September 13, 2017

REPORT: TRENDS

Constellation AstroChart™ for Digital Safety & Privacy

The Digital Safety & Privacy Business and Technology Trends Enterprises Must Track from 2017 to 2020

Steve Wilson

Vice President and Principal Analyst

Content Editors: Courtney Sato

Copy Editor: Maria Shao

Layout Editor: Aubrey Coggins

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Constellation AstroChart[tm] supplies a visual guide of the trends affecting Digital Safety & Privacy. After assessing boardroom priorities, organizations should employ AstroCharts to inform portfolio management.

This report contains two AstroChart: one identifying technology trends and one identifying business trends. The AstroCharts' vertical axes plot "organizational adoption" rates from mainstream to early adopter to bleeding edge. Horizontal axes plot "business impact", the impact of the trend on an organization's business model, from incremental to transformational to exponential. The Constellation AstroChart moves beyond both the hype and constraints of the standard 2 x 2 grid to identify the dynamics affecting the entire market.

This report applies Constellation's AstroChart to Constellation's business theme of Digital Safety & Privacy. Digital Safety & Privacy refers to the art and science of protecting information assets, including people, while promoting innovation. Constellation's Digital Safety & Privacy practice helps innovative organizations realize the full potential of the cloud, mobility, Big Data and the Internet of Things without compromising the safety of the business nor the privacy of users.

Business Themes

Digital Safety and Privacy

CONSTELLATION'S ASTROCHART OVERVIEW

Constellation's AstroChart has two axes: organizational adoption and business impact. The intent of the Constellation AstroChart is to move beyond both the hype and constraints of the standard 2 x 2 grid to identify trends affecting the entire market.

Its vertical axis of "organizational adoption" rates an organization's use of a new technology or practice based on three adoption styles:

- **Mainstream.** An organizational style that prefers generally accepted technologies.
- **Early Adopters.** An organizational style that begins using new and emerging technologies upon general availability.
- **Bleeding Edge.** An organizational style that proactively uses new and emerging technologies prior to general availability.

Its horizontal axis of "business impact" estimates the impact of the new technology or practice on an organization's business model, using three likely effects on business:

- **Incremental.** An effect that results in marginal improvement in the business.
- **Transformational.** An effect that results in a noteworthy improvement and innovation in the business.
- **Exponential.** An effect that results in extraordinary improvements and innovation in the business.

These two axes are applied to the technology trends and business trends in Digital Safety & Privacy.

Technology Trends

Constellation's AstroChart of technology trends estimates the adoption rate and business model impact of emerging technologies. Refer to this AstroChart to develop your overall technology investment strategy and as a benchmark of your organization's adoption rate.

