



PERSISTENT



Technology Predictions for 2019:

The Six Digital Currents
Steering Enterprises
into the New Age



Contents

Introduction	03
Data and Analytics	04
Artificial Intelligence and Machine Learning	07
Human-Machine Interaction.....	10
Internet of Things	13
Identity, Access and Security	16
Blockchain	19

Introduction



Welcome to Persistent Systems’ fourth annual white paper of predictions about technology trends that will drive enterprise digital transformation. We see no slowdown in the transformation of all enterprises—regardless of industry, value proposition, or customer set—into software-driven enterprises, not just in the back-office but all the way to customer experiences and business processes. For 2019, we have identified six digital technology trends as game changers.

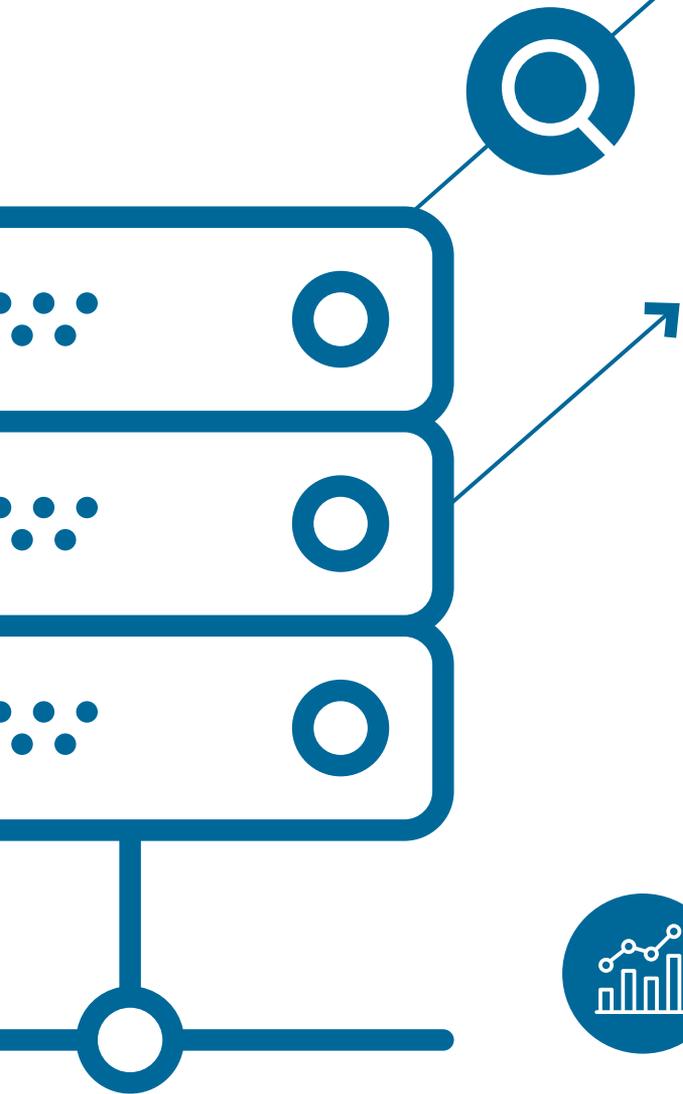
Each trend is broad and covers multiple individual fine-grained technologies spread across different levels of maturity. We describe this spread using a five-stage maturity model that we call the *EDIPS continuum*, from the first letters of the five stages: Evaluate, Demonstrate, Incubate, Proliferate, and Saturate. This model is conceptually similar to other technology maturity models used by industry analysts, the two principal differences being that we use verbs rather than nouns to denote the stages, and that our model is geared to the perspective of an enterprise user. The five stages of this model and their associated characteristics are shown below.

 Stage	 Definition	 For a technology at this stage,
 Evaluate	Internal assessment of advanced technology trends.	... your innovation teams should be exploring its value to your use cases, and building prototypes/accelerators.
 Demonstrate	Experiment with clients on validated advanced technologies.	... your innovation teams should be expanding the prototypes to proofs of concept with internal or external clients.
 Incubate	Bounded demonstration of technology in a business solution.	... it should be transitioning from your innovation teams to product management/development/delivery and be showing monetizable business value.
 Proliferate	Full-fledged delivery of technology solution to paying clients.	... you should be using it in your products or your internal operations and be demonstrating quantifiable revenue or cost savings.
 Saturate	Technology is considered standardized/commoditized and not “advanced”.	... you should have internalized its use in your products, services, solutions, and internal operations (or you are way behind the competition).

In the following sections, we describe each individual technology trend as well as enterprise scenarios where they can be brought to bear. To help you understand the two key questions that concern you as a CxO or Line of Business leader (first, the nature and degree of impact that each technology trend will have on your business; and second, how you can best leverage the trend to successfully execute your digital strategy and grow your business), we have provided a set of three business-centric recommendations with each trend to help you get started down the path of discovery, and have indicated individual fine-grained technologies within each trend along with their maturity levels.



Data and Analytics



Invigorating the Analytics Value Chain

Analytics has become a mainstream idea, as there is ample evidence that data-driven decisions tend to be better business decisions. However, simply integrating and governing data assets does not guarantee that business value is generated. Governance has to cover the analytics value chain and be integrated with an overall business strategy; using machine-learning to augment human intelligence and contextual awareness across this value chain will also help. Finally, we are witnessing a rapid increase in data privacy regulations across the globe, which will drive further governance and data management activity.



Demonstrating measurable business value through analytics to organization leaders will be inescapable

Analytics has now become pervasive in organizations, both in operational and in more general decision-making scenarios. However, the latter kind of solution, built on top of a data lake or a data warehouse gathering data from all around the organization, is a necessary but not sufficient condition to generate enterprise value. Not long ago, the main concern was lack of trust in the data. A first generation of data governance tools and processes introduced control policies, processes and accountabilities to transform data into a trusted corporate asset. However, this is not enough when data assets are too easy to copy around or to ingest in data platforms which are often poorly managed. Recent data governance tools address this data sprawl and disorganization problem by grounding themselves on a curated inventory of available, distributed assets (a Data Catalog).

A second, more fundamental problem is that simply having well-governed data assets does not guarantee that business value is being generated. Generating value from data requires a more intimate knowledge of the value-generating chain.

