Hype Cycle for Blockchain Technologies, 2020

Published: 13 July 2020 **ID:** G00441585

Analyst(s): Avivah Litan, Adrian Leow

Innovative solutions supported by blockchain are mainly in an experimentation phase or limited-scale production. Still, early adopters and application leaders are using blockchain to uniquely transform their digital businesses, especially with supply-chain-related and payments-related use cases.

Table of Contents

List of Tables

List of Figures

Strategic Planning Assumption

By 2024, the number of industry-specific standards enabling blockchain interoperability, and smart contract portability and interfaces with external data sources will increase from zero, but remain below 10.

Analysis

What You Need to Know

This document was revised on 17 July 2020. For more information, see the Corrections page on gartner.com.

Blockchain technology has evolved slowly, with most enterprise projects stuck in experimentation mode, lacking clear goals and measurements. Organizations are reluctant to turn over authority to multiparty consortia. Most permissioned blockchains are barely distributed, operating on just a few nodes managed by a single vendor or sponsor.

Unlike public blockchains, permissioned blockchains do not eliminate centralized authority. Nonetheless, they do uniquely support a single version of immutable records shared and trusted by network participants — a feature required to underpin digital transformation.

Over 50 central banks are researching or testing digital currencies on permissioned blockchains. China already launched its digital currency and is piloting consumer payments. At the outset of the COVID-19 pandemic, the need for transparent, trusted, end-to-end supply chain data pointed many to blockchains. Necessary standards for tokenized processes (for example, from InterWork Alliance) and supply chain information (GS1, EPCIS) are further evolving.

These events will drive blockchain's advancement up the Slope of Enlightenment.

The Hype Cycle

Blockchain as a market is sliding further into the Trough of Disillusionment on this Hype Cycle. Blockchain-enabling technologies used by organizations to carry out enterprise blockchain projects are still relatively nascent. There is diverse industry consensus on product concept, feature set, core application requirements and target market. For the next two to four years, Gartner expects the current multiblockchain platform and largely noninteroperable world to continue.

However, at the same time, we are seeing several developments that promise optimized convergence of private and public blockchains. In this scenario, private transactions are validated by public chain consensus. This provides the promised trust that blockchain supports, while preserving business confidentiality. This convergence will have a significant impact on blockchain platform design going forward — promoting interoperability, multibusiness process automation, privacy and trust.

Gartner believes we will see the market climb out of this Trough of Disillusionment over the next two to three years as pragmatic use cases are deployed and the technology evolves. Gartner expects that de facto standards (especially for data formats) will become more apparent, enabling better interoperability with less complex and costly integration. Moreover, we expect that leading software vendors will increasingly integrate blockchain technologies as a feature in their enterprise software.

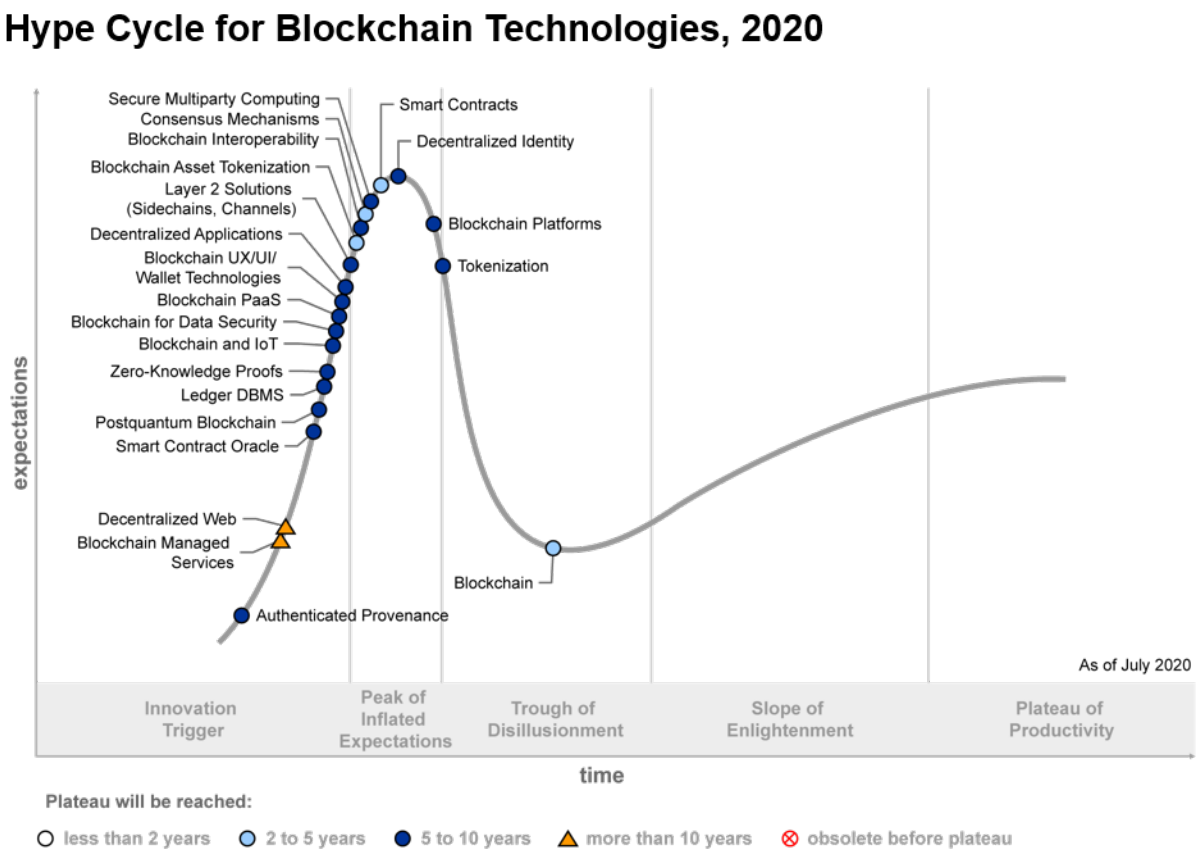
To provide application leaders with a snapshot of the rapidly evolving blockchain tools and innovations, this Hype Cycle reflects multiple IT perspectives on blockchain-enabling technologies

and their development. Its aim is to provide a view of technologies that will contribute to blockchain as a foundational technology, and to help clients to realize its potential in delivering significant added value and impact for business.

We have added new entries to this year's Hype Cycle to reflect the evolution of blockchain in the enterprise. These entries highlight the areas in which assets written and tracked on the blockchain are authenticated or tokenized. The new entries to this year's Hype Cycle are:

- Authenticated provenance
- Tokenization

Figure 1. Hype Cycle for Blockchain Technologies, 2020



Source: Gartner
ID: 441585

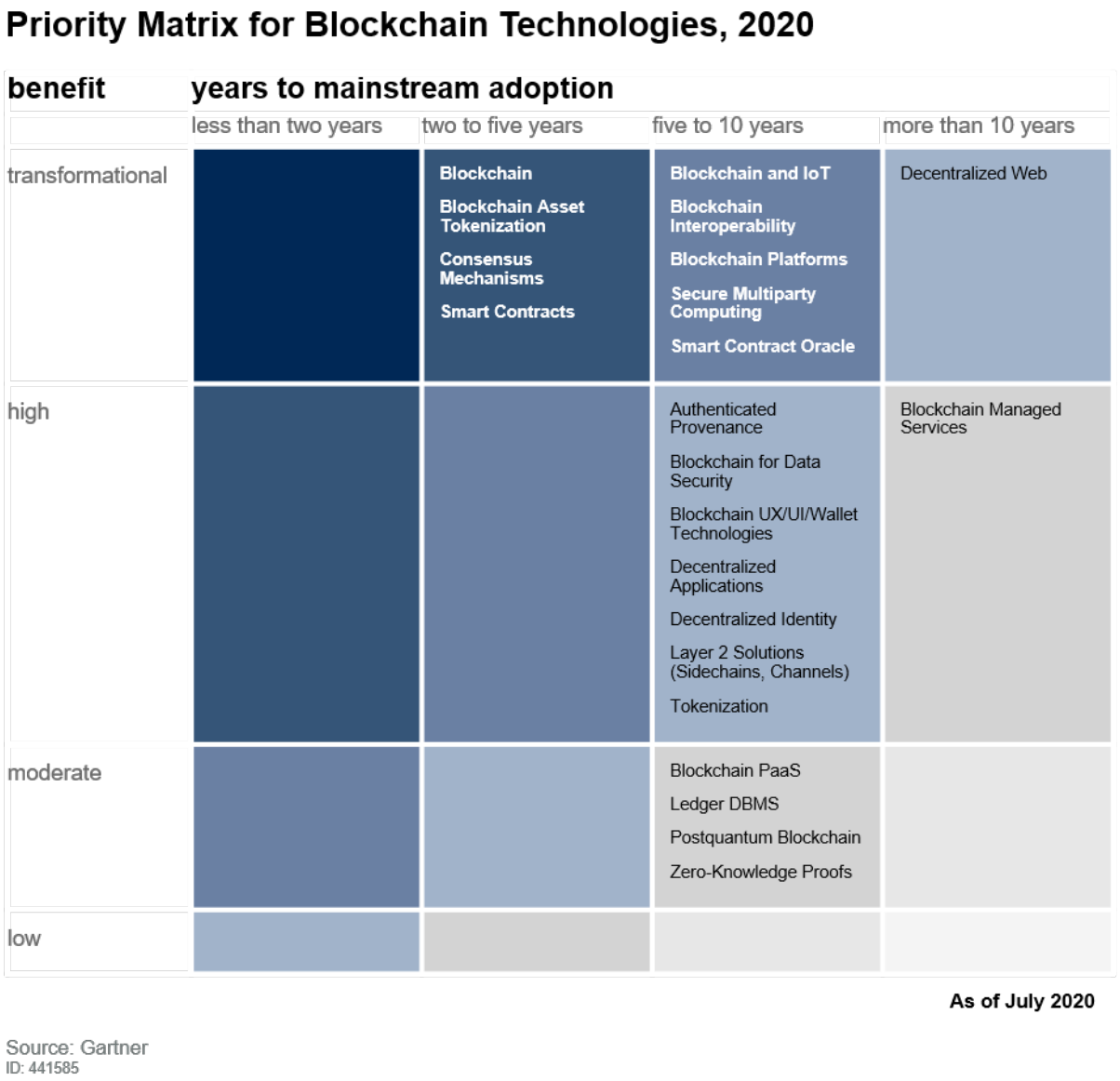
The Priority Matrix

Application leaders should prepare for some of the advanced capabilities that blockchains will enable during the next five years. In some cases, impacts will be significant enough that organizations cannot wait for the associated technologies to enter the "less than two years to mainstream adoption" category before addressing them. For instance, this may be the case with

decentralized applications, blockchain and IoT, decentralized identity, smart contract oracle, smart contracts and blockchain interoperability. Collectively, these technologies will support fully scalable blockchain projects and automation of multiparty business processes across multiple ecosystems.

A majority of the technologies profiled that have a rating of high or transformational will not become mainstream for another five to 10 years. The fact that organizations are so infrequently using blockchain features — such as decentralized consensus, tokenization and smart contracts — calls into question whether blockchain is even needed by these organizations. Yet, these more advanced blockchain features can underpin truly disruptive ways of doing business across parties that "don't trust each other," even if these features do introduce more implementation complexity. Once private transactions can integrate with public blockchain services such as decentralized consensus, these features will move into mainstream adoption.

Figure 2. Priority Matrix for Blockchain Technologies, 2020



Source: Gartner
ID: 441585

Off the Hype Cycle

This year, no technologies have reached the Plateau of Productivity or achieved mainstream adoption.

Due to the continuing evolution of technologies in this market, we have merged or renamed the following technologies to accurately reflect the content:

- "Cryptocurrency software wallets" has merged with "blockchain UX/UI technologies" and has been renamed "blockchain UX/UI/wallet technologies."

- “Distributed ledgers” has merged with “blockchain” under the “blockchain” title.
- “Blockchain (metacoin) platforms” has been renamed “blockchain platforms.”
- “Privacy-enhanced multiparty computing” has been renamed “secure multiparty computing.”

