Gartner®

Hype Cycle for Blockchain, 2021

Published 12 July 2021 - ID G00747513 - 84 min read

By Analyst(s): Avivah Litan, Adrian Leow

Initiatives: Applications and Software Engineering Leaders

Decentralized public blockchain applications are thriving, but successful permissioned enterprise blockchain projects are scarce. Applications and software engineering leaders must understand how new advances are supporting integration of enterprise requirements with public blockchain innovation.

Strategic Planning Assumption

By 2023, 35% of enterprise blockchain applications will integrate with decentralized applications and services.

Analysis

What You Need to Know

There is real business value in enterprise (that is, permissioned) blockchains, so long as participants agree to and abide by terms of participation. Fourteen percent of permissioned enterprise projects went into production last year, [1] but transaction volume is limited. Technology issues are not the main reason enterprise projects don't move into production. Rather, the obstacles are business processes, governance issues and the lack of clear objectives and ROI measurements.

Public blockchains are maturing quickly in contrast to enterprise permissioned blockchains. Public blockchains eliminate central authority, while permissioned blockchains replace it with task force authority, making it difficult to implement enterprise projects.

The future of permissioned blockchain is centralized services wrapped around and integrated with decentralized applications, starting with financial applications (CeDeFi), but also extending to other areas we call CeDeX (where "X" denotes anything and everything).

We also expect to see more gradual growth in:

- Private transactions on public blockchains, as privacy options and scalability improve.
- Well-aligned, interconnected enterprise blockchains, as interoperability options mature.

The Hype Cycle

Public blockchain innovations moved quickly through the Hype Cycle last year. Key drivers include:

- Mainstream adoption of Bitcoin, including El Salvador's adoption of Bitcoin as legal tender in June 2021 (see the innovation profile for cryptocurrencies). [2]
- Payment network, banking and social network adoption of distributed ledger technologies (DLTs) for money movement, with the expected deployment of central bank digital currencies (CBDCs) being a key influencer. [3]

- Decentralized finance (DeFi) applications offer substantially greater financial rewards than traditional finance. Centralized firms like hedge funds already take advantage of this (see the innovation profile for DeFi and CeDeFi/CeDeX).
- Tokenization of assets, including the explosive growth of NFTs (see the innovation profile for nonfungible tokens [NFTs]) and DeFi tokens, and the promise of tokens linked to physical assets in the future.
- Blockchains such as Binance and Solana offer viable cost-effective alternatives to Ethereum chain transactions (see the innovation profile for blockchain platforms).
- Monumental progress in blockchain interoperability, including gateways and abstraction middleware, already used today by DeFi applications (see the innovation profile for blockchain interoperability). [4]
- Blockchain migration from the proof-of-work (POW) consensus method (still used for Bitcoin) to more energy-efficient consensus methods such as proof of stake (PoS), Proof of Stake Alliance (PoSA) and proof of history (POH). The ongoing upgrade of Ethereum leads to this trend (see the innovation profile for consensus algorithms).

On the other hand, adoption of permissioned blockchains is moving much more slowly. Some use cases — especially around supply chain and authenticated provenance — are benefiting from ledger technology. However, most users are stuck trying to align use cases to the technology.

In early 2021, IBM folded its dedicated permissioned enterprise blockchain product group and Microsoft is retiring Azure Blockchain Service on 10 September 2021. [5, 6] Global regulations and accounting standards need clarification before most enterprises adopt cryptocurrency, and China continues to clamp down on crypto activities.

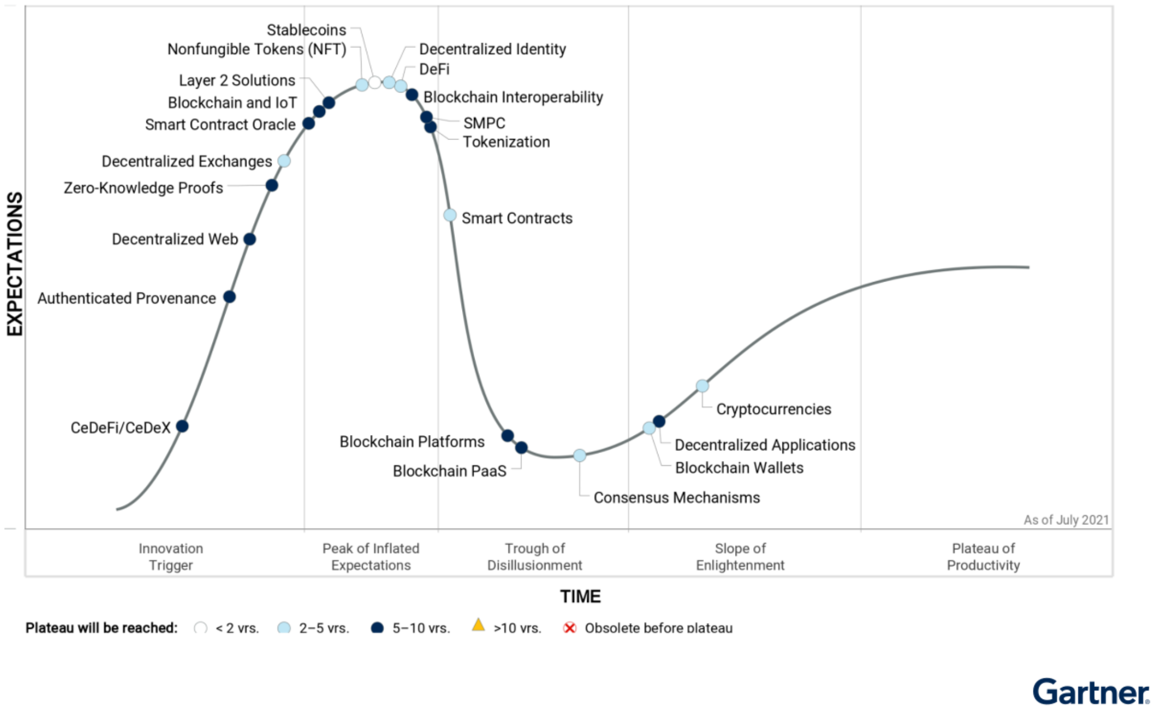
New Hype Cycle entries reflect the market evolution:

- CeDeFi/CeDeX
- Cryptocurrencies
- Decentralized exchanges
- DeFi
- Stablecoins

- Nonfungible tokens (NFT)

Several profiles were removed as noted in the Off the Hype Cycle section.

Figure 1. Hype Cycle for Blockchain, 2021



Source: Gartner (July 2021)

Downloadable graphic: Hype Cycle for Blockchain, 2021

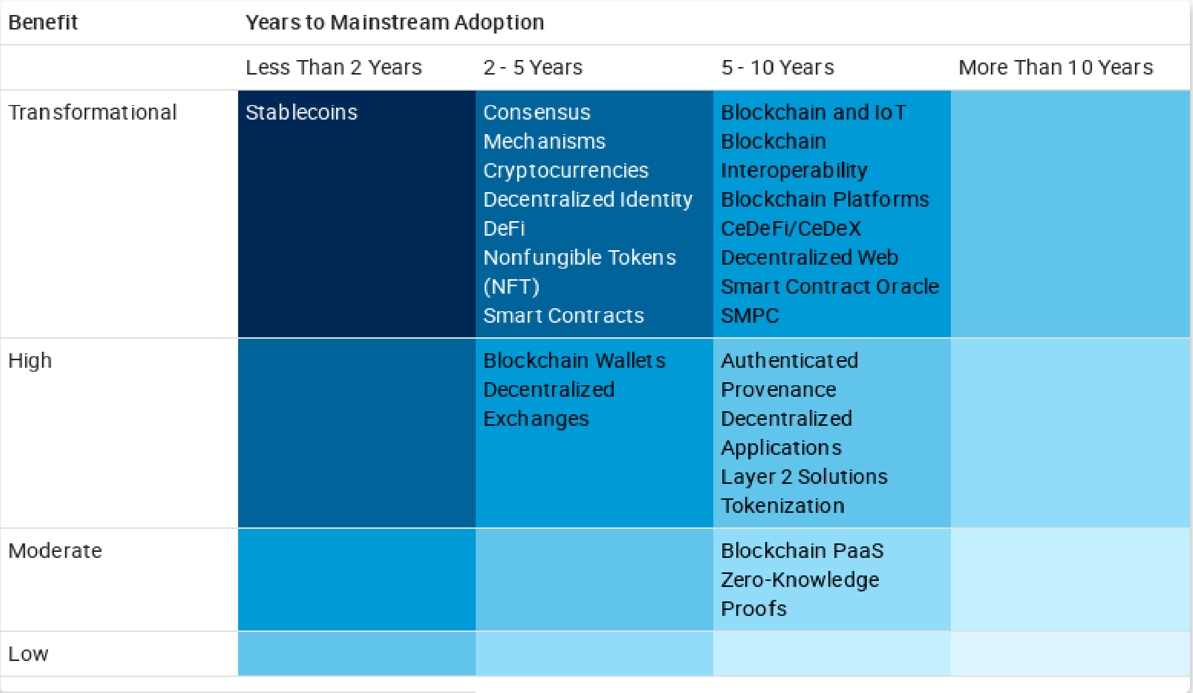
The Priority Matrix

Application and software engineering leaders should prepare for the high-priority and transformational trends that will become mainstream in the next two to five years. For some of these innovations — including smart contracts, consensus mechanisms, DeFi and decentralized identity — the impacts will be numerous and significant. Organizations cannot wait until associated technologies are less than two years to mainstream adoption before they address them. Collectively, these innovations will support technically and operationally scalable blockchain projects across business ecosystems.