Business Trends

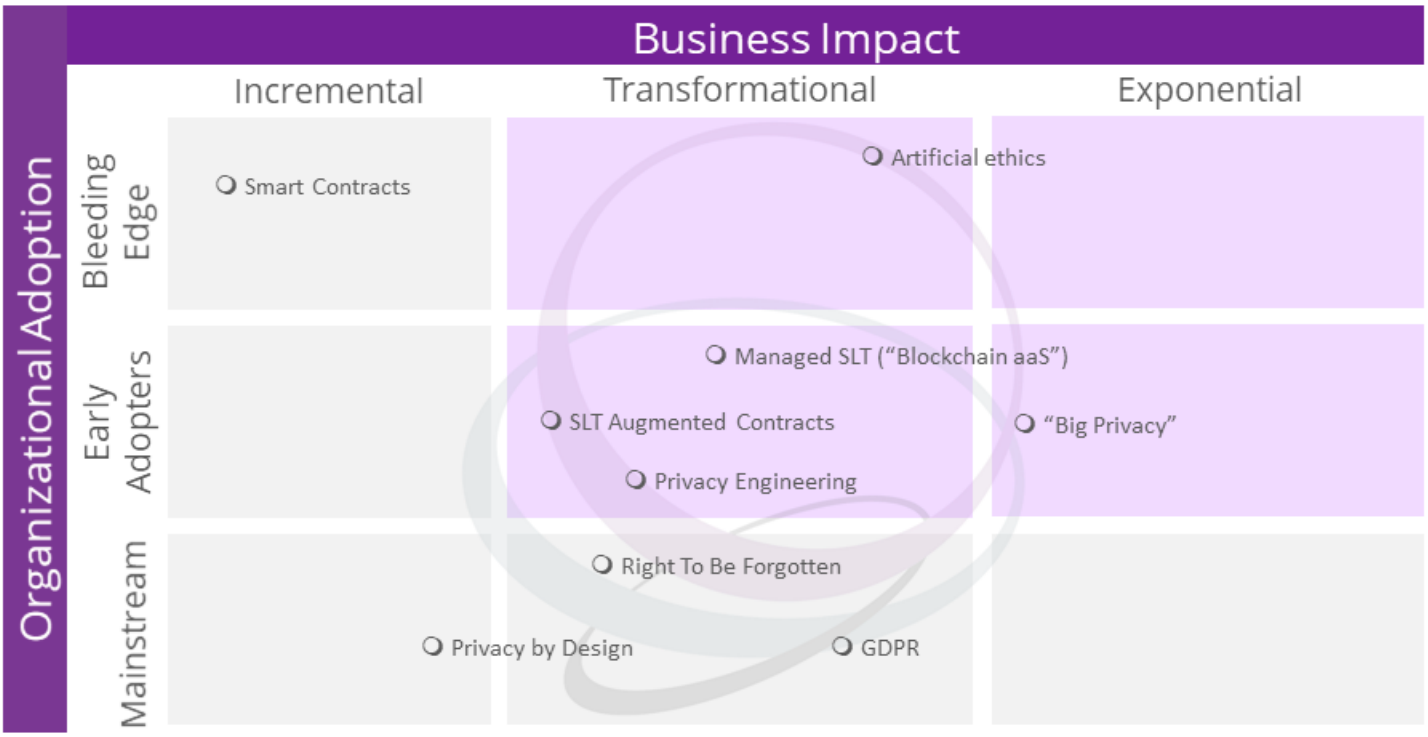
Constellation's AstroChart of business trends estimates the impact of trends on business models. These trends are identified via Constellation's Futurist Framework and PESTEL (Political, Economic, Societal, Technological, Environmental, Legislative) model as well as via inquiries to Constellation and primary research. Refer to Constellation's AstroChart of business trends to plan your corporate strategy, develop your overall boardroom strategy and identify your organization's business trend adoption style.

ABOUT DIGITAL SAFETY & PRIVACY

Digital Safety & Privacy refer to the art and science of protecting information assets, including people, while promoting innovation.

The digital world brings opportunities and risks that are without precedent. New business models that value information as a commodity can clash with traditional security and privacy practices. Constellation's Digital Safety & Privacy practice helps innovative organizations realize the full potential of the cloud, mobility, Big Data and the Internet of Things without compromising the safety of the business or the privacy of users.

CONSTELLATION'S ASTROCHART OF BUSINESS TRENDS



Description of Trends

Exponential-Early Adopter

- **Big Privacy**[1] is a new commitment to privacy brought about by the challenges of Big Data. Big Data's tremendous potential for transforming raw data into insights poses unintended threats to user privacy (not to mention over-reach). Big Privacy calls for restraint in using powerful analytic tools, transparency about data-driven business models, fair and negotiable offers for consumers' data in return for digital services as well as innovation in broad data safety alongside data mining. Read more about Big Privacy in the Constellation report, "Big Privacy Rises to the Challenges of Big Data."

Transformational-Bleeding Edge

- **Artificial Ethics** involves developing culturally appropriate decision-making faculties for artificial intelligence. For example, algorithms for machine vision should not exhibit overt prejudices; robots and autonomous vehicles should put people first and avoid conflicts that would pit the interests of one person against another. Constellation sees artificial ethics as crucial for the socialization of robots. While some academics are already debating "robots' rights", Constellation finds that artificial ethics has yet to be framed convincingly as a research field, and as such, will remain on the bleeding edge for some years to come.[2]

Transformational-Early Adopter

- **Managed Synchronous Ledger Technologies** (SLT or "Blockchain as a Service" according to some vendors) supply ledger technologies like the Blockchain in a managed service model. Managed SLT vendors provide a range of choices for customers, including consensus algorithm, access controls, participants and so on. Managed SLT providers also offer professional services to help early adopters understand and make best use of this still confusing technology. SLTs promise to radically improve data management in time-sensitive, multi-party transactions like trade documentation, trade finance and supply chain tracking. Early adopters are researching the application of SLT to achieve better data quality, better visibility of records, reduced fraud and faster dispute resolution. Be aware that pricing and support have some way to go before this offering can enter the mainstream.