Because this Hype Cycle pulls from such a broad spectrum of topics, many technologies are not tracked over a longer period of time, but may feature in the Hype Cycle for a specific year because of their relative visibility. This is not intended to imply that they are unimportant — quite the opposite. In many cases, these technologies are no longer “emerging.” They are becoming increasingly integral to business and IT. In other cases, technologies were removed from the Hype Cycle in order to highlight other newly emerging technologies. Technology planners can refer to Gartner’s broader collection of Hype Cycles for items of ongoing interest. To ensure that this Hype Cycle is focused on blockchain-enabling technologies that will provide transformational benefit for enterprise users, some technologies have been removed. Technologies that appeared in the “Hype Cycle for Blockchain Technologies, 2019,” but do not appear in this year’s report are:

- Cryptocurrency hardware wallets
- Cryptocurrency mining
- Distributed storage in blockchain

Links to additional research can be found at the end of this Hype Cycle lists. The research listed may be useful to those interested in blockchain technologies.

On the Rise

Authenticated Provenance

Analysis By: Avivah Litan; Svetlana Sicular

Definition: Authenticated provenance represents the authentication of assets that can be recorded and tracked on the blockchain. The provenance of these assets can later be digitally verified by blockchain network participants. There are many methods used to authenticate the provenance of assets, depending on their nature and whether they are digital or physical goods.

Position and Adoption Speed Justification: Counterfeit physical goods and fake digital content have become major national and health security threats at worse, and costly problems for organizations at best. Blockchain provenance and asset tracking applications are being adopted to address these issues, but these applications don’t address the problem of authenticating goods and content initially recorded on the blockchain. The question remains “How do you know what you are tracking on the blockchain is real to begin with”? The problem is made worse because on the blockchain, garbage in means garbage forever, since it can never be modified or deleted due to the immutable ledger.

Users considering blockchain provenance applications are aware of this limitation. Significantly, some regulators Gartner has spoken with have also noted the problem, which they say must be

addressed before blockchain can be used to authenticate provenance of goods, such as food or pharmaceuticals.

Gartner believes provenance authentication solutions will be in more demand in the coming years, as users adopt blockchain for provenance applications. They will become increasingly aware of the need to digitally "certify" the first mile, or onboarding of the goods or content being tracked on the blockchain in the first place. For now, that certification relies on manual audits or human trust. That is certainly not scalable. For example, human fact checkers cannot keep up with detecting fake content, despite the growth in independent English language fact checks by more than 900% from January to March 2020. See Reuters market study "Types, Sources, and Claims of COVID-19 Misinformation."

User Advice: CIOs, Enterprise Architects, Technology Innovation leaders and Application Leaders responsible for applications and systems that generate and receive goods and content within their organization should:

- Adopt technologies that can digitally authenticate and verify provenance to prevent fake or altered goods and content from being distributed and consumed.
- Work with your data scientists and IT teams to establish and track provenance of goods and content your organization produces and consumes, using supporting technologies like Blockchain, AI and factory component quality assurance testing.
- Work with peers and industry groups to form networks of active participants who can collectively and more effectively combat fake goods and content. Start by fixing the problem in your own organization.

Business Impact: The good news is that there are some emerging solutions on the market, for example that rely on spectral imaging, AI models, and factory quality assurance testing to authenticate the provenance of a goods or particles the technology can decipher and understand. These types of technologies have been applied to authenticating diamonds, wheat supplies, chemotherapy drugs and electronic components, and are getting promising results.

Intelligent automation that digitally authenticates and verifies content provenance is clearly and urgently needed. The more organizations that participate, the more effective the solutions. This is because content rarely stays within the confines of the environment in which it is produced, so solving this thorny fake goods and content problem very much depends on the growth of the network, including the authenticators and the verifiers that adopt the solutions.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Sample Vendors: IBM; ThinkIQ

Recommended Reading: "Leverage Blockchain Developments as Catalysts for Strategic Technology Planning Across the Supply Chain"

Blockchain Managed Services

Analysis By: Avivah Litan; David Groombridge

Definition: Blockchain managed services are a combination of professional and automated services that manage the entire stack of blockchain infrastructure and applications on behalf of end-user customers. They differ from blockchain platforms as a service in that they manage not only blockchain infrastructure and decentralized application tools and assets but also a particular industry solution, such as for a specific banking, healthcare or supply chain use case.

Position and Adoption Speed Justification: Across the world, public and private organizations interested in deploying blockchains are struggling to find technical expertise and resources skilled in this emerging and fast-changing technology. Many are turning to cloud service providers that support blockchain for help in developing, deploying and operating implementations. Others are relying on specialized blockchain consulting firms or other third-party software or services vendors with blockchain expertise to lead them through the blockchain project life cycle. Increasingly, they are asking these companies to run the entire application for them.

Some providers hesitate to get this involved in the application layer because it seems to run counter to the blockchain principles of decentralized autonomous organizations, whereby trust is not placed in any single central provider. However, providers can certainly provide a managed services stack for just one organization in their ecosystem, rather than for their entire ecosystem, and in this way further contribute to the distribution of blockchain operations.

For many clients, the benefits of using blockchain managed services will outweigh the costs, if customers retain logical control of their blockchain applications. Still this market is moving slowly as most enterprises still rely on customized professional and system integration services, rather than seek a provider who can manage the full stack of technology on their behalf.

User Advice: End-user organizations struggling to find skilled resources to help them develop and operate blockchain applications should consider using blockchain managed services. But to realize the full value of decentralized applications, end users who outsource the management of their blockchain applications must still retain oversight of these applications.

If you use blockchain managed services, we therefore recommend that you:

- Establish SLAs and clear terms of engagement with your managed service provider. These should set out and demarcate their responsibilities and yours.
- Require your managed service provider to maintain blockchain system interfaces with legacy systems and other blockchain environments.
- Set up controls to monitor your service provider's operation to ensure it has no write access to your blockchain application and that its privileges are confined to the services that you have agreed it should perform.
- Understand the logic and business rules of the smart contracts and set up a monitoring system to ensure they are producing the expected outcomes and are processing the right inputs.

- Require your managed service provider to monitor and audit any changes to smart contracts.
- Use identity access management and security analytics services (preferably from an independent provider or source) to monitor and analyze access to your organization's blockchain transactions in order to ensure only "authorized" and "legitimate" data is being appended and written.
- Ensure your service provider remains neutral to specific blockchain platforms and can keep your environment competitive and agile, so that it keeps pace with changes in blockchain platform technologies as they progress and mature.

Business Impact: Blockchain managed services should spur and support blockchain adoption by organizations that lack the requisite technical expertise or other resources to support their own applications. Gartner estimates that these services could grow over the next 10 years to support at least half of enterprise blockchain participants. We also think they will be especially popular with all blockchain newcomers, and with midsize and small enterprises that are part of blockchain consortium ecosystems.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Sample Vendors: Chainstack; IBM; Mangrovia Blockchain Solutions; NTT DATA; Rockside

Recommended Reading:

"How to Manage and Optimize Costs of Public Cloud IaaS and PaaS"

"Solution Comparison for Blockchain Cloud Services From Leading Public Cloud Providers"

"Blockchain Unraveled: Determining Its Suitability for Your Organization"

Decentralized Web

Analysis By: Avivah Litan; Adrian Leow

Definition: Decentralized web (or Web 3.0) is a new stack of technologies for the development of decentralized web applications that enables users to control their own identity and data. These technologies include blockchain as a trust verification mechanism, privacy-preserving and interoperability protocols, decentralized infrastructure and application platforms, decentralized identity and support for applications like decentralized finance. These will eventually realize the vision of a decentralized web.

Position and Adoption Speed Justification: Traditional web-enabled social media and electronic commerce have revolutionized social interactions, bringing suppliers and consumers of information, goods and services together in a peer-to-peer setup on a global scale. However, with Web 2.0, all these interactions and transactions require a digital platform (like those of eBay, Amazon, Alibaba

Group, Facebook, Google and Uber) acting as trusted provider or broker between entities who do not know or trust each other. These platforms have created a valuable peer-to-peer economy, but they also define the relationship rules and host all of the participants' data. Decentralized web promises to enable true peer-to-peer interaction and transactions with no reliance on centralized platforms and intermediaries.

Although it is likely that the future of internet technologies will be more decentralized, this is unlikely to eliminate centralized authorities and systems from most enterprise B2B and B2C use cases. This is because they will play a key role in the governance and oversight of digital ecosystems.

The Web 3.0 stack that will move Web 2.0 services into the Web 3.0 protocol has yet to be standardized. Other than platform-oriented specifications, all protocol standard initiatives are either at early stages of inception or under development. Examples of initiatives include the "Web3 Foundation," and ISO/TC 307 for blockchain and distributed ledger technologies. It is important to note that, although dapp architectures are more fault-tolerant and attack-resistant, they are currently slower than traditional systems.

One of the first technologies to come out of the Web3 Foundation is Polkadot, which had an alpha technology release, the Kusama network, in the Summer of 2019. The decentralized Polkadot network is still not launched. Gartner had not seen much end-user movement to Web 3.0 protocols during 2019 and early 2020, but developers for various technology components such as oracles, and decentralized file- and web-hosting protocol InterPlanetary File System (IPFS) continue to release new upgrades of their software.

User Advice: Enterprise architecture and technology innovation leaders adopting blockchain technologies should monitor developments in Web 3.0 protocols and standards by monitoring the initiatives of the Ethereum Foundation, Hyperledger, Trust over IP Foundation, Web3 Foundation and ISO/TC 307 for blockchain and distributed ledger technologies. Organizations that want to promote Web 3.0 concepts in their applications can further evaluate and pilot blockchain platforms that implement a Web 3.0 vision by giving end users control of their own identity data. These platforms include decentralized identity, verifiable claims, blockchain-based applications, and emerging blockchain-based decentralized finance platforms. Other blockchain applications in other domains will also emerge before Web 3.0 protocols and standards mature, and users may find it useful to work with these new applications as they come to market.

Business Impact: Web 3.0 will implement the protocols that support the most revolutionary aspect of blockchain technology, which is that it embraces a peer-to-peer decentralized design that eliminates central authority. To support this vision, users must be able to control their own identities and data. This, in fact, was the promise of the web before the large internet gatekeepers assumed their central and powerful positions over the past couple of decades. Blockchain-based technology and Web 3.0 have the potential to take the web to where it was originally "supposed" to be — to a point where consumers and end users have control of their own identity and data. Service providers will have to adapt their business models to work within the new paradigm. Those that figure out the new formulas for adopting Web 3.0 technology soonest will emerge as the success stories of the next decade.

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Algorand; Brave; Cosmos Network; Enigma; Ethereum 2.0 (Serenity); MetaMask; Opera; Polkadot; Sovrin Foundation

Recommended Reading:

"Guidance for Assessing Blockchain Platforms"

"Planning for Blockchain Solution Adoption"

Smart Contract Oracle

Analysis By: Martin Reynolds; Avivah Litan

Definition: Smart contract oracles are software mechanisms that trigger smart contracts based on events external to the blockchain (or DLT) that they support. Oracles enable smart contracts to automate transactions based on real-world data and events. Some examples are fetching commodity prices, getting notified of or adopting changing interest rates, and accepting traditional payments.

Position and Adoption Speed Justification: The demand for oracles is predicated on the growth of smart contract technologies for business applications that need to integrate with the world outside of a blockchain network. See the "smart contract" entry for more information on smart contracts. Distributed ledgers and smart contracts do not come with a mechanism to fetch data from the external world: all proposed transactions must be written to the blockchain transaction queue. For example, a trusted authority can use an API to write events to the blockchain that trigger a smart contract. The scope of external interactions and data needs for smart contracts is exhaustive, which will lead to a fragmented and disparate set of smart contract services.

In these cases, a smart contract oracle mechanism is critical to reliable and scalable development of the blockchain system. However, oracles also have their set of security weakness, as tampering with an oracle can suppress or miscue a smart contract. Emerging oracle technology offers independent oracle systems that are scalable, redundant, and robust against tampering or corruption. These integrity features again come from distributed consensus mechanisms, so that a corrupted or failing oracle is overridden by its oracle network partners. These decentralized consensus oracle systems can also validate events against other data sources, thereby improving blockchain system security.

Simple oracles are well developed, but face the issues listed above. Startups are now delivering the first distributed consensus systems, but it will take some years before these systems are robust enough for general use. However, they are ready for prototype systems today.