A majority of the technologies profiled that have a rating of high or transformational will not become mainstream for another five to 10 years. Blockchain technologies can underpin truly disruptive ways of doing business across parties that “don’t trust each other,” even if these features do introduce more implementation complexity. Once private transactions can integrate with public blockchain services such as decentralized consensus, these features will move into mainstream adoption.

Table 1: Priority Matrix for Blockchain, 2021

(Enlarged table in Appendix)



Benefit	Years to Mainstream Adoption			
	Less Than 2 Years	2 - 5 Years	5 - 10 Years	More Than 10 Years
Transformational	Stablecoins	Consensus Mechanisms Cryptocurrencies Decentralized Identity DeFi Nonfungible Tokens (NFT) Smart Contracts	Blockchain and IoT Blockchain Interoperability Blockchain Platforms CeDeFi/CeDeX Decentralized Web Smart Contract Oracle SMPC	
High		Blockchain Wallets Decentralized Exchanges	Authenticated Provenance Decentralized Applications Layer 2 Solutions Tokenization	
Moderate			Blockchain PaaS Zero-Knowledge Proofs	
Low				

Source: Gartner (July 2021)

Off the Hype Cycle

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

We have merged or renamed the following technologies to accurately reflect the content:

- “Blockchain UX/UI/Wallet Technologies” has been renamed “Blockchain Wallets.”
- “Layer 2 Solutions (Sidechains, Channels)” has been renamed “Layer 2 Solutions”
- “Secure Multiparty Computing” has been renamed “SMPC.”

Because this Hype Cycle pulls from such a broad spectrum of topics, many technologies are not tracked over a longer period of time, but may feature in the Hype Cycle for a specific year because of their relative visibility. This is not intended to imply that they are unimportant — quite the opposite. In many cases, these technologies are no longer "emerging." They are becoming increasingly integral to business and IT. In other cases, technologies were removed from the Hype Cycle in order to highlight other newly emerging technologies. Technology planners can refer to Gartner's broader collection of Hype Cycles for items of ongoing interest.

Some previous innovation profiles were removed to ensure that this Hype Cycle primarily focuses on the most relevant and transformational blockchain innovations. We also eliminated overlapping and redundant innovation profiles. Innovation profiles that appeared in the Hype Cycle for Blockchain Technologies, 2020 but do not appear in this year's report are:

- Blockchain — As the focus of the entire Hype Cycle, this innovation profile is now redundant.
- Blockchain asset tokenization — This has been made redundant by the tokenization innovation profile.
- Ledger DBMS — This technology is not directly related to blockchain.
- Postquantum blockchain — This technology is far out in the future.
- Blockchain managed services — These services were not well adopted.
- Blockchain for data security — This is a use case for blockchain and no longer warrants its own innovation profile.

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

CeDeFi/CeDeX

Analysis By: Avivah Litan

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition

Centralized decentralized finance (CeDeFi) represents the offering of decentralized financial products and services, such as peer-to-peer lending, by centralized financial companies, e.g., exchanges or banks. Similarly, centralized decentralized anything (CeDeX) represents the offering of any type of decentralized products and services, for example digital collectible trading applications, by centralized companies, e.g., issuers of digital collectibles and NFTs.

Why This Is Important

DeFi and other decentralized applications (DeX) such as NFT marketplaces are run by blockchain-based smart contracts, and as such do not require middlemen, intermediaries or central authorities. DeFi and NFT marketplaces are growing rapidly. These markets disrupt centralized businesses that will be sidelined if they do not engage with them.

Business Impact

Blended CeDeFi and CeDeX offerings bring together the best of centralized and decentralized systems: old school regulatory protections with new school innovative products. Transacting anonymously on DeFi and DeX comes with risks, such as smart contract logic hacks, and no legal protection when things go bad. CeFi and CeX services wrapped around DeFi and DeX offerings buttress these risks by offering services such as user onboarding, liability protection, insurance and escrow services.

Drivers

- NFT and DeFi applications are growing exponentially. The DeFi market grew from $700 million in December 2019 to around $40 billion in early 2021, according to industry data (see Forbes.com). Within the first three months of 2021, the combined market cap of major NFT projects increased by 1,785% (source: Bitdealer).

- Centralized companies are paying attention to this growth so they don't lose market share to decentralized applications. In fact, some already offer or are working on offering their customers decentralized services. Binance, a centralized cryptocurrency exchange, offers its customers technical support for DeFi products such as yield farming, making it much easier for users to navigate. They don't however offer protection against financial losses on DeFi. In April 2021, JP Morgan, Mastercard and UBS invested $65 million with ConsenSys, a major proponent and service provider for Ethereum blockchain projects. The new project aims to give the legacy financial institutions visibility into DeFi applications on Ethereum. No doubt, new CeDeFi projects will result. In April 2021, SIX Digital Exchange (SDX) announced support for the Enterprise Ethereum Alliance (EEA), and the Swiss digital asset trading venue's head of business, Tim Grant, joined the EEA board of directors. SDX previously worked with enterprise blockchain platform R3 Corda. Grant was quoted as saying, "You cannot ignore the Ethereum ecosystem as a driver of digital asset flow. The evolution of DeFi has now captured the attention of all our institutional clients, and being involved in driving where that goes is where we want to be positioned" (see Coindesk.com).
- Other centralized commerce services, for example, producers of digital collectibles or games, are similarly embracing decentralized applications like collectible trading or third-party games. They promote interoperability between their centrally issued digital assets and decentralized applications.

Obstacles

- Most legacy centralized organizations do not understand the technology and processes behind blockchain-based DeFi and decentralized applications (dapps). Centralized organizations need to be thoroughly familiar with decentralized business models and technology before they can add value around dApps.
- DeFi and DeX applications are very complex to use. Centralized companies that offer customers onramps to DeFi and DeX will have to vastly improve the user experience around them.
- Decentralized applications are primary targets for hackers who usually exploit smart contract logic. These vulnerabilities must be dramatically minimized, before centralized companies offer their customers decentralized products and services.
- Regulation of DeFi and DeX products and services will likely take three to five years to develop. Therefore, consumer protection against financial loss is similarly likely three to five years away, even with blended CeDeFi and CeDeX services.

User Recommendations

- Work with organizational counterparts to understand DeFi apps. Gain understanding of benefits, risks and requirements of decentralized finance applications as compared to centralized or consortia-managed blockchain applications.
- Keep apprised of CeDeFi applications as they become more widely available, and prepare to use them if they suit your use case.
- Stay up to date on DeFi applications by accessing Defiprime.com.
- Standardize on units of value or exchange by using tokens. Fungible and nonfungible tokens can be moved across disparate blockchains through various blockchain interoperability and smart contract options that support them.

Sample Vendors

Animoca Brands; SushiSwap; Aave; Uniswap; Compound

Authenticated Provenance

Analysis By: Avivah Litan, Svetlana Sicular, Rick Howard

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition

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

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, as users adopt blockchain for provenance applications. These users will become increasingly aware of the need to digitally “certify” the first mile — the onboarding of the goods, content or data being tracked on the blockchain in the first place. Over the past year provenance authentication at scale has accelerated due to the necessity of trusted vaccine distribution.

Drivers

- Today, authenticated provenance largely relies on manual audits or human trust. That is certainly not scalable. For example, human fact checkers cannot keep up with the volume of fake content and do not have the technological resources to do so.

- Environmental, social and governance (ESG) goals embraced by asset management firms are forcing companies to produce verifiable data and information 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.

- Consumers and businesses are placing trust in various labels and certificates, such as "organic" or "non-GMO," but they have no way of verifying the veracity of these assertions. Evidence has shown that these labels and assertions are often incorrect.

- Artificial intelligence (AI) is being successfully used to contextualize and synthesize data that can then be used to authenticate provenance of events and information (for example, detecting a leaking oil pipe). If necessary, findings can then be verified by human auditors.

- 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 is successfully providing a single system of record across multiple entities, based on immutable data and audit trails.

Obstacles

- The cost of immature technology is still high; ROI is still unproven.
- There is a need for new multiparty business agreements; and a need for entire ecosystems to participate.
- There is a lack of standards for data and processes in most domains.
- There is a lack of domain-specific tools for assessing "truth."
- 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.

User Recommendations

- Understand how blockchain, combined with other advanced technologies (most notably AI and IoT) can be used to support authenticated provenance.
- Understand project constraints — for example, new complex business processes, a lack of mature domain-specific tooling, the need for custom integrations, skill scarcity and the lack of experienced vendors.
- Where possible, capitalize on blockchain infrastructure that is already in place.
- Add authenticated provenance blockchain use cases, provided that they are relevant to your business and you can demonstrate ROI through improved efficiencies and new revenue streams.
- Public blockchains like Ethereum or Solana can also be utilized in many instances.
- Address customer demand for greater trust. These technologies give customers confidence in your brand and the provenance of your products.
- Aim to replicate what has worked in supply chain and other sector case studies.
- Start small with well-scoped use cases that need these technologies.

Sample Vendors

Circulor; Copperwire; Jitsuin; SettleMint

Gartner Recommended Reading

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

How to Detect Fakes in a Zero-Trust World Using Artificial Intelligence and Blockchain

Assessing the Optimal Blockchain Technology for Your Use Case

Garbage In, Garbage Forever: Top 5 Blockchain Security Threats

Decentralized Web

Analysis By: Avivah Litan, Adrian Leow

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition

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

Why This Is Important

Web 3.0 implements the protocols that support the most revolutionary aspect of blockchain technology, a peer-to-peer decentralized design that eliminates central authority. To support this vision, users must be able to control their own identities and data. This was the promise of the web before large internet gatekeepers assumed central powerful positions over our web interactions. Blockchain and Web 3.0 can take the web experience to where it was originally “supposed” to be.

