but we have yet to see a truly impactful application in banking.

The *Future of Retail Banking* report outlines a utopian vision of AI for financial services, stating: "AI will be a powerful tool in converting a transactional relationship, defined by apathy and distrust, into an

engaged partnership, where banks truly understand a customer's individual needs and design smart solutions to meet those needs."

That being said, concerns remain in what continues to be a conservative industry. The report states: "Of course, these are valid concerns, but they are not insurmountable. Leaders need to have the vision to understand the potential of AI, and then make the right decisions to rapidly overcome the data management and governance hurdles."

One thing that is for certain is that if the financial services industry were able to leverage machine learning in a meaningful way, it's the banks which have a head start. "Incumbents have the scale and the historic data to feed algorithms with huge amounts of data in order to build real granularity into their models and offer customers highly personalized experiences," the report states.

James Smith, Nationwide Building Society's director of mobile and digital say: "Greater processing power and larger data volumes will power new use cases for machine learning in the industry. These might include fraud identification, robotics, virtual money managers and digital assistants."

GAFA entrant?

Big banks have been talking about the potential threat of the tech titans Google, Apple, Facebook and Amazon (GAFA), for years now, but none have truly entered the financial services arena, yet.

"This year has seen many tech giants dipping their toes into the space, for example the Amazon and AMEX collaboration, or Google with Tez. They're a looming

threat and due to their brand and scale cannot be ignored. Amazon appears to have a bigger opportunity with AWS; something like 90 per cent of fintech is based on AWS, so it will be interesting to see what they do," David Brear from 11FS says.

The *Future of Retail Banking* report goes into some depth on this topic, stating: "The tech titans are a threat to both the challengers and incumbents – and it is a threat that is being taken seriously. After all, surveys suggest nearly a third of UK consumers would choose Amazon, Google, Facebook or Apple for banking services, and that rises to almost half of those aged 18 to 34. Industry insiders have long feared the intentions of Amazon, which in March 2018 was reported to be in talks with big banks about setting up a current account-type product for younger customers and those without a bank account."

That report points to regulatory hurdles as the main barrier for the GAFA companies, but the real issue is whether they even want to become banks.

"They do, however, want to grow their businesses by facilitating seamless social and commercial connections, and frictionless payments, just-in-time credit and in-transaction insurance are all part of this ambition," the report states. "This is not head-to-head competition with the banks, but instead a gradual erosion of banking value chains that may prove difficult to withstand." **Scott Carey**

Credit: iStock

Public sector technology predictions for 2019

Leading IT analysts describe the technology trends they expect to see in the public sector in 2019

In 2018, the public sector balanced its usual mix of IT blunders, skills shortages, questionable political appointments and dubious interventions from the private sector with some promising investments in emerging technologies and open data initiatives, while keeping one eye on the political elephant in the room.

In 2019, our impending departure from the EU will play a decisive role in public sector IT developments.

The government will need to ensure that its IT systems can cope with any outcome of Brexit. Gartner analyst Neville Cannon believes this will significantly reduce the time and investment available for major digital initiatives, particularly in the case of a no-deal Brexit.

"If a deal's accepted that makes life much more straightforward for the government departments," he explains. "Where existing reliance on European systems or integrations can take place then they're freer to start to develop and deliver the solutions they need to move the country forward as opposed to catch up with where they are now."

Skybox Security director Peter Batchelor expects Brexit to also drive a more mobile working environment in the public sector and force the government to develop IT systems that can handle changing staffing requirements. "Brexit will lead to the increase in the number of UK central government employees as the government bolsters the workforce to cope with the additional demands of leaving the EU," he says. "This will need a significant amount of effort to provide new identity access management solution and clean up endless users that still exist on the IT systems but not on the payroll."

Procurement models

Forrester analyst Duncan Jones advises public sector clients around the world on IT procurement, and they all have the same problem: rules and regulations prevent them from selecting the best vendor for the task.

Jones worries that this will be an even bigger barrier in 2019 as agile software development becomes more common. "As we're moving to much more agile

development and being much more iterative, the public sector procurement process just doesn't work," he says.