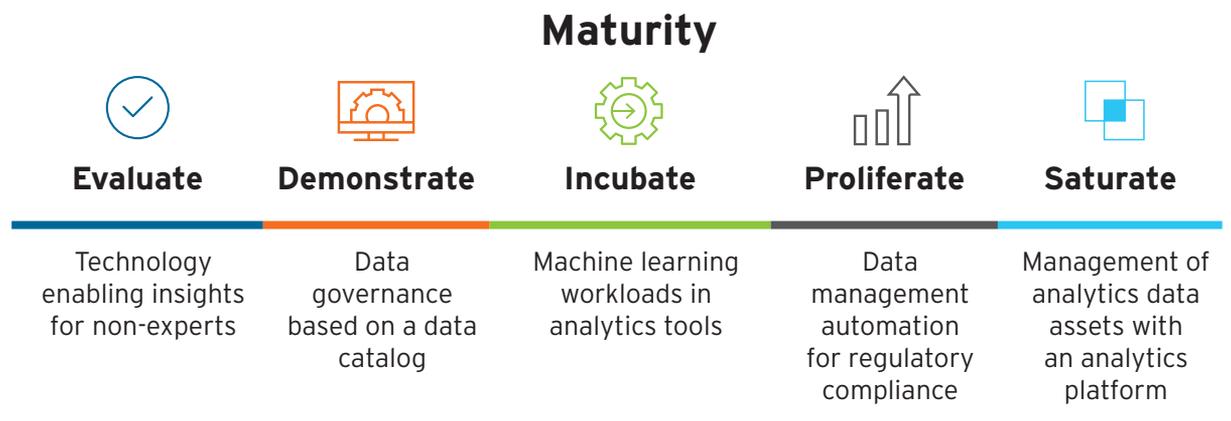
For this value to materialize, it is highly advisable to take into account:

- An expanded form of governance, called data value governance, covering the entire analytics value chain, from data and insights to people and business processes.
- An integration of this data value governance with an overall business strategy that aligns to a data-driven business model.

We are not yet at the point where data value models, metrics, and a supporting data value platform are universally understood, accepted and adapted to an organization’s needs. Nevertheless, the trend has started with an attempt to comprehend, catalog and publish the interactions between data assets, people, and business models and their supporting business process workflows, to better foster value creation from data. We foresee data value governance to mature based on stakeholder engagement with published data artifacts, derived insights and their use in action-based process workflows.

Machine Learning (ML) and Natural Language Processing (NLP) will accelerate the data to data-driven decision-making process

Central to the previous development is the use of machine learning automation to augment human intelligence and contextual awareness across the entire data and analytics workflow, from data to insight, and from insight to action.



Two examples of this trend are:

- Self-service data preparation platforms, where two different and complementary aspects are being developed to shorten the time in getting the data ready to train ML models. First, data preparation is being specialized by including new operations such as sampling, scaling, enhanced validation, and robust methods to deal with missing values. And second, ML technology is used to learn formats and schemas of data sets, and how users interact with data, to then recommend steps to expedite data preparation.
- Conversational analytics, backed by NLP technology, making the value generation process out of data accessible to all employees. Specific example technologies include smart searching with natural language (NL) queries, and NL generation to provide advice and next steps to the end-user in prescriptive solutions.

Privacy laws will soon be inescapable

The European Union's General Data Protection Regulation (GDPR) has been attracting attention because of its far-reaching impact on data privacy and security. There are several similar regulations coming up now:

- California's Consumer Privacy Act (CCPA) of 2018 mirrors many of the GDPR data

protections for California residents and extends those protections beyond the 'consumer' role to employees, patients, tenants, students, parents, and children.

- Vermont's data broker laws regulate businesses that buy and sell personal information to third parties, requiring them to register with the state, and mirror GDPR with respect to informed consent, opt-out, and security standards.

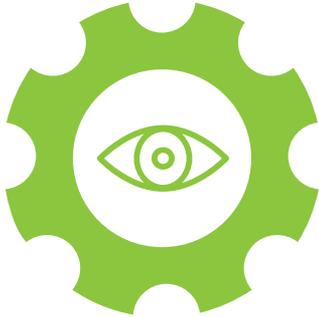
These type of regulations will soon spread globally. Indeed,

- Consumers have taken notice: In the wake of major data breaches and the Cambridge Analytica news in 2018, more than half the respondents in a recent poll expressed concerns about trusting companies to use their data properly.
- Policymakers continue to react: The EU Parliament has adopted a resolution for the suspension of the EU-US Privacy Shield, a data transferring agreement, seeking to bridge the respective data protection regimes, because it fails to provide enough data protection for EU citizens.
- Corporations are paying attention: Data privacy has become a board-level issue, as regulations are making businesses think about what data they collect and how they use it, not just how they protect it.



Recommendations

- 1. Make sure your data governance processes allow your data to be trusted for analysis.**
- 2. Align your data with your business strategy. Understand how data and analytics impact your business goals and how applicable regulations impact your current data management function.**
- 3. Expand the reach and relevance of analysis by using technology to enable casual users to access insights more easily.**



Machine Learning is Ready for Prime Time

A wave of emerging algorithms, massive data availability and accessibility and commoditization of infrastructure is driving the democratization of AI, where the complexity of model building, training and deployment will get simplified. Large platform players will play a critical role in this movement. Natural Language Processing (NLP) will get employed in many aspects of business processes. Deep Learning is emerging from academic research and is ready for business use cases. Enterprise ML initiatives will come out of pilot mode and become mainstream. Overall, machine learning is becoming a primetime reality in enterprises.