Business Impact

Decentralized web enables peer-to-peer interactions with no reliance on centralized platforms and intermediaries. This levels the playing field for all actors, who control their own algorithms, data and market participation. However, although future internet technologies will be more decentralized, this is unlikely to eliminate centralized authorities from most enterprise B2B and B2C use cases. This is because they will not be willing to give up governance and oversight of digital ecosystems.

Drivers

- Traditional web-enabled social media and electronic commerce have revolutionized social interactions, bringing suppliers and consumers of information, goods and services together in a peer-to-peer setup on a global scale.

- With Web 2.0, all these interactions and transactions require a digital platform (like those of eBay, Amazon, Alibaba Group, Google and Uber) acting as a trusted provider or broker between entities who do not know or trust each other. These platforms have created a valuable peer-to-peer economy, but they also define the relationship rules and host all of the participants’ data. This has proven to be an unscalable environment, as these platforms are forced into the roles of “policing” bad actors and misinformation.

- Decentralized web promises to enable true peer-to-peer interaction and transactions with no reliance on centralized platforms and intermediaries. Even Twitter CEO Jack Dorsey understands that social media platforms must move to the decentralized web (see project Bluesky), where users control their own algorithms, Twitter feeds and data.

Obstacles

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

- Web 3.0 network Polkadot, a Layer 0 blockchain, launched in its first phase in late 2020, but its full promise of parachain networks has yet to be fully tested and implemented. Meanwhile, other Web 3.0 protocols, such as oracles and the decentralized file- and web-hosting protocol InterPlanetary File System (IPFS), continue to mature, and are used in many public blockchain use cases today.

User Recommendations

- Keep abreast of developments in Web 3.0 protocols and standards by monitoring the initiatives of the Ethereum Foundation, Hyperledger, Trust over IP Foundation, Web3 Foundation and ISO/TC 307 for blockchain and distributed ledger technologies.

- Evaluate and pilot blockchain platforms that implement a Web 3.0 vision by giving end users control of their own identity data. These platforms include decentralized identity, verifiable claims, blockchain-based applications and maturing blockchain-based decentralized finance (DeFi) platforms.

- Other blockchain applications in other domains, such as decentralized NFT marketplaces and decentralized gaming, are also using Web 3.0 protocols, and users may find it useful to study these new applications as they come to market.

Gartner Recommended Reading

DeFi, CeFi and How Blockchains Interoperate: Case Study in Carbon Trading

Zero-Knowledge Proofs

Analysis By: David Mahdi, Bart Willemsen, Mark Driver

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 them is correct, without the requirement to transmit or share the underlying information. Blockchain platforms have been evolving to include this privacy-oriented mechanism.

Why This Is Important

Due to cyberthreats and privacy laws, security and risk management (SRM) leaders must support use cases that enable digital business while ensuring data protection. ZKPs enable entities to prove information validity, without the requirement to transmit sensitive data. These protocols limit the requirement for mass decryption/encryption of data elements, which benefits the efficiency of the network as well as the potential adoption of blockchain-based systems.

Business Impact

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

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 law violations (due to the exposure of sensitive information).
- Need for mitigation of sensitive data leakage and cyberattacks.

- Homomorphic encryption, which allows for computation on encrypted variables without revealing their values.

Obstacles

- Even with a variety of working groups (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 till 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 in order to be effective.
- ZKPs require integration into applications. Downstream applications, such as CRMs and databases, will need some modification.

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

Evernym; IBM

Gartner Recommended Reading

Top Strategic Technology Trends for 2021: Privacy-Enhancing Computation

Decentralized Exchanges

Analysis By: Avivah Litan

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition

Decentralized exchanges (DEX) are peer-to-peer cryptocurrency exchanges that operate without intermediaries that clear transactions. Instead, they are automated via smart contracts that support trading. In contrast to centralized exchanges, DEXs do not support any custodial or know-your-customer (KYC) services. This also means users must control their own wallets and private keys when transacting on DEXs.

Why This Is Important

Decentralized exchanges offer trustless smart contract-based peer-to-peer trading that gives users access to the burgeoning world of decentralized finance (DeFi). There were over 35 DEXs (see Defiprime.com) as of May 2021. The leading DEX, Uniswap, is reportedly generating between $2 million and $3 million in daily fees for the exchange's liquidity providers. Over time, more users will be attracted to the financial rewards of DeFi products and services, and will use DEXs to access them.

Business Impact

Enterprises with cryptocurrency holdings are motivated to leverage their holdings by using them as collateral in DeFi-based revenue-generating activities, accessible through Decentralized Exchanges. This will foster improvements in DEX user interfaces, and their surrounding and supportive decentralized services. These include decentralized smart contract logic and bug insurance, that make DEX interactions more palatable to relatively risk-averse enterprise users.

Drivers

- DeFi market innovation is rapid and DEXs are needed to support and access these new markets.
- DEXs provide trustless efficient peer-to-peer transactions executed by neutral and totally transparent smart contracts. This is in direct contrast to centralized banks and exchanges where central authorities must be trusted even though their inner workings and policies are opaque.
- Transactions on centralized systems are not fully transparent and cannot be tracked and traced through their life cycle, as they can on DEXs. This transparency is a major driver for DEX adoption.
- DEX transactions are anonymous; there are no KYC processes on DEXs. This is a major driver for users who want to remain anonymous and retain control over their own finances.
- Transaction fees on DEXs are much lower than on centralized exchanges where users pay for overhead and administration to central authorities and intermediaries.
- Trading of DeFi-supported stablecoins on DEXs grew from $2 billion in 2019 to well over $30 billion by February 2021.
- Users want to retain control of their own financial interactions. Traders manage their own self-hosted wallets and private keys on DEXs, as opposed to on centralized exchanges where they give control to the central organizations.
- DEXs give buyers and sellers access to thousands of cryptocurrencies that are not listed on centralized exchanges.

Obstacles

- DEX user interfaces are technically difficult to navigate and are not suitable for casual users. Typos and data entry mistakes are easy to make and may result in permanent loss of funds. Users must know how to connect self-hosted wallets to DEXs and how to fund wallets through various and complex cryptocurrency transfer protocols. For example, Bitcoin cannot live on Ethereum, the blockchain for most DEXs, so Bitcoin must be 'wrapped' into a coin that can exist on Ethereum before it can be traded in a DEX.

- DEXs do not directly interface with banking systems so it is technically cumbersome to get fiat money into DEXs and it is difficult to move cryptocurrencies from DEX back into bank accounts.

- Smart contracts are primary targets of hackers, who learn how to exploit their logic. Funds managed by a smart contract are therefore subject to theft, and fund recovery is almost impossible.

User Recommendations

- Wait for existing centralized financial services to interface with DeFi before your organization engages with decentralized exchanges, so that decentralized trading activities can be protected with regulations and legal frameworks and user interfaces can be improved.

- Ensure you have smart contract insurance that can protect any assets you have in DeFi against smart contract hacks, if you go ahead and engage in decentralized trading on DEXs before regulatory frameworks are in place.

- Stay abreast of developments in DEXs by monitoring them on Defiprime.com

Sample Vendors

Uniswap; Curve; PancakeSwap; SushiSwap

At the Peak

Smart Contract Oracle

Analysis By: Martin Reynolds, Avivah Litan

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition

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

Why This Is Important

Smart contract oracles enable blockchain smart contracts to interact with real-world events, thereby integrating blockchain systems into the world outside of a blockchain network.

As distributed ledgers and smart contracts do not otherwise have a mechanism to fetch data from the external world, smart contract oracles are the only way to build a mutually trusted mechanism to leverage blockchain into business processes.

Business Impact

The availability of reliable and effective oracles will play a crucial role in the development of smart contracts in most use cases involving real-world assets.

Once participants in a blockchain network recognize and trust the authority of a smart contract oracle, blockchain business processes can operate without supervision.

This unsupervised operation can deliver on the promise of blockchain efficiency.

Drivers

- **Recognition of smart contract 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, such as cash management in a supply chain. Oracles provide necessary controls and triggers to automate trustless smart contract operations.

- **Emergence of decentralized oracle systems that provide trusted transaction triggers.** Oracles dependent on a single source of information are vulnerable to accidental or deliberate interruption, potentially compromising the flow of business. Decentralized oracles provide significantly stronger mechanisms for trusted, reliable triggers to execute smart contracts.

- **New value propositions driven by smart contracts with authoritarian issuers.** Baseball trading card tokens, for example, represent a recent success story for smart contracts. The tokens represent a limited license to the card and image. However, these tokens and their smart contracts remain under control of the issuing entity. The entity has an authoritarian role in managing the asset and can therefore make unilateral changes to correct many transactional or ownership issues that arise. Eventually, control will have to pass to a decentralized or independent entity to continue growth. However, an authoritarian system is an effective defense against early implementation errors and enables ready evolution of the system.

Obstacles

- **Integration of blockchain ledgers with existing systems of record is challenging.** Blockchain systems represent an immutable, agreed record between parties. However, each party has internal systems of record, typically built on robust, but dated, systems and software. These systems must be updated to ensure that they agree with blockchain records. This upgrade is not a trivial task.

- **Oracles may be subject to tampering.** Oracles are dependent on the information sources that 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 would cause payments to pass without delivery of the product or service.

- **Compromised smart contract results are hard to correct.** If a smart contract commits an incorrect transaction to the blockchain, it is difficult to correct. In cases not involving anonymous parties, the transaction can be reversed by an appended counter transaction.

