Hype Cycle for Blockchain and Web3, 2023

Published 2 August 2023 - ID G00790911 - 105 min read

By Analyst(s): Adrian Leow, Avivah Litan, Homan Farahmand, Ray Valdes

Initiatives: Software Engineering Technologies; Adopt Modern Architectures and Technologies

Blockchain/Web3 is still gaining traction in the enterprise sector. Interest declined around 2020, when intrigue in DeFi grew exponentially. Despite this, global spending on blockchain solutions continues as private and public sector organizations evaluate and experiment with hyped up technologies.

Strategic Planning Assumption

By 2027, hybrid NFT (non-fungible token) identities (identity wallets, with both verifiable claims, and NFT identities) will be used by more than 50% of metaverse users for their online persona.

Analysis

What You Need to Know

Blockchain technology has evolved significantly and is being adopted by various industries. Software engineering leaders need to understand how to support potential use cases involving decentralized applications (dapps), decentralized finance and NFTs for example. However, there are still challenges to overcome, such as scalability, interoperability and regulatory compliance. With various blockchain platforms and consensus mechanisms available, it can be challenging to determine the best fit for a particular use case.

This Hype Cycle tracking blockchain and Web3 evolution can help software engineering leaders make informed decisions about the use of blockchain technology in their organizations. Software engineering leaders must prioritize developers' tasks and resourcing to focus on the blockchain projects and use cases that will yield tangible results.

The Hype Cycle

There has been a noticeable drop in interest in cryptocurrency and decentralized finance (DeFi) since the collapse of FTX, Three Arrows Capital, Genesis and several crypto exchanges. This erosion of trust in cryptocurrency is ironic since it was intended to be trustless as an exchange mechanism. Consumer adoption of blockchain has been more enthusiastic than enterprise adoption.

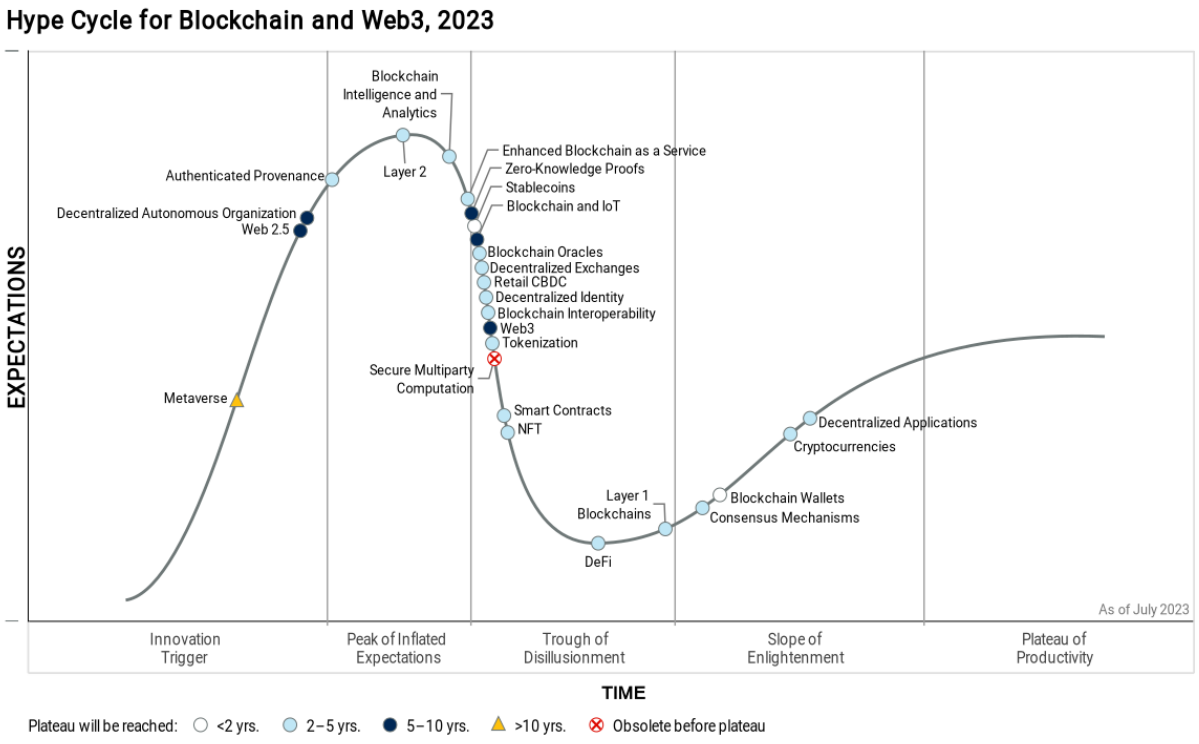
The blockchain design pattern is evolving around a multitier model that includes Layer 0 chains for cross-chain state interoperability, Layer 1 public blockchains for decentralization and security, and Layer 2 chains primarily for scalability. To gain mainstream adoption, the technology will become scalable, easier, safer to use and accessible using a wide range of off-the-shelf applications.

Tokenization plays a crucial role in driving the adoption of blockchain technology. By enabling the digitalization of assets, tokenization expands the utility of blockchain beyond cryptocurrencies by demonstrating how it can securely represent and transfer real-world assets. This has attracted interest from industries including energy, transport, smart cities and nongovernmental organizations (NGOs), as they recognize the potential for increased efficiency, transparency and cost savings. Tokens enable dapps and platforms by incentivizing users to contribute to the network and guaranteeing the system's proper operation. Overall, tokenization serves as a compelling use case for blockchain technology, helping to increase its mainstream adoption.

The addition of "Web 2.5" to this year's Hype Cycle is significant due to its key role in driving blockchain adoption. It represents the partial evolution beyond the current state of Web 2.0, involving integration of Web3 blockchain technology artifacts.

It should be noted that "blockchain platforms" has been renamed as "Layer 1 (L1) blockchains." Gartner sees this update as a more accurate description as L1 addresses decentralization and security requirements while L2 blockchains (or enterprise blockchains) address the scalability.

Figure 1: Hype Cycle for Blockchain and Web3, 2023



The Priority Matrix

The progress in blockchain technologies maturity indicates that it is no longer a mere hype but a valuable tool that can bring transformative changes to various industries. However, it is essential for organizations to plan their blockchain architectures in a way that allows for future upgrades and the integration of better solutions as they become available. The use of blockchain has extended beyond its early applications in finance and cryptocurrencies, and it is now being leveraged across sectors such as supply chain management, healthcare, logistics and more.

With the continuing maturation of key components such as stablecoins, blockchain wallets and cryptocurrencies, as well as the emergence of newer concepts like Web 2.5, blockchain intelligence and analytics and enhanced blockchain as a service (eBaaS), the foundations of the blockchain ecosystem are becoming more defined.

These movements provide both an opportunity and a note of caution for software engineering leaders. It shows that they must evaluate blockchain technologies as a strong candidate for their technology investments. However, it also indicates that they should still plan for an architecture that allows them to upgrade specific components or platforms as better solutions become available.

Table 1: Priority Matrix for Blockchain and Web3, 2023

(Enlarged table in Appendix)

Benefit ↓	Years to Mainstream Adoption: Less Than 2 Years ↓	2 - 5 Years ↓	5 - 10 Years ↓	More Than 10 Years ↓
Transformational	Blockchain Wallets Stablecoins	Blockchain Interoperability Blockchain Oracles Consensus Mechanisms Cryptocurrencies Decentralized Identity Layer 1 Blockchains NFT Retail CBDC Smart Contracts Tokenization	Blockchain and IoT Web 2.5 Web3	Metaverse
High		Authenticated Provenance Decentralized Applications Decentralized Exchanges DeFi Enhanced Blockchain as a Service Layer 2	Decentralized Autonomous Organization	
Moderate		Blockchain Intelligence and Analytics	Zero-Knowledge Proofs	
Low				

Source: Gartner (August 2023)

Off the Hype Cycle

This year, no innovations have reached the Plateau of Productivity.

We have renamed the following innovations to accurately reflect the content:

- Oracles has been renamed blockchain oracles.
- Blockchain platforms has been renamed Layer 1 blockchains.
- CeDeFi/CeDeX has been renamed “Web 2.5.”

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

On the Rise

Metaverse

Analysis By: Marty Resnick, Matt Cain, Tuong Nguyen

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Gartner defines a metaverse as a collective virtual 3D shared space, created by the convergence of virtually enhanced physical and digital reality. A metaverse is persistent, providing enhanced immersive experiences. Gartner expects that a complete metaverse will be device-independent, and will not be owned by a single vendor: It will have a virtual economy of itself, possibly enabled by digital currencies and non-fungible tokens (NFTs).

Why This Is Important

A metaverse is the next level of interaction in the virtual and physical worlds. It will allow people to replicate or enhance their physical activities. This could happen either by transporting or extending physical activities to a virtual world or by transforming the physical one. Although the goal of a metaverse is to combine many of these activities, there are currently many emerging metaverses with limited functionality.

Business Impact

Enterprises can expand and enhance their current businesses in unprecedented ways, opening up innovative opportunities. The following are examples of opportunities that metaverse offers to enterprises:

- Spatial computing (e.g., real-time shopping recommendations)
- Gaming (e.g., collaborative “serious games” for training)
- Digital humans (e.g., customer service representatives)
- Virtual spaces (e.g., live virtual events)
- Shared experiences (e.g., immersive meetings)
- Tokenized assets (e.g., NFTs)

Drivers

There are three drivers for the metaverse:

- **Transport:** The ability to "go and immerse oneself" in a virtual world. That world may be a 3D simulation and/or in virtual reality.
- **Transform:** Bringing digital to the physical world. This allows the user to have access to real-time information, collaboration and experiences in the physical world.
- **Transact:** The economic foundation of the metaverse through the use of cryptocurrency, NFTs and blockchain.

Some of the main activities for the metaverse that will require one or more of these drivers are:

- **Collaboration:** Encouraging collaboration and participation from a diverse group of stakeholders, wherever they may be located.
- **Engagement:** Employees and customers are often disengaged. The metaverse facilitates a feeling of presence ("being there") as if the participants were in-person, turning their focus to the task at hand with less distraction.
- **Connectedness:** Metaverse enables us to connect in a more immersive way with shops, work environments, schools and communities of interest — regardless of where or if they exist in the physical world.

Ultimately, people desire to enhance and/or augment their lives in digital and physical realities.

Obstacles

- The adoption of metaverse technologies is nascent and fragmented. Furthermore, this is a time of learning, exploring and preparing for a metaverse with limited implementation. The financial and reputational risks of early investments are not fully known, and caution is advised.
- Current manifestations of metaverses are siloed, app-based, noninteroperable experiences that do not satisfy the decentralized and interoperable vision of the metaverse. This current, walled-garden approach also strongly limits users' control of experiences.

- While technology plays a key role in achieving a mature metaverse, another challenge involves establishing user-centric guidelines for ethics and governance covering different aspects of the metaverse. This must include topics like privacy, data sovereignty, acceptable terms of use, accountability, identity and legal protections.

User Recommendations

- Task a specialized innovation team and/or vendors to look for opportunities where metaverse technologies could optimize digital business, or create new products and services.

- Identify metaverse-inspired opportunities by evaluating current high-value use cases vis-a-vis your product or service (internally and externally). Focus on ways the metaverse can enhance an experience and can accomplish engagements the physical world may find impossible.

- Be careful when investing in a specific metaverse, as it is still too early to determine which investments will be viable in the long term.

- Remember that the metaverse is an evolutionary stage. Similar to the shift from the original web to Web 2.0 and to Web3, it does not indicate a formal change in the nature of the web, or in this case, digital interactions and digitization in general, but describes a general change that will happen over time.

Sample Vendors

Animoca Brands (The Sandbox); Decentraland; Linden Lab; Meta; Microsoft; NVIDIA; Roblox

Gartner Recommended Reading

Emerging Tech: Top Enabling Technologies for Metaverse

Top Strategic Technology Trends for 2023: Metaverse

Building a Digital Future: The Metaverse

Infographic: Impact Map of the Metaverse

Emerging Tech Impact Radar — The Metaverse

Decentralized Autonomous Organization

Analysis By: Mordecai ., Rajesh Kandaswamy

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

A decentralized autonomous organization (DAO) is a digital entity, running on a blockchain, that can operate without conventional human management and engage in business interactions with other DAOs, digital and human agents, as well as corporations. DAOs rely on software consensus mechanisms and smart contracts for governance and to define and program the rules of commercial engagements — primarily in decentralized, away from a central authority, contexts.

Why This Is Important

DAOs are accelerating Web3 and proliferating in cryptocurrency and decentralized finance (aka DeFi), as well as culture, creator/collector, service, and social. DAOs are important governance mechanisms for Web3 projects and can enable collective decision making. DAOs can also fuel innovation by enabling independent contributors to share ideas and control over development projects. However, DAOs can also be high risk. A few high-profile DAO meltdowns have caused significant financial losses.

Business Impact

DAOs offer benefit to traditional corporate business models and ecosystems:

- Programmability can improve business agility.
- Decentralized creators can build consensus on development activities, outmaneuvering corporations.
- Smart contracts automate interactions with smart machines, humans and other organizations to drive new business models.
- DAO models for engagement can serve as templates for loyalty, audience and proxy models.
- DAOs may serve as a utility, and funding model, for innovation ecosystems.

Drivers

- Decentralized mechanisms counterbalance greater centralized control over programmable capabilities and market power concentration.
- Decentralization empowers market participants to initiate, gain fair access and be rewarded for socioeconomic activity.
- Investors/participants in DAOs can share in the development and future of a business, negating the need for greater centralized enterprise governance.
- DAO operations can provide more efficiency, productivity, speed of decision making and how digital business could be conducted and digital products created.
- Startup, administrative and operations costs are very low for DAOs, and ready tools exist not just for governance, but also for token issuance, code management, smart contracts, voting, underlying protocols and more.
- Enabling platforms that can enable you to easily pilot and explore governance features and other capabilities are quickly emerging and becoming more robust and intuitive.
- DAOs are gaining popularity in cryptocurrency and social good projects with several attracting considerable capital.
- The U.S. states of Wyoming and Tennessee have laws that enable a DAO to be registered as a limited liability corporation. This may attract filings through favorable corporate regulations, similar to the use of the state of Delaware for corporate registration.

Obstacles

- Autonomy interferes with accountability as DAOs can operate without executive leadership or full-time staff. Staff can also overwork creating an imbalance in leadership.
- Incompetence or poor design can create vulnerabilities as evidenced by Beanstalk DAO that was robbed of $182M.
- DAOs that are in reality centrally governed can also lead to failures. as unclear standards and false claims can lead to arbitrary decisions by controlling parties.
- Regulatory and legal ambiguity, e.g., who is legally liable should things go wrong, unclear legal jurisdiction and tax evasion.
- DAOs' open nature enables bad actors to analyze code and governance to find exploits.
- Companies and governments remain interested in centralized control, have a lack of trust, and will oppose DAOs.
- Underlying issues with cryptocurrencies such as financial transparency, volatility, legality and adoption may undermine reward mechanisms that are key to DAOs.