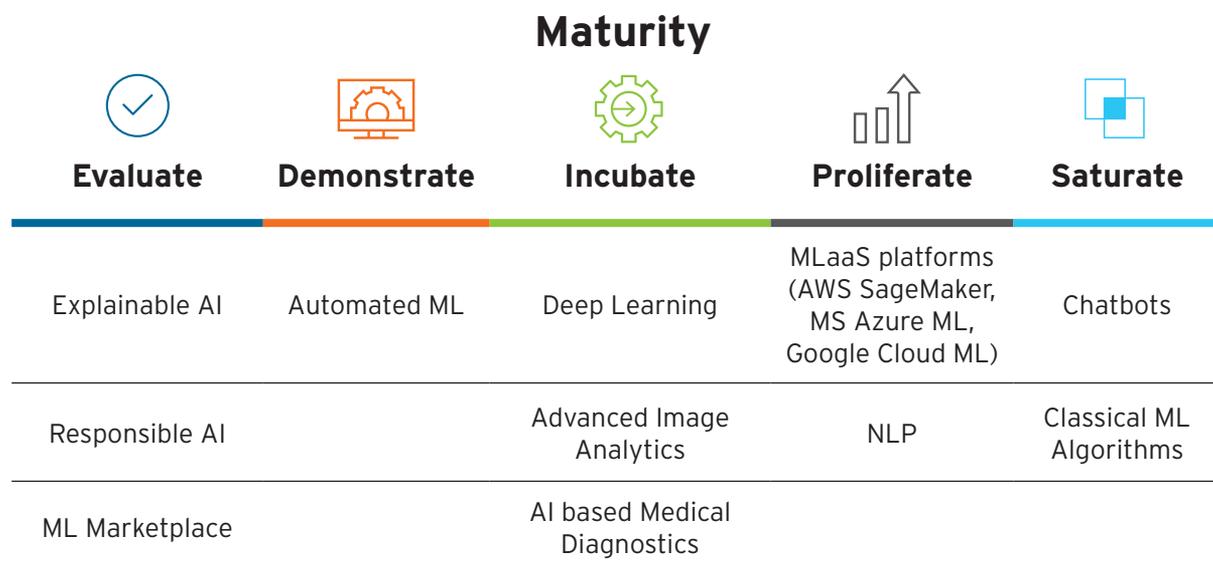
Analyst research predicts that by 2022, one in five workers will rely on AI to do some portion of their jobs. In the last couple of years, we have witnessed a trend of machine learning evaluation initiatives turning into mainstream projects and becoming an intrinsic part of enterprise automation roadmaps. Enterprises are investing in more practical usage of machine learning in areas such as human augmentation (automating complex processes, providing intelligence to aid human decisions), customer support and engagement, employee engagement, talent sourcing, sales and marketing.

While we see this increasing demand on one side, there is a shortage of qualified data science talent on the sourcing side and increasing complexity of algorithms on the business side. These factors are the driving force behind the trend of democratization of AI. Cloud providers like Amazon and Google are providing the means to quickly build and deploy ML models. Automated machine learning, (which attempts automation of exploratory analysis, feature engineering and selection, building and training multiple simultaneous models) is becoming more prevalent. Google recently released a service called Cloud AutoML that enables developers

with limited ML expertise to train high-quality models. Niche companies like DataRobot efficiently automate the process of building many ML models from open-source algorithms, for a given dataset and target variable.

We also see a pattern of common use cases across enterprises in horizontal areas like unstructured text insights, image analysis, and speech-to-text, where enterprises are seeking readymade ML models. On the other hand, AI start-ups in financial services, healthcare, and legal domains are mushrooming to target niche problems within a domain. Amazon AWS Marketplace recently launched ML models in the marketplace for a tailored selection of ML use cases. Overall, the industry is slowly gravitating towards a common ML solutions marketplace.

In terms of technology, two areas will be prominent in 2019 and beyond. The first one is NLP and text analytics. While chatbots and voice assistants have become commonplace in customer support and engagement, enterprises are realizing the need to go beyond the hype of chatbots, understand the complexities of human-machine interaction and employ NLP in every aspect of customer experience. Healthcare providers are trying to find hidden details in



nursing notes which can affect patient care plans or seeking to decipher patient sentiments from patient-nurse conversations. Banks are using NLP to assess the digital footprint of customers to feed into credit score calculations. Pharmaceutical companies are building NLP query interfaces for complex pharmaceutical regulation. The need to understand how human language works and how to employ it in business flow is becoming a key priority for practitioners of machine learning.

The second major technology that will matter in 2019 is deep learning. It is primarily getting leveraged in areas such as medical diagnostics, digital pathology, image and speech processing, and drug discovery. This is getting bolstered by a more open approach and willingness of regulators to approve the use of AI in clinical and diagnostic settings. In the US, the FDA recently gave a go-ahead for a decision support software that uses ML to assist the neurovascular specialists in their diagnosis. Other examples include use of deep learning based image classification in astronomy for galaxy classification, in life sciences for micro-organism classification, and in auto insurance for car damage inspection.

Explainable AI, which unlocks the black box of the underlying algorithm and explains the decision or prediction made by it, will become key to the adoption of AI and ML. This is especially critical in healthcare, where the physician's adoption of AI is heavily dependent on explainability. Tools such as IBM OpenScale attempt to address explainability of the underlying algorithm, demonstration of data bias (if any) and decoding the decision making as required for regulatory compliance.

Democratization and mainstream usage of ML however opens a Pandora's box—about ethics and responsible AI. Not everything that ML can do should be allowed to happen unchecked and unregulated. Additionally, given the fact that these outcomes are driven by the possible biases in the underlying data, it is important to have checks and balances on the outcomes. The Public Policy Technology and Law Commission in the UK is considering the regulation of AI. We predict that 2019 will see more constructive work in this area to define a regulatory framework through common efforts between industry and government.