User Recommendations

- **Identify integration and data needs with systems of record for smart contract use cases.** Integration with 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. These changes will extend to both old and new systems.
- **Build appropriate integrity and reliability mechanisms into oracle systems.** Your oracles are at risk from lost or corrupted input signals that can trigger fraudulent transactions or suppress legitimate transactions. Defend your oracles by selecting, validating, protecting and decentralizing their support systems.
- **Create processes to adjudicate and reverse incorrect transactions.** When a participant comes to you reporting a failed transaction, you need a predetermined agreement for handling these issues. Options for remediation include negotiated off-chain resolution; unilateral reversal in favor of the participant; arbitration; and dismissal.

Sample Vendors

Chainlink; Provable; Reality.eth; Town Crier

Gartner Recommended Reading

Managing the Risks of Enterprise Blockchain Smart Contracts

Predicts 2020: Blockchain Technology

Guidance for Blockchain Solution Adoption

Market Guide for Blockchain Platforms

Blockchain and IoT

Analysis By: Nick Jones, Avivah Litan, Benoit Lheureux

Benefit Rating: Transformational

Market Penetration: Less than 1% 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 the IoT can be combined in many ways for purposes such as machine payment, identity management, tokenization of IoT-related assets or services, identity validation, provenance tracking, sensor data authentication, utilization recording or billing, and secure firmware updates. This technology will enable enterprises to create new digital business offerings and ecosystems, and to manage requirements (e.g., proving provenance or compliance) in new ways.

Business Impact

Blockchain can provide a decentralized mechanism to secure the results of critical IoT data from hardware, software and systems operations through consensus. Combined with IoT data and processes, blockchain provides an immutable data audit trail. It also supports process automation in situations in which IoT devices create or consume value in a peer-to-peer context — e.g., by making payments, providing services or generating assets, such as solar power.

Drivers

Many blockchain platforms and IoT technology vendors have demonstrated integration between IoT and blockchain. In cases where there's a need to do so, it has proved to be feasible. Situations in which IoT and blockchain can be usefully combined include:

- IoT is performing critical functions — tampering with the system or the data it creates and uses could have major financial or safety implications.
- IoT devices need to make or take payments using a cryptocurrency.
- IoT is participating in advanced business models involving distributed applications (aka dapps) and smart contracts.
- IoT devices need to share immutable information with an ecosystem of business partners and other machines — for example, for product provenance and tracking, or supply chain applications.
- IoT needs to provide an immutable audit trail logging its actions, system updates etc.

- The IoT device needs strong proof of identity of itself and of other IoT devices with which it communicates.

Obstacles

Challenges include:

- Blockchain and IoT integration is still immature, facing challenges in areas such as scalability.
- Many IoT devices are computationally simple, with limited networking bandwidth. Hence, they are unable to act as primary nodes storing a copy of a blockchain, and as a result, they need to rely on proxies or gateways, which introduce risk and complexity.
- Blockchain is technological overkill when what's required is just immutable data storage without shared ecosystems, business rules or tokenization. In such cases, consider immutable databases or ledgers (e.g., Datomic or Amazon QLDB), or a centralized blockchain ledger.
- Many public blockchain systems evolve with regular forks and updates. This can pose challenges if it implies updates to large numbers of resource-constrained, long-lived IoT devices.
- Most IoT applications and data aren't critical enough to warrant the use of blockchain. Simpler alternatives include encrypted data and signed firmware updates.

User Recommendations

CIOs, enterprise architecture and technology innovation leaders should:

- Look for situations in which 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 adequate alternative solutions that are technically simpler, because combining blockchain and IoT is potentially complex. Focus on simple applications such as ensuring provenance, proving identity and securing system updates.

- As is the case with most blockchain applications, private blockchains with known ecosystem members are likely to pose fewer technical and governance challenges.
- Beware of applications involving long-lived IoT devices and data, which will require the ability to periodically deploy blockchain technology updates at scale.

Sample Vendors

Chronicled; IBM; IOTA Foundation (Tangle); modum.io

Gartner Recommended Reading

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

Top 10 Strategic Technology Trends for 2020: Practical Blockchain

Integrating Blockchain With IoT Strengthens Trust in Multiparty Processes

Survey Analysis: IoT Adopters Embrace Blockchain

Layer 2 Solutions

Analysis By: Adrian Leow, Avivah Litan

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition

Blockchain Layer 2 protocols are a type of distributed authentication protocol that authenticates groups of transactions without immediately committing them to the blockchain. Transaction chains are committed only when they affect the primary blockchain — this approach reduces network activity.

Why This Is Important

Blockchain systems today are limited in their transaction capacity because of the need to record every transaction at every node. Layer 2 solutions offload strings of grouped transactions to a sidechain, an approach that significantly increases the transaction capability of blockchain without compromising integrity.

Business Impact

If Layer 2 solutions such as channels and sidechains are eventually supported by most blockchain core protocols, blockchains could then support diverse scenarios for value exchange and promote interoperability. However, this kind of layering introduces additional complexity and governance challenges that will take time to overcome.

Drivers

- Layer 2 solutions offer a way of increasing transaction speeds and scaling, while benefiting from the security of the main chain. In some cases, they can process thousands of transactions per second, which will be needed if Ethereum is to achieve wider adoption.
- Layer 2 is what gets built on top of the base chain in order to improve scalability.
- “Channels” offer users a way of making multiple off-chain transactions, while submitting only two transactions to the settlement layer, i.e., Ethereum. This allows for high throughput at a low cost.
- “Plasma” solutions use Merkle trees to create an additional chain to the main blockchain. This facilitates fast transactions at a lower cost, as the blocks aren’t settled on the main chain — and there’s no need to store data on the ledger.
- “Sidechains” run separately from the main blockchain, and operate independently using their own consensus algorithm. They’re compatible with the Ethereum Virtual Machine and connect to Ethereum via a two-way bridge.
- “Rollups” execute transactions on Layer 2, while submitting data to the base chain. This means that they benefit from the security of Ethereum, but can perform transactions outside of Layer 1.
- If Ethereum achieves its full potential, becoming a global trust layer, it’s likely that these Layer 2 solutions will be required to scale the network in combination with Ethereum 2.0.

Obstacles

- Layer 2 solutions can offload transaction processing requirements from the main chain and thereby achieve scalability and performance gains. This approach, while promising, has yet to be proven in terms of scalability, security and manageability. For channels to work, participants are required to deposit funds into a multisig contract and need to be known in advance. That means the network needs to be regularly monitored to ensure that the funds are safe. It also takes time to set up channels between users, which doesn't allow for much open participation.
- There are limits to what you can do using Plasma. The framework only supports certain transactions, for example more complex DeFi activity isn't possible. Withdrawals are subject to potential challenges and longer waiting times.
- Sidechains are limited as they're less decentralized than the main network — the consensus algorithm isn't settled by Layer 1, and sidechain validators could coordinate to act maliciously.

User Recommendations

- Evaluate Layer 2 solutions as a potentially valuable mechanisms for improving blockchain scalability, interoperability and flexibility, but don't tie the success of your business initiatives to this mechanism in the short term.
- Monitor closely the progress and success of current implementations such as Lightning Network to determine the applicability of Layer 2 solutions and channels to your payment token use case.
- Monitor the continuing technical maturity of sidechains as a practical way to make your blockchain implementation more scalable whether you are using public or permissioned blockchains.

Sample Vendors

Connext; DeversiFi; Polygon; OMG; Lightning Network; Raiden Network; SKALE Network; StarkWare Industries

Gartner Recommended Reading

The Future of Blockchain: 8 Scalability Hurdles to Enterprise Adoption

Common Mistakes to Avoid in Enterprise Blockchain Projects

Nonfungible Tokens (NFT)

Analysis By: David Mahdi, Avivah Litan, Michael Kelly

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition

An NFT is a unique blockchain-based digital asset that links to real-world digital assets, such as digital art or music, or physical assets that are tokenized, such as houses or cars. Most NFTs today are unique ERC 721 tokens that live on Ethereum, but other blockchain platforms support them as well.

Why This Is Important

Nonfungible tokens (NFTs) offer the promise of digital ecosystems where owners of digital content (and in some cases physical content), such as artwork, music and games, can use NFTs to allocate digital ownership and rights. Hype and criticism of NFT as a concept has grown dramatically over the last month as the market valuation of NFTs went over $300m. NFTs have much broader applicability in many markets and will open up new types of marketplaces not possible without them.

Business Impact

NFTs present new ways for content creators to manage, promote and monetize their assets via ecosystems. Entities can depend on the validity, integrity and uniqueness of NFTs. Blockchain technology brings tamper resistance to the notion of NFTs, which is traditionally hard to do with many other kinds of digital assets.

Drivers

NFTs offer new methods to ensure trust and integrity with digital and physical content. In addition, 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 lieu of legacy digital signatures, which require a trusted relationship with certificate authorities and tedious 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.

Other driving factors include:

- 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
- Ability to authenticate/validate digital (and in some cases physical) goods. For example, authenticating artwork can be a tedious process today. By leveraging NFT's, ownership (in some cases) and authenticity can be validated in real-time. They can also be linked to applications in the enterprise space, such as with examples from WISeKey
- Evolution of standards required to ensure interoperability, longevity and utility. At this point in time the primary standards are Ethereum based; such as ERC (Ethereum request for comments). Specifically ERC721 aims to standardize NFTs. This standard helped with NFTs such as: Decentraland, CryptoBeasties, Etheremon and the crazed CryptoKitties

Obstacles

- NFTs have yet to demonstrate lasting business models and monetization for content creators, sellers and buyers, meaning that adoption is currently low.
- At this point in time, Ethereum leads the charge with NFT approaches and bridges for interoperability with other blockchains. This means that interoperability will need to expand to include direct connections between other blockchain networks and ecosystems. This will ensure that content is truly valid across digital ecosystems.
- With NFTs just starting to become a reality from a product and solution perspective, business models and approaches haven't fully been realized.
- 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.