User Recommendations

- Identify and track DAOs operating in your industry or in adjacent areas, especially in decentralized finance and data exchanges. Identify opportunities or threats, and incorporate your business strategy.
- Screen for DAOs that align with overall strategy. Allocate a small amount of capital to obtain voting rights and then participate in governance.
- Conduct rigorous technical and legal due diligence on DAO smart contracts and underlying technologies before participation.
- Analyze your extended ecosystem, identifying areas of common interest that could be served by a DAO. Develop a draft plan, pitch it to ecosystem participants and refine it based on feedback.
- Track regulatory proceedings, legislation and legal precedents to determine their potential impact on DAO adoption.
- Analyze customer behavior shifts and assess proclivity to use autonomous agents in purchasing.
- Follow DAOs aligned with business priorities; KlimaDAO (carbon offset), Opollis (solo workers), Bankless (media, social).

Sample Vendors

Aragon; BitDAO; Colony; DAOhaus; DAOStack; Lido; Maker; Moralis; Uniswap; Upstream

Gartner Recommended Reading

How Decentralized Autonomous Organizations Will Impact Digital Transformation

Innovation Insight for Decentralized Autonomous Organizations — A New Growth Model for IT Services Providers

Autonomous Business Is the Next Tech-Enabled Strategic Growth Curve for Pioneer Enterprises

Web 2.5

Analysis By: Avivah Litan

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Web 2.5 represents integration of Web3 blockchain technology artifacts, such as tokens, smart contracts and Web3 applications, with Web 2.0 applications and services. Web 2.5 application possibilities are endless. For example, decentralized peer-to-peer lending services (Web3) can be integrated into centralized bank (Web 2.0) product offerings. Similarly, news content can be tokenized (Web3) and sold by media companies using traditional Web 2.0 applications.

Why This Is Important

Web3 supports unique technological innovations that enable users to own and control their own content and money. It also supports a trustless shared system of record based on immutable data. However, enterprises are justifiably unwilling to give up governance, oversight and control of most business applications. Hence, they will mainly use Web3 innovations layered on top of their Web 2.0 applications and business models.

Business Impact

Blended Web3 and Web 2.0 applications bring together the best of centralized and decentralized systems by combining Web 2.0 business controls with decentralized blockchain technology. They support new business processes, such as automated management of tokenized assets across multiple parties in an ecosystem. Web 2.0 applications that use Web3 technologies buttress Web3 risks by supporting user onboarding, liability protection, customer service, insurance and regulatory compliance.

Drivers

- Enterprises are unwilling to give up control, which is needed to participate in Web3 applications. Hence, they are naturally inclined to adopt Web 2.5 instead.
- Innovative blockchain projects support the evolution of financial services systems into more modern infrastructure that represent a major technical upgrade of their rigid siloed and archaic rails.
- Digital asset tokenization used by traditional financial services firms are more efficiently managing fixed income assets. See Goldman Sachs' Tokenization Platform and Franklin Templeton Money Market Fund on Polygon. Other firms will follow their lead.
- Real-time, immutable and transparent payments and settlements are being supported by trusted regulated financial firms, such as Visa and Circle Internet Financial, using blockchain Web3 technology.
- Innovative blockchain projects are transmuting supply chains, document management, patent management and healthcare services, among others. Sponsoring organizations are not giving up organizational controls and are able to benefit from the technological innovations.
- Major drivers in nonfinancial sectors are: ESG and compliance, data integrity track and trace, provenance, retail/brand expansion, user-owned identity records (e.g., in healthcare and education).
- While Web 2.0 has enabled collaborative and social features that have transformed the internet, it still relies on centralized platforms and intermediaries to manage user data and transactions. This can lead to privacy and centralized gatekeeper concerns, which Web 2.5 alleviates.

Obstacles

- Most mainstream organizations do not understand Web3 or decentralized blockchain technology, and fail to articulate a clear business need for it. Organizations need to be clear on use cases that require Web3 technologies.
- Most Web3 technologies are still too hard to use. Progress is being made in improving development environments, user interfaces, and security controls, but are not widely available yet.
- Many brands are participating in Web3 applications by trading in various types of non-fungible tokens (NFTs), but most are still unclear on how they will profit.
- Decentralized applications are primary targets for hackers who usually exploit smart contract logic. These vulnerabilities must be dramatically minimized before organizations can risk funds held in smart contracts.
- Regulation of decentralized finance (DeFi) and NFT products and services varies widely across countries and, in most cases, will likely take three to five years to stabilize.
- “Web 2.5” is not yet a widely accepted industry standard or well-defined concept.

User Recommendations

- Work with organizational counterparts to understand how Web3 and blockchain technologies can improve your business opportunities. Gain an understanding of benefits, risks and requirements of decentralized applications as compared to centralized or traditional applications, and what the business benefits are of combining the two.
- Keep apprised of off-the-shelf Web 2.5 as they become more widely available, and prepare to use them if they suit your use case.
- Standardize on units of value or exchange by using tokens. Fungible and non-fungible tokens can be moved across disparate blockchains through various blockchain interoperability and smart contract options that support them.
- Ensure your security and risk management programs incorporate both Web 2.0 and Web3 technical controls.

Sample Vendors

Animoca Brands; Casper Labs; Context Labs; Finboot; Fujitsu; IPWe; NTT DATA; SettleMint; ShelterZoom; Sky Republic

Gartner Recommended Reading

FAQ for NFTs on Blockchains and Web3 Ecosystems

FAQ for Cryptocurrencies on Blockchains and Web3 Ecosystems

Quick Answer: What Is Web3?

Web3 and the Metaverse: Incomplete but Complementary Visions of the Future Internet

At the Peak

Authenticated Provenance

Analysis By: Avivah Litan

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Authenticated provenance represents the authentication of any asset that can be recorded and tracked on the blockchain, for example, a machine part, document, or software library. The provenance of these assets can later be digitally verified by users through applications. There are many methods used to authenticate the provenance of assets, depending on their nature and whether they are digital or physical goods.

Why This Is Important

At their worst, counterfeit goods, fake content, and erroneous data are national and health security threats. At their best, they are costly problems for organizations. Blockchain provenance and asset tracking applications are used to address these issues, but they don't address the problem of authenticating goods, data and content initially recorded on the blockchain. The question remains — how do you know that the things you are tracking on the blockchain are real to begin with?

Business Impact

Gartner believes that provenance authentication solutions will be in more demand in the coming years, especially as generative AI supports easy creation of "deepfake" objects and content. Blockchain provides an immutable record and audit trail for provenance applications. Users are becoming increasingly aware of the need to digitally "certify" the processes and materials that go into creating goods, content, data or any asset being tracked on the blockchain in the first place.

Drivers

- Today, authenticated provenance largely relies on manual audits or human trust, which is not scalable. For example, human fact checkers cannot keep up with the volume of fake content.

- Generative AI allows threat actors to easily use the technology to easily create “deepfakes,” or copies of products, and generate artifacts to support increasingly complex scams. It is becoming increasingly difficult, if not impossible to discern synthetic content from original forms.
- Environmental, social and governance (ESG) goals embraced by asset management firms and some regulatory authorities are forcing companies to produce verifiable data on the state of their organizations with regard to ESG indicators.
- Regulators and other government authorities do not have sufficient visibility into supply chains or complex multiparty ecosystems, and therefore cannot validate assertions about the state of goods or services that they are auditing and overseeing.
- New food safety regulations in the EU and the U.S. are prompting agriculture companies and food producers to ensure the quality of their food and the veracity of its provenance claims.
- Consumers and businesses are placing trust in various labels and certificates, such as “organic” but they have no way of verifying the veracity of these assertions. Evidence has shown that these labels and assertions are often incorrect.
- The Internet of Things (IoT) is being successfully used to track and record the state of “things” on IoT networks. This capability can be used to validate information used in business processes that rely on externalities.
- Blockchain and tokens are successfully providing a single system of record across multiple entities, based on immutable data and audit trails and is often used to record authenticated provenance.
- Authenticated provenance standards from organizations such as C2PA, IETF and Scitt.io are evolving and are steadily being adopted.

Obstacles

- Generative AI technology used to create synthetic (fake) content is progressing much faster than government regulatory frameworks and enforcement which can mitigate the widespread damaging effects of their dissemination.
- Efforts in the market to support and use open-source standard methods for authenticating provenance have not yet gained notable adoption.
- There is a lack of domain-specific tools for assessing “truth.” ROI is still unproven.

- There is a need for new multiparty business agreements; and a need for entire ecosystems to participate.
- Custom integrations are needed for analytics, AI, IoT and blockchain technologies.
- Many multiparty processes are complex and unproven.
- There is very little awareness of trust issues and the methods to address them.
- Still-maturing blockchain interoperability protocols are needed to track provenance as assets move across blockchains during the normal course of business.

User Recommendations

- Utilize open standards for authenticated provenance already in place, for example, from C2PA, IETF, and Scitt.io.
- Evaluate how blockchain, combined with other advanced technologies (e.g., AI and IoT) can be used to support authenticated provenance.
- Review the lack of mature domain-specific tooling, for example, that authenticates news textual or video content or organic food products, and be prepared to develop or assemble your own.
- Adopt authenticated provenance use cases, provided you can demonstrate ROI through improved efficiencies and new revenue streams.
- Utilize self-sustaining public blockchains like Ethereum when possible to avoid private infrastructure costs and to support greater trust in metadata stored therein.
- Address customer demand for greater trust. These technologies give customers confidence in your brand and the provenance of your products.
- Replicate what has worked in supply chain and other sector case studies as documented in Gartner recommended research.

Sample Vendors

Circulor; Context Labs; Finboot; RKVST; SettleMint

Gartner Recommended Reading

Truth and Transparency in Supply Chain: 3 Case Studies on How Blockchain, AI and IoT Are Shedding Light

Layer 2

Analysis By: Adrian Leow, Avivah Litan

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Layer 2 protocols are off-chain solutions that enhance blockchain scalability by processing transactions outside the mainnet Layer 1 blockchain. They reduce transaction fees and increase throughput while trying to maintain security and decentralization. Various mechanisms are used in Layer 2 protocols, such as state channels, sidechains or roll-ups. Layer 2 aims to provide efficient and scalable transaction processing on blockchain networks.

Why This Is Important

Blockchain technology is inherently limited in its capacity to process transactions, since many protocols rely on consensus across all or a large subset of nodes. Layer 2 solutions can help address this issue as they are crucial for blockchain due to their scalability, privacy, security, and cost benefits. They enable offloading transaction processing to a separate layer, increasing throughput, reducing cost and preventing attacks. State channels, sidechains and plasma chains are common types.

Business Impact

Layer 2 solutions such as channels and sidechains allow applications that benefit from Layer 1 decentralization and security to operate at scale with lower transaction fees and faster throughput. Therefore, they enable innovations of applications that need these characteristics. However, this kind of layering also introduces additional complexity and governance challenges that it will take time to overcome.

Drivers

- As blockchain adoption continues to grow, the existing infrastructure may not be able to handle the increasing demand for transaction processing. This makes it necessary to explore Layer 2 solutions to increase the throughput of the network.
- Transaction fees on the main blockchain can become prohibitively expensive during times of high network activity, making it challenging for small-scale users to participate. Layer 2 solutions can potentially reduce the cost of using blockchain technology and can make it more accessible to a wider range of users.
- In some cases, Layer 2 solutions can process thousands of transactions per second, which is needed for Ethereum to achieve wider adoption.
- NFT-based games are driving blockchain adoption and demand for scalable blockchain solutions. This creates a need for Layer 2 solutions, such as the Ronin Ethereum sidechain developed and used for the largest NFT game, Axie Infinity.
- Scalable payment solutions are also driving Layer 2 solutions, for example the Lightning Network used for Bitcoin payments.
- Ethereum requires Layer 2 scalability solutions to achieve its full potential and become a global trust layer.
- Layer 2 solutions can enable new use cases and applications that may not be feasible on the main blockchain due to scalability and cost limitations, driving the need for their adoption in the blockchain ecosystem.

Obstacles

- Some Layer 2 approaches, while promising, have yet to be proven in terms of scalability, security and manageability.
- Some Layer 2 solutions can be centralized, which can introduce single points of failure and undermine the decentralized nature of blockchain technology. Sidechains are sometimes less decentralized than the mainnet, and sidechain validators can theoretically coordinate to act maliciously.
- Layer 2 optimistic roll-ups depend on fraud solvers to find fraud before transactions are committed to the mainnet. This model is not widely proven yet and delays transaction finality.
- Sidechain bridges to mainnets can be breached and don't guarantee the same security that a decentralized mainnet does. This was vividly illustrated in the theft of $625M by breach of the Ronin network bridge in 2022.
- If there is insufficient liquidity on a sidechain, it may be challenging to move assets between the sidechain and the main blockchain network, limiting their usefulness.

User Recommendations

- Evaluate Layer 2 solutions as a potentially valuable architecture for improving blockchain scalability and cost-effectiveness for your applications. Monitor the progress of current Layer 2 implementations such as optimistic and ZK roll-ups to determine the applicability of Layer 2 solutions for your use case.
- Evaluate the use of ZK roll-ups when transaction confidentiality is important to you.

Sample Vendors

Arbitrum; Connext Network; Ethereum; Optimism; Polygon; StarkWare (StarkEx); zkSync

Gartner Recommended Reading

Quick Answer: How Are Decentralized Applications Different From Regular Apps?

Innovation Insight: Web3 and dApp Architecture

Blockchain Intelligence and Analytics

Analysis By: Ray Valdes, Balaji Abbabatulla

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Blockchain intelligence and analytics tools and services deliver insights on the provenance and flow of transactions in the blockchain ecosystem. These are also known as blockchain forensics tools. The tools produce analyses and reports on transaction flows, holdings and identities, including linkages to off-chain data sources. They address requirements of different players in the blockchain ecosystem: law enforcement, enterprise compliance officers, regulators and investors.

Why This Is Important

The health of the blockchain ecosystem depends on analytics tools because the transaction flows can be more complex than those in traditional technologies. Blockchain intelligence and analytics tools improve visibility and can increase trust among all key stakeholders. Furthermore, the blockchain ecosystem includes different bad actors — scammers, hackers, tax evaders and others — whose activities need to be tracked by regulators and law enforcement. In addition, there are legitimate transaction flows that need to be analyzed to ensure compliance and to identify potential investment opportunities and trends.