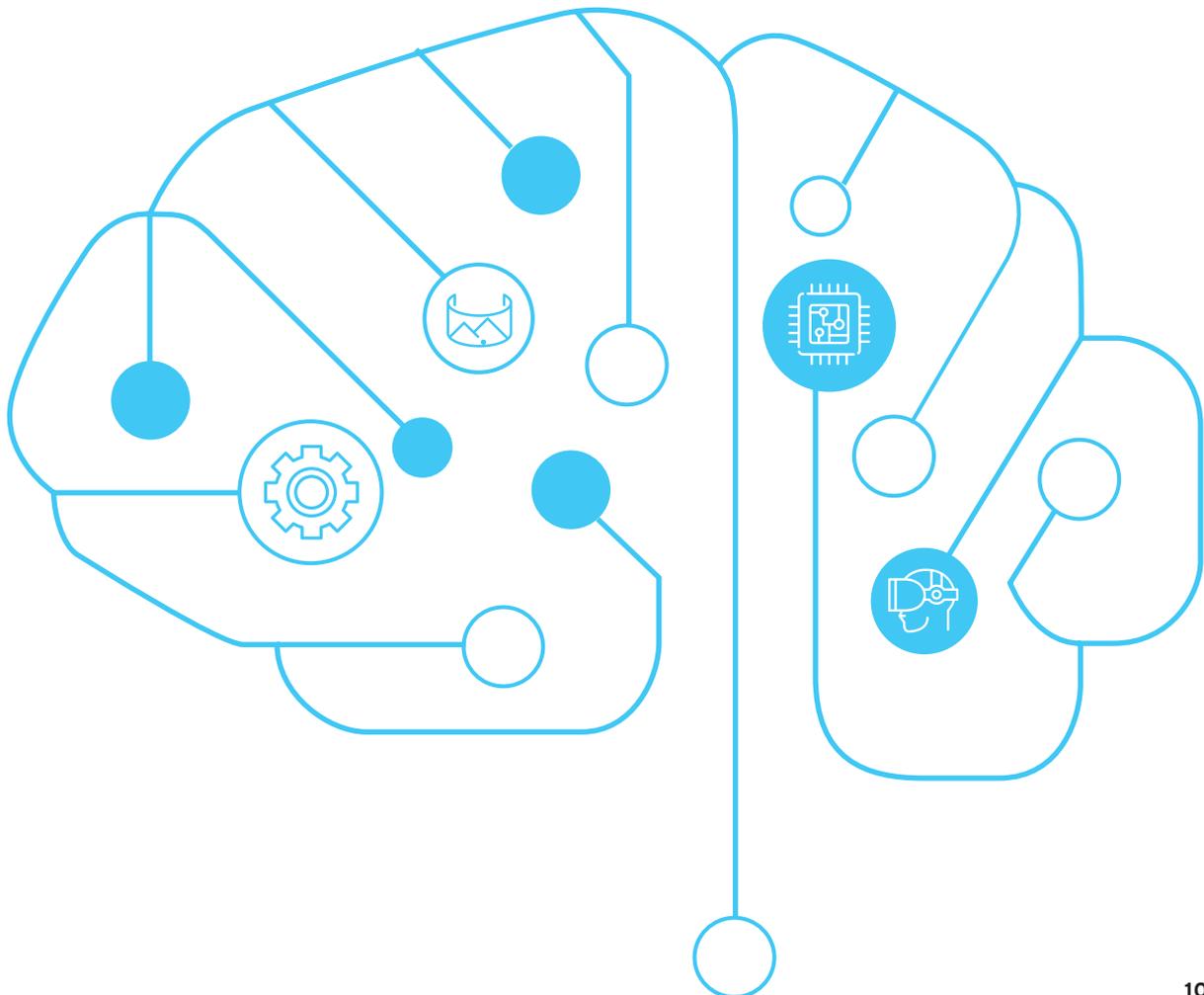


Recommendations

- 1. For faster time to market, adopt ML-as-a-Service platforms and ML marketplace models before building and training models from scratch.**
- 2. Look beyond chatbots and incorporate NLP in every aspect of customer experience.**
- 3. Evaluate explainable aspects of algorithms for better adoption of black box models.**

New-Age AR Experiences Are Here

Human-machine interaction (HMI) technologies such as augmented reality (AR), virtual reality (VR), and chatbots enable enterprises to create new innovative interaction models for business workflows and present data in a unique, immersive environment. While we have seen successful deployments of both AR and VR solutions in a few select industries, they are yet to find mainstream adoption. The software engines behind the technology, the devices to experience it and the immersive content that will be at the heart of it, all have to develop further before widespread adoption can happen.



Human-machine interaction (HMI) is all about how people and digital systems interact and communicate with each other. Chatbots, Augmented Reality (AR) and Virtual Reality (VR) are complementary HMI technologies that all have a great potential in both the enterprise and the consumer space for creating new interaction models for end-users. While adoption has been mixed so far, we are seeing these technologies steadily gaining adoption in the enterprise.

Enabled by artificial intelligence (AI) engines, today's chatbots are characterized by the ability to learn, adapt and respond to human queries and responses in diverse situations. According to a report by Global Market Insights, Inc., customer service is the highest contributing chatbot segment, with a 42.52% share. The global chatbot services market is projected to reach \$1.8 billion by 2022, at a compounded annual growth rate (CAGR) of 31.2% during the forecast period.

AR technologies augment the physical world with digital content and controls that provide the human user a richer context of their physical environment and enable interaction with the software through more natural physical actions like touch, gestures and movements. Current consumer use cases of AR are largely

around entertainment, education, retail or gaming; in the enterprise, the use cases are aimed at improving productivity, collaboration and customer support. The AR market, which includes hardware and software, is expected to grow to \$60.55 billion by 2023, at a CAGR of 40.29% between 2018 and 2023. Smartphone-based AR has established a strong foothold in the market due to its simplicity, ubiquity and a strong developer base. Special-purpose hardware such as AR glasses have entered the enterprise and industrial markets for applications ranging from equipment and safety training, operational guidance in industrial processes and diagnostics and repair. In order to provide a smoother, low-latency response experience, specialized, untethered AR headgears with more computing and memory will drive the next adoption wave in enterprises. Application creation for AR has become easier with major players like Google and Apple releasing ever more sophisticated AR SDKs, and we expect a slew of high-quality applications to emerge in retail, entertainment, manufacturing, healthcare, and training.

VR technologies immerse the user in rich three-dimensional digital realms to create experiences for entertainment, marketing, training, or operational assistance. The VR market is expected to grow to \$34.08 billion by 2023, at a

Maturity

 Evaluate	 Demonstrate	 Incubate	 Proliferate	 Saturate
Brain Computer Interface	Emotion detection and recognition	Virtual Reality	Augmented Reality	Conversational UI
Haptic Control Devices	Mixed Reality			NLP
				Chatbots

CAGR of 33.95% in the same period. VR headsets and applications will need to coalesce around common standards to enable wider developer and customer adoption. One of the barriers to wide adoption of VR is the lack of immersive content that delivers impactful and enjoyable experiences. In 2019, we expect to see more tools becoming available to content creators to democratize the creation of high quality content. The disorientation and discomfort that users experience as a side effect of using VR systems has been another impediment to greater adoption of VR. The release of untethered headsets, with WiFi connectivity but with more on-device processing, along with improved sensors will drive adoption of VR as well as mixed reality (AR+VR) experiences.