User Recommendations

- Conduct POCs. IT leaders that are interested in their potential, should conduct early stage research, and consider investigating how they are made, in addition to NFT ecosystems.
- 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 (see Garbage in, Garbage Forever: Top 5 Blockchain Security Threats). NFT storage should use a distributed file system, for example IPFS; nodes should be replicated across many servers. While NFTs are cryptographically secured on a blockchain it does not mean that the NFT is legitimate. Early reports of "sleepminting" attacks show that NFTs are minted to a well-known user/artist wallet and transferred to a hacker's wallet, without triggering smart contract security checks.

Sample Vendors

Animoca Brands; Fortunafi; OpenSea; Rarible; Ethereum; Kudelski Group; WISeKey

Gartner Recommended Reading

What You Need to Know About Blockchain DeFi

Garbage in, Garbage Forever: Top 5 Blockchain Security Threats

Stablecoins

Analysis By: Avivah Litan

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition

Stablecoins are blockchain-issued cryptocurrencies designed for stability by being pegged to a specific value. The most popular stablecoins today are centralized and collateralized by pegged fiat currencies or assets held in reserve. Other decentralized stablecoins leverage crypto assets as collateral, and the stablecoin is overcollateralized to maintain stability with volatile cryptocurrencies. Noncollateralized stablecoins are decentralized, and price stability is based on an algorithm.

Why This Is Important

As of May 2021, the cryptocurrency market was worth about $2.2 trillion in total, with half of that in bitcoin. Centralized stablecoins are gaining mainstream adoption for domestic and international transactions because of their efficiency, stability and low risk profile. Alternative (non-bank-led) payment companies appear to be preparing to support stablecoin payments, which will move payment volume off traditional payment rails to blockchain networks, threatening existing business models.

Business Impact

Central banks and traditional financial services companies may be caught off guard by the growing popularity of stablecoins, and miss new revenue opportunities that threaten legacy businesses. Stablecoins can undermine existing business models and change the way users interact with financial systems and engage in business. For example, Facebook-backed stablecoin Diem is set to launch in 2021. Diem interactions could rapidly become available to all Facebook users.

Drivers

- Payments today are mainly executed using opaque and highly centralized applications, where back-end systems are based on decades-old architecture. Payment initiators and recipients generally have no readily available and real-time visibility into the movement of their money. Payments today represent a highly inefficient and customer-unfriendly process.

- Most blockchain networks that support B2B and B2C applications today do not support payment settlement within the blockchain application. Instead, most initiate payment requests to a nonblockchain payment network, and use APIs to interface with the payment networks as the payment networks clear and settle the payment. This is a highly inefficient and disjointed process, because payments are not automatically integrated with the blockchain-based transactions.

- The largest stablecoin in circulation today is Tether, with $51 billion in circulation in May 2021. Tether's market cap in March 2021 grew past $40 billion, representing a tenfold growth in over 12 months.

- DeFi-supported stablecoins used in DeFi applications grew from $2 billion in 2019 to well over $30 billion in February 2021.

- Like other digital currencies, including cryptocurrencies, stablecoins can be used not only for payments, but also for leverage or collateral in income-generating applications, such as lending or liquidity-funding (aka yield-farming) applications in DeFi markets. These income-generating applications are especially attractive to users in the current low- to zero-government-interest-rate environments, though using them certainly comes with a lot of risk.

Obstacles

- Tether underwent intense regulatory scrutiny starting in 2019, when the company said it had only enough U.S. dollars in reserve to back 74% of its stablecoin. This situation highlights the need to institute regulatory oversight for fully collateralized stablecoins to ensure that reserves on hand are sufficient.
- 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.

User Recommendations

- Work with organizational counterparts (e.g., in treasury, finance, e-commerce, legal and compliance) to prepare to support implementations of desired functionality.
- Familiarize yourself with the numerous opportunities and risks of digital currencies and stablecoins, and what they mean to your application architecture.
- For payment applications, prepare to integrate stablecoin payments with applications that require it (e.g., B2B blockchain applications or B2C sales applications where 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.

Gartner Recommended Reading

Bitcoin Goes Mainstream: What It Means to You

Decentralized Identity

Analysis By: David Mahdi, Michael Kelley

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition

Decentralized identity (DCI) leverages technologies such as blockchain or other distributed ledger technologies (DLTs) to allow an entity to create and control its own digital identity. Thus, it provides an alternative to centralized IAM architectures by establishing trust in identities and resilience within the overall system, with little reliance on centralized arbiters or identity stores.

Why This Is Important

Isolated digital identities will not scale with the needs of digital business. Online and mobile identities continue to be in a fragmented state due to service providers (banks, retailers, social networks, etc.) forcing consumers to create individual identities for each and every service. DCI offers an alternative approach that does not have the security, privacy and usability issues associated with traditional, fragmented, digital identity approaches.

Business Impact

With DCI, users gain control of their identities and data, enabling service providers to interact with users with greater speed and confidence. Currently, providers typically hoard identity information about users. Leveraging DCI, identity and service providers will be able to increase security and access convenience for end users, while reducing exposure to data breaches and potential privacy compliance violations.

Drivers

- **Vendor investments in DCI:** Due to the ubiquity and influence of vendors investing in this space, there is high potential to drive the DCI market forward. Significant investments have been made by IBM and Microsoft. Other major developments in this space include the acquisition of ShoCard by Ping Identity, and funding received by vendors such as 1Kosmos and InfoCert.

- **Investments in BYOI:** Including investments in overall BYOI could also act as a precursor to DCI adoption. E.g., Microsoft enabling “external identities” with Azure Active Directory (Azure AD).

- **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, without the need to expose sensitive personal data.

- **Standards enabling consistency:** Standards are currently emerging, led by entities such as the World Wide Web Consortium (W3C) and Decentralized Identity Foundation (DIF), to create a consistent approach to DCI. These standards will help propel this technology forward.

Obstacles

- Despite a lot of promise and hype, adoption is slow due to lack of progress and inaction by most large ecosystem players, CIAM vendors and various IDPs including governments.

- Standards are still in the development stage.

- Lack of core DLT/blockchain performance, interoperability, scalability and maturity.

- Lack of clear security standards for DLTs, such as crypto-agility, wallet standards/adoption and security.

- Lack of production-level solutions, which prevents some organizations from deploying due to concerns of having to “rip and replace” in the near future when the solutions stabilize.

User Recommendations

- Deliver attainable use cases as POCs, such as a DCI solution focused on business partners (i.e., limited deployments, low in scale). Plan for, but don't rush, long-term, large-scale initiatives such as consortium and/or DCI interoperable global identity.
- Leverage market vendors, such as IBM, Microsoft or Ping Identity, to understand the possibilities and potential of DCI.
- Be cautious of overoptimistic vendor claims. Evaluate the technical security aspects of blockchain platforms under consideration. In particular, examine vendor plans for support of standards, such as W3C and DIF.

Sample Vendors

1Kosmos; Evernym; Finema; IBM; InfoCert; Microsoft; Ping Identity; SecureKey

Gartner Recommended Reading

Guidance for Decentralized Identity and Verifiable Claims

DeFi

Analysis By: Avivah Litan

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition

Decentralized finance (DeFi) refers to applications that now mostly run on the Ethereum public blockchain. DeFi eliminates the intermediaries and supports trustless, transparent, and immutable transactions between anonymous parties. When compared to centralized financial (CeFi), DeFi lowers transaction costs and improves process efficiencies. Based on open-source protocols, developers assemble financial primitives into reusable transformational applications that are not feasible using CeFi.

Why This Is Important

DeFi applications involve digital assets, smart contracts, and open-source protocols used to exchange value in a reliable and trustless manner between anonymous parties. DeFi implements reusable software modules that are assembled dynamically into applications, utilizing different prebuilt components. Innovation in financial services, commerce and all types of marketplaces is rampant, and promises to disrupt centralized systems and business models.

Business Impact

The DeFi market is embryonic but innovation is rapid. DeFi-supported stablecoins grew from $2 billion in 2019 to well over $30 billion by February 2021. Financial services represent a large chunk of global GDP, yet are opaque and highly centralized, and typically offer inflexible products and services. Back-end systems are based on decades-old architecture. DeFi upgrades this antiquated architecture and offers substantial value opportunities well beyond traditional financial services.

Drivers

- Only when using completely decentralized applications is it possible to avoid paying fees to banks and intermediaries when onboarding customers and managing multiparty processes.
- DeFi executes shared business processes through preagreed, decentralized smart contracts. Blockchain protocols keep transactions transparent, immutable and Byzantine fault tolerant (trustworthy).
- DeFi facilitates the creation of new products and services that the market will benefit from. One example is ilateral collateralized lending processes between two anonymized parties, underpinned by smart contracts that eliminate the need for cumbersome paperwork.
- DeFi facilitates faster, cheaper and transparent payments between businesses and individuals, leading to more pleasant user experiences.
- 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.
- Innovation is rampant within DeFi, as developers are incentivized by native lucrative rewards for widely adopted applications.

Obstacles

- There is no regulatory protection if things go wrong.
- DeFi technology is immature and hard to use, despite billions of dollars moving through it.
- DeFi applications are prime targets for hackers. Seventeen major DeFi exploits and hacks occurred in 2020, resulting in a loss of $154 million. See The DeFi hacks of 2020. Hackers typically exploit logic flaws in smart contracts. Users have no recourse by law, but can insure for certain smart contract bug conditions, using DeFi insurance from firms such as Nexus Mutual.
- Security risks are real from both a financial and product perspective. Over time, risk mitigation solutions will emerge and DeFi will go mainstream. It is far too potentially transformational to remain on the sidelines.