- **Privacy Engineering** is an evolving family of tools that help design privacy into IT initiatives by recognizing the various tensions between privacy and other system objectives (such as utility, security, usability and cost) and helping optimize information management accordingly. A number of useful guides have been developed by the National Institute of Standards and Technology (NIST), Constellation and other independent privacy consultants.[3] Constellation sees privacy engineering

superseding the earlier "privacy by design" movement (see below) by delivering more sophisticated technical privacy controls and methods.

- **Synchronous (or Distributed) Ledger Technology Augmented Contracts** result from the practical evolution of the more hypothetical "smart contracts" first envisaged for the Ethereum blockchain (described below). Smart contracts are thought by some to be capable of supplanting legal processes, but these idealistic proposals overlook that the process of forming a contract has to occur outside the blockchain and within conventional legal boundaries (see below). More legally sophisticated approaches to augmented contracts can leverage the interoperability of synchronous ledgers to deliver practical benefits such as making legal agreements machine readable, more standardized, and thus, faster and cheaper to strike up. Many legal researchers prefer the term "technology-augmented agreements" over "smart contracts".

Transformational-Mainstream

- **General Data Protection Regulation (GDPR)** is a sweeping reform and strengthening of privacy rules that safeguard data about European citizens in their home countries and around the world. The regulation affects all data and IT services operating in Europe and anywhere else if they are handling European Union (EU) citizens' personal information. The GDPR takes effect in 2018 and involves very substantial fines for serious non-compliance. Its far-reaching consequences make the GDPR a mainstream issue. The GDPR can be approached as an opportunity, a model for future data protection practices befitting Big Privacy (see above) and a way of future-proofing a business in the event that the U.S. enacts similar regulations.

- **Right To Be Forgotten (RTBF)** comes from a ruling of the European Court of Justice that requires search engine operators in the EU, on the request of a European individual, to delist the results of

name-based searches that are irrelevant, outdated and/or inaccurate. RTBF is frequently conflated with other privacy considerations, but the ruling is confined to web search. Constellation rates RTBF as transformational because it heralded regulatory intervention into the notoriously secretive workings of search algorithms. Activist data protection authorities may well go further in the name of transparency, and so web search operators should internalize the RTBF as a precedent.

Incremental-Bleeding Edge

- **Smart Contracts** were first proposed by blockchain technicians as programs executed "on" a blockchain or otherwise triggered by ledger transactions to automatically give effect to contract terms. For example, a Smart Contract can automatically initiate actions set out in the contract, such as workflows and/or payments, usually using the blockchain's native cryptocurrency. (Smart Contract principles are also being used in newer "augmented" contracts to automate and systematize the construction of contracts and their terms and conditions; see above). It is debatable if these mechanisms are sufficiently different from traditional embedded software to warrant the name "Smart Contract". Further, advocates have been prone to exaggerate the legal effect of Smart Contracts, sometimes claiming that all aspects of a binding agreement can be contained within a program, with a vague promise dubbed "Code Is Law" to make lawyers somehow obsolete (as if all the grounds for disputing a contract are ever documented in the contract). Therefore, the practical importance of Smart Contracts in regular business is rather limited, and Constellation expects the term may fall out of use, replaced by the more grounded "augmented" contract.

Incremental-Mainstream

- **Privacy by Design (PbD)** is a movement started in the 1990's by Ontario privacy commissioner Ann Cavoukian with the aim of embedding privacy "into the design specifications of technologies, business practices, and physical infrastructures". PbD is basically the same good idea as building