User Advice:

- List all your integration and data needs from nonblockchain systems as you evaluate smart contract use cases.
- Understand what oracle mechanisms are available and the viability of being able to provision such services through oracles for effective smart contract execution based on SLA requirements.
- Favor oracle systems over APIs, which are not as robust or secure.
- Ensure that the smart contract solution or platform you propose using has robust oracle capabilities to satisfy your integration, data and security needs.
- Understand your current data providers' plans to provide such oracle services in preparation for any smart contract initiatives in the future. Businesses need to understand the complexities of being able to get such data from unreliable or uninterested sources as they plan smart contract initiatives. They must evaluate business risks with "what if" scenarios around subverted, corrupted, unreliable or imperfect oracles.

Business Impact: The availability of reliable and effective oracles will play a crucial role in the development of smart contracts in most use cases. Distributed oracles with additional data validation checks improve reliability and security for sensitive or irreversible transactions. While a portion of these services could use the data feeds available today, a significant portion might be used in greenfield areas. For instance, a trade finance contract between banks, exporters and importers, which performs certain payment actions after a proof of delivery is confirmed, needs technology that can work reliably across multiple parties. Such complexity can vary across different use cases and across industries, and the oracles' algorithms can vary in turn.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Chainlink; Provable Technologies; Realitio; Town Crier

Recommended Reading:

"Managing the Risks of Enterprise Blockchain Smart Contracts"

"Predicts 2020: Blockchain Technology"

"Guidance for Blockchain Solution Adoption"

"Market Guide for Blockchain Platforms"

Postquantum Blockchain

Analysis By: Martin Reynolds; David Furlonger; Rajesh Kandaswamy

Definition: Postquantum blockchain is a form of blockchain technology using quantum-resistant cryptographic algorithms that can resist attack by future quantum computers. Quantum computing is a new model of computing that can solve previously intractable computational problems, including those used to protect data in blockchain platforms and in other financial systems.

Position and Adoption Speed Justification: Quantum computers are many years away from practical applications, but quantum computing technologies are attracting significant investment. Multiple universities and consortia are performing fundamental research that will lead to deployment of quantum technologies. Gartner believes that practical quantum computer applications will emerge in five to 10 years. However, cracking current encryption technology is 20 to 30 years away.

When quantum decryption systems become available for real-world use by enterprises, governments and well-funded criminal organizations, then the security of financial systems based on certain cryptographic mechanisms is at risk. Quantum resistance varies. SHA-256 and RIPEMD-160 cryptographic hashing, used to sign blocks of transactions, are weakened in the face of quantum computing attacks but remain computationally intractable for the foreseeable future. Account keys secured with RSA public-key cryptography (used by Bitcoin) and elliptic curve cryptography (used by Ethereum) are vulnerable to quantum attack. A successful attacker could transfer the value in the account to their custody.

These issues are well-understood in the financial, security and blockchain communities. Blockchain systems will likely move in parallel with the financial community, deploying quantum-resistant and quantum-safe algorithms as they become standardized.

These changes will be delayed by the natural resistance of the blockchain communities to change, but should be well in hand in five to 10 years.

User Advice: Although postquantum cryptography is not an essential requirement for the current generation of metacoin platforms and blockchain technologies, enterprises should ask for a cryptographic roadmap from potential vendors. This roadmap is required because credible platforms should have a plan to implement this over the next three to five years, prior to general deployment of quantum computers.

Furthermore, if an enterprise holds tokens in a public blockchain account, these tokens should be moved to accounts using updated algorithms within a year or two of deployment. The risk is in the far future, and relatively low, but keeping systems up to date is good practice.

Enterprises must also ensure that any private or personal data is stored under a symmetric key algorithm, and control the key such that deletion of the key is equivalent to deletion of the data. This approach requires careful design of off-chain systems that enable partners to enjoy the benefits of blockchain, but also deliver compliance with future laws relating to protection of personal data. In other words, assume that every record on a blockchain will at some point become readable, so sensitive data in the record must be encrypted under a controlled key.

Therefore, off-chain key storage and management for sensitive data is a critical decision point in building a blockchain architecture; such data must be protected with quantum-safe encryption.

Business Impact: Quantum computing, in general, could have a huge effect over time — in computationally intensive areas such as molecular modeling, optimization, code breaking, drug discovery and other previously intractable problems. Quantum computing will also drive mandatory upgrades in sensitive enterprises such as financial, healthcare and government systems. These upgrades will drive general awareness of security issues in blockchain systems. Cryptocurrencies that do not have a solid postquantum roadmap run the risk of collapse if confidence in their security is lost.

Businesses that are dependent on the integrity of cryptocurrency will fail without remediation, if they are not quantum-ready when quantum computing is here, although we believe that the matter is well in hand. On the other hand, businesses storing personal data on a blockchain will face stiff fines if the data is ever released. In the case of personal data, the data can be very long-lived (70 or more years), so a long-term plan is critical.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Embryonic

Sample Vendors: 01 Communique; Bitcoin; D-Wave; Ethereum; Google; IBM; Intel; Microsoft; Rigetti Computing

Recommended Reading:

“Emerging Technology Analysis: Act Now on Quantum-Safe Encryption or Risk Losing Deals”

“Better Safe Than Sorry: Preparing for Crypto-Agility”

Ledger DBMS

Analysis By: Donald Feinberg; Nick Heudecker

Definition: A ledger DBMS is an append-only, immutable DBMS with an embedded cryptographically verifiable audit trail. A ledger DBMS is useful for private and permissioned “blockchainlike” applications where distributed consensus is not required and one entity has control over the ledger and designates which parties, other than the owner, have access to and may add to it.

Position and Adoption Speed Justification: Ledger DBMSs provide many of the benefits of a blockchain platform, like data tampering detection and auditing without the complexity of configuring and managing decentralized environment. They are managed by a single entity, which makes their implementation and management far easier and more secure. Despite their utility, adoption of ledger DBMSs is evolving slowly as the benefits and potential use cases are being understood by the broader market. This technology has yet to reach the Peak of Inflated Expectations. It will take demonstrable market successes and additional product introductions to drive hype.

Most ledger DBMSs are new and relatively immature. The Amazon Quantum Ledger Database (QLDB) is an exception, because the service has been used internally by Amazon for many years (see "Amazon QLDB Challenges Permissioned Blockchains"). During the next few years, we believe there will be a number of new ledger DBMS products (especially for dbPaaS), which will increase the choices available. Thus far, Oracle has announced support for a feature it calls "blockchain tables" in version 20c of its eponymous DBMS.

User Advice: Review your organization's tactical and strategic requirements and be cognizant of the benefits and challenges of centralized, decentralized and distributed systems, so that you select the most business-appropriate platforms. Compare the suitability of ledger DBMSs against permissioned blockchain technologies by carefully considering your need for:

- A centrally administered data-auditing capability versus a decentralized network of peers.
- A single organization as the "source of truth" versus multiple potential validators.

Keeping business processes, and their associated data, private to a single organization versus the value of sharing business processes executed through smart contracts.

Business Impact: Today, many blockchain projects are forced to use public blockchain technologies when a DBMS would suffice. Ledger DBMSs represent a choice that is more manageable and easier to implement. This will enable businesses to use ledger technology where immutability is required in use cases such as audit trails, data lineage, digital assets and sharing data. The same goes for IoT and other use cases requiring smart contracts for digital signing of software updates. Ledger DBMSs will also have better performance, as there is no need for massive public participation in the consensus process.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Amazon Web Services; Fauna; Fluree; Oracle

Recommended Reading:

"Amazon QLDB Challenges Permissioned Blockchains"

Zero-Knowledge Proofs

Analysis By: David Mahdi

Definition: Zero-knowledge proofs (ZKP) are privacy-preserving messaging protocols that enable entities to prove that information available to both of them is correct, without the requirement to transmit or share the underlying information. Blockchain platforms have been evolving to include this privacy-oriented mechanism.

Position and Adoption Speed Justification: MIT first developed the concept of ZKP in the 1980s. In particular, the challenge was to overcome the possibility of fraudulent representation of information. Rather than just focusing on an entity (prover) who tries to persuade the receiver (verifier) that the information is accurate (either false or true), the goal is to also address the issue of a verifier learning more about the information than merely if it is accurate or not. This challenge has applicability in a wide range of use cases especially in the context of authentication and transaction verification. Other cases include payments, custody management, AML/KYC, consumer IAM, medical records, mergers and acquisitions, etc.

To operate effectively, ZKP must have completeness (of process), soundness (of information), and zero knowledge (of anything other than the proof). This challenge is highly relevant to blockchains and distributed ledgers as a core tenet of their operation is data sharing. The zero-knowledge approach is used by blockchain platforms and cryptocurrencies in the form of zk-SNARKS, which are better-suited to a blockchain context due to greater efficiency and reduced need for interactivity. Hawk is an application of ZKP to smart contract domain, where the state of the computation is encrypted. An enabling cryptographic construct for ZKP is homomorphic encryption, which allows for computation on encrypted variables without revealing their values. Zcash (and its predecessor, Zerocash) is an early example of applying ZKP as an extension to the Bitcoin Protocol. In July 2016, Ethereum developers (such as Vitalik Buterin, the founder of Ethereum) worked in combination with ZKP experts to add a lightweight implementation of zk-SNARKs to the Ethereum platform, called ZoE. It is likely that future versions of Ethereum will incorporate a more robust ZKP capability. Over time, major platforms that seek to compete with Ethereum and Bitcoin will add ZKP capability as well, and its value as a point of differentiation in a crowded competitive platform landscape will diminish. Overall, ZKPs are privacy-preserving messaging protocols that enable entities to prove that information available to both of them is correct, without the requirement to transmit or share the underlying information. Leveraging ZKPs limits the requirement for mass decryption and encryption of all the data elements, which has benefits for the efficiency of the network as well as the potential adoption of blockchain/distributed ledger technology. Ultimately, by leveraging ZKPs, service providers, and others can reduce their reliance on honeypots of user data, to help mitigate against mass data breaches.

A challenge is that variety of methodologies and the multiplicity of types of ledgers and approaches to data management inhibits adoption. Moreover, ZKP will need to scale at the rate of DL transactional volumes in order to be effective, and this is yet to be proven.

User Advice: We recommend the following:

- Work with security and risk management leaders to gain a deeper understanding of the nature of these controls, understanding that ZKP techniques are a paradigm shift.
- Understand how ZKP can benefit use cases that require privacy protection, but be realistic with the current immaturity of ZKP solutions and approaches.
- Evaluate how such controls may impact transaction authentication and ultimately consumers.
- Assess the impact on the broader information management strategy.

- Assess the architectural implications for using ZKP with different blockchains and distributed ledgers.

Business Impact: Most blockchain platforms today offer a number of core benefits, but namely, those of integrity and availability. And while this may benefit a number of approaches to ensure transaction and data security, confidentiality was not covered by the core of blockchain platforms. With the addition of ZKPs to blockchain platforms, security and risk management leaders now have the potential to cover information security use cases that require confidentiality, integrity and availability (CIA). Extending CIA, this also provides privacy focused security leaders with alternatives regarding privacy protection, and sensitive data minimization. Ultimately, business impact can be significant in terms of institutions and individuals being able to better protect and prove the context and details of information while simultaneously being able to maintain confidentiality. This would also limit the requirement for mass decryption and encryption of all the data elements, which has benefits for the efficiency of the network as well as the potential adoption of blockchain/distributed ledger technology.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Ethereum; Evernym; IBM; Zcash

Recommended Reading:

"Market Guide for Blockchain Platforms"

"A Technical Primer for Assessing a Blockchain Platform"

"Innovation Insight for Blockchain Security"

"Cool Vendors in Blockchain Technology"

"Predicts 2019: The Ambiguous Future of Privacy"

"Cool Vendors in Privacy Management"

Blockchain and IoT

Analysis By: Nick Jones; Benoit Lheureux; Avivah Litan

Definition: Blockchain and Internet of Things (IoT) refers to the use of blockchain in conjunction with IoT devices and technologies. Blockchain and IoT can be combined in many ways for purposes such as IoT payment, tokenization of IoT-related assets or services, identity validation, provenance tracking, utilization recording or billing, and secure firmware updates.