"Many large private sector organizations struggle as well. They're used to relying on a competition-based bidding process and that really doesn't work when you're trying to do agile development because you can't define up front what you want in enough detail to just have it bid out on a price basis. You're comparing vendors on different criteria. I think until the public sector gets that and abandons its obsession with competition, it's going to continue to have these huge failures that we see over and over again, where the requirements that are bid out turn out to actually not be what's required in the end. You never can predict before you start what you're going to end up with, and the public sector process kind of denies that reality."

Some governments abroad are challenging that procurement model. Jones points to the Netherlands as a promising example of a country that has started to recognise that competitive bidding isn't always the best approach, as sometimes long-term partners are required.

Procurement approvals there are now granted for a variety of reasons, and exceptions to the normal rules are made if they can be justified due to factors such as a lack of real competition or a need to prioritize long-term stability over price. However, Jones has little faith that the UK will be replicating the Dutch model in 2019.

"I don't see any sign that it's going to improve in the UK," he says. "There doesn't seem to be that will to change. There's an inherent resistance to change and the processes prevent change. They can't engage with consultants who will help them change because the sourcing process doesn't allow it.

"It's a catch-22 situation. I could convince a minister that I could help them transform the way they source technology, but then in trying to source my services, he wouldn't be able to do it. He'd have to put it out for bid and I would be undercut by somebody cheaper. They just can't change."

Jones feels the current procurement model could be particularly damaging to the successful adoption of software-as-a-service (SaaS), which will continue to gain popularity in the public sector.

"One of the problems with SaaS is the risk of lock-in, or at least the friction that builds up over time if you're using a particular platform for a long time," Jones explains. "I see a lot of naivety in sourcing. Failing to recognise that when the initial contract comes up for renewal, you're going to be in trouble unless you have an exit strategy sorted out.

"I think one warning about the growth of SaaS is that public sector procurement has to be a lot savvier in how to negotiate contracts and it has to realize that this is not about competition. If you sign a three-year contract with a vendor and that three years is coming towards the end, you can't rely on competition to negotiate. You've got to find some other way to negotiate."

Changing contracts

There may be greater hope for change in the prevailing government contracting model. Jones' fellow Forrester analyst Paul McKay believes that the days of big outsourced IT contracts may be coming to an end.

"I think you're going to see much more atomic examples of government procurement looking to buy smaller technology projects or services that have much

more tightly defined and clear business benefits... These large IT programmes, which failed to deliver on their benefits, typically get a fairly rough ride in the public accounts commitment and also from the National Audit Office," he argues. "I think you're going to see departments move away from that big bang model and try to look towards smaller-scale innovation."

The NHS, stung by the experience of the failed National Programme for IT, is already exploring small-scale innovations from the private sector that could gain traction organically than the traditional large IT programmatic approach.

Online consultations with doctors delivered by Babylon and Push Doctor recently became available on the NHS, but McKay anticipates a tough road towards widespread NHS adoption for private companies

"I think they're going to try but I think there are significant structural challenges to them doing that within the NHS," he says. "The NHS is quite complicated from a procurement perspective, so I think for them to figure out who are the right people to talk to, it's going to be a very long hard slog for them because they're having to engage almost on a trust by trust basis.

"Yes, there's the NHS Digital organization that they can try and get stuff through, but ultimately, things get implemented by local hospital trusts and primary healthcare trusts. They're going to try that, but they're going to come up against stiff opposition, not just from management within the NHS but also from doctors."

Cloud growth

Gartner analyst Cannon expects the public sector's move to the cloud to accelerate dramatically in 2019.

His public sector clients used to ask whether they could or should move to the public cloud, but now the line of questioning has shifted to how they can do it.

This changing mentality has been driven by a growing belief that the public cloud is typically more secure than on-premise solutions and that the cloud can add the scalability and elasticity that departments need to quickly introduce new services for citizens.