Business Impact

The blockchain ecosystem is challenged in attracting new users due in part to the perception of lack of transparency in applications such as crypto exchanges. For users to adopt blockchain, there must be a threshold level of comfort with regard to safety and security of transactions and blockchain-related interactions. Blockchain intelligence tools help achieve that goal, by identifying bad actors for law enforcement, ensuring compliance with financial regulations, and monitoring and flagging problematic transactions with questionable participants.

Drivers

- As the blockchain ecosystem grows, and total value processed increases, there is a concomitant increase in bad actors and illicit activity. There is an increased need to search for patterns of fraud and criminal behavior, both for identifying and capturing perpetrators and for recovering stolen funds that have been sequestered.
- The evolving geopolitical climate, such as economic sanctions around the Russian invasion of Ukraine, has driven flows of funds toward cryptocurrency channels, increasing the need for blockchain analytics and forensics.
- Economic trends have led to certain nation states (North Korea) initiating systematic attacks and subterfuge on financial services, including blockchain DeFi protocols, in order to obtain hard currency. According to reports, the frequency and sophistication of attacks has risen (see 2022 Biggest Year Ever For Crypto Hacking, Chainalysis).
- Terrorist activities remain a serious concern for governments across the world. The nature of what is identified as "terrorist" has shifted in concert to changing political currents and rise of extremist politics that are different from years past. The need for tools to monitor and identify terrorist financing continues.
- Criminal activities such as illicit drug markets continue to expand, according to a UN report released June 2023 (see UNODC World Drug Report 2023 Warns of Converging Crises as Illicit Drug Markets Continue to Expand, UN). Drug trade patterns have shifted due to the Russian invasion of Ukraine and agricultural changes in Afghanistan. This means an ongoing need for analysis of money laundering and terrorist financing across all financial sectors, and specifically in the cryptocurrency sector.
- In the cryptocurrency sector, fraud and crashes such as FTX and Terra (LUNA) have increased demand for regulatory and compliance reporting solutions that can track and monitor blockchain-related transactions.
- Adoption is driven by the ability to improve trust among regulators and the need to convey safety of assets and identify potential investment opportunities to users.

Obstacles

- Growth in volume and diversity of illicit activities.
- Coin mixers like Tornado Cash and Blender.io used for money laundering have evolved. Sinbad is a new coin mixer based on Blender, according to a report by blockchain analytics firm Elliptic (see Has a Sanctioned Bitcoin Mixer Been Resurrected to Aid North Korea's Lazarus Group?, Elliptic).
- Further challenges in analyzing flows arise from use of cross-chain gateways, bridges, wormholes and Layer 2 chains, as well as privacy-oriented coins like Monero.
- Analytics tools can be expensive to procure and complicated to operate, requiring specialized knowledge that most enterprises lack.
- Addressing diverse needs requires a complete and powerful analytics system that combines both on-chain data across multiple chains, as well as correlation with off-chain data repositories.
- Correlating on-chain activity with off-chain data repositories can be a challenge in cases where data sharing agreements and licenses are required.
- Data volumes to track flows across multiple chains, exchanges and intermediary entities can consume significant resources for a blockchain analytics provider
- Shifting and potentially contradictory regulatory requirements in different jurisdictions can be a challenge to keep pace with.

User Recommendations

- Identify clear goals and requirements regarding blockchain intelligence and analytics, such as compliance, law enforcement, investment analysis or real-time transaction monitoring. Then evaluate and select the analytics tools that best align with your requirements.
- Do not rule out use of multiple tools from different vendors and services providers, used in combination with each other, to meet complex requirements for large organizations.
- Track on an ongoing basis the activities of bad actors, as well as the improvements in blockchain intelligence and analytics tools, to ensure that your evolving requirements will continue to be met.

Sample Vendors

BlockTrace; Chainalysis; Ciphertrace; Coinfirm; DMG Blockchain Solutions; Elementus; Elliptic; Kaiko; Scorechain; TRM

Enhanced Blockchain as a Service

Analysis By: Adrian Leow, Avivah Litan

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Enhanced blockchain as a service (eBaaS) is a cloud-based service that provides an application layer for developers to build, deploy and host their blockchain-based applications, functions and smart contracts. eBaaS abstracts the underlying blockchain infrastructure, enabling developers to focus on the application layer without having to worry about the underlying blockchain technology. It enables developers to deploy their applications across multiple clouds and blockchains.

Why This Is Important

eBaaS simplifies blockchain adoption for enterprises and accelerates deployments by providing a secure and scalable environment for app development and deployment. It offers standardized APIs and tools for easier development and integrates with existing enterprise systems. With robust monitoring and management capabilities, eBaaS ensures optimal operation, supports multiple blockchain platforms and provides greater flexibility and choice for developers and enterprises.

Business Impact

eBaaS unlocks new opportunities for businesses to leverage blockchain technology by reducing entry barriers, accelerating time to market and fostering business-related innovation. With the ability to integrate with existing enterprise systems, eBaaS can improve efficiency, security and transparency across industries, helping businesses stay competitive in a rapidly evolving digital landscape. eBaaS removes a good portion of the technical obstacles for businesses looking to take advantage of the benefits of blockchain technology.

Drivers

- eBaaS enables enterprises to focus on their applications without worrying about which blockchain and cloud to use, which smart contract development platform to use and how to connect legacy data to new Web3 applications.
- The benefits of unique blockchain features, such as smart contracts and immutable distributed ledgers, are much more accessible to enterprises when they use eBaaS, as they are shielded from most of the complexities of blockchain infrastructure and protocols.
- Low-code development environments enable developers to deploy applications quickly and avoid costly professional services.
- Some eBaaS vendors have off-the-shelf application templates that accelerate deployment for specific use cases.
- Blockchain application maintenance and performance monitoring are simplified through eBaaS services.
- Some eBaaS vendors support the relatively straightforward migration of applications from permissioned blockchains to public blockchains that support security through decentralization.

Obstacles

- Most eBaaS vendors support limited options for back-end blockchains, so users may be tied to the vendor's blockchains of choice. The historical lack of industry standardization across different blockchain platforms can make it challenging for businesses to select the best fit for their use cases, whether they use eBaaS or not.
- eBaaS vendors may lag in the adoption of public chain innovations unless their architectures are modular and open to allow easy integration of new capabilities.
- For a successful blockchain deployment, enterprises must participate equally with other organizations using their applications. eBaaS services may find it difficult to satisfy the requirements of multiple organizations.
- Enterprises participating in eBaaS (or any non-eBaaS application) must agree on data exchange formats, governance and permissions before deploying their applications.
- Enterprises are often confused on how they can use and benefit from blockchain technology in the first place. eBaaS can help guide them toward worthwhile business scenarios, but does not guarantee alignment.

User Recommendations

- Evaluate and use eBaaS services to accelerate the deployment of your applications, once you have agreed on business and process terms and addressed funding and governance issues with your ecosystem partners.
- Select an eBaaS provider that targets your use case or industry and has experience with it.
- Select an eBaaS provider that supports permissioned blockchain today, and which either can or is planning to support public blockchains in the future. This will ensure that your organization benefits from blockchain decentralization and fast-moving innovations in the public blockchain arena.

Sample Vendors

Alchemy; Fujitsu; IBM; Kaleido; NTT DATA; Oracle; SettleMint; Sky Republic; Vendia

Sliding into the Trough

Stablecoins

Analysis By: Balaji Abbabatulla, Avivah Litan

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Stablecoins are a type of cryptocurrency backed either by reserves of fiat currency/cryptocurrency or commodities like gold to offer stability and the flexibility of a digital asset. Algorithmic stablecoins are pegged to the supply-demand ratio of an on-chain protocol or cryptoasset determined by an algorithm.

Why This Is Important

Stablecoins act as a bridge between volatile cryptocurrencies and fiat currencies. Many exchanges enable transactions using stablecoins at a lower cost and with greater ease than fiat currencies. Thus, stablecoins enable users to engage in digital asset transactions without being concerned about the price volatility of cryptocurrencies.

Business Impact

Stablecoins that function reliably will encourage higher activity in the digital asset marketplace by:

- Delinking the value of a transaction from subsequent cryptocurrency price volatility.
- Providing relative price stability, thus making them more useful as a medium of exchange, a store of value, or a unit of account, as well as enabling more new players to enter the digital asset marketplace.
- Underpinning cryptocurrency markets and decentralized finance (DeFi) to encourage mainstream adoption.

Drivers

- Stablecoins attempt to maintain price parity against fiat currencies and hence are a solution to exchange value in cryptocurrency and other blockchain networks.

- Growth in DeFi and cryptocurrency trading has been a key enabler since they rely on stablecoins as a medium of exchange and also serve as collateral.
- Stablecoins offer a much more seamless and efficient payment initiation and settlement mechanism than the current payment mechanism supported by most blockchain solutions. Currently, most solutions initiate payment requests to a nonblockchain payment network, and they use APIs to interface with the payment networks as the payment networks clear and settle the payment.
- Blockchain solutions powered by stablecoins offer a highly efficient and user-friendly mechanism to replace current opaque and highly centralized applications. Such payment solutions offer initiators and recipients real-time visibility into the movement of their money, which will drive adoption.
- Regulations that are being deployed will drive consistent settlements globally, and country-specific regulations also will improve the trust in stablecoins.

Obstacles

- Failure of algorithmic stablecoins, such as TerraUSD (UST) due to large-scale unstaking and sell-offs or that of Fei (FEI) due to concerns about future regulatory risks, raises concerns about the longevity of such coins.
- Overheads due to upcoming regulations globally, and for specific countries, could make the business case for stablecoin issuers less attractive.
- Central banks that issue digital currencies may find stablecoins based on their reserved fiat currency a direct threat to their need to control their own currency issuance and circulation. Using government regulations, these central banks could hinder stablecoin operations and product innovation, should they pose any real or perceived threats to the financial system.
- U.S.-dollar-backed and other fiat-currency-backed stablecoins could become less stable if the value of the fiat currency itself destabilizes.
- Skepticism, especially among enterprises, about the business impact of blockchain-based solutions.

User Recommendations

- Prioritize stablecoins over cryptocurrencies for digital asset transactions to overcome the risk of cryptocurrency price volatility, as stablecoins are becoming an integral part of digital asset marketplaces.

- Create a cross-functional team, including finance, legal and treasury experts, to analyze the impact of upcoming global and country-specific regulations.
- For payment applications, prepare to integrate stablecoin payments with applications that require it (e.g., B2B blockchain applications or B2C sales applications in which customers want to pay with digital currencies). In addition, work with payment processors to integrate digital currency payment functions into existing processes.
- For leverage applications (such as lending and borrowing), ensure internal control and security requirements are satisfied by the service used for leverage functionality.

Sample Vendors

Binance (Binance USD [BUSD]); Circle (USD Coin [USDC]); Dai (DAI); Frax Finance (Frax [FRAX]); Gemini (Gemini Dollar [GUSD]); Paxos (Pax Dollar [USDP]); Tether (Tether [USDT]); TrueUSD (TrueUSD [TUSD]);

Gartner Recommended Reading

Bitcoin Goes Mainstream: What It Means to You

Define and Map Cryptocurrencies, Digital Currencies and NFTs to Future-Proof Your Digital Transformation

Zero-Knowledge Proofs

Analysis By: Mark Horvath, Bart Willemsen

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Zero-knowledge proofs (ZKPs) are privacy-preserving messaging protocols that enable entities to prove that information available to either or both of them is correct, without the requirement to transmit or share the underlying (identifiable or otherwise sensitive) data. ZKPs enable entities to prove information validity without the requirement to transmit personal or confidential data.

Why This Is Important

Following increasingly imminent digital threats and legislative data protection requirements, security and risk management (SRM) leaders must support use cases that enable digital business while ensuring in-use protection. These protocols limit the requirement for mass decryption/encryption of data elements, which benefits the efficiency of work — including potential adoption of blockchain-based systems.

Business Impact

ZKPs are being applied for many use cases, especially in the context of authentication and transaction verification. Other use cases include payments, decentralized identity, custody management, anti-money-laundering (AML), know your customer (KYC), consumer identity and access management (IAM), age verification, etc. With the addition of ZKPs to blockchain platforms, SRM leaders can cover information security use cases that require confidentiality, integrity and availability (CIA). Some blockchain platforms have evolved to include this.

Drivers

- Traditional data protection techniques typically focus on data in motion (i.e., transport layer security) and data-at-rest encryption. Data-at-rest encryption, as commonly implemented, does not provide strong protection from data theft and privacy disclosures. It is unable to secure data in use and data sharing scenarios.
- New use cases and maturing privacy legislation worldwide present new privacy and cybersecurity concerns that require data-in-use protection. There are also scenarios where the data itself does not need to be shared. ZKPs enable such data-in-use protection.
- Concerns about data security in several scenarios, including collecting and retaining sensitive personal information, processing personal information in external environments such as the cloud and information sharing.
- Privacy violations (due to the exposure of sensitive information).
- Need for mitigation of sensitive data leakage and cyberattacks.

Obstacles

- Even with a variety of web applications (e.g., ZKProof), ZKPs remain in an emerging state. They still require a common framework for applications to leverage.
- Only a limited number of practical implementations have emerged to date.
- The variety of methodologies and the multiplicity of approaches to data management inhibit adoption. ZKPs will need to scale at the rate of blockchain transactional volumes to be effective.
- ZKPs require integration into applications. Downstream applications, such as CRMs and databases, will need some modification.
- Some ZKPs, like ZK-SNARK, have a dependency on existing encryption/hashes (ECDSA in this case) as part of their implementation. This adds a potential complexity in upgrading them to quantum-safe protocols and limits available staff/experts.

User Recommendations

- Work with SRM leaders to gain a deeper understanding of the nature of these controls, understanding that ZKP techniques are a paradigm shift.
- Be realistic with the current immaturity of ZKP solutions and approaches when evaluating ZKP benefits for privacy protection.
- Evaluate how ZKP 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.

Sample Vendors

DropSecure; Evernym; IBM; Ligero; Microsoft; Ping Identity; QEDIT; Sedicii; StarkWare

Gartner Recommended Reading

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Emerging Tech: Assess Zero-Knowledge Proof Technologies to Strengthen Competitive Advantage in Decentralized Ecosystems

Predicts 2022: Privacy Risk Expands

Top Strategic Technology Trends for 2022: Privacy-Enhancing Computation

Blockchain and IoT

Analysis By: Nick Jones, Avivah Litan

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Blockchain and the Internet of Things (IoT) describes blockchain technology used in conjunction with IoT devices or IoT-enabled solutions.