Position and Adoption Speed Justification: The combination of blockchain and IoT:

- Enables an immutable audit trail of key IoT data and related business events that is shared across multiple participants and can be independently verified by each party.
- Supports management of IoT objects by providing more-secure ways to identify them and perform tasks such as firmware updates.
- Can use IoT technology to provide secure hardware tokens to identify objects to blockchains.
- Will support smart contracts and distributed applications (aka dapps) that will enable sophisticated business models involving machines and people, or other machines.

The combination of IoT and blockchain is immature and faces many technical and business challenges. Many IoT devices are simple and lack adequate computational or networking resources to act as full nodes in a blockchain, so you must rely on proxies or gateways. The relative volatility of blockchain implementations involving protocol changes may be a challenge for long-lived IoT devices. Some blockchain implementations struggle to scale to the transaction rates that can be generated by large numbers of connected "things." In the long term, we expect the combination of IoT and blockchain to enable innovative devices and business models; however, the necessary evolution in blockchain and IoT will take five to 10 years to achieve maturity.

User Advice: CIOs, enterprise architects and technology innovation roles should look for situations in which IoT and blockchain enable new business capabilities and solve real-world problems, and where technology's immaturity and rate of change aren't impediments. Several large IoT platform vendors have demonstrated integration between their technology and blockchains, providing a simple path for pilot projects. There is also a good selection of smaller vendors and startups that support integration of IoT and blockchain. Private blockchains with known ecosystem members are likely to pose fewer technical and governance challenges. Beware of applications involving long-lived IoT devices and long-lived data, which will require the ability to periodically deploy blockchain technology updates in scale.

In situations where all that's required is immutable data storage without shared ecosystem ownership, business rules, or tokenization, consider immutable centralized databases or ledgers such as Datomic or Amazon QLDB as alternatives to blockchain.

Business Impact: Business opportunities often involve situations where the IoT devices participate in ecosystems where untrusted partners must store and share immutable information, or where tokenization enables a new business opportunity. Examples include:

- Smart packaging to track supply chain provenance of high value, sensitive or regulated products, such as food, pharmaceuticals, human tissue/biological materials, medical shipments
- Business models in which trustworthy tracking of equipment utilization or status is critical, or required by regulations (e.g., truck leasing or insurance)
- Business models that combine IoT and tokenization (e.g., smart trash cans providing credits for recycling)
- Cases in which blockchain can contribute to increased trust or security for IoT (e.g., trusted machine identity, trusted firmware updates)

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Chronicled; IBM; IOTA Foundation (Tangle); modum

Recommended Reading:

"Top 10 Strategic Technology Trends for 2020: Practical Blockchain"

"Integrating Blockchain With IoT Strengthens Trust in Multiparty Processes"

"Survey Analysis: IoT Adopters Embrace Blockchain"

Blockchain for Data Security

Analysis By: David Mahdi

Definition: Blockchain-enabled data security applications leverage blockchain's decentralization capabilities to offer alternative methods to establish data protection, with minimal reliance on centralized arbiters. Blockchain-enabled data security methods can enhance use cases involving chain of custody ensuring data integrity, as well as encryption, (e.g., offering a decentralized key repository for decentralized PKI).

Position and Adoption Speed Justification: At the core of blockchain is the ability to ensure that participants with no other trust relationship have access to identical ledgers. This property provides two key data security attributes to the ledger data: integrity and availability. An additional property, confidentiality (i.e., data encryption), is typically done as an additional step to ensure data protection. Data protection methods can be completed on-chain or using integrated off-chain methods, but leverage blockchain technology to ensure all aspects of confidentiality, integrity and availability. However, there are vendors such as ALTR that provide aspects relating to integrity, availability and confidentiality by leveraging blockchain technology.

Overall, leveraging blockchain core decentralization capabilities, combined with complementary data security approaches, offers IT leaders new methods to ensure integrity, availability and, in some cases, transparency.

User Advice: To illustrate a blockchain-based approach to data security, consider ensuring data integrity for a dataset. By storing a representation of the dataset (i.e., a hash) in the blockchain, all nodes will now be aware of the status. Any attempt to change the data will require consensus among the nodes. Therefore, any data logged in the blockchain becomes a part of the immutable decentralized ledger. Common data security approaches that may benefit from a blockchain-based approach, such as PKI, key management and tokenization, can all gain resilience, reliability, transparency and trust due to blockchain's ability to decentralize these functions.

Data security leaders should familiarize themselves with blockchain through early stage research. One such approach is by following publicly known proofs of concept. In doing so, leaders can gain insight into new ideas and approaches that may be relevant. A number of new and well-established vendors are experimenting with data security applications in areas such as:

- Ensuring the integrity of data and/or devices (including things in the IoT)
- Data transparency (e.g., smart contracts or land registries)
- Mitigating trust issues (e.g., distributed/decentralized authority)

Data security leaders should work with developers/architects to establish at least a high-level position on blockchain's relevance and a vision for future adoption. Blockchain-based data security initiatives differ dramatically from legacy business technology and processes. Therefore, data security leaders should take a bimodal approach and experiment with blockchain-based initiatives as Mode 2 projects.

Business Impact: Blockchain has the potential to increase resilience, reliability, transparency and trust in a variety of common data security functions that hinge on centralization such as PKI, key management and tokenization. Blockchain applied to data security applications offers alternative methods that allow businesses to gain further trust in their data by ensuring integrity and availability. This can be enhanced further by layering in data protection techniques such as data encryption that could be done off-chain.

An example is in securing and sharing public records such as a land registry digital document. The traditional approach is to host the document in a central database maintained by a select number of administrators. This model potentially suffers from weaknesses with resilience and transparency. What is to stop a malicious actor from modifying the land registry? In contrast, if the document or a pointer to the document was stored in a blockchain, then availability, transparency and integrity are maintained via the distributed cryptographic nature of blockchain. Any change or attempt to change the document is evident and requires consensus among the nodes. Most important, all of these transactions are made public via the nature of blockchain.

This is in direct contrast to traditional approaches that would have the data stored in a central repository that typically doesn't require multiple parties to manipulate the data. As such, Gartner has witnessed increased client interest in leveraging blockchain to establish integrity and overall trust in data.

Finally, due to the absence of meaningful regulation or standards, governance must be exercised to limit risk within organizational tolerance and also must ensure that enterprise risk appetite will allow for experimentation and eventual adoption of the new technology.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: ALTR; Guardtime; IBM; Remme

Recommended Reading:

"Innovation Insight for Blockchain-Enabled Data Security Applications"

"Innovation Insight for Blockchain Security"

"Evaluating the Security Risks to Blockchain Ecosystems"

Blockchain PaaS

Analysis By: Adrian Leow; Rajesh Kandaswamy; Paul Vincent

Definition: Blockchain platform as a service (bPaaS) is a set of blockchain software platform services offered to subscribers in the cloud by a vendor. Services can include some or all of the distributed ledger, node or consensus mechanisms, and other ancillary services to manage a network of distributed ledgers on the vendor's cloud infrastructure. bPaaS is separate to blockchain managed services, which include management of the solution and application stack on top of bPaaS.

Position and Adoption Speed Justification: BPaaS is a cloud service offering from enterprise cloud vendors such as Alibaba, Amazon Web Services (AWS) IBM, Microsoft and Oracle; also small technology startups such as BlockApps, BlockCypher and Wanxiang Blockchain Labs. Solutions in the market today are in the early stages of development and adoption, and are mostly used for performing proofs of concept (POCs). Developers seeking to implement blockchain-based applications require specific services that span compute, application, storage, network and especially integration services, both for initial implementation and ongoing operations. The cloud vendors aim to combine these services to provide enterprises with a one-stop service shop that brings the benefits of cloud elasticity and compute costs to blockchain. Each bPaaS vendor attempts to add unique elements around support for multiple blockchain platforms, security, interoperability, analytics and performance in order to differentiate their offerings in exchange for single-sourcing and centralization of public execution and ledger storage.

These offerings are new, and we expect the field of competitors to grow over time. In many cases, the cloud vendor's bPaaS supports one or a few blockchain platforms. Support for different consensus mechanisms, tools, frameworks and smart contract capabilities remains limited and continues to evolve. Interoperability for distributed ledgers across competing platforms or clouds is extremely limited at this early stage of evolution. But relying on one vendor for all nodes of the distributed ledger negates some of the advantages of using a distributed ledger in the first place. The core value of a distributed ledger, which has fueled the hype and interest among many in the technology industry, is to enable decentralized/distributed open-source applications that avoid reliance on just one organization, server, data center or network. Most versions of bPaaS trade this core value for the convenience of vendor assistance, although this trade-off is expected to be addressed by greater interoperability and standardization in the future.

BPaaS encompasses platform services or cloud-based blockchain developer toolsets. Over time, however, we expect other blockchain-based application and business services to become available

in the cloud as blockchain-based SaaS. Full-stack blockchain managed services are starting to emerge and are being supported by several vendors.

Currently, in most cases the primary value of bPaaS is to "jump-start" the ability of enterprise developers to rapidly set up an initial test system or prototype — as opposed to a truly decentralized production system. Because bPaaS is dependent on a restricted perspective of blockchain, and is also affected by blockchain's immaturity, it remains "on the ramp" toward the Peak of Inflated Expectations.

User Advice: Current bPaaS offerings can primarily help jump-start your POCs, smaller projects, or your experiments with blockchain technologies, as long as you are comfortable with limiting your experience to what bPaaS can provide. As blockchain technologies and bPaaS offerings evolve, we expect a wider range of options to be available, with additional services and increased interoperability. Be aware that cloud providers support a limited set of platforms, yet the overall landscape of choices is large and rapidly evolving. Enterprises that avail themselves of PaaS services might also consider the same vendor's bPaaS services.

Every blockchain platform will undergo major changes during the next two to five years. Some platforms, however, will keep up with evolutionary changes that keep them scalable and competitive. Enterprises should, therefore, avoid commitments to bPaaS for mission-critical initiatives until greater maturity occurs, and until platforms and services are interoperable across heterogeneous environments. Understand all aspects of the blockchain technologies you will need, and ensure they can be supported on the bPaaS offering of interest.

Business Impact: BPaaS will initially be attractive to enterprises for limited-scale experiments and POCs — until they mature, become interoperable and fully support multiple key blockchain platforms. For blockchain projects with a limited number of participants, an agreement on common bPaaS platforms and tools will be easier to attain. The list of vendors providing capabilities in this area continues to expand.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Amazon Web Services (AWS); Ant Financial; IBM; Microsoft; Oracle; Wanxiang Blockchain Labs

Recommended Reading:

"Market Guide for Blockchain Platforms"

"Platform as a Service: Definition, Taxonomy and Vendor Landscape, 2019"

"Amazon QLDB Challenges Permissioned Blockchains"

Blockchain UX/UI/Wallet Technologies

Analysis By: Nadine LeBlanc; Avivah Litan

Definition: Gartner defines user experience (UX) as "the sum of the effects caused by a person using a digital solution." Designing user experience for an emerging and fast-changing blockchain industry is complex. Many technologies such as wallets can be used to act as the user interface (UI), providing interaction between a user and blockchain technologies. Blockchain UX supports decentralized user-owned data that is explicitly and only shared with others upon user consent.

Position and Adoption Speed Justification: Blockchain commercialization for applications and platforms is at an early stage. UX design is not only necessary for blockchain to reach mainstream adoption, but also essential to establish UX design principles, ultimately leading to a leading to a global standard interface for blockchain. Blockchain supports Decentralized Identities (covered also in this Hype Cycle), where users own and manage their own identity data. That transformative management function is typically built into wallets, one key component of the blockchain UX.

A successful UX is when an intuitive, accommodating interface enables end users to achieve their desired outcomes with very little effort.