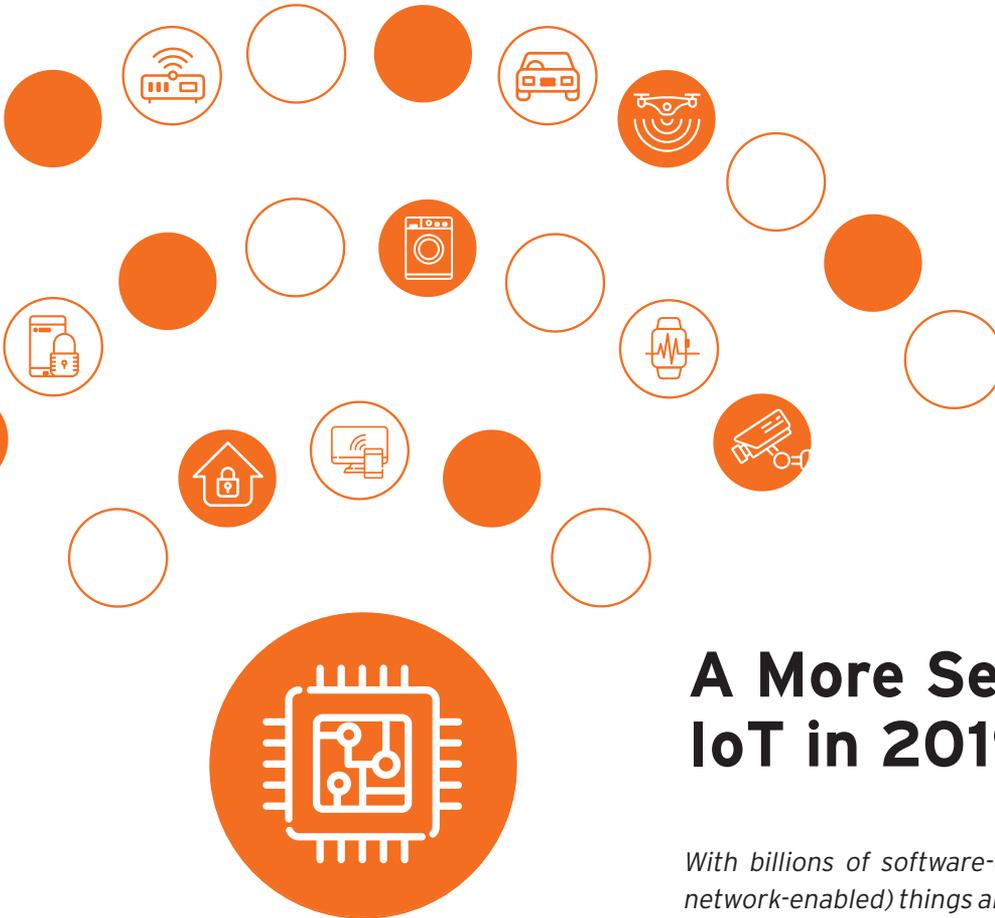
The technology giants are making big bets on chatbots, AR and VR. Microsoft recently acquired XOXCO, maker of the botkit framework that creates conversational bots for team collaboration. Apple acquired AR headset startup Vrvana. Amazon launched a new cloud service called Amazon Sumerian, for building AR, VR and 3D apps.

Enterprises, especially within the Industry 4.0 framework, are using HMI technologies to create immersive and more interactive customer experiences to engage them and create a stickier experience. The Fraunhofer institute for Factory Operation and Automation uses Microsoft HoloLens in its mixed reality lab to show machines, factories or entire cities on a 360-degree surface, giving customers the impression of standing right in the planned factory. Shell has effectively used VR for scenarios that are too dangerous or too expensive to recreate for real. It uses VR for safety instruction procedures at a deep-water oil project in offshore Malaysia. Ford is using VR to create a virtual workshop where geographically dispersed engineers can collaborate in real time on holograms of vehicle prototypes. Logistics company DHL, which provides AR glasses to its warehouse employees, has witnessed a 10-15 percent gain in their productivity. Boeing cut its wiring production time by 25% and reduced error rates effectively to zero. GE Aviation experiences an average of 8-12 % in efficiency improvement on their assembly lines by assisting assembly technicians with AR.



Recommendations

- 1. Create an AR customer outreach strategy. With smartphone as a conduit, AR has tremendous marketing potential to reach your customers wherever they are interacting with your brand / products, be it online or in-person.**
- 2. Digitally transform your assembly line and drive up productivity by bringing in AR/VR applications for human assistance in manufacturing as well as diagnostics and repairs.**
- 3. Build rich and immersive training programs by simulating costly, complex or dangerous-in-physical-world scenarios in safe and cost-effective AR/VR applications.**



A More Secure IoT in 2019

With billions of software-defined (programmable and network-enabled) things already active, and a predicted steep rise in their numbers, the Internet of Things (IoT) is already here. The number of applications, use cases and projections about overall business impact of IoT is growing every year. The trends strongly indicate architectural shifts in IoT deployments. For example, a preference to edge computing and machine learning at the edge is becoming prevalent. Security and privacy of the systems and collected data will continue to be the most impactful factors towards the success of IoT. Globally, emerging privacy regulations will accelerate the improvements in security and privacy. On the other hand, emerging technologies like blockchain and newer network connectivity standards will impact IoT over a longer time horizon.

The estimated number of active IoT devices is expected to grow from the present 7 billion to 25 billion by 2025. The IoT acceleration will continue in all major areas like Industrial IoT (IIoT), smart homes, smart cities, agriculture, healthcare and connected cars. This is being driven by the ever-present demand for improved operational efficiency and better quality of life through technology use. The evolution of IoT platforms, collaborative ecosystems, choice of connectivity technologies and cheaper hardware are the growth engines for IoT adoption. The challenges for this growth include insufficient clarity of business vision around IoT, security, deployment complexities, lack of interoperability and slow adoption of emerging standards. Here are our predictions for the most influential aspects of IoT for 2019.

IoT Security

The large-scale attacks, over the years, on and enabled by vulnerable IoT devices, have made everyone pay serious attention to IoT security. Analysts estimate that the overall IoT security expenditure will grow from \$1.5 billion in 2018 to \$3.1 billion in 2021. Security considerations will become one of the most important and fundamental design aspects and security will improve as the industry learns from bigger and more complex deployments. The ability

to remotely upgrade IoT devices will become a must-have feature as it provides a chance to fix security issues post-deployment. The increased awareness, best practices, proposed regulations and laws will give rise to compliance standards and certification in IoT security.

Edge Computing

Edge computing has become the new center of attention, especially for the Industrial IoT (IIoT). Various market research reports estimate that by 2023, the edge computing market will grow at a minimum of 34% CAGR from the current \$1.5 billion. All major cloud-IoT platforms have their own seamlessly integrated edge components that are feature-rich and powerful. Analytics and machine learning at the edge will become mainstream and change the way IIoT systems are being designed, with preference to carry out most computation at the edge. The choice of hardware platforms for edge computing are expanding from low-power, low-performance units to high-power GPU systems enabling a wider range of applications. The 'edge-first' approach will become the most preferred approach for IoT deployments as it provides better security (data protection, privacy), mitigates the impact of network latency and reduces data transportation needs and costs.