Why This Is Important

Blockchain and related technologies, such as non-fungible tokens (NFTs), enhance the IoT. Examples include machine commerce, identity management, tokenization of IoT devices, assets or services, identity validation, provenance tracking, data authentication, IoT infonomics, and secure firmware updates. This technology will enable enterprises to create new digital business offerings and ecosystems, and to manage challenges (e.g., proving provenance or compliance) in new ways.

Business Impact

Blockchain can provide a decentralized mechanism to support a wide range of IoT activities — for example, providing trusted machine identity and immutable data audit trails. It also supports peer-to-peer IoT business activities (e.g., when IoT devices make payments, measure temperatures, provide services or create digital assets). IoT devices and the data or services they provide can be represented as digital assets in the form of NFTs to support innovative business models.

Drivers

- The IoT's creation of new forms of digital assets, which must be tracked, exchanged or monetized.
- The IoT's participation in advanced business models involving distributed applications (aka dapps) and smart contracts.
- IoT devices need to share trusted immutable information with an ecosystem of business partners and other machines — for example, for product provenance and tracking, supply chain applications, or for measuring greenhouse gas (GHG) emissions.
- IoT devices need an immutable audit trail logging their actions, system updates, etc.
- An IoT device needs strong proof of identity of itself and of other IoT devices with which it communicates (e.g., for warranty management or data authentication).
- Many IoT devices, data and services are effectively digital assets. NFTs that support smart contract automation provide a framework for such tasks as IoT management, machine payment and data ownership that are more advanced than simple blockchain distributed ledgers.
- As blockchain technologies mature, they're being embedded increasingly in more-business-oriented vertical solutions that reduce the cost and risk of adoption.
- Blockchain technology is used by the new smart home standard "Matter" to validate the authenticity of devices.

Obstacles

- Blockchain/IoT integration is immature, and faces challenges in areas such as scalability.
- Many IoT devices are computationally simple, with limited networking bandwidth. Hence, they are unable to act as primary blockchain nodes, so they rely on proxies or gateways; this introduces risk and complexity.
- Blockchain is overkill when immutable data storage is all that's required. In such cases, consider centralized immutable databases or ledgers (e.g., Amazon Quantum Ledger Database [QLDB] or SQL Server features).
- Public blockchains can have forks, posing challenges if it implies updates to large numbers of resource-constrained, long-lived IoT devices.
- Many IoT applications and data aren't critical enough to warrant the use of blockchain. Simpler alternatives include encrypted data and signed firmware updates.
- Domain immaturity means vendors tend to change strategies and business models frequently.

User Recommendations

- Look for situations in which the IoT and blockchain enable new business capabilities and solve real-world problems, and where the technology's immaturity and rate of change aren't impediments.
- Ensure that there are no simpler alternative solutions, because combining blockchain and IoT can be complex. Focus on simple applications, such as ensuring provenance, proving identity, and securing system or data updates.
- Beware of applications involving long-lived IoT devices and data, which will require the ability to periodically deploy blockchain technology updates at scale.
- Seek prepackaged vertical solutions, rather than trying to develop blockchain IoT systems from first principles.

Sample Vendors

Filament; Helium Foundation; IBM; IOTA Foundation

Gartner Recommended Reading

Predicts 2022: Prepare for Blockchain-Based Digital Disruption

Quick Answer: What Are Suitable Projects for Blockchain Technology?

Top Five Reasons CIOs Should Care About Blockchain

Blockchain Oracles

Analysis By: Avivah Litan

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Blockchain oracles are services that support the secure interaction of smart contracts with systems external to a blockchain (or distributed ledger). Oracles enable smart contracts to automate transactions based on real-world data and external events. They enable, for example, the fetching of commodity prices and notifications of changing interest rates.

Why This Is Important

Oracles enable blockchain smart contracts to interact with real-world events, thus integrating blockchain networks to the external world. As distributed ledgers and smart contracts do not have a mechanism to interact with, or process data from, the external world, decentralized oracle networks can help build a trusted mechanism to utilize blockchains in business processes. They contrast with APIs, which represent centralized points of potential compromise.

Business Impact

The availability of reliable and effective blockchain oracles will play a crucial role in the integration of smart contracts with real-world assets and events. Once participants in a blockchain network recognize and trust the authority of an oracle, blockchain business processes can operate without supervision of data inputs and outputs to/from smart contracts. This unsupervised operation can deliver on the promise of blockchain efficiency and trust minimization.

Drivers

- **Recognition of smart contracts' value in reducing transaction costs:** Smart contracts, by reducing human recording, authentication and reconciliation of business transactions, enable a significant increase in the granularity and efficiency of transactions. Blockchain oracles provide necessary controls, triggers and off-chain computation for automating trustless smart contract operations.
- **Decentralized oracle systems provide trusted transaction triggers in support of processing:** Decentralized oracle networks provide security for interfaces between off-chain events and on-chain smart contracts. Multiple nodes participate in validating and processing inputs to smart contracts and the outputs they generate.
- **Needed security:** Decentralized oracle interfaces to blockchain smart contracts are needed in light of severe hacks against centralized interfaces. Sufficient decentralization will mitigate security risks posed by illegitimate data interfacing with smart contracts.
- **Trustworthy data:** Decentralized oracle systems reach consensus on the data that is used to feed smart contracts. This mitigates the risk of incorrect data coming from a single source into a smart contract, which could have damaging consequences. For example, an incorrect exchange rate provided by a single "bad" source could force collateralized loan liquidations that would not occur if the correct exchange rate had been fed into the lending smart contract via a decentralized oracle network.
- **Increasing adoption of decentralized applications (dapps),** which will drive growth in blockchain oracles as they play a critical role in enabling dapp interactions between external systems and smart contracts.

Obstacles

- Integrating existing systems of record and data with blockchain oracles is challenging. Enterprises have internal systems of record, typically built on robust, but dated, systems and software. These systems must be updated to ensure they can interface with blockchain oracle systems.
- Blockchain oracles are dependent on the information sources they draw from. If these data sources are compromised and the network is not sufficiently decentralized, oracles could report falsified transaction events. These falsified events could, for example, cause payments to pass without delivery of products or services.
- If a smart contract commits an incorrect transaction to a blockchain, it is difficult to adjust the records. In cases not involving anonymous parties, the transaction can be reversed by an appended counter transaction.
- There are very few decentralized blockchain oracle network protocols. The market needs more competition to ensure long-term viability for blockchain participants.

User Recommendations

- **Identify integration needs between systems of record with blockchain oracles.** For enterprises, integration of oracles with existing systems of record is critical for a successful blockchain implementation. This integration is not a trivial exercise, so develop plans to identify contact points and define changes where necessary.
- **Build appropriate integrity and reliability mechanisms into blockchain oracle systems.** Unless sufficiently decentralized, blockchain oracles are at risk from lost or corrupted input signals that can trigger fraudulent transactions or suppress legitimate transactions. Choose oracles by carefully selecting and validating their state of decentralization and security.
- **Create processes to adjudicate and reverse incorrect transactions by creating new ones.** When a participant comes to you reporting a failed transaction, you need a predetermined agreement for handling this issue.

Sample Vendors

Band Protocol; Chainlink; DIA; XYO Network

Gartner Recommended Reading

Managing the Risks of Enterprise Blockchain Smart Contracts

How to Mitigate Web3 Blockchain Risks and Security Threats

Guidance for Blockchain Solution Adoption

Blockchain Interoperability

Analysis By: Avivah Litan

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Blockchain interoperability represents the functionality needed for entities to seamlessly interact and interoperate across multiple blockchains — for example, by transferring assets and information from one blockchain network to another. These entities include applications, services, software, systems, processes and organizations.

Why This Is Important

Blockchain platforms do not natively interoperate. This means users must carefully choose the platform they build their applications on, as the partners and protocols they need to interact with must reside on the same platform. This is an impractical and suboptimal environment for a thriving ecosystem. The need to share information across different blockchain networks will become more important as the use of blockchain grows.

Business Impact

Blockchain interoperability enables individual markets to thrive by expanding markets they can easily access. Users and services can trade assets and information across blockchain networks with other participants and services. The cross-chain network is more powerful than the sum of individual blockchains because of the network effect. For example, an issuer of a tokenized bond that resides on one blockchain will be able to sell the bond to a user trading in other blockchain-based bond markets.

Drivers

- Disparate blockchain networks are growing individually in their own separate ecosystems. As transaction volume grows, these networks will need to securely interoperate. Solutions must prevent double spending when transactions are posted from one blockchain to another, and must ensure transaction finality.
- More secure solutions for blockchain interoperability continue to gain adoption and minimize the attack surface when compared to most cross-chain bridges. These include special purpose “blockchain of blockchain” networks such as Polkadot or Cosmos and new smart contract messaging protocols, such as those from LayerZero.
- Users and networks need to interact with each other. For example, supply chain networks on one blockchain platform must interoperate with supply chain and logistics networks on other blockchains.
- Payment volume across the globe is migrating and growing on blockchains due to growth in cryptocurrencies, stablecoins and central bank digital currencies. Global payment demand is driving the need for blockchain network interoperability.
- Extensibility of decentralized identity use cases will greatly benefit from blockchain interoperability.
- Decentralized applications on decentralized finance (DeFi) networks, primarily Ethereum or Ethereum virtual machine (EVM) compatible, also need to interoperate with different blockchain networks so that information and assets can be freely traded and shared with expanded markets.

Obstacles

- Interoperability options have mainly been developed for public blockchain cryptocurrency use cases and some non-fungible token (NFT) trading. Enterprise requirements have not yet been fulfilled by most of them. Interoperability is not important yet in most enterprise blockchain projects due to low transaction volume.
- Crypto interoperability bridges on public blockchains are a prime target of hackers who have stolen hundreds of millions of dollars' worth of cryptocurrency from these bridges.
- Interoperability is not important yet in most enterprise blockchain projects due to low transaction volume.
- The absence of widely accepted standards for blockchain interoperability is a significant challenge. Different blockchain networks are often developed by competing organizations with different business models, interests, and goals. This can create a lack of incentive for these organizations to collaborate which will help interoperability succeed.

User Recommendations

- Experiment with different blockchain interoperability protocols by working with systems integrators or protocol development teams that can help you integrate these interoperability options with your applications.
- Favor interoperability options that minimize a hacker's attack surface, for example, by limiting potential hacks to one smart contract at a time. Favor interoperability options that provide a layer of abstraction middleware to your applications and handle the complexities of interoperating across blockchains.
- Be careful when using cryptocurrency bridges that aggregate assets to support interoperability. Try to validate their security standards and practices and seek insurance on your assets if you use them.
- Prioritize "blockchain of blockchain" network solutions if you are building an entire use-case-specific ecosystem that will need to interoperate with other use-case-specific ecosystems that are integrated into the same "blockchain of blockchain" network.

Sample Vendors

Axelar; Cosmos; LayerZero; Polkadot; Quant Network

Gartner Recommended Reading

Emerging Tech Impact Radar: Blockchain and Web3

Guidance for Blockchain Solution Adoption

Decentralized Exchanges

Analysis By: Ray Valdes

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Decentralized exchanges (DEXs) use decentralized protocols to enable peer-to-peer cryptocurrency exchanges that operate without intermediaries to complete transactions. In contrast to centralized exchanges, DEXs do not support any custodial or know-your-customer (KYC) services. Instead, users rely on their decentralized identity (embodied in their digital wallet) when transacting on DEXs.

Why This Is Important

DEXs support trustless, smart-contract-based, peer-to-peer trading and direct access to decentralized finance applications. DEXs enable users to trade tokens outside of a centralized exchange, leading to increased market adoption of blockchain and cryptocurrency, as it becomes available to a wider audience.

DEXs can provide new opportunities for the unbanked across the world, as they can promote financial inclusion, allowing anyone connected to the internet to exchange value (digital assets), regardless of location or political environment.

Business Impact

In May 2023, there were over 380 DEXs. The leader, Uniswap, recorded $535M in daily trading volume. Back in 2019, Uniswap trading volume grew 15000%. In April 2023, volume on Uniswap exceeded Coinbase, the leading centralized exchange (CEX), for four months straight, proving the viability and disruptive power of innovative DEXs over traditional CEXs.

Uniswap runs on Ethereum. Other blockchains have launched their own DEXs, and as a result, the overall ecosystem has improved, in terms of user growth and decentralization of value exchange.

Drivers

- Innovation in decentralized finance (DeFi) markets is rapid, and DEXs are often needed to support and access the evolving portfolio of services. Innovations, such as liquidity pools, automated market-making mechanisms and order books, solve liquidity-related problems. They are responsible for the rapid growth of DEXs and the increased popularity of DeFi protocols, as users access DEXs to gain financial rewards from DeFi products and services.
- DEXs provide trustless and efficient peer-to-peer transactions executed by neutral and transparent smart contracts. This is in direct contrast to centralized banks and exchanges where layers of central authority must be trusted, even though their inner workings and policies are opaque.
- Compared to DEXs, transactions on centralized systems are not fully transparent and cannot be tracked and traced through their life cycle. This transparency is a major driver of DEX adoption.
- DEX transactions are pseudonymous, meaning there are no KYC processes on DEXs. This is a major driver for users who want to retain control over their identity and finances.
- Transaction fees on DEXs are much lower than on centralized exchanges where users pay overheads and administration costs to central authorities and intermediaries.
- DEX traders typically manage their own self-hosted wallets and private keys, in contrast to centralized exchanges that give control to central entities that may block or seize funds.
- DEXs give buyers and sellers access to hundreds of liquidity pools, cryptocurrencies and financial instruments that are not listed on centralized exchanges.

Obstacles

- DEX smart contracts strongly attract hackers due to high-value traded assets, and recovery of stolen funds can be a problem. Notably, Uniswap smart contracts have never been hacked, despite years of effort by motivated hackers.
- Regulators continue to evaluate DEXs along with stablecoins commonly used in liquidity pools. Future regulations could hinder market growth.
- Casual users might find DEX UIs difficult to navigate. Typographical errors and data entry mistakes in addresses and keys may lead to permanent loss of funds.
- Users must learn to connect self-hosted wallets to DEXs and fund them through various complex cryptocurrency transfer protocols. For example, Bitcoin (BTC) is not native to Ethereum, and thus, must be “wrapped” into a BTC-equivalent coin before trading. In contrast, centralized exchanges provide an intermediary service to cover the issue.
- Most DEXs do not interface with banking systems, so it is cumbersome to get fiat money into DEXs and move cryptocurrency back into bank accounts.
- DEX scalability is subject to underlying blockchain network throughput and network fees.

User Recommendations

- Wait for existing centralized financial services to interface with DeFi applications before letting your organization engage with DEXs so that decentralized trading activities can be protected with regulations and legal frameworks and UIs can improve.
- Evaluate smart contract insurance that can protect assets you have in DeFi against smart contract hacks or design flaws, if you engage in decentralized trading on DEXs before regulatory frameworks are in place.
- Stay abreast of developments in DEXs by monitoring them on websites such as DefiLlama, Messari or DeFiprime.com.