Blockchain UX/UI technologies include:

- Wallets, either software or hardware based offered by various vendors and most commonly used to manage user cryptocurrency access and decentralized identity data. (for example, Exodus, Trezor, ArcBlock)
- Add-ons to web browsers such as Google Chrome or Apple Safari (for example, MetaMask)
- Add-ons to smartphones, mobile browsers for iOS and/or Android (for example, Coinbase [Cipher Browser], Trust)
- Stand-alone decentralized web browsers (such as Nimiq)
- Stand-alone decentralized and tokenized web browsers (such as Brave and Blockstack)
- Browser/app-based wallet (e.g., Mist, Status, Coinbase [Toshi])

Blockchain UX/UI technologies are gaining traction, and we expect them to pick up significantly in 2021 due to the roll-out of sovereign digital currencies. The initial test launch of China's digital currency in April 2020 was coupled with the release of a digital currency mobile wallet developed by one of the four banks participating, Agricultural Bank of China. The wallet claims several capabilities, such as allowing users to track their transactions and link the wallet to their existing bank accounts. The anticipated gradual rollout of the Calibra wallet from the Facebook-led Libra cryptocurrency project in 2021 will also start to vastly accelerate blockchain UX/UI adoption in the next four to five years. In the near future, it is expected that blockchain UX/UI technologies will engage in a battle similar to the internet browser wars fought by Google Chrome, Mozilla Firefox, Internet Explorer and Safari, which led to today's internet standards. As such, Gartner's view is that it will take between four to five years for blockchain UX/UI technologies to reach the Plateau of Productivity.

User Advice: Application leaders, CIOs and other IT Leaders should be aware that technologies such as blockchain have the potential to revolutionize the world of UX, by moving control of identity and personalization data to the end user. In the meantime, learn, experiment and pilot new blockchain UX/UI technologies for the following use cases:

- User controlled management of decentralized identity data such as user credentials, payroll and benefit payments, health educational and work records.
- User controlled privacy management.
- Cryptocurrency wallet features
- Digital advertising and services
- Serverless publication of webpages
- Browse and run decentralized applications (dapps)
- Visualize and manage crypto tokens
- Perform crypto-payments and transactions
- Communicate via messaging
- Internet browser integrations

Additional advanced functions may include:

- Advanced analytics (such as user-controlled algorithms on local devices)
- dapps development, API toolkits and testing with testnets

In addition, investigate new forms of UX from academia, research and technology organizations. Be prepared to mix traditional forms of UX with other emerging technologies such as conversational platforms and augmented reality (AR).

Business Impact: Per Gartner's 2019 CEO Survey, 64% of CEOs believe that digital giants such as Google and Apple will be in their industry in the next five years. Of these CEOs, about half believe that digital giants will cause significant or existential threats to incumbents (see "2019 CEO Survey: CEOs Are Divided on the Impact of Digital Giants — Now Is the Time for CIOs to Act").

Depending on whether digital giants will be considered an opportunity or a threat, CEOs could mitigate the risks of disruption by raising awareness of blockchain UI/UX/wallet technology as alternatives to web and mobile engagement channels. These technologies play an important part in the effort to give users control over their own data, privacy and data security, support compliance with data privacy laws such as the EU's GDPR, and minimize an organization's data breach exposure. Be aware that the technology has yet to mature and demonstrate adherence to existing security, legal, regulatory and compliance standards.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Blockstack; Brave; Coinbase; MetaMask; Mist; Nimiq; Status; Trust

Recommended Reading:

"Defining a Good User Experience With the Gartner User Experience Model"

"13 Principles for an Effortless User Experience of IT Solutions: Redefining UX in the Era of Digitization"

"Is Conversational AI the Only UX You Will Ever Need?"

Decentralized Applications

Analysis By: Adrian Leow; Rajesh Kandaswamy

Definition: Decentralized applications (dapps) are internet applications which run on a peer-to-peer (P2P) network and blockchain. Compared to traditional internet applications which are based on a centralized server which acts like the controlling authority to the whole application, dapps instead are based on decentralized networks (P2P and blockchain), which means that no particular entity is the base point of the system.

Position and Adoption Speed Justification: Dapps form a basis of disruptive competition for enterprises, and are part of ecosystem reinvention as new software constructions that have emerged from blockchain platform technologies. They provide the ability to build complex, multiparty applications that rely on underlying distributed ledgers. These are early days for blockchain, and even earlier ones for dapps. They are not yet proven to satisfy enterprise needs of reliability, security, performance or scalability. Because a dapp is connected to the blockchain via a smart contract with its back-end code running on the blockchain, the evolution of dapps rely on the growth of blockchain platforms and smart contract technologies. dapps offer potential to bring a layer of computation on blockchain for enterprises, but much more technology maturity will be required for that to occur.

User Advice: Application leaders exploring the use cases and applicability of blockchain dapps should:

- Understand that current-generation dapps capabilities are not yet robust enough to make large commitments. Major commercial applications will be limited until dapps and blockchain technology mature, and existing legal, regulatory and compliance standards are mitigated or resolved.
- Prepare to join a digital ecosystem using blockchain by starting with simple use cases. Expect to incur migration costs every 18 to 24 months until the technology matures.

Business Impact: In the long term, dapps advance the promise of transactions and interactions without a middleman. In the short term, they need to bring blockchain closer to enterprise

applications. The dapp is a front-end to the blockchain function and usually presents a user interface. It is essentially an off-chain application that calls the smart contract function within the blockchain.

The dapps market will enable organizations to collaborate and transact as part of business ecosystems. It will develop and focus on a common set of capabilities across blockchain early adopters — especially for financial services, government, healthcare, education, manufacturing and utilities.

Dapps can help enterprises adopt blockchain, but can also become a force that creates decentralized competitors that threaten their business models. Both require more technology maturity in terms of scalability, interoperability and performance of the blockchain platforms to succeed. Many of the enterprise applications involving multiple parties that are candidates for blockchain will require some amount of back-end computation and front-end access, which lead to a role for dapps.

Dapp technologies need to evolve to support production needs as well as tools and technologies that enable development of dapps. Dapp technologies will grow by startups creating innovative business and technology solutions on top of blockchain technologies. As they grow, they will make available a broader set of tools that enable decentralized applications, providing substitute and competitive services to those offered in traditional industries.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Ethereum Foundation; Golem; Hyperledger; MetaMask; Monax; SecureKey; uPort

Recommended Reading:

“Market Guide for Blockchain Platforms”

“Use Gartner’s Blockchain Conceptual Model to Exploit the Full Range of Possibilities”

“Guidance for Assessing Blockchain Platforms”

At the Peak

Layer 2 Solutions (Sidechains, Channels)

Analysis By: Adrian Leow; Avivah Litan

Definition: Layer 2 solutions enable blockchain scalability and are all based on the premise that not all nodes need to process all transactions. Emerging solutions include “off chain” protocols that generally move transactions off the main chain to a second-layer messaging system unencumbered

by main chain consensus protocols and data structures. They also include sidechains which are blockchains that handle assets off the main chain and can return them to the main blockchain at a future date.

Position and Adoption Speed Justification: Layer 2 solutions are extensions to the blockchain protocols to enable scalability and to support diverse scenarios of value exchange, including microtransactions, by offloading the development, test and implementation cycle away from the main chain. For example, a private Ethereum-based network that had a linkage allowing Ether to be securely moved from the public Ethereum main chain onto it, and back, would be considered a Layer 2 solution of the public network. There is no single mechanism — Layer 2 solutions represent a collection of elements for facilitating the transfer and synchronization of tokens, or other value representations and digital assets, between entities supported or backed by the blockchain network. For example, instead of adding new features directly to the main chain, Layer 2 solutions allow developers to attach new features and validation processes to a separate chain. Since the chains are still attached to the main chain, the features can take advantage of the network effects, and can test and implement those applications without harming the main network should vulnerabilities arise. They can also offload transaction processing requirements from the main chain and thereby achieve scalability and performance gains. This approach, while promising, has yet to be proven about scalability, security and manageability. Implementing the full vision of Layer 2 solutions requires changes to the core protocols that are still in process — such as Segregated Witness (SegWit), new opcodes, multiasset issuance and confidentiality.

Another development in this area are payment channel networks, such as the Lightning Network for Bitcoin, and Raiden Network for Ethereum. These are another form of Layer 2 solutions that are still being developed and struggling to take hold across the networks.

Other concepts involve drive chains, SPV sidechains, and hybrids as well as the establishment of state channels where interactions occur off the main chain to better manage risk. Most notably, this is in the form of payment channels for instant payments sent directly between two counterparts as noted above with Lightning and Raiden.

The goal is to increase speed and scalability and reduce network operating costs.

User Advice: Application Leaders who use public blockchains should consider Layer 2 solutions as a potentially valuable mechanisms for improving blockchain scalability, interoperability and flexibility, but should not tie the success of your business initiatives to this mechanism in the short term. It is, yet, unproven and not widely adopted. Closely monitor the progress and success of current implementations such as Lightning to determine the applicability of Layer 2 solutions and channels to your payment token use case. Users of both public and permissioned blockchains should also monitor the continuing technical maturity of sidechains as a practical way to make your blockchain implementation more scalable.

Business Impact: If Layer 2 solutions such as channels and sidechains are eventually supported by most blockchain core protocols, blockchains could then support diverse scenarios for value exchange and microtransactions, and support promote interoperability. There is then the potential to address many of the original issues around scalability and trustless environments. However, this

kind of layering introduces additional complexity and governance challenges, which will take time to overcome; during which period, alternative techniques may emerge.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Ardor; Blockstream; Bloq; Elements; Lightning Network; MimbleWimble; Raiden Network

Recommended Reading:

"The Future of Blockchain: 8 Scalability Hurdles to Enterprise Adoption"

"Common Mistakes to Avoid in Enterprise Blockchain Projects"

"Guidance for Assessing Blockchain Platforms"

"Market Guide for Blockchain Platforms"

Blockchain Asset Tokenization

Analysis By: Christophe Uzureau; David Furlonger; Ali Merji

Definition: Blockchain asset tokenization is the process of creating or representing value, such as an asset (monetary value or data, or an ID), and/or conveying the right to use such an asset. The rules that define the creation, representation and exchange of the assets are executed via a smart contract. The exchanges can occur via almost any medium, including person-to-person, machine-to-machine, person-to-machine and machine-to-person.

Position and Adoption Speed Justification: This profile takes into account multiple types of tokens enabled by blockchain technology; as a result, their maturity levels differ. Careful consideration should be made of the multiple types of tokens. For example:

- Stablecoins, initially designed to support cryptocurrency trading but can be used to improve settlement in a given ecosystem. There are three different types of stablecoins, those pegged to fiat currency, a publicly traded commodity or another cryptocurrency, or relies on an algorithm attempting to replicate the actions of a central bank's open market operations.
- Utility tokens which are a crowdfunding method to finance the development of a product, service or platform enabled by blockchain technology and provide access to it as an incentive mechanism.
- Security tokens which give their holders a share in the issuing entity, in the same way a stockholder has a share in a publicly traded company.
- Data tokens that represent a data point or the right to access or/and process such data

Protocols to create tokens, such as the Ethereum Request for Comments (ERC) have been available for a few years — for example, the ERC-20 (to support creation of utility tokens). Regulatory pressures and the demand for more programmability to accommodate decentralization of finance and data monetization remain a challenge. There is still fragmentation of protocols, as well as a lack of digital assets marketplaces and certification of the participants.

However, while not necessarily blockchain based, experiments with central bank digital currencies (CBDCs) — in part driven by FOMO toward Libra Association as well as the acceleration of cash replacement before and during the COVID-19 crisis, — as well as the use of nonblockchain tokens for financing (such as Jet Blue with Barclays ["Jet Blue Sells Loyalty Points to Bolster Cash by $150 Million." Payment Source.]) — have hastened conversations and experiments about tokens. This accounts for the two to five years' time to plateau.

User Advice:

- Map your token universe by inventorying the tokens that are in use by your enterprise, as well as in your ecosystem, to discover new financing and value exchange opportunities. These include identity and data tokens.
- Experiment with the decentralization of finance, especially in relation to pandemic reset as new economic models may be required.
- Monitor the progress of security tokens and CBDC initiatives and educate your peers about the different types of digital currencies (including stablecoins and cryptocurrencies) and the main impacts of central banks' policies on these currencies.
- Use tokens as another lever to compete against and disrupt digital giants. Tokens can be used to nudge and reward customers, help them manage consent and to share their personal data more selectively.
- Prepare for autonomous digital business (enabled by enhanced blockchain solutions that include IoT, ML and blockchain) by testing tokens as mediums of exchange for microtransacting between smart things, as well as for monetizing and exchanging items of data.

Business Impact: While a lot of attention to tokenization has focused on new settlement mechanisms (stablecoins) and cryptocurrencies as an attempt to replace fiat and existing payment mechanisms. The real transformational potential of blockchain-enabled tokens resides in the decentralization of finance (security tokens) and the creation of data tokens, as well as related decentralized self-sovereign IDs (SSIs).