Maturity

 Evaluate	 Demonstrate	 Incubate	 Proliferate	 Saturate
Application of Blockchain in IoT	Machine Learning at the Edge	Integrated ML at Edge and Cloud	Edge Platforms	IoT Use Cases
GDPR Impact on IoT	Edge Analytics	Emerging wireless connectivity technologies	IIoT Deployments	Applications
	IoT ML in Cloud		IoT Security Regulations	IoT Platforms
			IoT Standards	

IoT Platforms

The competition between the major and most popular general-purpose platforms (Azure IoT, AWS IoT, IBM) is intense, with nearly identical offerings and mature features such as edge computing, machine learning, streaming analytics, visualization tools, and integration with third-party ecosystems. These IoT platforms are part of their larger cloud offerings and will continue to benefit from the addition of newer features there. These platforms will become the first-choice for brown-field deployments because many customers are already using the associated cloud platforms. The IoT-specific platforms (e.g., GE Predix and SAP HANA) will face stiff challenges because of this as well as the overall pricing. The new model of 'develop in the cloud, deploy at the edge' will become popular for IoT especially for, but not limited to, applying machine learning on IoT data, since it requires large data sets and computational power.

IoT Connectivity

Connectivity choices in IoT are ever-expanding, with a wide variety of old and new technologies in the wireless domain (WiFi, Zigbee, ZWave, BLE, 6LoWPAN, LoRa, SigFox, LTE, 5G). The selection criteria for a given application includes aspects like range, performance, power, cost and availability. Newer technologies are being adopted slower than expected, and the bulk of

deployments are still using well-established technologies like WiFi, ZigBee and BLE. The latest and upcoming entrant - 5G - may not have much impact in the next two years for IoT, because of the costs involved and lack of widespread availability. With the advent of edge computing the need for the benefits offered by 5G will be limited to some application areas, such as those requiring low-latency live streaming and remote control, e.g., drone applications.

Privacy, Blockchain and IoT

The European Union's General Data Protection Regulation (GDPR) will influence IoT significantly because of the rules and compliances around data collection, retention and deletion. A breach due to any vulnerability in the IoT deployment chain will likely lead to GDPR non-compliance. GDPR-imposed monetary penalties along with bad publicity will force manufactures and service providers to be careful about IoT security and change operational policies. Because of the multiple ecosystem partners involved in the end-to-end IoT solutions, GDPR compliance for IoT becomes a complex undertaking.

Blockchain is an important emerging technology that is expected to have positive impact on IoT solutions, and implementations tuned for various IoT applications have started appearing. In the near term blockchain's influence on IoT will likely remain limited to more secure device lifecycle management.



Recommendations

- 1. Consider IoT security as the most important aspect while designing and deploying every IoT solution.**
- 2. Move as much functionality as possible to the edge to enhance performance, reduce costs and provide better security compliance.**
- 3. Ensure that there is complete clarity of expected business outcomes and technology roadmaps before embarking upon IoT projects.**



Identity, Access and Security

Becoming a Zero-Trust Enterprise

It is well-known now that today's enterprise network boundaries are highly fluid, given the extent of user-owned devices on the network and an ever-expanding digital ecosystem of vendors and partners. To mitigate the continuously evolving threats in this type of an environment, enterprises must begin the process of becoming a zero-trust enterprise. A zero-trust enterprise works on the principle of 'never trust, always verify' and treats every network flow, every data movement, every access request as suspicious and evaluates it for risk, without relying on a static authentication of the user. Enterprises can begin the zero-trust journey by designating critical data, building virtual perimeters inside the network and adopting dynamic, risk-based access control.



Omni-channel security

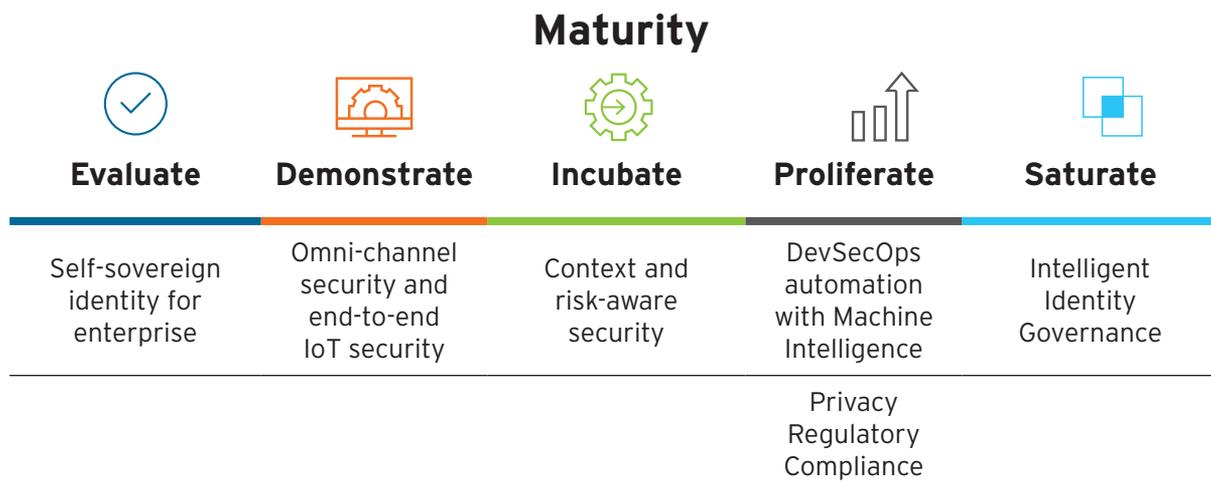
Omni-channel security will continue to take priority in the enterprise to prevent breaches and fraud across multiple access channels. When it comes to enterprise networks and systems, newer access channels increase the attack surface increasing the risk. A comprehensive review of access channels (such as web, mobile, API, B2B, VPN), process and technology is recommended from a security and risk perspective. Two major trends we see towards effective omni-channel security are around intelligent threat detection and adaptive access control.

The use of machine intelligence in threat monitoring and detection is now well established. Given the fluid enterprise border, the diverse and inter-connected software supply chains and the meteoric rise in zero-day exploits, machine intelligence enabled tools are the only way an enterprise can stay ahead of the attackers to detect ever-evolving and unknown threats. Adoption of these tools will rise significantly in the coming years as high-quality, high-accuracy tools become more accessible and available in the cloud without requiring complex deployments and configuration by every enterprise. These tools will treat every network flow as suspect until it is cleared by the threat engine and form a key building block of a zero-trust enterprise.

Given that users are often the weakest link in enterprise security, relying on credentialed access alone is no longer sufficient, since credentials are easy to compromise. We will see a surge in adaptive risk-based authentication and authorization solutions being deployed in the enterprise. These have matured significantly in recent years and are more than ready for prime time. These solutions are key to creating a zero-trust enterprise, where every action attempted by the user is assessed for risk based on a range of factors including role, device, location, time-of-day, and application. Depending on the risk, additional multi-factor challenges may be issued to the user before allowing the action.