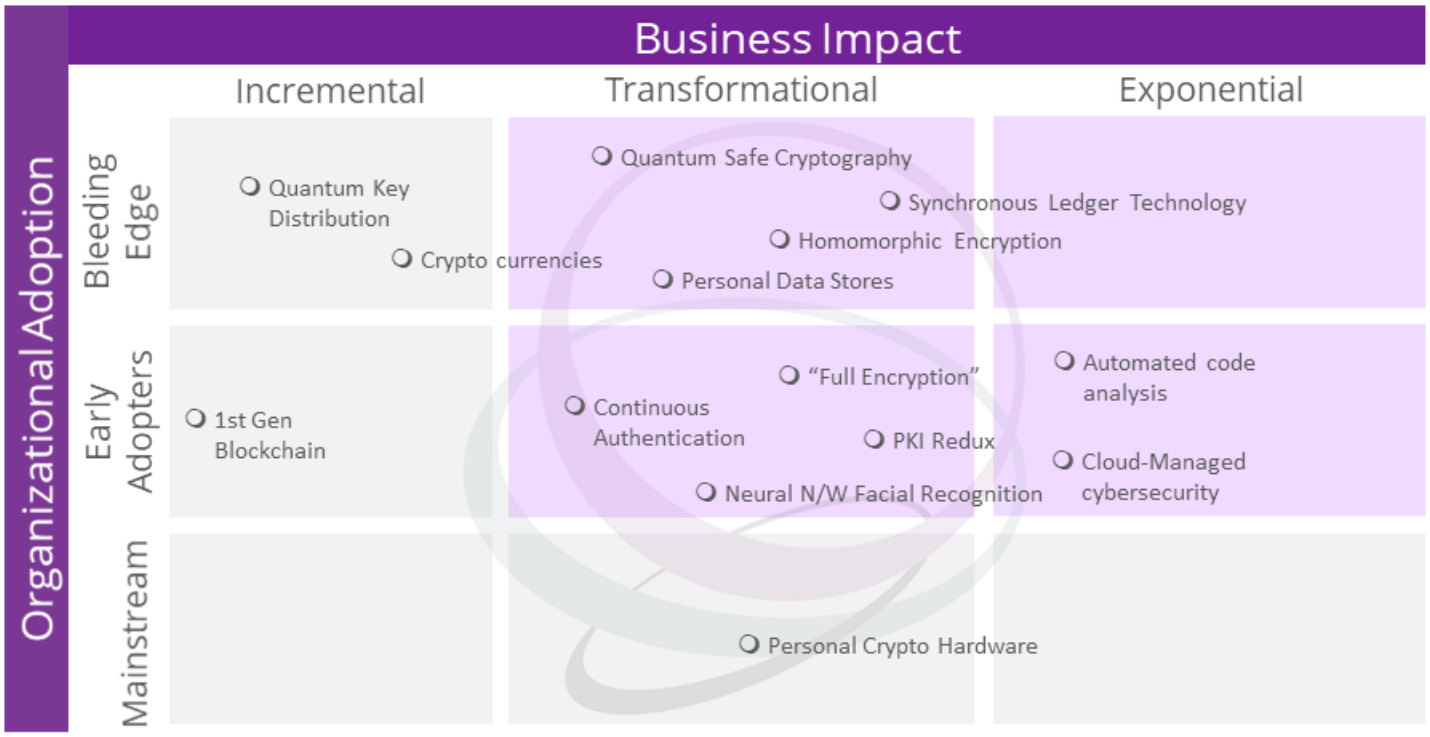
in security or building in quality so as to avoid the higher costs and possible damages that result when proper risk management is delayed. Privacy by Design has been widely promulgated and even mandated by various privacy offices, but PbD falls well short of the methodological formality required for effectiveness and has not had much measurable effect. Constellation finds that PbD does not add value over and above regular data protection principles, whereas the more technical privacy engineering tools (see above) are more engaging for engineers and IT professionals.

Analysis & Recommendations

Constellation observes the following:

1. **Assess boardroom priorities.** Take stock of strategic priorities and use the AstroChart to guide portfolio management.
2. **Experiment with caution.** Logarithmic, bleeding-edge projects require very informed or founder-led boards.
3. **Invest appropriately.** Identify the organization's adoption type and invest accordingly. Market leaders invest 50 percent of their portfolios on disruptive projects and 30 percent of their portfolios on bleeding edge projects. Fast followers invest 80 percent of their portfolios on early adopter projects.

CONSTELLATION'S ASTROCHART OF TECHNOLOGY TRENDS



Description of Trends

Exponential-Early Adopter

- **Cloud-Managed Cybersecurity** means hiring an outside firm for cyber-security. The "managed security services provider" (MSSP) idea predates the cloud itself and is finally arriving. Since 2000 or earlier, there has been an argument that cybersecurity is too specialized to be managed in-house and that it would be better to outsource. Many enterprises find it hard to stay up to date with security developments, retain quality security professionals and keep them busy and motivated. And yet, despite the compelling logic of outsourcing security operations, legal unknowns hampered MSSP uptake. With little demand, managed services tended to be generic, which only made them less attractive. So there was a vicious cycle that kept MSSPs unpopular. But now, the industry is seeing micro-customizable security policy and mature cybersecurity supply chains that deliver practical and

specific security functions at attractive price points. Options include cloud encryption, cloud identity management, tokenization and even blockchain-as-a-service. Managed cybersecurity could improve corporate dependability and resilience to the same degree as cloud computing has improved cost and elasticity of enterprise IT.