Security tokens provide an opportunity to broaden the pool of investors, by fragmenting the ownership of the assets, especially a certain class of physical assets that are usually difficult to invest in, such as high value objects, real estate etc. and illiquid capital assets on enterprise balance sheets. In this way, new opportunities exist for financing, investing, supply chain management and ecosystem development and participation.

Data tokens allow data producers (individuals and companies, citizens, institutions and governments) to opt into sharing certain pieces of information and access new processing capabilities. They enable creation and discovery of new markets for data — which will reach its full

potential with enhanced-blockchain solutions (see “Apply the Gartner Blockchain Spectrum to Inform Investment Decisions”).

Another important business contribution is that tokens can be used as incentive mechanisms, such as to positively incentivize citizens’ behavior while allowing individual choice, offers a different set of opportunities to repair economic structures and prepare for a post-COVID-19 world.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Brave; Datawallet; ECO coin; Fetch.AI; swytchX; Swarm; Tether; The Libra Association

Recommended Reading:

“Expand Your Token Universe to Create New Business Models”

“Guidance for Blockchain Solution Adoption”

“Shape Your Digital Strategy With Central Banks’ Intentions Toward Digital Currencies”

“Facebook Libra — Liberator or Trojan Horse?”

“Use Gartner’s Strategic Tokenization Decision Framework to Boost the Value of Digital Business Ecosystems”

Blockchain Interoperability

Analysis By: David Furlonger; Rajesh Kandaswamy

Definition: Blockchain interoperability is the ability of blockchain platforms that use different distributed ledgers to seamlessly interact and transfer assets and other information from one blockchain network to another, and to other systems of record. This is done without an explicit per-use-case custom platform-to-platform gateway or exchange.

Position and Adoption Speed Justification: Blockchain ledgers are mostly discrete protocols, but are expected to be the primary store of data for assets and transactions for which processes are managed on the blockchain network. This has created the need for blockchain interoperability — sometimes called “interchain.” Such capabilities will allow different chains to make state changes on other chains. Interoperability can also enable a form of twinning, whereby assets on one chain can be replicated on a different chain to improve liquidity. This requires synchronized signature verification and complicated proofs. Organizations should recognize that blockchain value exchange interoperability differs from typical information exchange interoperability. In addition to message format and protocol translation, the former must implement measures to protect against double spending problems when transactions are posted from one blockchain platform to another.

Three core types of interoperability have been identified by the market — notary schemes, relays and hashed time locks. See “Guidance for Blockchain Solution Adoption” for more information on these schemes. An array of startups, such as Aion, the Blockchain Interoperability Alliance, Quant Network, Hyperledger Quilt, the Blocknet Protocol, Wanchain, the Lightning Network, Cosmos Network, Komodo, ARK, Fusion Foundation and Polkadot attempt to support system, information, identity and asset interoperability.

Transfer of value is done mostly through digital exchanges, and information exchange is managed via off-chain interfaces. Approaches such as synthetic tokens and atomic swaps have emerged, but much work remains to be done before they are ready for enterprise consumption. Further, smart contracts and decentralized applications (dapps) are likely to require interoperability across different blockchain networks and must be interdependent with nonblockchain systems. This will require open APIs and general-purpose standards. The European Union Blockchain Observatory and Forum released a report in March 2020 calling for greater levels of interoperability and scalability standards (“Scalability, Interoperability and Sustainability of Blockchains.” [PDF] The European Union Blockchain Observatory and Forum) with the intent to help guide policymakers and industry initiatives.

User Advice: As blockchain business and IT leaders, you should:

- Assume that standardized blockchain interoperability will not be viable in the near future and plan your architecture and vendor engagement accordingly.
- Be cautious of using blockchain as the primary source of truth, where the system of trust needs to extend across platforms or where you have extensive linkages with other systems, until viable commercial solutions are available.
- Identify the extent to which the assets, information or transactions that you plan to store on a blockchain might be needed externally. Ensure that you architect appropriate, secure and performant integrations for it.
- Prioritize design validation and testing for all integration points for any proposed blockchain projects, especially security hardening.
- Ensure blockchain vendor solutions have a planned solution for interoperability.

Business Impact: Interoperability is a critical requirement for blockchain systems to become primary sources of truth. Such interoperability, when available, can transform transaction flows and asset exchanges across industry networks, partner ecosystems and many other B2B and B2C digital markets. At present, the evidence of large-scale blockchain networks is sparse. Therefore, there is no immediate need for them to connect to each other. However, growth of blockchain networks, standards, protocols and their interoperability will occur in parallel, making it crucial that enterprises manage the peripheral activity in the ecosystem around blockchain systems that will have an impact on their own implementation.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Aion; Cosmos Network; Hyperledger Quilt; ICON Foundation; Interledger; Metronome; Polkadot; Wanchain

Recommended Reading:

"Guidance for Blockchain Solution Adoption"

"Market Guide for Blockchain Platforms"

"The Evolving Landscape of Blockchain Technology Platforms"

Consensus Mechanisms

Analysis By: Adrian Leow

Definition: A consensus mechanism is a process by which all nodes in a distributed network agree on proposed transactions, which ensures data integrity, immutability and consistency for information recorded in the ledger. Consensus mechanisms are distributed network governance rules and protocols that enable the recording, completion and execution of transactions under certain conditions.

Position and Adoption Speed Justification: Proof of work (PoW) was a consensus mechanism used by the first distributed ledger, embodied in the Bitcoin blockchain. PoW is the result of applying computational resources by miners (participants in a distributed network who confirm transactions) in a series of competitions to earn the right to add a block to the blockchain. The design of the PoW process — one block of approximately 2,000 transactions every 10 minutes on the Bitcoin blockchain — has set some upper bounds to transaction volume. Currently, for Bitcoin this is around three transactions per second (tps) in practice and seven tps in practice on the Ethereum blockchain, which raises concerns about scalability.

Newer mechanisms have been developed to address problems of scalability, expense, network latency and so on, including:

- **Proof of Stake (PoS) —** More than a dozen variants of PoS models include transparent forging and delegated PoS. Ethereum uses PoW but has done a "first release" of a PoS consensus mechanism (titled "Casper") code to GitHub. Ethereum software clients can begin scripting the software into their individual coding languages and testing the software, with the intention of Ethereum migrating to a full PoS system in the future. Nxt, among others, currently uses PoS.
- **Proof of Authority (PoA) —** Leverages the value of identities, which means that block validators are not staking coins but their own reputation instead. Therefore, PoA blockchains are secured by the validating nodes that are arbitrarily selected as trustworthy entities. Model relies on a limited number of block validators and this is what makes it a highly scalable system. Blocks and transactions are verified by preapproved participants, who act as moderators of the system.

- **Practical Byzantine Fault Tolerance (PBFT) —** An algorithm that predates cryptocurrencies and blockchain. No hashing power is required to validate transactions. The advantage of PBFT is that it can be more efficient than PoS and PoW, allowing throughput of thousands of transactions per second. The disadvantage is that it has only been used for small numbers of nodes in closed networks. It is suitable for some private blockchain scenarios, and is currently used by Hyperledger Fabric.
- **Proof of Space, Proof of Importance —** Based on holdings of a cryptocurrency and the volume of transactions a stakeholder undertakes. NEM Foundation uses this mechanism for its currency XEM.
- **Other Consensus Algorithm Mechanisms —** These include Federated Byzantine Agreement (FBA), Byzantine Altruistic Rational (BAR), proof of burn, quorum slicing, prediction markets, Unique Node Lists, Tangaroa, proof of DDoS, Sieve, Raft and proof of elapsed time.

These examples illustrate the diverse options available and new approaches to these mechanisms still being added. They highlight a technology that is still evolving, with each new mechanism offering its own set of benefits and trade-offs. All these mechanisms face challenges, including crash failure (when a process abruptly stops), byzantine failure (for example, conflicting data causing long delays), market adoption, ledger interoperability and skills availability. Some mechanisms challenge basic decentralization principles as well. These represent critical operational risks.

User Advice: We recommend:

- Educate IT and business leaders as to the importance of decentralization and the role of consensus mechanisms in influencing control for example over decision making, data, customers, tokens etc.
- Gain a greater understanding of how various consensus mechanisms work and their likely viability based on the specific use case intended for the blockchain being selected.
- Ensure you have sufficient understanding and analysis of how different platform providers use their respective consensus mechanisms, and the relationship to resources (that is, energy) consumption, token applicability and market adoption.
- Ensure you have sufficient technical expertise to recognize mechanism failings as a key component of blockchain adoption and managing operational risks.

Business Impact: Different consensus mechanisms will have significant impact on the long-term viability of the underlying blockchain/distributed ledger. For example, PoW has major issues with scalability and the cost of computational resources, but an almost unblemished record of security, availability and resiliency. PoS has many variants, most yet to be proven. PBFT is proven but only for a relatively small number of machines, usually with a single point of vulnerability built in (the central access control over the close private network). There are promising algorithms such as proof of elapsed time and proof of space, but these have yet to be fully implemented or tested. Unless and until the viability of different mechanisms can be proven in multiple business contexts, the future of blockchain/distributed ledgers at an industrial scale will be limited. Consensus mechanisms will directly impact how organizations will distribute execution liabilities.

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: Bitcoin.org; Coin Sciences (MultiChain); Ethereum Foundation; Hedera Hashgraph; IBM Blockchain; IOHK (Ouroboros); IOTA Foundation (Tangle); NEM Foundation

Recommended Reading:

"Market Guide for Blockchain Platforms"

"Guidance for Assessing Blockchain Platforms"

"Assessing the Optimal Blockchain Technology for Your Use Case"

Secure Multiparty Computing

Analysis By: David Mahdi; Bart Willemsen; Brian Lowans

Definition: Secure multiparty computing (SMPC) is a method of distributed computing and cryptography that enables entities (applications, individuals or devices) to work with data while keeping data or encryption keys in a protected state. Specifically, SMPC allows for multiple entities to share insights while working with confidential data.

Position and Adoption Speed Justification: With increasing demands of privacy protection and adequate, contextualized security controls, security and risk management (SRM) leaders struggle to achieve balance between data protection requirements and business objectives. Regulations focused on privacy and data protection further complicate the processing of (personal) data.

Historically, data protection has focused mainly on two states: securing data at rest and in transit. However, with SMPC-based methods and key splitting, it is possible to employ data protection in use. Data protection in use introduces a new paradigm to the arsenal of security methods and enhances traditional security approaches. The application of SMPC extends to combating data residency concerns, for example, balancing a single-point-of-failure risk regarding a cloud service provider's environment. SMPC can empower cloud key management with the ability to "split" cryptographic keys in a manner such that it ensures protection and privacy in the cloud. Most importantly, it facilitates data sharing for analytics in a protected state, across multiple contributors.

User Advice: SMPC-based solutions offer new methods to ensure scalable, private and secure data processing and sharing. With SMPC just starting to become a reality from a product and solution perspective, a number of new vendors are solving data security and privacy use cases with SMPC-based technology, often in combination with other capabilities. Use cases include:

- Cloud computing (confidentiality with data in a cloud environment)
- Privacy-preserved (personal) data analytics

- Encryption key management
- Cryptographic key protection
- Scalable software-defined hardware security modules (virtual HSMs)
- Secure and private data mining
- IoT security
- Blockchain security
- Analytics of data using proprietary algorithms

Data management strategies that include SMPC-based approaches enable secure and private sharing and analytics of data. For example, an organization that aims to extract value from customer data but has to adhere to strict privacy laws can maintain information value to extract insights while ensuring that the data is kept in an unidentifiable state. SRM leaders should work with developers/ architects to establish a high-level position on its relevance and a vision for the future adoption.

Furthermore, trust in the SMPC algorithm(s) and their respective security posture are crucial to SMPC's effectiveness as a privacy-preserving technology. SRM leaders must continue to gain insight into the technology development to provide trust-invoking transparency.

Business Impact: As organizations face ongoing pressure to ensure that their data is secure and private throughout the data life cycle, SRM leaders will need sustainable, effective and efficient ways to comply and treat risk.

SMPC, while known to academia for a few decades now, is only now starting to become commercially viable.