Data security and privacy

With GDPR already in place and newer consumer privacy protection laws on the horizon (e.g. CCPA and others across the globe), organizations need to find out what data they are storing, along with how and why it is essential for their business. If a business or regulatory justification is not found, it is prudent to discard all personally identifiable information of users that is stored. User consent also will play an essential role in usage of personal data in business analysis and transactions. New laws mandate consent, along with ability to show and purge data if requested by the data subject (or the owner). There is no comprehensive



solution yet that can discover, classify, tag and enable management of personally identifiable information by internal administrators, data subject and auditors. However, a good understanding of current organization processes and inventory of personal data is essential to start complying with these regulations.

Automation

Efficiency and operational excellence are key drivers for automation when it comes to security operations. Automation is being widely adopted in security and compliance for last-mile provisioning, access requests and help-desk automation. In 2019 we expect to see pervasive automation during the modernization of security processes and infrastructure. Automation is the first step; beyond it, building intelligence is essential to implement preventive controls. The areas where artificial intelligence and machine learning will play a key role in 2019 are log analysis, access certification, user behavior analysis for risk scores, and continuous authentication.

Self-Sovereign Decentralized Identity

User owned and managed (a.k.a. self-sovereign) decentralized identities anchored on a blockchain, provide the features required for a collaborative ecosystem or consortium of organizations, where no single member “owns” the user’s identity and each member wants to collaborate and share the user’s digital identity, with user consent. Self-sovereign identities will become more prevalent in use cases where an identity needs to be presented by users to a variety of service providers, where selective sharing, and data privacy is of the essence. Such domains include insurance, healthcare, hospitality, and education.

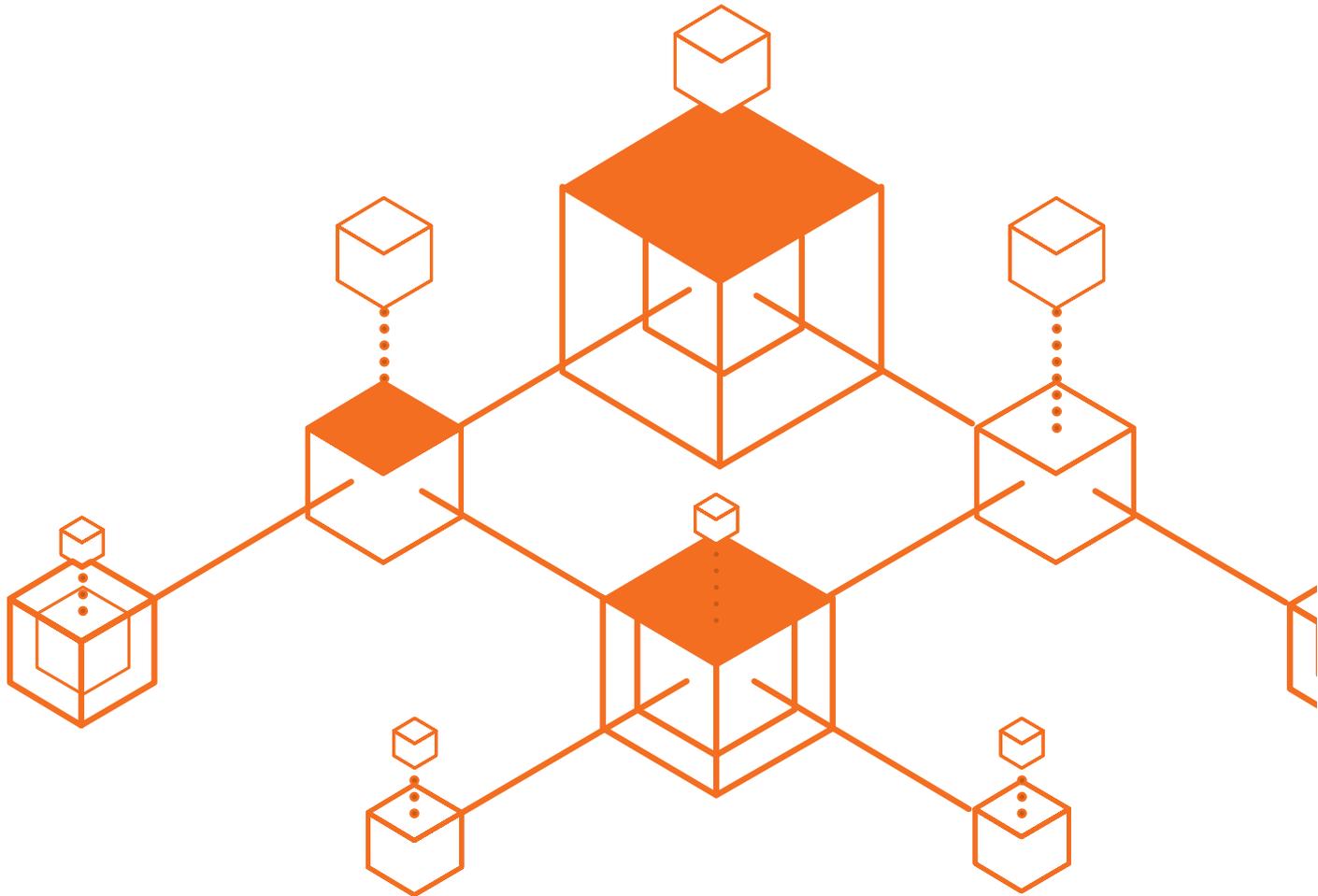
Shift to Managed Services

We see more and more organizations (especially mid-size) moving to a managed services security model as security monitoring and response are becoming critical to business operations. This becomes more of a reality as cloud infrastructure, automation and intelligence start enabling better, faster and cost-effective services.



Recommendations

- 1. Begin the process of creating a zero-trust enterprise by designating critical data, building virtual perimeters inside the network and adopting dynamic, risk-based access control.**
- 2. Establish an omni-channel security posture by leveraging machine intelligence driven security monitoring tools and an automated framework for rapid and precise response.**
- 3. Create a cohesive data security and privacy plan to remain compliant with the increasing number of data privacy regulations globally.**



From Disillusionment to Enlightenment

The dust has settled on the blockchain hype. All the crypto tokens and coins have seen dramatic loss in value, and only the ones with fundamentally sound technology, decentralized value proposition and transparent, decentralized governance will rise from this in 2019. On the enterprise blockchain front, only those enterprises that can effectively combine the technology with consortium governance will succeed in creating business value.