User Recommendations

- Prepare to integrate DeFi into their application portfolios if there are DeFi modules that uniquely solve an existing problem or create a new business opportunity. By the end of 2021, DeFi technology will be ready for early enterprise adoption, as long as regulatory guidance is clear.
- Integrate DeFi modules with existing CeFi 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 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 the marketplace in the future.

Gartner Recommended Reading

What You Need to Know About Blockchain DeFi

DeFi, CeFi and How Blockchains Interoperate: Case Study in Carbon Trading

Blockchain Interoperability

Analysis By: Avivah Litan

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

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

Dozens of blockchain platforms exist today, yet they 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 the markets and data they can easily access. Users and services can trade assets and information across blockchain networks and with other participants and services. The uber-network is more powerful than the sum of the individual blockchain ones because of the network effect. For example, a seller of Ethereum NFT art will be able to sell the art to users trading in other blockchain markets.

Drivers

- Disparate blockchain networks are growing individually in their own separate ecosystems. See Blockchain Platforms Reviews and Ratings for a sample list of platforms.

- 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 DeFi networks, primarily Ethereum, are also quickly expanding. These applications need to interoperate with centralized finance networks, along with non-Ethereum networks, so that information and assets can be freely traded and shared with expanded markets.

- There are many emerging and now-maturing solutions for blockchain interoperability. Blockchain-neutral Oracles integrate legacy systems and data with smart contracts on multiple blockchains, so that users do not have to rewrite their applications for different smart contract protocols. Digital currency and token exchanges/bridges enable the exchange of one fungible token for another, and support the transfer of non-fungible tokens from one blockchain to another. Special purpose blockchain interoperability protocols or ecosystems support “blockchain of blockchain” networks such as PolkaDot or Cosmos.

Obstacles

- Blockchain interoperability differs from typical system interoperability. In addition to message format and protocol translation, the former must protect against double spending or entries when transactions are posted from one blockchain platform to another.
- Competition in approaches is healthy, but translates to market confusion in the short term.
- Interoperability methods other than fungible token exchange have not been thoroughly tested and vetted.
- Interoperability options have been largely developed for public blockchain cryptocurrency use cases. Enterprise requirements may not be fulfilled by most of them.
- Enterprise blockchain use cases are still struggling to find traction in most cases. Less than 20% of enterprise projects have moved into production, and the existing production volume is still small relative to public blockchain use cases. Interoperability is, therefore, not at the forefront of enterprise blockchain project user requirements.

User Recommendations

- Work with blockchain platforms and system integrators that make these interoperability options easily and readily available to your applications.
- Favor interoperability options that provide a layer of blockchain abstraction middleware to your applications, and which handle the complexities of interoperating across blockchains.
- Prioritize use of evolving token gateways and exchanges if your needs boil down to needing to transfer tokens from one blockchain to another.
- Prioritize use of oracles if your needs center around writing off-chain services and linked smart contracts that are blockchain neutral.
- 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.

Gartner Recommended Reading

DeFi, CeFi and How Blockchains Interoperate: Case Study in Carbon Trading

Guidance for Adopting a Blockchain Solution

SMPC

Analysis By: David Mahdi, Bart Willemsen, Brian Lowans

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition

Secure multiparty computation (SMPC) is a method of distributed computing and cryptography that enables entities (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 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 overall business objectives. Historically, data protection has focused mainly on two states: securing data at rest and in transit. However, SMPC-based methods introduce data protection in use. This is a new paradigm to the arsenal of security methods and enhances traditional security approaches.

Business Impact

Due to their reliance on data for AI-based decision making and the sharing of insight from those decisions between multiple parties, SRM leaders need privacy-enhanced approaches to protect data amid a landscape of maturing data protection regulations. SMPC allows for the secure enablement of business, enabling organizations to leverage their data while addressing security and privacy concerns.

Drivers

- Traditional 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.
- SMPC-enabled data security allows for the protection of data while in use; thus providing SRM leaders with another data protection technique, which can be applied to new and existing use cases (such as multiparty data sharing).
- New use cases such as big data analytics, artificial intelligence (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.
- Relative to other privacy protection methods, such as homomorphic encryption, SMPC can be much faster.
- SMPC helps ease fear of privacy law violations (due to the exposure of sensitive information).
- SMPC enables mitigation of sensitive data leakage, and overall reduction and mitigation of cyberattacks.

Obstacles

- SMPC algorithms can be latency-sensitive. As such, performance in some cases might not meet client requirements or expectations.
- Although considerable academic research has been conducted on SMPC, relatively limited number of practical implementations have emerged so far.
- When compared to existing techniques (such as cryptography based on hardware-generated and stored keys), clients could have potential issues with audits, especially if they have to adhere to standards like Federal Information Processing Standards (FIPS) certifications.

User Recommendations

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

Sample Vendors

Baffle; Cybernetica; Inpher; IXUP; LiveRamp; Nth Party; Sepior; Snowflake (CryptoNumerics); Unbound Security; Ziroh Labs

Gartner Recommended Reading

Achieving Data Security Through Privacy-Enhanced Computation Techniques

Top Strategic Technology Trends for 2021: Privacy-Enhancing Computation

Tokenization

Analysis By: Martin Reynolds

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition

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

Why This Is Important

Tokenizaton is the bridge between business processes and the blockchain, and is therefore on the critical path for every business blockchain project that manages real-world assets through tokens on a blockchain. Correctly implemented, tokenization makes a business project run smoothly by creating clear, manageable connections between the blockchain world below and the business world above.

Business Impact

Tokenization is key to implementing a blockchain project involving real-world assets. Today's systems rely on trust in other parties. Weak tokenization strategies work in a private blockchain where a single entity can readily correct errors. However, for a blockchain operated by a consortium, a strong tokenization strategy with verified implementation is critical to acceptance and success.

Drivers

- **Blockchain smart contract and tokenization platforms are well-advanced.** Ethereum is a representative example because of its high value and broad adoption, which indicates that the underlying platform is secure. Other solutions exist.

- **Tokens are well-developed on the Ethereum platform.** Ethereum was designed to support multiple dependent tokens through its smart contracts. These dependent tokens typically follow Ethereum standards, enabling interoperability across tokens. As tokens draw attributes from the underlying platform, security and functionality are well-developed.

- **Tokens provide an effective bridge to real-world assets.** The underlying integrity of the blockchain system delivers a trustworthy attestation of token ownership, strong enough that tokens can be legally linked to real-world assets.

- **Tokens enable new business models around real-world assets.** Once an asset is legally linked to a token, ownership can be fully managed on the blockchain. Furthermore, blockchain techniques enable partial shares in an asset without a complex legal process.

Obstacles

- **Linking tokens to real-world assets requires effective legal frameworks.** Although ownership of a token is trustless, provable and possibly anonymous, linking the token to a real-world asset is dependent on the legal system. In many cases, the legal system will not support such a link (for example, paper land records are the ultimate authority — not a blockchain token). Therefore, legal frameworks have to develop further to support electronic ownership.

- **Authenticating blockchain events is not necessarily a trusted process.** Smart contracts will transfer a token if the appropriate input conditions are recorded on the blockchain. If those input conditions are compromised, the smart contract output may be incorrect.

- **Coding errors can be expensive.** Flaws in the blockchain protocol or smart contracts will result in erroneous transfers of assets. Proper vetting and testing of critical smart contracts is a difficult process, particularly if the code is complex.

User Recommendations

- **Engage legal assistance to secure real-world relevance.** Engage your legal team to create enforceable contracts that support the blockchain initiative. These contracts will span multiple legal jurisdictions and must be designed to reduce legal interventions.

- **Ensure data sources that trigger transactions are appropriately vetted.** The events that trigger a smart contract are a critical control point in a blockchain system. Therefore, these events must be carefully selected, vetted and implemented outside the blockchain system.

- **Use redundant oracles when public data sources have material influence on transactions.** Any single oracle can be compromised. By aggregating data from multiple oracles, smart contract inputs become more trustworthy.

- **Thoroughly vet your code, system and protocols before opening to multiple masters.** By limiting the system to a single master, code can be updated and erroneous transactions reversed. We anticipate that many systems will never deploy to multiple masters.

Sample Vendors

Chainlink; Provable; R3

Gartner Recommended Reading

Managing the Risks of Enterprise Blockchain Smart Contracts

4 Blockchain Silver Bullets That Will Not Solve Business Problems

Garbage In, Garbage Forever: Top 5 Blockchain Security Threats

Sliding into the Trough

Smart Contracts

Analysis By: Martin Reynolds, Avivah Litan, Adrian Leow

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition

A smart contract is a type of blockchain record that contains externally written code, and controls blockchain-based digital assets. When triggered by a specified blockchain write event, a smart contract immutably executes its code and may result in a cascading blockchain event. Smart contracts can only read from, and write to, the blockchain. All off-chain interactions with smart contracts must be handled by agents that map between off-chain assets and on-chain digital assets.

Why This Is Important

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

Business Impact

Once smart contracts and business blockchain technologies are functional and effective, smart contracts can significantly improve capital efficiency by cutting administrative overhead and reducing working capital. We estimate that in, for example, manufacturing, smart contracts could increase cash efficiency by 5%.

Drivers

- **Ethereum smart contracts represent proven technology.** Ethereum smart contracts run not just the Ether cryptocurrency, but also enable the derivative cryptocurrencies that run using the Ethereum blockchain. Ethereum smart contracts represent a valuable target for attackers, but attackers have only succeeded in exploiting errors in smart contract implementations, not the Ethereum smart contract system.