Sample Vendors

1inch Network; Curve Finance; dYdX; Kyber Network; Madfish; Orca; PancakeSwap; SushiSwap; Uniswap; Vertex

Gartner Recommended Reading

Emerging Tech Impact Radar: Blockchain and Web3

Decentralized Identity

Analysis By: Michael Kelley, Akif Khan, Arthur Mickoleit

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Decentralized identity (DCI) allows an entity to control their own digital identity by using decentralized identifiers (DIDs) to connect and authenticate themselves to other entities. Private keys and verifiable credentials (VCs) are contained in digital wallets, supported by an identity trust fabric for making DIDs discoverable. By establishing trust, privacy and security, DCI is an attractive alternative to traditional models of storing, sharing and verifying identity data.

Why This Is Important

Identity fragmentation is a problem due to service providers (banks, retailers and governments) forcing consumers to create individual identities for every service. DCI offers an attractive approach with increased security, privacy and usability compared to traditional digital identity approaches like federated identity. While legislative efforts to secure privacy and ensure interoperability are multiplying around the world, standards continue to be refined, and DCI use cases continue to emerge.

Business Impact

Users gain greater control of their identities and data, and service providers gain higher trust, speed and confidence. Currently, providers collect huge amounts of identity information about users to increase assurance to an acceptable level. DCI can provide trust, security, privacy and convenience, and can provide portability of identity data for end users without needing centralized data, reducing risks of data breaches, account takeovers and privacy compliance violations.

Drivers

- Vendor investments in DCI: Due to the volume and influence of vendors investing in this space, there is high potential to drive the DCI market forward, and significant investments have been made by IBM, Microsoft and Ping Identity. In addition, Gartner has been tracking more than 80 startups and vendors of DCI technologies and DCI components (e.g., digital wallets and trust fabrics).
- Government activity: Public sectors are increasingly shaping digital identity trends around DCI. The EU, national governments like Finland or Canada, as well as states and provinces like Utah and Ontario are actively pursuing and investing in DCI use cases that span public and private sector interests.
- Privacy regulations: Countries continue to formalize the requirement for user privacy, specifically for collecting and securing large amounts of user data through regulations. DCI provides a more user-centric way of complying with privacy regulations through decentralized user data.
- Client and overall market interest in DCI: Interest is increasing due to attractive elements such as the ability to enable new digital business opportunities while maintaining client privacy. For example, using DCI to share verified claims, such as age/income, employment status, professional credentials, educational credentials without exposing sensitive personal data.
- Standards: Standards are maturing, led by entities such as the World Wide Web Consortium (W3C), the Decentralized Identity Foundation (DIF), the OpenWallet Foundation and OpenID for verifiable credentials to create a consistent approach to DCI. Expanding and maturing standards will help move the market forward.
- User experience: Asking users to repeatedly go through identity proofing and affirmation processes for every online interaction with a service provider is a broken model. Significant friction can be removed from UX if users could assert their identity using a digital wallet with full control over their identity data.

Obstacles

- Authority of issuers: Ensuring that an organization is authoritative to issue a VC (e.g., only an accredited facility issuing educational credentials).
- Adoption: Service providers may resist accepting identity claims via DCI unless they see user adoption, and users may be reluctant to adopt DCI wallets unless they see meaningful use cases for them.
- Interoperability: Adoption is slow due to most development taking place in pockets and a continued lack of standards.
- Technical challenges: Concerns about performance, interoperability, scalability and maturity, as well as wallet standards.
- Regulations: More work is required for how verifiable claims can be used in regulated use cases such as KYC, as required in financial services, online gambling and other industries. Governments are exploring regulatory needs for citizen interactions.
- User interface challenges, ID proofing and account recovery processes are vulnerable for security and privacy, and will require standard approaches.

User Recommendations

- Explore use cases for verifiable claims by identifying tasks and processes that are expensive, complex and time-consuming in the real world, which will benefit from a verifiable claims approach.
- Build a business case for trialing acceptance of DCI by targeting reduced identity proofing and affirmation costs and an improved UX.
- Identify attainable use cases through following successful POCs, such as a DCI solution focused on remote employee onboarding, educational credentials, health credentials and passwordless authentication.
- Partner with existing vendors to understand the possibilities and potential of DCI. Track government activities around use cases for citizen IDs.
- Be cautious of overly optimistic vendor claims. Evaluate the technical security aspects of centralized and partially decentralized identity trust fabrics or using blockchain platforms under consideration. In particular, examine vendor plans for support of standards, such as W3C, DIF and the OpenWallet Foundation.

Sample Vendors

1Kosmos; Evernym; IBM; IdRamp; Microsoft; Nuggets; Ping Identity; Scytale; SecureKey; Wise Security Global

Gartner Recommended Reading

Guidance for Decentralized Identity and Verifiable Claims

Innovation Insight for Decentralized Identity and Verifiable Claims

Predicts 2023: Users Take Back Control of Their Identities With Web3 Blockchain

Top Trends in Government for 2022: Digital Identity Ecosystems

Retail CBDC

Analysis By: Christophe Uzureau, David Furlonger, Peter Ryan

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

A retail central bank digital currency (CBDC) is a digital currency issued by a central bank as an account-based system or a fiat token, and distributed via digital wallets at the central bank or at affiliated and licensed financial institutions. As it has a central bank liability, it is often referred to as digital cash. It is open to be used by the public and companies.

Why This Is Important

Most central banks look at retail CBDCs as a way to improve financial supervision and inclusion, the effectiveness of monetary policy, reduce systemic risks and improve compliance. For banks and their clients, a retail CBDC would impact banking interfaces, ERP and treasury systems, and also lead to adjustments in product pricing and loyalty programs.

Business Impact

Banks and their clients need to pay attention to the degree of programmability. For example, Banco Central do Brasil selected nine projects, including the use of smart contracts to support programmable money, which would impact banks' payment, risk management and loan origination operations (see Central Bank of Brazil Chooses Nine Institutions to Study Digital Real Possibilities, Bitcoin.com). The programmability of a retail CBDC could deal with financial inclusion (notably for microbusinesses) driving the demand for banks' embedded finance solutions.

Drivers

- The drivers for retail CBDCs vary per country and may have divergent impact on commercial banks; however, the objective is to retain or augment the role of the central bank in the financial services ecosystem and maintain two-tier market structures (in part as a defense against decentralized finance).
- For example, in China, the digital yuan is part of an effort to level the playing field in the digital payment space and dilute the market power of Alipay (Ant Group) and WeChat Pay (Tencent). In the Bahamas, the Sand Dollar was launched as part of creating a more resilient payment system.
- The announcements by central banks to experiment and develop CBDCs are raising interest in offline payment solutions that attempt to replicate the capabilities of cash. For example, the Central Bank of The Bahamas launched its retail CBDC in December 2020, enabling offline transactions (see History, Sand Dollar).
- The development of CBDCs is also associated with the use of smart contracts to inject some programmability into payment value chains and support the design of programmable money. This enables new use cases and models such as developing rural finance (Brazil), dealing with specific commercial value chains (China). For example, Bank of China, Chengdu, uses smart contracts to manage the deposit for extracurricular school activities.
- Financial inclusion is also an important driver in markets with less developed payment and banking infrastructures, such as Bank of Jamaica's JAM-DEX and Central Bank of Nigeria's eNaira. Where a retail CBDC is used to improve financial inclusion, banks offering CBDC accounts can gain new customers and their retail CBDC payment history can be used as data for credit decisions.

- The real-time settlement properties of CBDCs are being explored to reduce administration associated with complex transactions. For example, using a smart contract in a retail CBDC to synchronize the settlement of the different legs of a property transaction.

Obstacles

- The creation of a CBDC requires new legal frameworks and potentially adjustments to risk management and core systems.
- Retail CBDCs impact geopolitics and the ability of smaller economies to control monetary policy and risks facilitating capital flights, thus destabilizing local economies.
- Most central banks are looking at a two-tier model that involves commercial banks, who are worried about the risk of disintermediation and increasing funding costs.
- Political debates surrounding the use of programmability and traceability will delay development.
- Consumers are reluctant to change their payment habits, and customer education will also be a challenge since some targeted customer cohorts are the least literate with respect to technology and finance.
- The creation of a new CBDC demands updating existing compliance processes (anti-money-laundering/know your customer), launching new authentication and authorization services, and educating the financial services workforce.

User Recommendations

- Prepare to launch digital wallet functionality for retail CBDCs, depending on the plans of the central bank, to capture the velocity of money (and data) in new transactional environments (machine to machine and smart cities).
- Plan to integrate the retail CBDC wallet into the existing digital banking/mobile banking capabilities.
- Plan now for a dedicated customer onboarding experience by focusing on the management of new identity document requirements initiated by the retail CBDC.
- Use retail CBDC financial inclusion initiatives to gain market share.
- Prepare for a modernization of the money management and credit scoring tools to accommodate the transactional data generated by the retail CBDC.
- Participate in CBDC initiatives that involve the use of smart contracts to drive the programmability of money and to get exposure to related regulatory considerations.
- Explore use cases that leverage the real-time settlement properties of retail CBDCs to reduce the administration costs for corporate customers.

Sample Vendors

Bitt; ConsenSys; Giesecke+Devrient; Hyperledger Foundation; MIT Digital Currency Initiative

Gartner Recommended Reading

Creating Business Value From Central Bank Digital Currencies

Banking CIOs Must Prepare Now for the Programmability of Money and Data

Top Technology Payment Trends Driving Change for Banking CIOs for 2023

Define and Map Cryptocurrencies, Digital Currencies and NFTs to Future-Proof Your Digital Transformation

How to Model the Programmable Economy to Assess Digital Business Growth Opportunities

Web3

Analysis By: Avivah Litan, Adrian Leow

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Web3 is a new stack of technologies, business and governance constructs that support decentralized web applications that enable users to control their own identity and data. 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 partly decentralized web.

Why This Is Important

Web3 enables new business and social models. Smart contracts run applications that eliminate intermediaries and administrative overhead controlling centralized entities. Tokens (including cryptocurrencies) power the business models and economics of Web3 and are built into blockchain protocols. Web3 provides building blocks for new types of applications. It supports user ownership of their data and content, and new business opportunities, such as authenticating and tracking carbon emissions data.

Business Impact

Web3 offers new features to manage digital assets and ownership rights for content creators. Other benefits include:

- Trustless transaction verification
- Smart contract automation of shared processes
- Tokenization of digital or physical assets
- Self-sovereign identity

Existing Web3 applications, such as decentralized finance (DeFi), and non-fungible tokens (NFTs), have yielded previously unachievable benefits for everyday users, investors, artists, content creators and communities.

Drivers

- Blockchain infrastructure is becoming more mature, scalable and cost-efficient to support mainstream usage. For example, Ethereum transitioned to a new consensus mechanism in September 2022, resulting in over a 99% drop in its energy consumption.
- Web3 empowers content creators to sell their work in the form of NFTs that ensure they — and not intermediaries — are paid for their work based on contract terms they set themselves whenever, for example, they sell an artwork.
- Tokenization of real-world assets can benefit from Web3 applications, and early adopters are realizing new business benefits that were not possible before. For example, the tokenization of carbon certificates and credits is helping Williams, a natural gas infrastructure company, its partners and customers lower their carbon footprint.
- Web3 apps are useful for authenticating and trading data. For example, blockchain marketplaces are used for managing IP portfolios (see IPwe) and fixed-income portfolio management (see Goldman Sachs' Digital Asset Tokenization Platform).
- DeFi protocols, such as Aave and MakerDAO, provide users with lending and borrowing services run by smart contracts that eliminate the need for intermediaries, thereby enabling higher yields and returns, albeit with much more risk.
- Brands are realizing new revenue streams with Web3 apps, especially with NFT issuance and sales.

Obstacles

- Web3 poses many risks, such as lack of customer protections, security threats and swings toward centralized control. Although future internet technologies will be more decentralized, they will not eliminate centralized authorities from enterprise B2B and B2C applications.
- Enterprises are unwilling to give up control of most business applications. We expect enterprises to continue using Web 2.0 for most applications through 2030, and layer Web3 technologies on top of them in a Web 2.5 configuration.
- Some early Web3 activities have achieved success, but much work remains to improve performance, governance, risk management and user interfaces. Additionally, success in well-established industries remains sparse.
- The current lack of widely applicable Web3 business applications for enterprises is hindering enterprise adoption of Web3.
- Lack of clear regulatory frameworks in the United States and some other countries continues to hinder Web3 innovation and user adoption.

User Recommendations

- Pay attention to innovative and successful Web3 initiatives and use cases in areas such as tokenization of real-world assets, decentralized identity, DeFi, art, entertainment and sports for ideas and partnerships.
- Keep abreast of developments in Web3 protocols and standards by monitoring the initiatives of Ethereum and Web3 Foundation for blockchain and distributed ledger technologies.
- Evaluate and pilot blockchain applications that implement a Web3 vision by giving end users control of their own identity data and compliant access to Web3 apps. These applications include decentralized identity, verifiable claims, cryptocurrency payments and investments, and new apps that are yet to appear.
- Evaluate projects that use Web3 technologies layered on top of Web 2.0 applications, giving organizations the ability to leverage unique Web3 features, such as smart contracts and tokenized assets, retaining process control.

Gartner Recommended Reading

FAQ for NFTs on Blockchains and Web3 Ecosystems

FAQ for Cryptocurrencies on Blockchains and Web3 Ecosystems

Quick Answer: What Is Web3?

Web3 and the Metaverse: Incomplete but Complementary Visions of the Future Internet

Secure Multiparty Computation

Analysis By: Joerg Fritsch, Bart Willemsen, Brian Lowans

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Secure multiparty computation (SMPC) is a method of distributed computing and cryptography that enables entities (e.g., applications, individuals, organizations or devices) to work with data, while keeping data or encryption keys in a protected state. Specifically, SMPC allows multiple entities to share insights while keeping identifiable or otherwise sensitive data confidential from each other.

Why This Is Important

Security and risk management (SRM) leaders struggle to achieve a balance between data security and privacy when processing (personal) data. This is further complicated by regulations and business objectives. Historically, data protection has focused on securing data at rest and in transit. However, SMPC-based methods introduce data protection in use, much like homomorphic encryption. It supports processing of data confidentially in analytics and business intelligence, using untrusted computing environments.

Business Impact

Due to their reliance on data for artificial intelligence (AI)-based decision making and the sharing of insight from those decisions among multiple parties, SRM leaders need privacy-enhancing approaches to protect data amid an evolving landscape of maturing data protection regulations. SMPC supports the secure enablement of business, enabling organizations to uncover and exchange information, while addressing security and privacy concerns.