"When we talk about cloud computing with the likes of the innovations from AWS, Azure and Google, it's way beyond just compute and storage," explains Cannon. "It's around IoT gateways, it's around artificial intelligence, it's about all of these things, and about the additional services that they are able to provide on top, and giving people in government access to the best tools available."

Forrester analyst McKay echoes Cannon's thoughts: "I think you're going to see a lot more of a transition away from the idea that as a rule government departments and local public sector agencies should be making a habit of deploying these things internally – which involves a cost and skills that are required to do that – and pushing more of that out to the cloud and becoming more comfortable with the idea of using the cloud as a collaboration tool and an enabler.

"In the work I do with Microsoft from a security perspective they are certainly looking to help the public sector make the most of the investment that they have in their technology and you'll see that other cloud providers are also trying to do the same."

Exploring new technologies

The skills gap could be bridged by automation. Terry Walby, CEO and founder of RPA company

Thoughtonomy, has high hopes that the public sector will become the leaders in AI and RPA adoption.

"We've already seen the benefits that intelligent automation is bringing to public services," he says. "As budgetary pressures become ever more severe, skills become in even shorter supply post-Brexit and demand continues to increase, there will be a marked shift towards digital labour as a way to drive efficiency and free up time amongst frontline staff.

"We expect to see public sector organizations operating a higher virtual worker: employee ratio than any other sectors. No longer the laggards, automation will see the public sector become pioneers within AI adoption."

He predicts that automation will be used to deliver joined-up public services, particularly within health and social care and policing, as organizations share best practices and standardize processes. He also expects new AI-focused roles to be created in senior government, including perhaps a minister for AI, to promote and scrutinize the technology as "we shift towards a hybrid human-virtual workforce".

Gartner analyst Cannon agrees that RPA and AI will be used in an expanding range of public sector applications. "Expect to see more chatbots and service centres trying to get ahead of the curve and use these types of capabilities now to drive efficiency and release people for other activities," he says. "More and more is going to be supported by using some sort of SaaS model."

He has less faith in the near-term benefits of blockchain. Proponents of the technology argue that governments could use the technology as a centralized

trust model, but Cannon believes that it largely remains a solution looking for a problem, even in the apparently promising area of digital identity management.

"Government has some specific uses around identity where an immutable record isn't necessarily the best thing," he says. "If you think about the witness protection programme, if you want to take somebody away who's involved in a serious criminal case and they need protection, then they need a new identity. You can't just reinsert that somewhere back in the chain. There are issues around that for government."

Shifting skills

The growth of AI in the public sector will only work if staff have the required skills, which Forrester's Jones believes will be a challenge: "If you want to apply artificial intelligence techniques to a data set to come up with some insight, you probably can't hire the people yourself. You've to source them in. That's why the change in the sourcing process is so important, because you're trying to source rare skills.

"Enterprises have the same challenge. They have to source often because they can't hire the right people. And because these people are in high demand they can attract a premium price so if you're looking for the cheapest all the time or you're making a vendor compete with ten other guys for your contract, they're going to say I'm not going to bother. I can sell my people. It's my people that are the scarce resource. I can get more money elsewhere from a better customer."

The move to the public cloud will mean that there is also an increased demand for cloud computing skills, while the growing threat to critical national

infrastructure (CNI) will need to be met by improved cybersecurity skills.

Kaspersky Labs expects that during the next year there will be some occurring attacks on CNI, especially in retaliation to political decisions. Forrester's McKay predicts that the UK's defences will be hampered by a lack of security skills in the regulatory bodies that will be responsible for defending their sectors.

"As a nation, we've decided to take a sectoral-based approach to implementing that, so, for example, Ofgem is responsible for regulating utilities," he says.

"To date, those regulators have not had specific oversight of cybersecurity for the organizations that they regulate, so it's quite a new thing for them to be having to do this. And while of course the National Cybersecurity Centre will be heavily supporting them with that, they're going to have to acquire some of their own cybersecurity skills and expertise in a regulatory capacity. And I think for the usual reasons that exist within the public sector around trying to get any form of technology workers from the private sector you're going to see them really struggle to acquire that talent because of the pay and the remuneration restrictions that exist in the public sector at the moment."