- **Oracles provide trusted contract triggers.** Smart contracts operate only on records committed to the underlying blockchain. Distributed oracle technologies that record smart contract trigger events on the blockchain provide the trust necessary for business operations.

- **Use cases demonstrate blockchain links to the real world.** In 2020 and 2021, markets emerged for collectible assets linked to nonfungible tokens (NFTs) through smart contracts (ERC-721 standard). Trading cards, images and art are three such applications. Although the long-term value may be questionable, the cash paid for NFTs demonstrates confidence in the underlying blockchain technology.

Obstacles

- **Legal systems not ready for blockchain.** Enforcing the link between the blockchain token and the real-world asset may not withstand legal challenges, particularly if an asset is incorrectly transferred and the current holder does not relinquish ownership. The problem compounds with disputes that cross legal systems, for example with one party in the U.K. and the other in Brazil.

- **Immaturity of off-chain systems and blockchain code.** Although multiple smart contract platforms exist, few have been tested to an extent sufficient to guarantee correct behavior. In many cases, operation in a controlled environment with a trusted adjudicator can compensate for any issues that emerge, but adjudicators may be unwilling to engage in resolving disagreements.

- **Complexity of smart contracts.** Smart contracts are code, and code has bugs. In a complex smart contract, a developer may even conceal code for personal profit that may be difficult to remove.

User Recommendations

- **Ensure legal agreements bound behavior of your blockchain partners.** Although enforcement may be difficult, a clear framework defining what the platform does and does not do, and how disputes are escalated and arbitrated, is essential.

- **Budget for unresolved errors in smart contracts.** There will inevitably be some failures in smart contracts, and the arbitrator may not be willing to step in if the issue is not significant and obvious. Therefore, you should expect some losses and gains on smart contracts. Focus only on major or systematic errors that are worth the effort of remediation.

- **Manage the risk of smart contracts by means of open code and third-party providers.** There are three mechanisms that can protect against errant smart contracts. The first is to request published source code. The second approach is to use a smart contract mutually sourced from a third party, with guarantees of correct operation. The last approach is to use a third party for indemnification only.

Sample Vendors

Chainlink; Ethereum; Solana; Valid Network

Gartner Recommended Reading

Managing the Risks of Enterprise Blockchain Smart Contracts

Predicts 2020: Blockchain Technology

Guidance for Blockchain Solution Adoption

Garbage In, Garbage Forever: Top 5 Blockchain Security Threats

Blockchain Platforms

Analysis By: Rajesh Kandaswamy, David Furlonger

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition

Blockchain platforms provide the foundation to create and run blockchain solutions and decentralized networks. This includes support for distributed ledgers, decentralized consensus, tokenization and smart contracts. They enable creation of blockchain solutions that provide immutability, transparency, decentralized contract execution, and tokenization of physical or digital assets.

Why This Is Important

Blockchain platforms are the foundation on which blockchain applications are built and managed. The key aspects of blockchain — such as a distributed ledger, immutability, transparency, tokenization and support for smart contracts — are implemented through use of a blockchain platform. They also provide supporting services, such as developer languages, performance tuning and monitoring, security services and support for blockchain interoperability.

Business Impact

Blockchain platforms can play a key role in creating blockchain solutions and networks that change the commercial terms and governance structures of business and society. This is achieved by decentralizing and automating digital business, offering capabilities that support and foster autonomous, peer-to-peer (P2P) transactions, diverse value-exchange scenarios, on-demand markets, smart assets, smart contracts and the operation of decentralized autonomous organizations (DAOs).

Drivers

- Blockchain platforms continue to evolve to support the core elements of blockchain technologies identified in the Definition section.
- Platform developers are also attempting to build out traditional application stack capabilities. These include better modelling support, developer tools, frameworks, integration mechanisms and software development kits (SDKs).
- Feedback from early adopters along with enhanced design is leading to improved performance of the leading platforms.
- Development continues to progress in design, testing and piloting across different industries and has gained more traction with the digital acceleration fostered by addressing the challenges brought about by COVID-19.
- As digital acceleration pervades all industries and the public sector, more attention is being paid to specific use cases that blockchain platforms can support — such as the provenance of data or goods, portable identity, asset tokenization, payments, central bank digital currencies, among others.

Obstacles

- Lack of clear success and proven use cases have been a challenge for promoting adoption.
- Most projects require cooperation among different entities, but achieving governance and cooperation across multiple enterprises is proving difficult.
- Adopting blockchain features and capabilities to provide business value requires that enterprises process adjustments which are disruptive to today's business processes that most enterprises are not willing to bear.
- For enterprises, the full scope of decentralization demands that the platform has to solve competing demands in terms of cost, performance and security. This is while trying to match or better traditional features expected of enterprise software, including ease of use, developer support, reporting, interoperability and integration.

User Recommendations

- Evaluate your strategy for pursuing one of five solution archetypes (see Use 4 Business Currencies and 5 Archetypes to Evaluate Blockchain Initiatives). Once chosen, assess vendor offerings extremely carefully using a technology-agnostic function framework to ensure an apple-to-apple comparison (see Guidance for Assessing Blockchain Platforms).
- Prepare for continued evolution, a shifting competitive landscape and consolidation of offerings.
- Check the level of platform openness, decentralization and tokenization functionality throughout the platform stacks carefully, as well as upgrade paths — especially in a multiparty business setup and/or consortia.
- Assess vendor capabilities for protocols, interoperability, integration, security mechanisms, performance, manageability, tooling and support.

Sample Vendors

Enterprise Ethereum; Hyperledger; Nexledger Universal; R3 Corda

Gartner Recommended Reading

Guidance for Assessing Blockchain Platforms

Guidance for Blockchain Solution Adoption

Use 4 Business Currencies and 5 Archetypes to Evaluate Blockchain Initiatives

How to Operate and Support Blockchain Platforms

How to Position Blockchain Platforms to Increase Adoption

Blockchain PaaS

Analysis By: Adrian Leow, Avivah Litan

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition

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

Why This Is Important

Developers seeking to implement blockchain-based applications require specific services that span compute, application, storage and network services, both for initial implementation and ongoing operations. bPaaS is a cloud service offering from enterprise cloud vendors. The cloud vendors aim to combine these basic blockchain services to provide enterprises a one-stop service shop that brings the benefits of cloud elasticity and compute costs to blockchain.

Business Impact

bPaaS is attractive to enterprises experimenting with blockchain. But enterprises quickly move past needing basic blockchain infrastructure services.

Microsoft, the first cloud vendor to offer bPaaS in 2017, is exiting this business in September 2021. Enterprise developers need assistance with much more complex capabilities higher up the stack. Vendors such as ConsenSys, Kaleido, SettleMint and Simba offer more advanced services with multiple clouds, multiple protocols and services for applications, and interoperability between blockchains and legacy systems.

Drivers

- The core value of a distributed ledger, which has fueled the hype and interest among many in the technology industry, is to enable decentralized/distributed open-source applications that avoid reliance on just one organization, server, data center or network. Most versions of bPaaS trade this core value for the convenience of vendor assistance, although this trade-off is expected to be addressed by greater interoperability and standardization in the future.

- Currently, in most cases, the primary value of bPaaS is to “jump-start” the ability of enterprise developers to rapidly set up an initial test system or prototype — as opposed to a truly decentralized production system.

- Because bPaaS is dependent on a restricted perspective of blockchain, and is affected by blockchain’s immaturity, its future prospects are limited compared to enhanced competitive services.

- Each bPaaS vendor attempts to add unique elements around support for multiple blockchain platforms, security, interoperability, analytics and performance to differentiate their offerings in exchange for single-sourcing and centralization of public execution and ledger storage. In many cases, the cloud vendor’s bPaaS supports one or a few blockchain platforms. But relying on one vendor for all nodes of the distributed ledger negates some of the advantages of using a distributed ledger in the first place.

Obstacles

- bPaaS encompasses platform services or cloud-based blockchain developer toolsets. Over time, however, we expect other blockchain-based applications and business services to become available in the cloud as enhanced blockchain-based SaaS.

- Full-stack blockchain managed services are starting to emerge and are being supported by several vendors.

- Support for different consensus mechanisms, tools, frameworks and smart contract capabilities remains limited and continues to evolve. Interoperability for distributed ledgers across competing platforms or clouds is extremely limited at this early stage of evolution.

- Every blockchain platform will undergo major changes during the next two to five years. Some platforms, however, will keep up with evolutionary changes that keep them scalable and competitive.

User Recommendations

- Use current bPaaS offerings to primarily help jump-start your POCs, smaller projects or your experiments with blockchain technologies, as long as you are comfortable with limiting your experience to what bPaaS can provide.

- Expect a wider range of options to be available, with additional services and increased interoperability, as blockchain technologies and enhanced bPaaS offerings and platforms evolve.

- Be aware that cloud providers support a limited set of platforms, and their goal is to sell you more of their own services, rather than support blockchain projects in a cloud-neutral environment.

- Avoid commitments to bPaaS for mission-critical initiatives until greater maturity occurs, platforms and services are interoperable across heterogeneous environments, and services move up the stack.

- Determine all aspects of the blockchain technologies that you will need and ensure they can be supported on the bPaaS offering of interest.

Sample Vendors

Amazon Web Services (AWS); Ant Group; IBM; Oracle

Gartner Recommended Reading

Common Mistakes to Avoid in Enterprise Blockchain Projects

Consensus Mechanisms

Analysis By: Adrian Leow

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition

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

Why This Is Important

Blockchain consensus mechanisms guarantee that all transactions on a network are authenticated and synchronized. Such consensus mechanisms are necessary for blockchain networks to ensure that every node is connected to the same network and all transactions are regularly verified. Every blockchain network generally doesn't use the same consensus mechanism since different outcomes are desirable with different applications.