As volumes of both structured and unstructured data continue to grow, SRM leaders will need scalable, privacy-centric approaches to protect data amid a landscape of maturing data protection regulations. This is particularly important in areas such as cloud, Internet of Things and data mining or monetization.

SMPC can alleviate privacy concerns in the areas of big data analytics, machine learning (ML) and artificial intelligence (AI). SMPC helps SRM and data and analytics leaders to benefit from data insights that are derived from ML and AI while keeping the data secure and private. As ML and AI mature, SMPC will need to account for performance issues with specific algorithms such as recursive algorithms. Overall, SMPC allows for the secure enablement of business, enabling organizations to leverage their data while mitigating security and privacy concerns.

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Baffle; CryptoNumerics; Cybernetica; DataFleets; Inpher; Unbound Tech

Recommended Reading:

"The State of Privacy and Personal Data Protection, 2019-2020"

Smart Contracts

Analysis By: Martin Reynolds; Avivah Litan; Adrian Leow

Definition: A smart contract is a type of blockchain record that contains externally written code, and controls blockchain-based digital assets. When triggered by a specified blockchain write event, a smart contract immutably executes its code and may result in another blockchain event.

Smart contracts are neither smart nor contracts, and can only read from, and write to, the blockchain. All off-chain interactions with smart contracts must be handled by agents that map between off-chain assets and on-chain digital assets.

Position and Adoption Speed Justification: Smart contracts are well-developed for on-chain actions. For example, many cryptocurrencies are funded using an Ethereum smart contract style defined as ERC-20. These cryptocurrencies have not been hacked, despite the considerable financial gains to be made.

However, coupling a smart contract to business actions remains a challenge. This coupling works through external agents (for example, blockchain oracles) that write blockchain records to trigger a smart contract, and then read a blockchain record written by the smart contract to execute a business action.

Creating these external agents is just as challenging as creating a blockchain. This challenge arises because a corrupted agent could pervert an input to the smart contact by writing a modified record, or ignore an output record from a smart contract. Therefore, these external agents need redundancy and trust mechanisms that complement the blockchain system.

Blockchain's consensus mechanism is currently the only mechanism that supports functional smart contracts.

User Advice: Smart contracts can automate business transactions, executing transactions under mutually agreed terms embodied in the code. This approach eliminates human delays and costs, and potentially allows companies to execute far more transactions. This increased capacity comes at minimal incremental cost, thereby increasing efficiency, reducing operating costs, and opening new business models. Smart contracts, for example, can allow competitors to collaborate over shared resources without compromising their independence.

Application leaders looking at developing a strategy to deploy smart contracts should:

- Ensure that smart contract implementations are properly covered by legal agreements, such that unexpected or undesirable results are reversible outside of the blockchain.
- Identify use cases that can derive significant benefit from the contract automation processes promised by smart contracts and associated oracles. Such use cases will deliver some

combination of, for example, accelerated business processes; reduced transaction costs; asset sharing with competitors; or new business models.

- Research the emerging platforms, technology, tools and frameworks to determine the level of resources needed for smart contract development.
- Identify integration points with existing processes to determine their impact on core industry and ecosystem value propositions. Assess the implications for your information management architecture, legal compliance policies, payment systems, customer service and other core business processes.
- Develop policies and processes to create reliable smart contract code and ensure that you have the tools to monitor its correct execution.

Business Impact: Smart contracts will develop in different forms and with differing levels of impact. Many will simply replace existing transactional tracking mechanisms and execution systems such as used in blockchain-based supply chain management use cases. As such, smart contracts will be impactful. However, only when truly secure and proven smart contracts and related off-chain interaction systems develop will smart contracts have the potential to transform commercial relationships through granular obligation recognition and secure value transference.

The future vision of smart contracts includes a potential replacement for simple or complex legal documents and transactions, and integration with AI systems. However, there are many obstacles to be overcome, such as organizational readiness, integration with systems of record, unanticipated "follow on" smart contracts, perceived lack of enforceability, potential evidentiary gaps, regulatory compliance, which may take many years to resolve.

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Sample Vendors: Augur; Ethereum Foundation; Gnosis; Hyperledger; Monax; Provable Technologies; R3

Recommended Reading:

"Managing the Risks of Enterprise Blockchain Smart Contracts"

"Predicts 2020: Blockchain Technology"

"Guidance for Blockchain Solution Adoption"

Decentralized Identity

Analysis By: David Mahdi; Michael Kelley

Definition: Decentralized identity services leverage technologies such as blockchain or other decentralized ledger technologies (DLTs) to decentralize an identity system by distributing it across

a large number of nodes or participants. Thus, they provide an alternative to siloed legacy IAM architectures by establishing trust in identities and resiliency within the overall system, with little reliance on centralized arbiters or identity stores.

Position and Adoption Speed Justification: Decentralized identity (DID) differs from traditional IAM approaches due to the concept of centralized, versus decentralized, generation and storage of identities. Traditional IAM approaches, storing identity and entitlement data in central authoritative sources can be problematic from the perspectives of liability, security, scalability, reliability and privacy.

A decentralized approach minimizes these problems due to its core architecture being decentralized, distributed and transparent. It has the potential to increase trust, scale and resiliency, possibly with a more equitable and efficient economic model.

Standards are currently emerging, and at a fast rate. However, the market will take time to reach a steady state. However, development and innovation are increasing at a rapid pace, actively supported by financial and government institutions. On the standards front, the WC3 group, along with the decentralized identity foundation, (DIF), have created open standards which DID vendors can use to align their technology and vision with the rest of the market. In addition, the recently launched Trust over IP (ToIP), offers some promise in the area of standardization as well (see "Guidance for Decentralized Identity and Verifiable Claims").

A growing number of IAM approaches are reflecting blockchain-based enhancements including bring your own identity (BYOI) and decentralized identity. Mid 2019 and early into 2020, saw new entrants into the space such as Mastercard, Microsoft, Ping Identity (acquired ShoCard March 2020) Workday (acquired TrustedKey August 2019). Implementations are still primarily in POC, however, initiatives are gaining traction (such as Verified.Me in Canada).

Decentralized identity now sits at the peak; however, we have extended time to plateau. Practical blockchain-based solutions were overhyped and have made less headway than expected. Furthermore, effective solutions will depend on secure (formerly "privacy-enhanced") multiparty computing and zero-knowledge proofs, which have longer timescales.

User Advice: IAM leaders should familiarize themselves with decentralized identity through early stage research. In doing so, leaders can gain insight into new ideas and approaches that may be relevant. Ultimately, leaders must base all planning decisions on a clear understanding of the core differences between decentralized identity and traditional IAM approaches. A number of new and well-established vendors are experimenting with IAM applications in areas such as:

- Identity registration and verification.
- Ensuring integrity of devices (including things in the IoT).
- Enabling identity data sharing while preserving privacy ("consent control").
- Mitigating trust and transparency issues by using the distributed/decentralized model.
- Enhancing the ability to handle identities, attributes and relationships at massive scale.

- Enabling bring your own identity and/or self-sovereign identity. (Self-sovereign identity is another description for decentralized identity, or user managed identity; see “Blockchain: Evolving Decentralized Identity Design”).

IT leaders with an interest in decentralized identity approaches must recognize that leveraging this technology today requires proofs of concept to learn about the technology and, ultimately, the new business models and identity ecosystem that can be realized. Leveraging in market vendors, such as Microsoft, Workday, InfoCert, or IBM, is one option to understand the possibilities of decentralized identity applied to their use case(s). Customer identity and access management, (CIAM) use cases in particular offer potential for a DID approach.

Business Impact: Ultimately, with decentralized identity, users gain control of their identities and related attributes (i.e., personal information such as address, age and credentials), and service providers will be able to onboard and interact with users with greater speed and confidence. This is in contrast to many online services today, where digital identity and access are siloed, and service providers are forced to horde identity information about users. This has led to data breaches and other security and privacy issues. In the age of GDPR and privacy-conscious consumers, service providers will need to reevaluate their stance on the identity data they store. By leveraging decentralized identity, service providers could liberate themselves from storing sensitive data, instead relying upon assertions generated by identity providers.

Leveraging decentralized identity has the potential to allow service providers to increase security and convenience of access for end users, all while reducing exposure to data breaches and potential privacy compliance violations.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: 1Kosmos; Evernym; Hyperledger; IBM; InfoCert; Microsoft; Ping Identity; SecureKey; Sovrin; Trusted Key

Recommended Reading:

“Innovation Insight for Decentralized and Blockchain Identity Services”

“Innovation Insight for Bring Your Own Identity”

“Guidance for Decentralized Identity and Verifiable Claims”

“Top 10 Strategic Technology Trends for 2020: Practical Blockchain”

Blockchain Platforms

Analysis By: Rajesh Kandaswamy; David Furlonger

Definition: Blockchain platforms provide the foundation to create and run blockchain solutions. This includes support for distributed ledgers, peer-to-peer decentralized networks and smart contracts. They enable creation of blockchain solutions that provide for immutability, encryption, broad scale distribution, decentralization and tokenization.

Position and Adoption Speed Justification: Blockchain platforms are still evolving in their ability to support the core elements of blockchain technologies identified in the definition above. In addition, platform developers are also attempting to build out traditional application stack capabilities. Examples of these are usability and modeling support tools, frameworks and SDKs, native horizontal (e.g., sharing to multiply the number of chains) and vertical (e.g., parallel processing) scalability mechanisms, and security and fraud prevention controls. Development progress continues to progress in design, testing and piloting across different industries. There are more than a 100 solutions in the market that vary significantly in structure and scope. These include degrees of overlap in capability to implement smart contracts and distributed ledgers, levels of openness and decentralization, supplier viability and architectural approaches to permissionless and permissioned deployment styles. The market consolidation has not occurred, but COVID-19's impact can prove to be a catalyst. COVID-19 can impact enterprise technology purchases as well as dampen the mood for investment into platforms that have not proven themselves yet. Both can weed out the weaker market players. This early stage market is slowly morphing into two design patterns for public and enterprise blockchain platforms, with the expectation of further blurring between the two patterns via interoperability protocols. While there is no evidence of pilots moving into industrial scale production-scalable offerings, we have observed limited production deployments with a small number of nodes and a constrained scope of services. Architecting and implementing a blockchain platform is a complex and challenging undertaking, not the least in terms of overcoming business, in addition to technical challenges. Blockchain platforms will continue to evolve rapidly, which will result in a cycle of obsolescence that is less than two years.

User Advice: Evaluate any vendor offerings extremely carefully using a technology-agnostic function framework to ensure an apple-to-apple comparison (see "Guidance for Assessing Blockchain Platforms"). Be prepared for rapid evolution, early obsolescence, a shifting competitive landscape, significant consolidation of offerings and the potential failure of seemingly viable early stage technologies/functionality. Check the level of openness and decentralization throughout the platform stacks carefully as well as upgrade paths, especially in a multiparty business setup and/or consortiums. Ensure adequate understanding of the core platform concepts such as coordination protocols (i.e., distributed consensus or endorsement and ordering technologies), the operational role of tokens, data structures used, validation, interoperability, authentication mechanisms, ability to scale, manageability, scope, tooling, security and privacy treatments, and third-party ecosystem support.

Business Impact: Blockchain platforms can become significant enablers of the programmable economy with the capability to support and foster autonomous microtransactions, diverse value-exchange scenarios, on-demand markets, smart assets, smart contracts and the operation of distributed autonomous organizations (DAOs). It could usher in a whole new economic and societal model based on machines that are able to act on behalf individuals or businesses and make decisions or choices. They also could substantially change the nature of traditional IT from both a

supplier and user standpoint as open-source capabilities and decentralized applications (dapps) gain market traction.

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Digital Asset; EOS; Ethereum; Hyperledger (Fabric); MultiChain; NEO; R3

Recommended Reading:

"Guidance for Assessing Blockchain Platforms"

"How to Operate and Support Blockchain Platforms"

"How to Position Blockchain Platforms to Increase Adoption"

"Market Guide for Blockchain Platforms"

Tokenization

Analysis By: Martin Reynolds

Definition: Tokenization is a blockchain convention that links a physical asset or financial instrument to a blockchain token. These tokens can be transferred via the blockchain and represent ownership or custody of the asset. The tokens may also be managed by smart contracts, enabling automated, deterministic asset transfers.