Planning ahead

Jones advises IT managers in the public sector formulating strategies for 2019 to focus on the needs of users. "Think of the citizen," he says. "Think what it is your group that citizens really care about and use that as the guiding principle.

"A lot of things that I've been talking about arise from policy for its own sake. We know that it's silly, but

the politicians tell us to do it that way. The project ends up being a disaster, but it was a cheaper disaster than it would have been if we hadn't sourced it that way. No, actually, citizens want you to spend their money wisely, but they want you to deliver great software as well that makes it easy for you to engage with government organizations."

Cannon echoes the sentiment, adding that it's crucial to concentrate on the use of data for civic purposes.

"Focus on the data," he says. "Understand how the data can be used and shared between agencies. Have those conversations with the citizens about the reuse of their data. Don't shy away from having the difficult conversations about how and what's required to join up government in order to deliver the commercial-grade interactions that citizens really want from government. We need to be responsive to the sensitivity and privacy issues and security issues, but equally, we need to be able to use that data to provide those evidence-based decisions and policies that everybody wants to see going forward." **Tom Macaulay**

Credit: iStock

Blockchain and cryptocurrency trends

Our top predictions for blockchain and crypto in 2019

In 2008, shortly following the cataclysmic subprime mortgage crash, for some a beam of hope shone out: the promise of a completely decentralized monetary system, distinct from the irrationalities of the market and the destructive tendencies of government and banks 'too big to fail'. The insurgent idea, leaked quietly onto niche Internet forums, was bitcoin.

Cryptocurrency has not completely upended the established economic structures as some had hoped, but it has certainly made an impact on the world.

Despite initially being pounced upon by cybercriminals as a means to facilitate illicit transactions, cryptocurrencies still hold potential as a vehicle for frictionless, anonymous payments across borders for the average citizen.

What is more interesting for many other segments of industry is the underlying technology, blockchain. The transparency blockchain systems afford, along with their ability to provide a shared view of every transaction that occurs within the system combined with the difficulty of hacking them make blockchain an attractive technology.

The level of decentralization varies depending on how open the blockchain system is. While the initial champions of blockchain – and some decentralized apps today, as we'll see – advocate for completely public blockchains, private or semi-private blockchains have proved more palatable to big business.

Here's what we expect to see in 2019.

Banks and cryptocurrency

One industry that took notice of blockchain from the beginning is banking. For some years now banks have experimented with blockchain, particularly with applications in making transactions cheaper and more effortless. While one of the primary features of bitcoin was conceptualized to be decentralization, centralized banks are examining ways in which they could absorb certain blockchain-like systems.

Take the cryptocurrency Ripple, which was founded in San Francisco in 2012 and has since had success working with major banks. One of its products, xCurrent, is used by a number of banks including Santander and

vastly speeds up the process of checking the information required to make transactions.

Ripple also launched xRapid in 2018, which is aimed at businesses that have a presence in emerging markets where preloaded local currency accounts are generally required for payments – pushing up transaction costs and time. Instead, xRapid will quickly convert fiat money into a cryptocurrency, XRP, to move it through the system before converting back into whatever the required currency is at the end.

At the time of launch, the CEO of Ripple, Brad Garlinghouse, predicted that most major banks would adopt the service in 2019 as a liquidity tool.

However, despite some companies, including Western Union and Moneygram, trialling xRapid, Garlinghouse has said the lack of uptake is due to uncertainty around the regulatory constraints on blockchain.

This could be set to change with the establishment of legitimate coin exchanges in Gibraltar and Malta.

Goldman Sachs has expressed interest in setting up a cryptocurrency trading desk, although nothing is set in stone and the company appeared to backtrack from the idea when Business Insider reported that the company had dropped the idea.

However, as the value of cryptocurrencies went into freefall, this was rebuked with a counter statement from the bank decrying the report as ‘fake news’.