- **Automated Code Analysis** helps screen code for bugs. As the "world is being eaten by software", the quality of software is becoming one of the most critical success factors in security. Increasingly, large pieces of infrastructure are suffering catastrophic outages due to software errors. New software and existing legacy code need to be screened for bugs and automatic code analysis tools will make a huge difference to reliability in the medium term.

Transformational-Bleeding Edge

- **Personal Data Stores (PDS)** are a tool for strengthening and restoring individuals' control over their personal information. PDSes can be cloud-based or can be implemented in local devices, typically smartphones. PDSes can be distinct personal data wallets or they can be embedded in other applications such as digital drivers' licenses. When combined with cryptographic keys and verified identity attributes, PDSes promise to transform privacy and security by cutting identity theft and enabling more reliable, streamlined personal commerce, especially in higher-value financial services, healthcare, travel, voting and so on.

- **Homomorphic Encryption** (where cyphertext has the same format and properties as the original plaintext yet cannot be understood) promises to allow encrypted data to still be processed by its owner while being held by a third party such as a cloud provider. While privacy and security are strong drivers for encryption in outsourced data management settings, they come at a great cost to the utility of the data. That's because encrypted data becomes difficult or impossible to search, index, sort

and otherwise manipulate. Prototypical homomorphic encryption methods like Format Preserving Encryption (FPE) have been effective for specially formatted data like credit card records, but full-fledged homomorphic encryption remains elusive. It might never prove practicable.

- **Synchronous Ledger Technologies (SLTs)**, a designation created by Constellation in 2017, refers to an ever-growing range of advanced transactional data management techniques derived from the earlier blockchain. Broadly, SLTs are more widely applicable than the original blockchain (which was specific to cryptocurrency) but share certain blockchain characteristics such as redundancy, decentralization and participation by multiple parties in agreeing on the state of a dataset. In appropriate applications, SLTs promise to radically transform the efficiency and certainty of complex multi-party transactions such as trade documentation, trade finance, supply chain tracking and complex inter-bank settlements. While some adopters of this technology will develop and/or implement it for themselves, Managed SLT (or "Blockchain as a Service") is also coming rapidly onto the market, shifting this category from bleeding edge for a technology to early adopter for a business trend (see Business Trends above).

- **Quantum Safe Cryptography** is a new class of encryption algorithms in the early stages of R&D, in response to the threat posed by "quantum computing." Not to be confused with Quantum Key Exchange (also known as quantum cryptography), quantum computing poses a significant threat to many of today's cryptographic systems. Many encryption algorithms are based on the "one-way functions" that are infeasible to calculate using classical arithmetic, but they can be undone, in principle, by new quantum computing algorithms. Such is the long-term threat that the U.S. National Institute of Standards and Technology (NIST) has launched a research project to develop new encryption methods resistant to quantum computing attacks.[4] Constellation recommends calm. There is probably very little prospect of widespread quantum computing in less than 10 years and indications are that increasing encryption key lengths may provide reasonable defense against attacks for some time after that. So conventional encryption will remain reliable for many years yet, and

quantum safe cryptography is not an urgent matter for many industries. Only a few very sensitive applications will need to adopt these methods, as and when they become available, but others should keep watching this technology trend.

Transformational-Early Adopters

- **"Full Encryption"** is one service provider's marketing name for an increasingly prevalent cloud storage posture where data held on behalf of clients is not accessible to anyone other than the client. That is, encryption is managed with keys that are controlled by the client and not the service provider. This level of protection is driven by several considerations, including privacy, resistance to insider attack and (post-Snowden) opposition to government surveillance or law enforcement access. Cloud service providers are increasingly adopting a highly principled stance in which they cannot access client data, even if they wanted to. A classic example of the tensions this creates was seen with the "Apple versus FBI" case where the locked iPhone of a criminal suspect was of intense interest to police but could not be unlocked by the manufacturer.

- **Continuous Authentication** means using a variety of real-time signals about a user's behavior so as to keep the user appropriately logged on to an online service. Security policy often dictates that a password be re-entered after periods of inactivity, when a user changes profiles or when the user tries to access a new service from his or her device. The disruption and friction that go with these changes can be reduced by continuous authentication, using geolocation, biometrics and other device-based intelligence to decide seamlessly the user's bona fides.