Drivers

- Traditional data-at-rest encryption, as commonly implemented, does not provide strong protection against theft and data breaches. It is incapable of securing data in use and data-sharing scenarios.
- SMPC-enabled data security enables the protection of data while in use, providing SRM leaders with another data protection technique. This can be applied to new and existing use cases (e.g., multiparty information sharing).
- New use cases — such as big data analytics, AI or machine learning (ML) model training — present new privacy and cybersecurity concerns that require data-in-use protection.
- Concerns about data security in several scenarios, including collecting and retaining sensitive personal information, are driving SMPC adoption.
- SMPC helps ease fear of privacy law violations (due to the accidental exposure of sensitive information).
- SMPC supports the mitigation of sensitive data leakage, and the overall reduction and mitigation of cyberattacks.

Obstacles

- Commercial SMPC implementations have not reached the end customer traction they could have had because implementations do not frequently match clients' needs. For example, commercial implementations may only be applicable to selected identifiers, or be only practical to protect smaller amounts of data, such as encryption keys.
- Low-end customer awareness or traction for products based on SMPC technologies outside certain niches (e.g., encryption key management or DSaaS for advanced analytics of numerical data).
- When compared with existing techniques (i.e., cryptography based on hardware-generated and stored keys), end customers could have potential issues with audits, like when their accreditation authority is not familiar with SMPC.
- If the obstacles are not addressed successfully to reignite end customer interest, SMPC will most likely head into obsolescence and will need to be removed from the Hype Cycle for data security.

User Recommendations

- Work with developers/architects to establish a high-level position on SMPC relevance and a vision for future adoption, including proofs of concept (POCs).
- Evaluate use cases such as cloud computing, focusing on confidentiality with data in a cloud environment; privacy-enhancing (personal) data analytics initiatives; and cryptographic key protection, including encryption key management initiatives (i.e., for protection of data at rest). Also look at secure and private data mining for data and analytics use cases, including data lake security and blockchain security (e.g., wallet protection and/or quorum-based multisignature operations).

Sample Vendors

Baffle; Cybernetica; Inpher; IXUP; LiveRamp; Nth Party; Ziroh Labs

Gartner Recommended Reading

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Tokenization

Analysis By: Balaji Abbabatulla, Avivah Litan

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

A blockchain-based token is a cryptographically secured representation of any asset — physical or virtual — on a blockchain network. Users can create (or mint) tokens, assign unique ownership, prevent duplication, transfer or trade such assets, and remove (or burn) tokens from circulation on blockchain networks. In addition, tokenization through blockchain offers the additional features of fungibility, programmability and fractionalization.

Why This Is Important

A digital representation of physical or virtual assets enables enterprises to identify, track and manage such assets more efficiently. Blockchain-based tokens offer additional security compared to contemporary token management applications and create opportunities for enterprises to participate in new business models. Advanced capabilities, such as programmability or fungibility, enable enterprises to be prepared for the new digital world that is beginning to emerge.

Business Impact

Every physical or virtual asset will need to have a digital identity and have the ability to interact with other digital entities in the emerging world. Advanced capabilities such as programmability will make blockchain-based tokens the preferred tokenization technology. While current deployment is largely confined to cryptocurrencies and decentralized finance (DeFi), Gartner's case-based research indicates early investments in other use cases, such as cleantech, local governments, gaming and the metaverse.

Drivers

- **Adoption of innovative business models** — Enterprise leaders are actively exploring innovative business models to enable growth despite economic and business uncertainties. Participation in digital marketplaces and investing in intelligent applications powered by generative AI is emerging as a top trend among enterprises. Autonomous participation in such initiatives requires a high degree of trust, security, fungibility and programmability that blockchain-based tokens can offer.
- **Maturity of the blockchain technology ecosystem** — The underlying components of the blockchain-based solution ecosystem, such as wallets, smart contracts and oracles that power tokenization, are maturing. Users and product leaders of solution providers are becoming more conversant with the roles of these ecosystem components.
- **Improving awareness of risks and benefits** — Growth in deployment of tokens for cryptocurrencies and DeFi is leading to increasing awareness of the benefits and the risks of tokens among users, developers and regulators. Blockchain forensics solutions are enabling higher confidence among regulators about their ability to trace events on a blockchain network.
- **Increasing support for tokens across blockchain platforms** — The Ethereum platform has provided a foundation for a variety of token projects. ERC standards have been broadly accepted and support a variety of token scenarios. Other platforms, such as Hyperledger and Cardano, have started offering native tokenization capabilities.

Obstacles

- **Early adoption of autonomous digital business** — Adoption of autonomous, decentralized digital business requires a significant change in traditional ways of doing business. While such change is easier to implement for newer business models, such models account for a relatively small share of business.
- **Lack of effective regulations** — An effective legal framework provides credibility to blockchain-based tokens in the eyes of enterprise leaders and users. However, regulators do not have a very good understanding of the risks and benefits of such tokens yet to roll out effective regulations.
- **Switching costs from today's business networks and systems** — The shift to token-based systems in current businesses requires all parties involved to agree, build and move to a new token-based system that is quite different in technology. This switch needs to be done in a coordinated fashion, without impacting all dependent systems.

User Recommendations

- **Prioritize projects for innovative business leaders, assets, and business models** — Innovators are more likely to invest in blockchain-based tokens to deliver exponential business value. Measure the business impact and demonstrate the incremental value delivered through blockchain-based tokens.
- **Increase awareness about the risks and benefits across all stakeholders** — Gather insights from multiple sources about the current understanding of risks, and highlight these risks along with the potential benefits that could accrue to all stakeholders.
- **Look at the additional capabilities of tokenization, beyond representation** — Investigate how you can employ fungibility, programmability and fractionalization to uncover new value.
- **Understand financial and legal implications** — Work with your legal and financial departments on the implications of holding blockchain-based tokens. Engage with external communities to understand best practices across the industry.

Sample Vendors

Cardano; ConsenSys; Digital Asset; Ethereum; Hyperledger; R3

Gartner Recommended Reading

Emerging Technologies: Blockchain-Based Tokenization Is for More Than NFTs and Cryptocurrencies

Define and Map Cryptocurrencies, Digital Currencies and NFTs to Future-Proof Your Digital Transformation

Quick Answer: How to Protect and Secure the Use and Trading of NFTs

NFT

Analysis By: Avivah Litan

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

A non-fungible token (NFT) is a unique programmable blockchain-based digital item that publicly proves ownership of digital assets, such as digital art or music, or physical assets that are tokenized, such as houses, cars or documents. Many NFTs today live on Ethereum, but are increasingly supported by other blockchain platforms. NFTs store data and logic that manages the token and, typically, links to off-chain records for storage purposes.

Why This Is Important

NFTs support user asset ownership and rights. NFTs also enable trust, authentication, visibility and tracking of any nonfungible asset ranging from identity to digital art, documents or physical world assets. NFTs enable new economic models, e.g., where content creators perpetually retain share of the revenue from sales of their works. Enterprises are beginning to tokenize real-world assets for many advantageous purposes. NFTs have broad applicability in many markets.

Business Impact

NFTs present new ways to solve old business problems. Creators can monetize their assets. Entities can depend on the validity, integrity and uniqueness of NFTs. Blockchain technology brings tamper resistance to NFTs, which is hard to do with other kinds of digital assets. Enterprises are beginning to tokenize real-world assets for new economic opportunities such as tracking an automobile's history, controlling content distribution rights, and for negotiating contracts represented as NFT records.

Drivers

- NFTs offer new methods to ensure trust, integrity and visibility into digital and physical content such as carbon credits, luxury watches, and airline parts. For example, authenticating artwork and tracking its provenance can be a tedious process today. By leveraging NFTs, ownership and authenticity can be validated in real time.
- NFTs enable the technology and support the standards that allow content creators, sellers and buyers to transact with trusted digital (and sometimes physical) content. In the absence of legacy digital signatures, which require a trusted relationship with certificate authorities and workflows, NFTs leverage public blockchains such as Ethereum.
- Due to the nature of a public blockchain, any entity can create and transact with NFTs. Backed by emerging standards, such as ERC721, the potential for vibrant digital ecosystems for digital content is possible.
- New business models for content creators, for example blockchain/decentralized gaming.
- New products and services, such as escrow, insurance or persistent secure storage, that make NFTs more transparent and trustworthy.
- Enterprises are creating or buying NFTs to appeal to their customers, especially those engaged in Web3 virtual environments and games.

Obstacles

- NFTs are unique within a single blockchain network. Blockchain interoperability needs to expand to ensure NFTs retain uniqueness and integrity across digital ecosystems.

- NFT business models and approaches haven't fully been realized by enterprise users. Actual utility and value is still unclear for most enterprise users.
- Enterprises are just beginning to experiment with tokenizing real-world assets for future economic benefits.
- Buyers are sometimes duped into buying an NFT that is not what it pretends to be. Scams and security threats are prevalent, and fraud prevention must become stronger and ubiquitous.
- Buyers are not aware of the numerous risks/constraints on their ownership rights. For example, copyright issues that prohibit transferring their object to other forms, or storage configurations that don't provide persistence and security for their objects.
- NFT play-to-earn game currencies have been manipulated by traders. Controls must be instituted to prevent this usurious activity.

User Recommendations

- Conduct Proof of Concepts. IT leaders that are interested in the potential of NFTs should conduct early stage research, and consider investigating how they are made, distributed and monetized.
- Engage with relevant business leaders to inform and advise on the risks, benefits and limitations of emerging NFT technology.
- Conceptualize potential business and monetization models.
- Leverage good cybersecurity to ensure that risks are understood and mitigated. As NFTs increase in value, so will attacks.
- Use a distributed file system, for example IPFS-based for large amounts of content associated with them. Nodes should be replicated across many servers. While NFTs are cryptographically secured on a blockchain, it does not mean that the NFT is legitimate. NFTs can be misrepresented to buyers.

Sample Vendors

Animoca Brands; Centrifuge; Coinbase NFT; Magic Eden; OpenSea; Rarible; SuperRare

Gartner Recommended Reading

Quick Answer: What Is Web3?

Quick Answer: How to Protect and Secure the Use and Trading of NFTs

FAQ for NFTs on Blockchains and Web3 Ecosystems

Smart Contracts

Analysis By: Ray Valdes, Chet Geschickter, Avivah Litan

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Smart contracts are computer programs written to execute on blockchain platforms for the purpose of managing blockchain-based digital assets and fulfilling other requirements of decentralized applications (dApps). Smart contracts are neither smart nor contracts, but are more like stored procedures in a SQL database. Smart contracts are stored on-chain and are as immutable and secure as other blockchain data.

Why This Is Important

Smart contracts are an essential means of adding programmability to blockchain transactions, as part of decentralized applications (dApps). This enables a wide range of use cases, such as token-swap value exchange, digital asset marketplaces, automation of business transactions and enabling secure agreements across multiple partners. Smart contracts, as part of dApps, enable different organizations to achieve their business objectives with other business entities, using shared resources without compromising their independence.

Business Impact

Smart contracts can improve efficiencies in business ecosystems in various ways:

- Eliminating middlemen and intermediaries
- Supporting trust-minimized value exchange
- Avoiding different interpretations of mutual arrangements through self-enforcing agreements
- Enabling immutable record of high-value data

- Supporting new business models for digital assets (possibly using various token types, including fungible, non-fungible and semitransferable tokens)

Drivers

- **Need for mechanisms to codify and automate business logic and rules on distributed ledgers:** Distributed ledgers provide the mechanism to store immutable and transparent records across multiple nodes. However, they need a programmable mechanism to represent and execute rules, agreements and processes that need to be executed. Smart contracts serve as that mechanism. They enable the blockchain vision of “programmable money.”
- **Innovation of blockchain use cases in new and often complex areas:** Smart contracts enable programmable assets, which can be represented and traded through various token-economic models, including fungible, non-fungible and semitransferable tokens. Smart contracts enable new token types to be invented on an ongoing basis, limited only by the imagination of the developer. This is similar to derived financial instruments in traditional finance, except that smart contracts enable self-enforcing agreements, without reliance on external parties such as financial institutions, law firms or investment bankers. Examples of new use cases beyond traditional financial services are decentralized exchanges (DEXes), peer-to-peer lending, NFT marketplaces, flash loans, peer-to-peer insurance, yield farming and securing the network through staking.

Obstacles

- **Immaturity of blockchain platforms:** More than 150 smart-contract platforms (also known as Layer 1 or L1 platforms) compete with and are mostly incompatible with each other. Beyond the top 10 platforms, most of these lack sufficient adoption to have been battle-tested and thereby garner a track record for security and performance. Most of these minor L1s have only a sparse collection of tools, frameworks, support networks and audit services, and a small pool of skilled developers. Even the major L1s suffer from immaturity when compared to established traditional technologies such as enterprise Java or Microsoft .NET.
- **Smart contracts can only read from, and write to, the blockchain,** which means dApps need additional mechanisms such as data oracles to provide external data and integrate with other systems. These mechanisms can be a source of complexity and security vulnerability.
- **Smart contracts are tied to the underlying L1 platform:** They are mostly incompatible with other platforms because of different languages and programming models. This means, for example, that code written in Golang for a platform such as Hyperledger Fabric will need to be rewritten to run on a different platform, such as Solidity language on the Ethereum platform.
- **Bugs and security vulnerabilities:** Smart contracts are computer code like any other software. All software, regardless of platform, is vulnerable to bugs and security vulnerabilities. Hackers can potentially exploit these to steal funds, in some cases resulting in total loss for the company that owns the funds. This is more likely for smart-contract applications because these are often used for value exchange, unlike traditional platforms used for diverse scenarios such as HR or salesforce automation that don't make use of fund transfer APIs. There is a lack of awareness among traditional developers about mitigating risk through development methodologies that include the use of auditing services and code analysis tools.
- **Legal precedents are few:** Smart contracts should not be confused with legal contracts, despite early ambitious rhetoric from platform developers. There is not much legal clarity for enterprises regarding the factors governing the execution and disposal of assets managed by smart contracts.

User Recommendations

- **Use smart contracts to strengthen the core capabilities of blockchain,** namely: immutable data record, unmediated funds transfer, flexible value exchange and innovative token-economic designs.
- **Focus on simple business rules, rather than complex legal agreements.** Smart contracts, by their name, give an assumption of a better way to manage contracts. This is a misnomer and currently impractical, due to the complex legal issues involved. But smart contracts do provide a mechanism to represent shared business rules and processes for blockchain projects across multiple entities.
- **Mitigate the risk of bugs and security vulnerabilities** by adopting more rigorous development methodologies and engage with external security audit services.
- **Ensure traditional legal agreements bind the behavior of your blockchain partners.** Although enforcement may sometimes be difficult, establish a clear legal framework defining what the platform does and does not do, and how disputes are escalated and arbitrated.