“A big question for cryptocurrencies in 2019 is whether we will see an Exchange Traded Fund approved by [American regulatory body] the SEC,” says Ruchir Dalmia, Blockchain Consultant at Deloitte. “Such an approval would likely be a catalyst to further investment from institutional investors, such as funds and trusts, into

crypto markets and demand for cryptocurrency. There are several experienced applicants under consideration currently but, after several rejections and deferrals during 2018, it remains unclear whether the SEC will be prepared to permit such a venture in the near term."

Importantly, Christine Lagarde, chairwoman of the International Monetary Fund (IMF), made comments recently that seemed to encourage banks to become more engaged in cryptocurrencies, even suggesting that banks should experiment with launching their own cryptocurrencies to prevent cryptocurrencies becoming havens for fraudsters.

It could also suggest that Lagarde believes that cryptocurrency could one day break out of its relatively niche user base and enjoy widespread uptake.

This eventuality could prove worrying to central banking systems as it would pose a direct challenge to their hegemony. Given that this would only happen if cryptocurrencies became much easier for the average person to use, perhaps Lagarde wishes to negate this possibility by encouraging banks to become frontrunners in this charge – and offer a more user-friendly crypto product before others do.

Although much of this seems counter to the raison d'être of crypto, there are ways of creating coins that are less decentralized, and incorporate a central mechanism that controls the supply of 'coins'. This means it would be possible for the banks to launch their own form of crypto without embracing a truly decentralized system.

To this end, there is also an increasing market for 'stablecoins', which are tethered to price fluctuations of an established fiat currency, for example, the dollar. Initially suggested as a means of negating the wild price

fluctuations suffered by bitcoin and the like, clearly, this offers a mechanism whereby a digital currency could offer the benefits of crypto but without truly challenging the underlying economic systems at work – a prospect which may prove very enticing to central banks.

However, it should be noted that at present due to regulatory ambiguity, in theory companies could also launch their own forms of cryptocurrency.

Given that tech giants such as Google and Facebook can move much more swiftly than government in creating and adopting technologies there is also a possibility that these companies could become interested in launching their own cryptocurrencies – even taking over the economic reins from central banks if they wished.

Our bet is that 'crypto' of some form will catch on eventually, given the massive incentives in terms of frictionless and low-cost payments, but it is unlikely to be tied up in any true 'decentralized' forms of banking in the near term.

Regulatory hurdles persist

Of course, for this to happen, there would need to be definite change to the current regulatory framework for crypto and blockchain, both in the UK and globally.

In the UK, there is currently no official legislation for the use of blockchain technologies from the Financial Conduct Authority (FCA), the UK's regulatory body on finance. While the FCA does not explicitly regulate cryptocurrency, applications built on top of blockchain in the fintech space are under the organization's remit.

Early in 2018, a speech by Mary Starks, director of competition at the FCA, outlined the major applications of blockchain as "records, including records of contracts,

transactions, asset holdings and proof of identity". She noted that the "two purposes of regulation are to protect the consumer, and to help innovation flourish". She added the importance of ensuring global collaboration on this issue, pointing to Global Digital Finance as one such international body that is aiming to push forward the adoption of digital finance technologies.

Among other things, the FCA has created a sandbox initiative allowing companies to test out blockchain applications and experiment with the tech within an enclosed environment.

However, 2019 could be the year that regulation becomes more conducive to experimenting with the technology in the financial and commercial spheres.

At a recent Blockchain Live event, held in London, minister for digital and the creative industries Margot James signalled the British government's interest in developing blockchain capabilities in UK industry.

"As the prime minister said recently, the UK is 100 per cent committed to supporting the development and adoption of new technologies," said James, drawing a parallel between the government's interest in blockchain and the push to roll out 5G.

However, James stressed the importance of looking at the applications of blockchain beyond the financial world. She highlighted a number of blockchain projects for particular praise, including the partnership between IBM, Nestlé and Unilever to improve the traceability of contaminated food.

"Actions like this, which work behind the scenes for consumer protection, have the capability of making huge improvements to peoples' lives," she added, noting that in recent months she had met a number of companies

developing blockchain applications to improve supply chains and increase trust in social funding.

James added that the British government had committed £10 million to fund blockchain projects in areas such as energy, voting and charity through Innovate UK and research councils.