- **Neural Network Facial Recognition** uses new neural computer architectures to process and match biometric facial features. It is one of the most active areas of applied research and product development for neural nets, with autonomous vehicles being among the current commercial uses. Neural nets promise more natural, fault-tolerant and self-learning solutions for image processing,

object recognition and classification. However, by their nature, these mechanisms sometimes behave in unpredictable ways and the ways they fail can be surprising.[5] A great deal of work remains to be done.

- **"PKI Redux"** captures a number of reforms to Public Key Infrastructure (PKI), a long-established category of cryptographic identity management. PKI has been a critical security technology for decades but has proven problematic in end user identity management, thanks to multiple factors such as complex policies and complicated stand-alone business models. Simpler and embedded forms of PKI are emerging; protocols from the FIDO Alliance and the blockchain communities, for example, represent the next generation of PKI. Public key certificates may become essential for conveying specific attributes of users (instead of general purpose identities) and properties of devices in the Internet of Things, possibly powering a fresh demand for managed PKI services.

Transformational-Mainstream

- **Personal Crypto Hardware** is when hardware-based cryptographic processing capabilities, also known as Secure Elements, are embedded in personal devices such as mobile phones, smartcards, SIMs, USB keys or wearables. The FIDO Alliance, a global consortium dedicated to interoperability among strong encryption devices, was motivated largely by the emergence of powerful cryptographic capabilities in mobile phones and portable chipped devices. Embedded cryptography in chip cards has been core to the global success of the cell phone system and Chip-and-PIN payments. With smartphones, applications can access the encryption and digital signature functionality of the hardware for security, privacy and sophisticated work flow authorizations. Personal crypto hardware will quickly expand beyond cell phones into smart devices, medical equipment, automobiles and so on.

Incremental-Bleeding Edge

- **Quantum Key Distribution (QKD)** is a method for encryption keys to be shared between parties over public channels in a way that is, in theory, completely impervious to eavesdropping. Key distribution – getting the keys needed to decrypt a sender's encoded communications into the hands of the receiver – is the essential precursor for encryption and for decades has been achieved using "public key algorithms". But public key algorithms tend to be slow and awkward and add an extra layer of complexity, which in turn, creates vulnerabilities. QKD involves direct transmission of keys by polarized laser beams (in free space or perhaps through fiber) which, when set up carefully, betray any attempt to intercept them. The types of applications that need this level of protection are rare and tend to be confined to national security (although some financial services players evidently enjoy the cachet of purportedly "perfect security"). QKD is not for everyone, and despite the strength of the theory, it still requires very careful engineering to maintain the extreme security promise. Constellation advises that security managers inform themselves sufficiently to judge the importance of quantum key distribution in their organizations' environments.

- **Cryptocurrencies** refer to the broad category of math-based payments protocols where there is no physical or government-backed "fiat" money. Cryptocurrencies boomed after the advent of Bitcoin. Dozens of competing digital denominations have emerged in the past five years, and with the current craze for Initial Coin Offerings (ICOs), new derivative currencies are appearing ever faster. Most are used merely as tokens for value in fund raising exercises, while a few are in circulation for payments. The vision of Bitcoin's founders was for cryptocurrency to displace regular government-backed money, but this seems unlikely. Constellation sees cryptocurrency having only incremental impact on the whole money system for the foreseeable future. If hybrid government-backed digital money emerges, Constellation will reevaluate the placement of this trend.

Incremental-Early Adopter

- **First-Generation Blockchain** is a category of ledger technology originally designed to prevent Double Spend in the first cryptocurrencies, including Bitcoin and Ethereum. First-generation blockchains have been applied for numerous non-currency use cases with limited success. These structures incentivize their participants with native cryptocurrency and their sustainability for other applications is yet to be proven. Further, Constellation's detailed technical analysis casts doubt on the efficiency and benefits of going to the trouble of merging conventional information management with the special-purpose public blockchain algorithms.[6] These platforms will continue to host all manner of experimentation and serve as a proving ground with incremental benefits for early adopters, while managed Synchronous Ledger Technologies (SLTs) become mainstream.