Sample Vendors

Algorand; Avalanche; Cardano; Digital Asset; Ethereum Foundation; Hedera; Hyperledger Foundation (Fabric); R3; Solana Foundation; Tezos Foundation

Gartner Recommended Reading

Managing the Risks of Enterprise Blockchain Smart Contracts

Guidance for Blockchain Solution Adoption

Garbage In, Garbage Forever: Top 5 Blockchain Security Threats

DeFi

Analysis By: Avivah Litan

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Decentralized finance (DeFi) refers to smart contract-based financial applications running on public blockchains. DeFi eliminates intermediaries and supports trustless, transparent and immutable financial transactions between pseudo anonymous parties. When compared to traditional finance (TradFi), DeFi lowers transaction costs, improves yield and returns, albeit in a nonregulated environment. Based on open-source protocols, developers assemble financial primitives into reusable applications.

Why This Is Important

DeFi implements reusable software modules assembled dynamically into applications. DeFi enables anyone with an internet connection to participate in financial services. DeFi disrupts centralized systems and business models. DeFi eliminates middlemen and batch processes, and supports more modern and efficient financial systems architecture than legacy systems. Users are attracted to high rewards but these applications come with high risks that regulators are keen to understand and rein in.

Business Impact

The DeFi market is still emerging and mainstream adoption has not taken hold. TradFi represents a large chunk of global GDP, yet is opaque and highly centralized. Back-end systems are based on decades-old architecture. DeFi can upgrade this antiquated architecture, offering substantial value opportunities beyond traditional financial services. There is reduced mainstream interest in leveraging this architecture since the 2022 public blockchain scandals, but technical advantages remain.

Drivers

- Prior explosions of cryptocurrency markets led to large amounts of capital that fueled investment and speculation into derivatives based on crypto. Since the end of 2022, activity has dramatically slowed down and DeFi values have contracted, but growth in active addresses and other metrics indicate DeFi activity steadying.
- DeFi executes shared business processes through preagreed, decentralized smart contracts. Blockchain protocols keep transactions transparent, immutable and Byzantine fault tolerant.
- Some traditional finance firms engage in DeFi trading in a regulatory compliant manner. For example, a permissioned version of the popular DeFi protocol, Aave, launched in January 2022, giving bank participants the ability to trade with whitelisted participants in a “walled garden” version called Aave Arc.
- DeFi eliminates the need to pay intermediaries, thereby streamlining financial processes.
- DeFi facilitates the creation of modernized financial products. One example is collateralized lending processes, underpinned by smart contracts that eliminate the need for cumbersome paperwork, and support automated real-time loan closings when collateral is no longer sufficient to support the loan (for example, because of currency volatility).
- DeFi facilitates new transaction-based insurance products that are triggered based on terms codified in smart contracts; for example, a condition change like temperature increase.
- DeFi enables trades of tokenized assets that can represent just about anything: skilled labor hours available for hire in labor marketplaces, where contracts and payments are automated with smart contracts; fractional components of a valuable piece of art that can be traded; fractional components of financial instruments like certificates of deposit (CDs) that can be traded individually, so that CD holders are no longer penalized for “breaking the CD”; and automated issuance of IPOs and debt, and new types of structured debt instruments.

Obstacles

- There is no regulatory protection if things go wrong.
- U.S. dollar stablecoins are used widely in DeFi, as they mitigate effects of market volatility, but this concerns some regulators, especially in the United States. In 2023, the The Securities and Exchange Commission took several enforcement actions against companies who issue or list stablecoins on exchanges.
- DeFi technology is immature and hard to use.
- DeFi applications are prime hacker targets. Hackers exploit logic flaws in smart contracts, or centralized interfaces into them. Users have no recourse, but can insure for certain smart contract bug conditions, using DeFi insurance from firms such as Nexus Mutual.
- Security risks are imminently concerning. Over time, risk mitigation solutions will emerge.
- Mainstream users pulled back from adopting DeFi applications in 2022 and 2023, due to market manipulations in the cryptocurrency market that had nothing to do with DeFi code itself.

User Recommendations

- Consider integrating DeFi applications into compliant financial services if there are DeFi modules that uniquely solve an existing problem or create a new business opportunity. DeFi technology is ready for early enterprise adoption, as long as regulatory guidance is clear and complied with.
- Integrate DeFi modules with existing TradFi services and operations to support efficient, transparent, peer-to-peer versions of traditional financial products and entirely new ones that support new mediums of exchange and value.
- Stay up-to-date with new DeFi modules and how financial organizations are leveraging them in a compliant manner, to expose yourselves to new opportunities and business models that your organization can benefit from. For example, NFTs may be used in the future for distributed e-books, cutting down considerably on logistical and overhead costs. NFT books may be bought, sold and traded using a DeFi application available in a marketplace in the future.

Sample Vendors

Aave; Avalanche; Curve; Ethereum; MakerDAO; Solana; SushiSwap; Uniswap

Gartner Recommended Reading

FAQ for Cryptocurrencies on Blockchains and Web3 Ecosystems

Quick Answer: What is Web3?

Layer 1 Blockchains

Analysis By: Homan Farahmand, David Furlonger

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

The Layer 1 (L1) blockchains are a type of operating system that enable secure, decentralized computing. Blockchain establishes a shared trust infrastructure in a digital ecosystem, which enables organizations to run a business function as a protocol among participants. This includes the trusted issuance, registration and exchange, or verification and tracking of digital assets, by deploying smart contracts that define and manage appropriate tokens (assets) relevant to these business functions.

Why This Is Important

In the same way internet protocols decentralized connectivity, blockchain protocols are decentralizing computing as the trust foundation of the next-generation web (Web3). Blockchains provide features such as a distributed ledger, immutability, transparency, tokenization and support for smart contracts in a multilayer architecture. L1 blockchains address decentralization and security requirements, while Layer 2 (L2) blockchains (or enterprise blockchains) address the scalability.

Business Impact

Blockchains can change the terms and governance structures of business and society by enabling autonomous and peer-to-peer transactions, based on a variety of asset tokenization and value-exchange scenarios. Public L1 blockchains provide an open trust layer, enabling a plug-and-play platform for smart contracts or L2 chains. This is in contrast to enterprise blockchains, which provide a closed trust layer that requires ongoing governance, setup and maintenance among permitted participants.

Drivers

- Blockchain core technologies continue to evolve steadily to support key features such as more efficient consensus mechanisms, enhanced execution environments, enabling L2 chains, cost optimization and privacy improvements, which vary by each L1 blockchain.
- Blockchain developers are making progress in building traditional application stack capabilities to enable integration with blockchains. These include better modeling support, developer tools, frameworks, smart-contract templates, security audit, formal verification, interoperability, integration mechanisms and software development kits (SDKs).
- Feedback from early adopters indicate the blockchain design pattern is evolving around a multitier model. This model includes L1 public blockchains for decentralization and security, and L2 chains primarily for scalability. Also, there are emerging Layer 0 chains for cross-chain state interoperability.
- Development continues to progress in design, testing and piloting across different industries, and has gained more traction with the digital business, considering the promise of high speed and efficiency.
- As digital acceleration pervades all industries and the public sector, more attention is being paid to specific Web3 use cases that blockchains can support, such as digital currency, decentralized autonomous organization (DAO), decentralized applications, decentralized identity, decentralized finance, GameFi, TradeFi, non-fungible token (NFT), and metaverse.
- There is a proliferation of blockchain-inspired solutions that mimic blockchain features, but are using centralized components. These solutions are more concerned with transaction validation from a business-rule perspective. Decentralization and trust are not inherent in the protocol, and are achieved using traditional centralized processes and technologies.
- Many enterprise application use-case requirements that can be satisfied by blockchain-inspired technologies, instead of a true L1 blockchain.

Obstacles

- Blockchain may expose the enterprise to regulatory uncertainty, as governments are still working to understand the implications of blockchain solutions. Examples are asset securitization, money laundering and/or privacy compliance issues.
- Blockchain's vulnerabilities should be tracked carefully, considering its constant evolution. Attacks on blockchains can affect the operation or cause financial losses due to faulty smart contracts.
- Blockchain relies heavily on cryptographic algorithms, which require careful consideration of the migration path to new post-quantum-era cryptography.
- Blockchain adoption may run into challenges such as the lack of success and scope definition, misaligned expectations, determining viable use cases, and developing future-proof architecture.
- Blockchains can be disruptive by changing the business models and governance structures of enterprises, based on autonomous and peer-to-peer transactions using asset tokenization.

User Recommendations

- Evaluate blockchain relevance to the current (and future) enterprise business model. Decide on a realistic progressive adoption approach based on priorities.
- Develop a blockchain-agnostic architecture strategy for decentralized application use cases to address security and scalability requirements.
- Ensure the architecture enables business innovation in the short term and a migration pathway to more suitable blockchain technologies in the long term.
- Assess your candidate blockchain technologies using the normalized functional model provided in Guidance for Blockchain Assessments.
- Ensure that your preferred blockchain platform has modernization pathways to support future Web3 requirements where it is applicable.
- Minimize any proprietary blockchain infrastructure technology and/or vendor lock-in by adopting open-source infrastructure technology with multiple independent implementations.
- Ensure support for future migrations to other winning blockchain technologies in the long term.

Sample Vendors

Algorand; Avalanche.org; ethereum.org; Hedera; Hyperledger Foundation; Quorum; R3; Solana Foundation; VeChain Foundation; VMware

Gartner Recommended Reading

Guidance for Blockchain Assessments

Guidance for Blockchain Solution Adoption

Climbing the Slope

Consensus Mechanisms

Analysis By: Homan Farahmand

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Consensus mechanisms provide coordination, validation and agreement among participants in decentralized computing systems to finalize any transaction reliably. Consensus algorithms are complex and require many properties (such as being fair, fast, provable, Byzantine fault tolerant, efficient, inexpensive, time-stamped and denial-of-service-resistant) to ensure decentralization, correctness and security autonomously.

Why This Is Important

Consensus mechanisms provide a protocol for generating trust in decentralized systems when participants do not trust each other. That's why consensus protocol design is critical in determining how well a system can achieve decentralization and security, autonomously. The type of consensus algorithm is key to eliminate the risk of successful attack on the blockchain. It also ensures the process terminates when all honest nodes agree on a proposed block and that block is generated by an honest node.

Business Impact

Consensus mechanisms are critical to moving from a single-authority computing model to a distributed or decentralized computing model:

- Efficient consensus enables the trust and economic model of the blockchain ecosystems, while minimizing the energy consumption.
- Scalable consensus supports secure execution of smart contracts and tokenization of different types of assets at a reasonable cost.
- Reliable consensus drives the ecosystem growth by attracting more operators, developers and users.

Drivers

- Consensus mechanisms design is critical in determining how well a system can achieve decentralization and security autonomously. Consensus protocols strive to implement Byzantine fault tolerant (BFT) systems. They usually use a random mechanism, such as competing (by nodes that race to complete a task such as proof-of-work [PoW]) or voting (by nodes that are selected randomly such as proof-of-stake [PoS]), to decide which node proposes the next block.
- Consensus mechanisms are preferred in public blockchains to ensure fairness and safety. In addition to node availability, they ensure that the algorithm terminates when all honest nodes agree on the value and the value has been generated by an honest node. The key factors that practically eliminate the risk of a successful attack on the blockchain are type of consensus algorithm, number of nodes and cost of any attack. New enhancements are being considered to separate nodes that propose and build blocks to ensure segregation of duties (SOD).
- Consensus mechanisms are different from endorsement-based protocols, which are common in enterprise blockchains or blockchain-inspired technologies. These protocols implement BFT-like coordination protocols that are not fully decentralized, but are, at best, fault tolerant. There is less reliance on randomness because coordination is achieved through traditional agreements among entities in a closed/permissioned environment. They usually rely on a few predefined nodes to validate, endorse, notarize, and/or order transactions to allow commitment and block formation.
- Some consensus mechanisms are leader-based (e.g., Paxos and its variations, such as practical Byzantine fault tolerance [PBFT]) or authority-based (e.g., proof of authority [PoA]). These mechanisms require a distinguished node to coordinate the protocol tasks to make progress. Using a less random approach to select nodes for ordering and endorsing transactions substantially reduces blockchain decentralization.
- The examples of protocols gaining traction include proof-of-stake (PoS), proof-of-work (PoW), proof-of-authority (PoA), Hashgraph, practical BFT, Istanbul BFT and RAFT.

Obstacles

- Consensus mechanisms can have different business outcomes and are increasingly becoming the subject of regulatory scrutiny. This includes debates on the environmental impact of PoW protocol or contradicting opinions on the impact of PoS on classifying tokens as securities.

- Consensus algorithms are complex and require technical properties and business processes (such as governance and policies) to ensure their correctness and security (such as being fair, fast, provable, BFT, efficient, inexpensive, time-stamped and denial-of-service-resistant).
- Less-proven consensus mechanisms are potentially more at risk of cyberattacks, considering that vulnerabilities have yet to be fully discovered. These vulnerabilities can be exploited to orchestrate different attacks that can affect the blockchain operation.
- The variety and constant evolution of consensus mechanisms in blockchains are hard to navigate and can be confusing. This makes an apples-to-apples comparison of these protocols more difficult.

User Recommendations

- Educate IT and business leaders on the importance of decentralization, in both technical and governance context, to deliver business functions as a protocol. Highlight the role of consensus mechanisms to establish a shared or public trust foundation for decentralization.
- Ensure you have sufficient understanding and analysis of how different blockchains use their respective consensus mechanisms to address requirements for block production, blockchain trilemma (security, decentralization and scalability), enabling a viable economic model, resilience, and sustainability, as well as general strengths and weaknesses.
- Develop sufficient technical expertise to recognize mechanism dependencies, vulnerabilities and failings as key components of blockchain adoption and managing operational risks.
- Follow the evolution of your relevant consensus mechanisms in terms of current and future capabilities, features and cryptographic agility to ensure alignment with your desired specifications.

Gartner Recommended Reading

Guidance for Blockchain Assessments

Designing Blockchain Smart Contract Security and Access Control

Blockchain Wallets

Analysis By: Balaji Abbabatulla

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Blockchain wallets store critical information — such as private keys — that users need to conduct cryptocurrency transactions, including buying, selling or viewing cryptocurrencies. Also known as crypto wallets, these can be accessed online, via a mobile app, or using a dedicated hardware device. Most casual users use wallets hosted by a cryptocurrency exchange that manages users' private keys and secures access via a user password, device confirmation and two-factor authentication (2FA).