However, the Britain and other governments across the world are still struggling to develop a regulatory framework for blockchain given that the decentralized elements pose important legal issues, let alone settling on a common framework.

ICOs and dApps

In 2018, the market for 'Initial Coin Offerings' (ICOs) – an alternative funding method whereby a blockchain startup raises capital in exchange for tokens – boomed compared to 2017, but this could be a trend we see declining in 2019.

As the market was ramping up alongside growing hysteria around blockchain, there was high demand for ICOs both from true blockchain believers supporting decentralized systems for ideological reasons, or for opportunistic investors looking for get-rich-quick schemes. Given their notoriety for pump and dump schemes – allowing fraudsters to artificially inflate the price of tokens before cashing in – there is evidence that the lawless 'anything goes' days may be drawing to a close for ICOs.

Research suggests that it is becoming harder to gain sufficient funding this way. A high-profile failure was Civil, a blockchain-based news organization that failed to meet its market cap despite wide ranging publicity, including from the *Financial Times*, and the *New York Times*.

Harder to say is once the first movers' excitement has fizzled away, what will be left? Will the whole market sag into obscurity? Or will only the truly committed evangelists remain? If it's the latter, can interest be sustained long enough to gain mainstream appeal?

"It would appear that beyond any initial interest in a dApp [decentralized application], they struggle to maintain any form of meaningful user base once all the excitement has died down," says a spokesperson from Everledger, a UK start-up that has built a scalable commercial application for the diamond industry, coloured gemstones, art and wine on top of blockchain technology. "For most, it appears that dApps are a challenging concept to understand in comparison to popular, easy-to-use web-based apps like Facebook, Instagram and Twitter, which are all free to use too – if you set aside the rampant harvesting of personal data and the exploitation of users, that is."

But barring mainstream appeal, considerable hurdles remain such as the need to invest in a 'cold wallet' and sometimes going through a complex registration process in order to participate in this ecosystem.

Organizations such as Token Foundry are trying to bring legitimacy to the area by requiring a more rigorous approach to the registration of buyers.

Deloitte's Ruchir Dalmia tells us that the services multinational has recorded declines of more than 80 per cent across most crypto assets due to lack of returns and cancelled projects.

"As investors and regulators become savvier, token projects are being held to higher standards, and clearer regulatory guidance is pushing new crypto ventures to adopt better processes, as well stronger teams and

technology," Dalmia argues. "This, however, comes at considerable cost. Combined with the already high cost of blockchain product development, the effect of asset-rich teams selling off ICO incomes to fund ongoing product development has produced difficult market conditions, which is why we expect the market for ICOs to remain subdued in 2019."

In the UK, Digital Catapult, a quango that promotes digital technology and innovation, conducted research on more than 260 distributed ledger technology (DLT) companies. Informed by this research, it divided the DLT companies into four major categories: distributed ledger developers (13 per cent), decentralized app developers (35 per cent), service providers (37 per cent), and centralized systems (15 per cent).

Despite the focus on finance and fintech, it found that these companies spanned a number of industry verticals, including the manufacturing and creative industries. In fact, 38 per cent of the companies interviewed feel that their technology could be applied to all vertical markets, not just fintech.

Regulatory uncertainty was cited as the most pressing concern by 74 per cent of these companies, with the irreconcilability of GDPR with public blockchain and a lack of clarity around ICO regulation being the top issues. Of these companies, 45 per cent had to consult specialist lawyers to help establish their organizations, but were uncertain as to whether they'd received valid advice due to the novelty and complexity of the area.

Tokenization

To discuss tokenization, it's important to delineate different kinds of tokens, which are each tied to a

different kind of blockchain ecosystem. Altcoins are forms of cryptocurrency so named because they are an 'alternative' to bitcoin.

Utility tokens: originally dubbed 'appcoins', these are tokens that are primarily used within the ecosystems of blockchain-based platforms. They hold internal value on the platform, but can also be swapped for different currencies on exchanges. They can also act as 'shares' in blockchain platforms.