Enterprise Blockchain applications: rubber meets the road

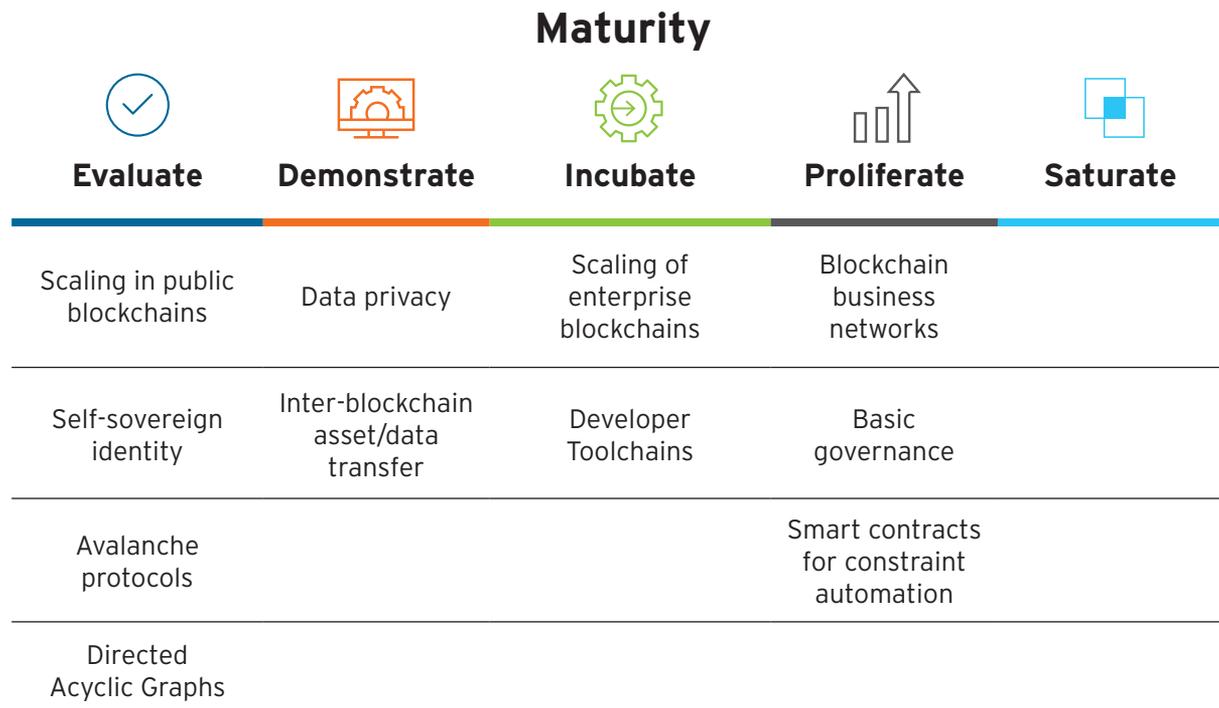
With the availability of robust production grade platform releases last year, a lot of enterprises have built products and services with the leading blockchain or distributed ledger platforms, such as Corda, Hyperledger Fabric and Quorum. Multiple high-profile enterprise blockchain pilots were rolled out in 2018 and live production-level transactions were demonstrated. As more of these pilots go into production, the community is gaining insights into what works with enterprise blockchains and what doesn't, especially in the areas of governance structures, identity, security, enterprise integration, performance and efficiency. The performance of blockchain platforms will play a key role in their success. We expect 2019 to be the year where governance structures standardize, multiple inter-ledger protocols for asset and data movements across different blockchain platforms become available, enterprise-grade tools for operational automation and deployment (on-premise and multi-cloud) emerge, nodes scale horizontally

and tools for advanced performance tuning become available.

Blockchain-enabled self-sovereign Identity as a viable and powerful identity alternative

We see blockchain as being one of the key enablers for self-sovereign identity. Self-sovereign identity is a decentralized identity that is created and managed by the user, enabled by blockchain as the underlying decentralized infrastructure. Self-sovereign identity applications allow users to securely store their identity information with them and only share it when necessary with concerned parties with user-consent. Users can obtain digital attestations from issuers and present these attestations to verifiers to simplify their onboarding for different service offerings.

In 2018, we saw many self-sovereign identity solutions using blockchain in development or early trials. In 2019, we expect to see this technology mature to a level where it will be considered a viable alternative to today's siloed and federated identity solutions both in the enterprise and public blockchain spaces.



Public blockchains will emerge stronger from the ashes

2018 saw a comprehensive and brutal rout among public blockchains in the cryptocurrency and ICO space. This was a much-needed bursting of the irrational bubble that had built around public blockchains, tokens and cryptocurrencies. Most projects were either vaporware, ill-conceived or outright scams. Those hopefully will no longer be around. We expect to see several technically sound projects emerge from this meltdown and do well in 2019. Bitcoin has launched the lightning network as a low-fee, high-speed settlement layer (layer-2) atop bitcoin's slower, more secure (layer-1) network. This is seeing rapid growth in the network and increasing user adoption. Questions around its viability remain, given the capital requirements for channel creators, but despite those, layer-2 solutions will gain ground in 2019. Ethereum similarly will see successful layer-2 scaling with "Plasma" sidechains and will see more efficiency in the layer-1 network with the launch of Casper,

which shifts the consensus layer from proof-of-work to proof-of-stake. This change will allow Ethereum to increase its transaction throughput significantly. While platforms like Bitcoin and Ethereum continue to innovate in areas like transaction scaling and sharding, we are very excited about a newer platform Blockstack that just had its first major release. Blockstack is a global blockchain platform for decentralized apps (dApps) which integrates identity, storage, authentication, encryption and decryption mechanisms that allow apps to be built in such a way that users control their identity as well as their app data. Blockstack is light-weight and offloads most of the data and computation off-chain. It is built based on a virtual chain concept, which allows it flexibility to use any blockchain as a building block and allow for migration to a different blockchain if there are issues with the underlying blockchain. These features and the grounds-up, user-centric, decentralized design make it a compelling project to track and innovate with this year.



Recommendations

- 1. Have a boardroom conversation about blockchain first before having a technology conversation. Blockchain value creation requires a business strategy shift and alliance formation even before the technology adoption.**
- 2. Plan who will be the key stakeholders participating in your business blockchain network as users, network participants, operator(s), and governing authority. The value proposition and incentives for each of them will be different.**
- 3. Investigate if your business model or domain can be disrupted by a decentralized peer-to-peer workflow without requiring a trusted third party. If yes, you need to pre-empt that disruption by re-thinking your business model.**