Why This Is Important

Wallets enable safekeeping of critical information required to access and transact blockchain-based assets such as cryptocurrencies to non-fungible tokens (NFTs) on blockchain-based marketplaces and solutions. Users have complete control over their own wallet contents, such as cryptocurrencies, identity data or NFTs. Wallet capabilities are advancing quickly as users are demanding more features and providers are delivering wallets designed for different types of users.

Business Impact

As cryptocurrencies, NFTs, decentralized finance (DeFi) and blockchain businesses gain adoption, users must be able to store and gain secure access to blockchain-based assets. User access is enabled through a private key, but private keys represent a single point of failure. User account takeover is the topmost attack vector for bad actors who steal blockchain-based funds or assets. Solution providers should carefully design their wallets to overcome such vulnerabilities.

Drivers

- As cryptocurrencies gain adoption, organizations that provide customer services need custodial wallet services from trusted wallet providers, because they do not have the expertise to manage the wallet functions on their own. These types of organizations include institutional investors, corporations, token issuers, and service providers such as payment services, brokers, banks and exchanges. Advanced custodial wallets can satisfy organizational needs for master wallets and subwallets — for example, for a broker that manages a group of corporate accounts.
- Decentralized cryptocurrency traders and DeFi users need to use self-hosted wallets, meaning they are responsible for the safekeeping of their own assets and for any key recovery that must be done in the event of key or device loss. Users of DeFi services often choose wallets based on their ability to swap one cryptocurrency for another.
- Recent growth in the purchase of NFTs is expanding the use of wallets beyond cryptocurrency.
- Most mainstream users cannot manage the complexities of cryptographically secured access and need to outsource it to a trusted wallet provider.
- Advancing needs are driving innovations in wallets. For example, some wallets implement policies that disallow transactions from certain applications and blockchain addresses. Others are purpose-built for cryptocurrency exchanges so that the exchanges can easily transfer assets among them.
- Secure multiparty computation (SMPC) is a feature of some wallets for users who want to avoid having a single point of failure imposed by a private key. SMPC uses shared-key methods across multiple parties.
- Decentralized, blockchain-based, self-sovereign identity systems need wallets for users to store their own data and credentials. Similarly, hybrid identity systems tied to blockchains — where issuers issue identity credentials but users control the release of their credentials — also need wallets that give access to blockchain records and protocols.

Obstacles

- The user experience involving wallets is significantly different from that of traditional software solutions. Adoption of wallets is linked to the acceptance of the new experience by users.
- User concerns about potential compromises of private keys stored in wallets that could lead to a complete loss of their blockchain assets.
- The most secure wallet secures users' private keys offline, but they are difficult to use and safeguard. Offline storage of keys enables "cold storage," most commonly implemented using a hardware wallet or dedicated device.
- Determined criminals circumvent most phone authentication techniques used to protect online user wallets. Criminals use methods such as "SIM swaps" or malware on a victim's phone that directs SMS messages to the hacker's phone.

User Recommendations

- Educate users about the benefits of adopting the new wallet experience to improve the security of their blockchain-based assets over traditional storage and access.
- Secure your organization's cryptocurrency wallet(s) using the strongest security measures that your organization can manage.
- Use an online wallet available through a "reputable" exchange for ease of use. Use multifactor authentication and, potentially, multisignature payment options to secure it.
- Invest in one or more hardware wallets that enable "cold storage" if you want a more secure wallet option and wish to retain stored cryptocurrency balances on the blockchain. Carefully secure the hardware wallet and its recovery key.
- Use advanced custodial wallets that come with many security, policy, account and key management features.

Sample Vendors

Coinbase; Conio; ConsenSys; SatoshiLabs

Cryptocurrencies

Analysis By: Ray Valdes, Balaji Abbabatulla, David Furlonger

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

A cryptocurrency is a digital currency that is hosted on or enabled by blockchain platforms, and secured by various cryptographic mechanisms and distributed protocols. It enables peer-to-peer transfer of value without relying on a central authority such as a bank or government.

Why This Is Important

Cryptocurrencies do not need a central authority such as a bank or government in order to enable value exchange between parties on a blockchain network. The network provides transaction immutability and replicates the core functions of conventional money without government intervention. While often speculative, cryptocurrencies can enable mechanisms to fund business investment, accelerate P2P transactions and drive market liquidity. Cryptocurrencies gain transformative potential when coupled with smart contracts, which enables the emergence of programmable money.

Business Impact

- Cryptocurrencies enable new ways of doing business, participative business models, and new kinds of products and services to new types of buyers and users.
- Cryptocurrencies can make some business processes more efficient and cost-effective via faster transfers of value, lower transaction costs, global reach and more secure transfers.
- Some cryptocurrencies have deflationary economic models built in as part of the protocol, and this can have a beneficial effect.

Drivers

- For some users, the pseudoanonymity that blockchain-resident cryptocurrencies provide is a strong part of their appeal.
- Current estimates of crypto ownership are about 450 million users worldwide, with rapid growth over the past several years.
- Cryptocurrencies are not controlled by governments or traditional financial institutions. They provide an alternative way to acquire, store and exchange value.
- Cryptocurrencies have gained popularity outside of the traditional financial sector: for example, in the world of decentralized finance (DeFi), which includes applications such as NFT marketplaces, peer-to-peer lending, and crowdfunding. Use cases are oriented to individual users or SMEs rather than established institutions.
- The value of cryptocurrencies is determined not only by their scarcity (in a supply-vs.-demand dynamic) but can also be determined by their utility as elements of a transactive realm. Utility is enabled in part by programmability achieved through smart contracts and by using cryptocurrencies in various DeFi services.
- The future use of cryptocurrencies could depend on how well they can meet users' needs compared with competing electronic payment systems, such as central bank digital currencies (CBDC) and digital payment systems operated by large internet companies (Tencent, Apple, Google, Alibaba).
- Adoption will also depend on cryptocurrencies' investment value, their programmability and effectiveness in various use cases, and their utility in systems allowing for interaction in business, social networks, gaming and entertainment.

Obstacles

- Cryptocurrency prices can be highly volatile and unpredictable, which can mean an unacceptable level of “foreign exchange” risk for some use cases.
- Although major cryptocurrencies like ETH and BTC are proven and relatively stable (when compared to national currencies of small developing nations), there are more than 20,000 other currencies that are not only highly volatile, but also can be manipulated by bad actors due to low levels of liquidity.
- User experience for average users is challenging: installing and using crypto wallets; being cognizant of fiat-to-crypto conversion; estimating sufficient gas fees for transactions; and safely managing private keys. Broad adoption will depend on costs, incentives and convenience for users. Traditional financial services like PayPal and Mastercard have added user support for crypto, but results are not stellar.
- Uncertain and inconsistent currents in regulation from multiple official bodies.
- Cryptocurrencies compete with many centralized digital payment mechanisms available globally to banked and unbanked individuals. Adoption of cryptocurrencies is hindered if there are options that are easier to understand, backed by recognizable brands or institutions, or have lower or more predictable transaction costs.
- Anonymity can be limited by regulation and off-network forensic analysis. Organizations with the resources and third-party services may discover more details about cryptocurrency transactions than some kinds of intentionally obfuscated conventional transactions.

User Recommendations

- Carefully evaluate the use and expected benefits of cryptocurrency, and do diligent research across the 20,000-plus cryptocurrencies (the vast majority of which have unacceptable levels of risk).
- Understand the difference between a native cryptocurrency like Bitcoin and a derived token like the many ERC-20 tokens, stablecoins, and other financial instruments, which can address a wider range of use cases.
- Formulate a blockchain strategy that includes system and data integration in terms of products, pricing, accounting, taxes and so on.
- Identify use cases, such as games, virtual worlds or other realms in which value can be converted to tokens, where cryptocurrency might be more effective than other mechanisms.
- Consider centralized exchanges or services that provide cryptocurrency conversion and compliance with government regulations, as long as these align with your security requirements.
- Monitor the ongoing changes in the regulatory environment (both local and global) around your organization's activities. Regulatory changes are often driven by shifting political and economic winds and therefore hard to predict.
- Update your organization's compliance and risk policies, and seek external legal advice on cryptocurrency use.
- Create technology and business roadmaps for the potential integration of cryptocurrencies with mainstream mediums of exchange.

Gartner Recommended Reading

Bitcoin Goes Mainstream: What It Means to You

Define and Map Cryptocurrencies, Digital Currencies and NFTs to Future-Proof Your Digital Transformation

Decentralized Applications

Analysis By: Adrian Leow, Rajesh Kandaswamy

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Decentralized applications (dapps) are applications connected to a decentralized, blockchain peer-to-peer (P2P) network. Unlike traditional internet applications, which are based on a centralized server that functions as a controlling authority, dapps use and often rely on smart contracts for their application logic — meaning no single entity controls smart contracts.

Why This Is Important

Dapps are the primary means to build applications on the blockchain. They provide new opportunities for innovation and collaboration, and help drive the adoption of decentralized and more democratic systems. Dapps can build complex, multiparty applications and bring a layer of computation that relies on and is tied to underlying smart contracts sitting inside distributed ledgers. Although promising, dapps are still in the early stages of technology maturity.

Business Impact

- Large-scale, complex enterprise applications involving multiple parties need a layer of trust. Through dapps using smart contracts, they provide a trusted interface to interact with a blockchain platform ledger.
- Dapps can streamline business processes by automating tasks and reducing the need for intermediaries, leading to increased efficiency and reduced costs.
- Dapps can generate new opportunities for businesses to raise capital by creating decentralized finance (DeFi) platforms and other blockchain-funding mechanisms.

Drivers

- Many dapps have seen significant market traction, with notable success in financial, infrastructure and gaming industries — which has occurred largely outside the enterprise sector.
- Dapps use cryptocurrencies as the built-in medium of exchange, which could potentially increase mainstream adoption of cryptocurrencies. DeFi applications are among the first interactions individuals have with dapps.
- Dapps enable new ways of organizing economic activities, reducing costs and time associated with intermediaries, and strengthening trust.
- Each party in the decentralized structure can run apps without trusting other parties. This has resulted in faster application adoption, primarily outside the enterprise sector. Since dapps aren't hosted on single IP addresses, there is less authority in owning a dapp's network — and it's more difficult for external authorities to prohibit a dapp.
- Dapps do not have a single point of failure, meaning they are more resistant to attacks than traditional single-server applications. Dapps will only fail if most computers in the network fail, which is highly improbable.
- Data and other information added to the blockchain is immutable, including the smart contract code itself. This means dapps are more resistant to changes or restrictions.
- Dapps don't require connectivity to a single centralized server, making them more robust and flexible than centralized applications. Therefore, enterprises can ensure maximum business continuity and resilience with minimal interruptions and downtime.
- Dapps' growth will be led by startups creating innovative businesses and technology solutions on top of blockchain technologies. As soon as they mature, a broader set of tools will enable decentralized applications, providing substitute and competitive services to those offered in traditional industries.

Obstacles

- Dapps are not yet proven to satisfy enterprise needs of reliability, security, performance or scalability as they have been in public blockchains.
- Dapps must evolve to support production needs, tools and technologies that enable their development.
- Dapps' user experience (UX) is often difficult to navigate since they don't function like centralized applications.
- Although high-risk gambling dapps is only one of dapps many applications, this could limit dapp's public perception to merely risky financial incentive programs.
- Given DeFi's increasing popularity, some users are being priced out of the dapp ecosystem due to Ethereum's occasional spikes in transaction fees — which are being addressed by multiple enterprise integration platform (EIP) proposals.
- Because dapps are tied to smart contracts with back-end code running on the blockchain, dapps' evolution relies on blockchain platforms' and smart contract technologies' growth.

User Recommendations

- Experiment with dapps and understand their use according to your organization's needs, as they are unproven in the enterprise. The enterprise has yet to move to decentralized blockchains since they haven't been proven to meet data privacy and confidentiality, and scalability requirements.
- Limit major commercial applications until dapps and blockchain mature, and existing legal, regulatory and compliance standards are mitigated or resolved.

Sample Vendors

Aave; Aragon; Axie Infinity; Compound; Decentraland; Curve; MakerDAO; OpenSea; PoolTogether; Uniswap

Gartner Recommended Reading

Quick Answer: How Are Decentralized Applications Different From Regular Apps?

Ethereum Merge Is a Large Step Toward Proving the Viability of Public Blockchains

Appendixes

See the previous Hype Cycle: Hype Cycle for Blockchain and Web3, 2022

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media 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 innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation 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 innovation'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 innovation 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 innovation to reach the Plateau of Productivity.

Source: Gartner (August 2023)

Table 3: 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 (August 2023)

Table 4: Maturity Levels

(Enlarged table in Appendix)

Maturity Levels	*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 constraints replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (August 2023)

Document Revision History

Hype Cycle for Blockchain and Web3, 2022 - 12 July 2022

Hype Cycle for Blockchain, 2021 - 12 July 2021

Hype Cycle for Blockchain Technologies, 2020 - 13 July 2020

Hype Cycle for Blockchain Technologies, 2019 - 11 July 2019

Hype Cycle for Blockchain Technologies, 2018 - 25 July 2018

Hype Cycle for Blockchain Technologies, 2017 - 31 July 2017

Hype Cycle for Blockchain Technologies and the Programmable Economy, 2016 - 27 July 2016

Hype Cycle for the Programmable Economy, 2015 - 23 July 2015

Recommended by the Authors

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

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Guidance for Blockchain Solution Adoption

Guidance for Blockchain Assessments

Predicts 2023: Users Take Back Control of Their Identities With Web3 Blockchain

FAQ for Cryptocurrencies on Blockchains and Web3 Ecosystems

FAQ for NFTs on Blockchains and Web3 Ecosystems

Garbage In, Garbage Forever: Top 5 Blockchain Security Threats

---

Table 1: Priority Matrix for Blockchain and Web3, 2023

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational	Blockchain Wallets Stablecoins	Blockchain Interoperability Blockchain Oracles Consensus Mechanisms Cryptocurrencies Decentralized Identity Layer 1 Blockchains NFT Retail CBDC Smart Contracts Tokenization	Blockchain and IoT Web 2.5 Web3	Metaverse
High		Authenticated Provenance Decentralized Applications Decentralized Exchanges DeFi Enhanced Blockchain as a Service Layer 2	Decentralized Autonomous Organization	
Moderate		Blockchain Intelligence and Analytics	Zero-Knowledge Proofs	

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Low				

Source: Gartner (August 2023)

Table 2: Hype Cycle Phases

Phase	*Definition*
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media 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 innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation 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 innovation'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 innovation 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 innovation to reach the Plateau of Productivity.

Phase	Definition

Source: Gartner (August 2023)

Table 3: 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 (August 2023)

Table 4: Maturity Levels

Maturity Levels ↓	*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 constraints replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (August 2023)