Finally, security tokens embody the value of real-world assets, for example, real estate.

"We believe tokens are the catalyst for re-imagining completely new constructs and building completely new systems," Sanaya Mirpuri, head of product marketing at Token Foundry, says in relation to utility tokens. "We believe in projects creating token-powered ecosystems. So, not just payment tokens or tokens that people can pump and dump, but creating an ecosystem, where people can actually use the tokens."

But decentralized companies supporting token economies adopt a radical new model of enterprise, where monetization can be a dirty word.

"We don't like using the term 'monetization' because we think that is essentially what the centralized platforms – Periscope, Instagram, YouTube – do," Kevin Yeung, CEO of FanX, an upcoming decentralized live streaming platform explains. "They monetize their users and content generators."

Therefore, it's difficult to see how these types of businesses will fit under the accepted model of commerce. However, a token economy could also appeal to established traditional companies. For example, CEO of YEAY, a decentralized social media

platform, Melanie Mohr tells us: “Looking into other apps that could also use the WOM token, frankly, it could even be pursued by Snapchat or Bitmoji.”

However, it’s not certain that these decentralized ecosystems will ever become mainstream. A more mainstream potential application of tokenization is in security tokens. Security tokens can render trading more seamless and inclusive due to lack of barriers between different currencies and countries.

As ICOs are increasingly clamped down upon, Security Token Offerings (STOs) are on the rise, due to their greater regulatory compliance. In fact, security tokens are already fully compliant with SEC regulations, unlike utility tokens. This is primarily because the value of security tokens is linked to value that already exists in the world. For example, real estate, stocks or items of value that are assigned a value in fungible tokens. Many of the STOs that have launched to date are types of investment funds.

Everledger commented on the fact that the UK government is pushing regulation forward: “Cryptoassets that are security tokens fall within the existing regulatory perimeter as specified investments. However, the Taskforce recognised that the novel nature, complexity and opacity of many cryptoassets means it is difficult to determine whether they qualify as security tokens. To provide further clarity in this area, the FCA will consult on perimeter guidance on the application of regulation to these tokens by the end of this year.”

Blockchain and big industry

Some high-profile blockchain startups focused on the financial sphere include the R3 consortium made up

of over 200 companies, including Barclays, Accenture and AWS. In 2016, they created the open source Corda platform – designed for anyone to build on – as well as the Corda Enterprise platform, which can be adapted by different businesses for different use cases.

Another group is the Hyperledger Fabric from IBM, an open source blockchain framework that is designed to help you create a blockchain for your business network, with paid options also available.

Businesses outside of the financial industry have been particularly interested in leveraging the tracking capabilities afforded by blockchain technology. A partnership by IBM, Nestlé and Unilever resulted in the development of blockchain to improve the traceability of contaminated food.

Blockchain may also have a growing application in health and pharmaceuticals. IBM and the US Food and Drug Administration (FDA) have partnered on building a scalable health data exchange using blockchain, with the aim of addressing a lack of transparency in health data and improving trust on patient privacy.

Logistics giant DHL meanwhile is currently working with Accenture to develop a blockchain-based track-and-trace serialization system in six areas around the world.

This is still a fledgling area, but increasingly, tech giants are offering 'blockchain-as-a-service' options, making the tech more accessible than ever. Some of the companies offering products such as these include Oracle, IBM and Microsoft.

A Deloitte survey earlier this year finds that 84 per cent of respondents now view blockchain systems as more secure than systems built using conventional technologies. Deloitte's Ruchir Dalmia says that there is

growing momentum for the use of blockchain platforms within business and we are beginning to see the launch of large-scale platforms.

"Business leaders are beginning to take ambitious steps to move from small-scale experimentation to real world execution, with organizations pooling resources and expertise towards building shared platforms," Dalmia said. "Investment in consortium-led projects has taken hold across most sectors, for instance in the launch of VAKT, an organization backed by several major energy corporations, which launched its commodity post-trade management platform earlier this month.

"In 2019, we expect the launch of several new large-scale enterprise solutions." **Laurie Clarke**