Position and Adoption Speed Justification: Tokens represent a stored value that is transferred between accounts or between users. Blockchain systems, such as Ethereum, provide mechanisms to create and manage tokens other than the native cryptocurrency. These mechanisms underpin many of the Ethereum-based tokens deployed today. As such, tokens are well-vetted from a security and reliability perspective.

Linking these digital tokens to real-world assets through tokenization, however, has two challenges. The primary challenge is authenticating external events that trigger smart contracts to transfer the token. This authentication comes from off-chain systems, such as oracles, that translate real-world actions into a blockchain event. These events trigger a smart contract that consequently executes the transaction. However, oracles are subject to manipulation. Consensus-based oracles that cannot be subverted or suppressed are in early deployment and are an important component of tokenization systems. The second challenge, asserting rights over a transferred asset, is beyond the scope of tokenization and belongs in the area of business relationship and enforcement.

User Advice: In designing your tokenization strategy, the single most important item is the protocol for updating the blockchain from external events. These events represent the real-world actions that cause a token to change state. In many cases, these actions will come from a trusted authority such as a bank, a government agency or a trusted business partner. In these cases, normal business

checks and balances secure the authority of the actor. In the case of a major transaction (for example, the transfer of a deed to a property), designing a process that requires two or more authorities is a reasonable and practical approach, mirroring real-world protocols.

However, when blockchain triggers are updated by automated sources, these sources may be subject to corruption or suppression. For example, a bad actor might suppress a market data feed, and instead substitute with data designed to cause a distorted transaction. Falsifying a commodity price would be one example; suppressing a delivery notification would be another. Correcting these transactions may be simple, or it may involve the complications of legal action.

In many cases, blockchain systems managing tokens may remain under control of a single authority, which provides an effective mechanism to deal with software bugs and incorrect transactions. However, once these systems move to distributed authority, errors are difficult to impossible to fix. Therefore, a tokenization system must be thoroughly vetted before (and if/when) it opens to multiple masters.

IT leaders trialing blockchain projects should:

- Ensure data sources that trigger transactions are appropriately vetted
- Use human authorities for significant transactions that do not demand automation
- Use redundant oracles when public data sources have material influence on transactions
- Thoroughly vet your code, system and protocols before opening to multiple blockchain masters

Business Impact: Tokenization is the bridge between business processes and the blockchain, and is therefore on the critical path for every business blockchain project that manages real-world assets through tokens on a blockchain. Correctly implemented, tokenization makes a business project run smoothly by creating clear, manageable connections between the blockchain world below and the business world above. Without clear lines between these layers, managing assets becomes potentially risky, and could destroy confidence in a blockchain project if the records diverge from reality. Although weak tokenization strategies work in a private blockchain where a single entity can readily correct errors, for a blockchain operated by a consortium, a clear tokenization strategy and verified implementation is critical to acceptance and success.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Chainlink; Provable; R3

Recommended Reading:

“Managing the Risks of Enterprise Blockchain Smart Contracts”

“4 Blockchain Silver Bullets That Will Not Solve Business Problems”

Sliding Into the Trough

Blockchain

Analysis By: David Furlonger; Rajesh Kandaswamy; Christophe Uzureau

Definition: A blockchain is an expanding list of cryptographically signed, irrevocable blocks of records shared by all participants in a peer-to-peer (P2P) network. Each block of records is time stamped and references links to previous data blocks. Anyone with access rights can historically trace a state change in data or an event belonging to any participant. Distributed ledgers are design limited and lack decentralized and tokenized elements.

Position and Adoption Speed Justification: A blockchain is an expanding list of cryptographically signed, irrevocable blocks of records shared by all participants in a peer-to-peer (P2P) network. Each block of records is time stamped and references links to previous data blocks. Anyone with access rights can historically trace a state change in data or an event belonging to any participant. Distributed ledgers are design limited and lack decentralized and tokenized elements.

User Advice: We recommend:

- Educate senior leaders about the opportunities and threats that blockchain capabilities introduce. Use clear language and definitions in internal discussions about how distributed ledgers may or may not improve existing systems and processes.
- Continue to develop proof of concepts (POC) — especially in the context of market ecosystems. Identify integration points with existing infrastructures (for example, digital wallets, core systems of record, customer service applications and security systems). Analyze the role, maturity and interdependence of synergistic technologies such as artificial intelligence (AI) and the Internet of Things (IoT) as key levers in the evolution of blockchain complete and enhanced solutions.

Executives planning on deploying blockchain solutions must:

- Ensure sufficient innovation capacity is applied to the evolution of distributed ledgers and blockchains outside of your immediate industry.
- Identify integration points with existing legacy infrastructures. Evaluate the total cost of ownership against existing systems. Be very cautious about vendor lock-in and merely replatforming the enterprise without any additional value.

Business Impact: Blockchain provides an opportunity for enterprise leaders to imagine new kinds of business models and revenue flows. In particular, leaders decentralize commercial exchange, thereby reducing friction and cost, by monetizing multiple forms of assets. Enterprise leaders also face a threat from startups and businesses that can use the five core elements of the blockchain concept to disrupt and disintermediate markets and industries. This is done by offering capabilities like identity portability, trustless interactions, smart contracts and new forms of value exchange. These opportunities and threats will evolve over the next 10 years in varying degrees, affording strategic planners an opportunity to proactively address opportunities and threats. Regulation will

play a significant role in the speed of evolution. Recent developments around the framing of compliance for token use and initial coin offerings (ICOs) are to be watched, as well as general consumer behavior toward, and acceptance of, multiple forms of assets. Progression with identity management will change the power structure in many industries and should be viewed through both a business and technology lens.

For distributed ledger concepts to really transform industry operating models via automation, and for economies of scale to improve efficiency, there needs to be a wholesale reimagination of digital transformation. COVID-19 may provide that catalyst. However, rather than encourage collaboration, it may increase fragmentation, making it harder for cross-industry and cross-jurisdiction consortia to be successful. Multiple business use cases have yet to be proven, and accurate value outcomes have yet to be calculated. It is unclear whether current approaches for using distributed ledgers provide sufficient differentiation compared with existing, proven messaging and data technologies. Clearly, interoperability of both technologies and processes is a significant requirement.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Algorand; Block.one; Cardano; Ethereum; Hyperledger; Neo; R3; Zilliqa

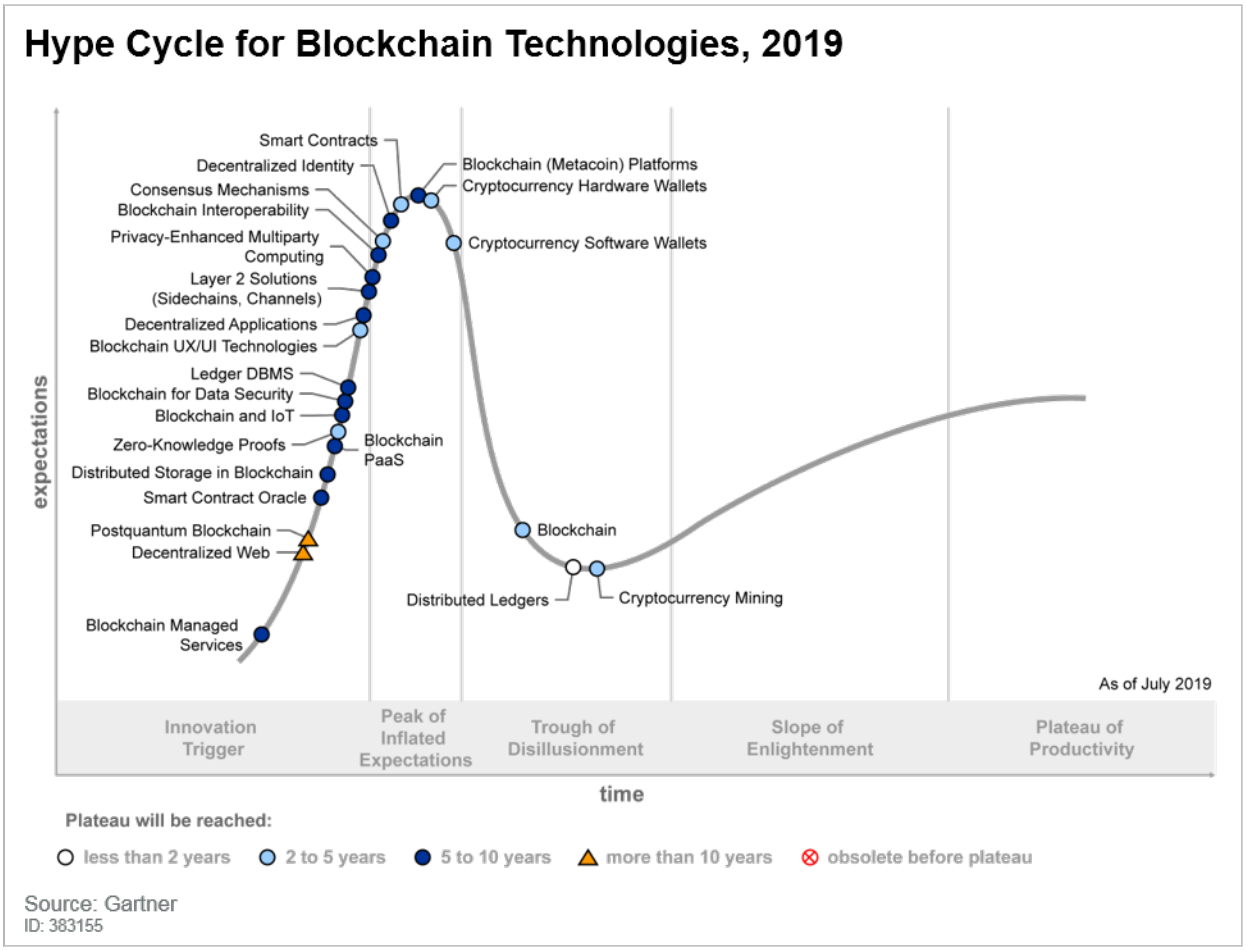
Recommended Reading:

“Understanding the Gartner Blockchain Spectrum and the Evolution of Technology Solutions”

“Guidance for Blockchain Solution Adoption”

Appendixes

Figure 3. Hype Cycle for Blockchain Technologies, 2019



Source: Gartner
ID: 383155

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1. Hype Cycle Phases

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant press and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the technology is pushed to its limits. The only enterprises making money are conference organizers and magazine publishers.
Trough of Disillusionment	Because the technology does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the technology's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the technology are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the technology to reach the Plateau of Productivity.

Source: Gartner (July 2020)

Table 2. Benefit Ratings

Benefit Rating	Definition
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2020)

Table 3. Maturity Levels

Maturity Level	Status	Products/Vendors
Embryonic	■ In labs	■ None
Emerging	■ Commercialization by vendors ■ Pilots and deployments by industry leaders	■ First generation ■ High price ■ Much customization
Adolescent	■ Maturing technology capabilities and process understanding ■ Uptake beyond early adopters	■ Second generation ■ Less customization
Early mainstream	■ Proven technology ■ Vendors, technology and adoption rapidly evolving	■ Third generation ■ More out-of-box methodologies
Mature mainstream	■ Robust technology ■ Not much evolution in vendors or technology	■ Several dominant vendors
Legacy	■ Not appropriate for new developments ■ Cost of migration constrains replacement	■ Maintenance revenue focus
Obsolete	■ Rarely used	■ Used/resale market only

Source: Gartner (July 2020)

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Common Mistakes to Avoid in Enterprise Blockchain Projects

Assessing the Optimal Blockchain Technology for Your Use Case

The Future of Blockchain: 8 Scalability Hurdles to Enterprise Adoption

Market Guide for Blockchain Platforms

Blockchain Trials Show Pragmatism Emerging Across Industries

Guidance for Blockchain Solution Adoption

Key Takeaways From Gartner Survey of U.S. and China Enterprises to Guide Your Post-COVID-19 Blockchain Future

Predicts 2020: Blockchain Business

Predicts 2020: Blockchain Technology

Evidence

Organizational interest in enterprise blockchain is tightly correlated with the rise and fall in Bitcoin prices. This finding is supported by Gartner's correlation analysis of social media conversations on enterprise blockchain with the price of Bitcoin, as published in our Gartner blog.

More on This Topic

This is part of an in-depth collection of research. See the collection:

- 2020 Hype Cycle Special Report: Innovation as Strategy

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."