Analysis & Recommendations

Constellation recommends:

1. **Mainstream Technologies.** Organizations must make adoption and implementation of these technologies an enterprise-wide standard. Invest in market-leading suites. Organizations should invest in best-of-breed players or do custom building only for logarithmic categories.
2. **Early Adopter Technologies.** An implementation decision should be tied back to a business model. Expect five to 10 vendors in each category.
3. **Bleeding Edge Technologies.** An implementation decision should be tied to proof-of-concept projects. Expect offerings to come from early-stage startups willing to co-innovate and co-create.

FREQUENCY OF EVALUATION

Trends in a Constellation's AstroChart will be updated every updated every year as needed.

EVALUATION SERVICES

Constellation clients can work with the analyst and research team to conduct a more thorough discussion of the AstroChart. Constellation provides guidance about mainstream, early adopter and bleeding edge technology providers associated with the coverage area of the AstroChart.

ENDNOTES

[1] *"'Big Privacy' Rises to the Challenges of Big Data", Steve Wilson, Constellation Research, April 11, 2014, https://www.constellationr.com/research/big-privacy-rises-challenges-big-data.*

[2] *"The limits of algorithms and the implications for AI safety", Steve Wilson, AI in Asia - Ethics, Safety and Societal Impact, 16 December 2016, Seoul, Korea.*

[3] *"Getting Started Guide: Privacy Engineering", Steve Wilson, Constellation Research, April 27, 2015, https://www.constellationr.com/research/getting-started-guide-privacy-engineering.*

[4] *Post-Quantum Crypto Project, National Institute of Standards and Technology, http://csrc.nist.gov/groups/ST/post-quantum-crypto.*

[5] *"Researchers figure out how to trick facial recognition systems", Chris Kanaracus, ZD Net, December 2, 2016, http://www.zdnet.com/article/researchers-figure-out-how-to-trick-facial-recognition-systems.*

[6] *"Blockchain has no meaning - and that's its magic trick", Steve Wilson, Constellation Research, July 20, 2016, https://www.constellationr.com/blog-news/blockchain-has-no-meaning-and-thats-its-magic-trick.*

Steve Wilson

Vice President and Principal Analyst

Steve Wilson is Vice President and Principal Analyst at Constellation Research, and leads the firm's work in Digital Safety and Privacy. A 20-year veteran in cyber security, Wilson is one of the world's most original thinkers in digital identity.

Wilson is a researcher, innovator and R&D leader with 30 years of experience in information technology. Since 1995, he has been dedicated to digital identity and privacy, responsible for numerous breakthroughs in smart technologies, identity management, privacy enhancing technologies and national identity frameworks. Wilson has been awarded nine cyber security patents, and is currently undertaking a Ph.D on the evolution of identity ecosystems.

Wilson advises Chief Information Security Officers, Chief Privacy Officers, strategists and ICT architects seeking to optimize data protection in complex digital systems. He provides Privacy Impact Assessments, builds robust security strategies, and helps architect identity for Big Data, Internet of Things and cloud rollouts. His coverage areas include: Digital Safety and Privacy, Data to Decisions and Consumerization of IT.

@Steve_Lockstep | www.constellationr.com/users/steve-wilson | au.linkedin.com/in/lockstep

ABOUT CONSTELLATION RESEARCH

Constellation Research is an award-winning, Silicon Valley-based research and advisory firm that helps organizations navigate the challenges of digital disruption through business models transformation and the judicious application of disruptive technologies. Unlike the legacy analyst firms, Constellation Research is disrupting how research is accessed, what topics are covered and how clients can partner with a research firm to achieve success. Over 350 clients have joined from an ecosystem of buyers, partners, solution providers, C-suite, boards of directors and vendor clients. Our mission is to identify, validate and share insights with our clients.

Organizational Highlights

- Named Institute of Industry Analyst Relations (IIAR) New Analyst Firm of the Year in 2011 and #1 Independent Analyst Firm for 2014 and 2015.
- Experienced research team with an average of 25 years of practitioner, management and industry experience.
- Organizers of the Constellation Connected Enterprise – an innovation summit and best practices knowledge-sharing retreat for business leaders.
- Founders of Constellation Executive Network, a membership organization for digital leaders seeking to learn from market leaders and fast followers.

www.ConstellationR.com

@ConstellationR

info@ConstellationR.com

sales@ConstellationR.com

San Francisco | Belfast | Boston | Colorado Springs | Cupertino | Denver | London | New York | Northern Virginia
Palo Alto | Pune | Sacramento | Santa Monica | Sydney | Toronto | Washington, D.C

constellation RESEARCH