Business Impact

- An effective consensus mechanism is critical to moving from a single authority blockchain to a distributed authority consensus mechanism.
- Distributed authority is an essential component of a trusted, shared blockchain system.
- A successful consensus mechanism attracts participants and increases the business value of blockchain.

Drivers

Proof of work (PoW) is a consensus mechanism used by the first distributed ledger, embodied in the Bitcoin blockchain. The design of the PoW process — one block of approximately 2,000 transactions every 10 minutes on the Bitcoin blockchain — has set some upper bounds to transaction volume. Newer mechanisms have been developed to address problems of scalability, expense, network latency and so on, including:

- Proof of Stake (PoS) — More than a dozen variants of PoS models include transparent forging and delegated PoS. Ethereum has done a “first release” of a PoS consensus mechanism (titled “Casper”) code to GitHub, with the intention of Ethereum migrating to a full PoS system in the future.
- Proof of Authority (PoA) — PoA blockchains are secured by the validating nodes that are arbitrarily selected as trustworthy entities. Model relies on a limited number of block validators; this is what makes it a highly scalable system. Blocks and transactions are verified by preapproved participants, who act as moderators of the system.
- Practical Byzantine Fault Tolerance (PBFT) — The advantage of PBFT is that it can be more efficient than PoS and PoW, allowing throughput of thousands of transactions per second. The disadvantage is that it has only been used for small numbers of nodes in closed networks. It is suitable for some private blockchain scenarios, and is currently used by Hyperledger Fabric.
- Proof of Space, Proof of Importance — Based on holdings of a cryptocurrency and the volume of transactions a stakeholder undertakes. NEM Foundation uses this mechanism for its currency XEM.
- Other Consensus Algorithm Mechanisms — These include Federated Byzantine Agreement (FBA), Byzantine Altruistic Rational (BAR), proof of burn, quorum slicing, prediction markets, Unique Node Lists, Tangaroa, proof of DDoS, Sieve, Raft and proof of elapsed time.

These examples highlight a technology that is still evolving, with each new mechanism offering its own set of benefits and trade-offs.

Obstacles

- There are promising algorithms such as proof of elapsed time and proof of space, but these have yet to be fully implemented or tested.
- Unless and until the viability of different mechanisms can be proven in multiple business contexts, the future of blockchain/distributed ledgers at an industrial scale will be limited.
- For example, PoW has major issues with scalability and the cost of computational resources, but an almost unblemished record of security, availability and resiliency. PoS has many variants, most yet to be proven.
- PBFT is proven but only for a relatively small number of machines, usually with a single point of vulnerability built in (the central access control over the closed private network).
- All of these mechanisms face challenges, including crash failure (when a process abruptly stops), byzantine failure (e.g., conflicting data causing long delays), market adoption, ledger interoperability and skills availability.

User Recommendations

Application and software engineering leaders evaluating what benefits could result from embarking on a blockchain project should:

- Start with a central authority, and plan to move to distributed authority when all bugs are resolved.
- Educate IT and business leaders as to the importance of decentralization and the role of consensus mechanisms in influencing control, for example, over decision making, data, customers, tokens, etc.
- Ensure you have sufficient understanding and analysis of how different platform providers use their respective consensus mechanisms, and the relationship to resources (that is, energy) consumption, token applicability and market adoption.
- Ensure you have sufficient technical expertise to recognize mechanism failings as a key component of blockchain adoption and managing operational risks.

Sample Vendors

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

Gartner Recommended Reading

Guidance for Assessing Blockchain Platforms

Assessing the Optimal Blockchain Technology for Your Use Case

Climbing the Slope

Blockchain Wallets

Analysis By: Avivah Litan

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition

Blockchain wallets store critical information, such as private keys, that users need to conduct cryptocurrency transactions, including buying, selling or viewing cryptocurrency accounts. Wallets 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 provide critical safekeeping of and access to blockchain-based assets, ranging from cryptocurrencies to non ungible tokens (NFTs). Wallets are the gateway to blockchain-based marketplaces and transactions, and different types of wallets serve very different types of users. Users have complete control over their own wallet contents, such as cryptocurrencies, identity data or NFTs. Wallet capabilities are advancing quickly as users demand more features from them.

Business Impact

- As cryptocurrencies, NFTs, decentralized finance (DeFi) and blockchain businesses become mainstream, users must secure access to these transactions and services. Wallets are essential to enabling decentralized applications and businesses to thrive, so they must be carefully architected.

- User access is enabled through a private key, but private keys represent a single point of failure.

- User account takeover is the No. 1 attack vector for bad actors who steal blockchain-based funds or assets.

Drivers

- Most mainstream users cannot manage the complexities of cryptographically secured access, and need to outsource it to a trusted wallet provider.

- As cryptocurrencies move into the mainstream, 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. Some DeFi wallets offer asset management features attractive to advanced DeFi users.

- 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 computing (SMPC) is a feature of some wallets for users who want to avoid the problem of 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

- Compromises of private keys stored in wallets subject users to complete loss of blockchain holdings.

- Determined criminals circumvent most phone authentication techniques used to protect online user wallets. Criminals use methods such as “SIM swaps” or via malware on a victim’s phone that directs SMS messages to the hacker’s phone.

- 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.

- Hardware wallet keys are kept off the internet, and transactions are confirmed in the device. Access to a hardware wallet can be further secured by multifactor authentication. Three aspects of these wallets make them difficult for the average organization or user to use. The user interface is relatively primitive and sparse. Complex methods of key recovery are required when hardware wallets are lost. And the hardware wallet itself must be secured.

User Recommendations

- Secure your organization's cryptocurrency wallet(s) using the strongest security measures that your organization can manage.

- For ease, use an online wallet available through a "reputable" exchange. Use 2FA and, potentially, multisignature payment options to secure it.

- Keep any online wallets empty and unlinked from your organization's bank account until you choose to use them for ransomware payments.

- 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.

- Custodians of user crypto accounts: Use advanced custodial wallets that come with many security, policy, account and key management features.

Sample Vendors

Conio; MetaMask; TokenSets; Trezor; Trustology

Decentralized Applications

Analysis By: Adrian Leow, Rajesh Kandaswamy

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition

Decentralized applications (dapps) are applications that connect to a decentralized Ethereum blockchain peer-to-peer (P2P) network. Compared with traditional internet applications that are based on a centralized server that is a controlling authority for the whole application, dapps use Ethereum-based smart contracts for their application logic. This means no single entity controls the application logic.

Why This Is Important

Dapps form a basis of disruptive competition for digital business; they are part of an ecosystem reinvention of new software constructions that emerged from blockchain platform technologies. They provide the ability to build complex, multiparty applications that rely on underlying smart contracts sitting inside distributed ledgers. Dapps offer the potential to bring a layer of computation that ties to blockchain smart contracts, but much more technology maturity is required for that to occur.

Business Impact

The dapps market will enable organizations to collaborate and transact as part of business ecosystems:

- It will develop and focus on a common set of capabilities across blockchain adopters — especially in financial services, government, healthcare, education, manufacturing and utilities.
- Many of the enterprise applications involving multiple parties that are candidates for blockchain will require some amount of pre-agreed-upon third-party smart contract logic, which leads to a role for dapps.

Drivers

- Many dapps are nascent and considered experimental in testing decentralized network possibilities. Many dapps have seen significant market traction, with notable success in financial, infrastructure and gaming.

- Dapps use cryptocurrencies as the built-in medium of exchange, which could dramatically boost mainstream adoption of cryptocurrencies. With all the hype around decentralized finance (DeFi), 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 the app without trusting any other party. This results in faster application adoption. Since dapps aren't hosted on any particular IP address, there is less authority 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 unlike traditional single-server applications, they are more resistant to attack. A dapp will only fail if every computer in the network fails, which is highly improbable.

- Data and other information added to the blockchain is immutable, meaning dapps are more resistant to modifications or restrictions.

- Dapps don't require connectivity to a single centralized server, making them more robust and flexible than centralized applications. Enterprises can ensure maximum business continuity and resilience with minimal interruptions and downtime.

- Dapp technologies will grow by startups creating innovative business and technology solutions on top of blockchain technologies. As they grow, a broader set of tools will enable decentralized applications, providing substitute and competitive services to those offered in traditional industries.

- Some of the biggest progress has been made by enterprises that don't seek to develop their application as fully decentralized and don't use the blockchain's full capabilities.

Obstacles

- Dapp technologies must evolve to support production needs, tools and technologies that enable dapp development.
- Dapps' user experience is often difficult to navigate since dapps don't function in the same way as centralized applications.
- Many high risk and gambling dapps that are deployed could narrow the potential use case of blockchain in the public's minds to only risky financial incentive programs. In reality, this is just one of many applications that this technology can be implemented in.
- Given DeFi's increasing popularity, some users are being priced out of the dapp ecosystem due to Ethereum's high fees.
- Dapps are not yet proven to satisfy enterprise needs of reliability, security, performance or scalability as they have been in public blockchains.
- Because a dapp is connected to the blockchain smart contract with back-end code running on the blockchain, dapps' evolution relies on blockchain platforms' and smart contract technologies' growth.

User Recommendations

- Experiment and understand dapps' use in your organization 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 technology mature, and existing legal, regulatory and compliance standards are mitigated or resolved.

Sample Vendors

Ethereum Foundation; MetaMask

Gartner Recommended Reading

Guidance for Assessing Blockchain Platforms

Cryptocurrencies

Analysis By: Adrian Leow

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition

A cryptocurrency is a distributed protocol for creating and exchanging digital assets that represent stored value. Cryptocurrencies use a distributed peer-to-peer network to create and transfer digital assets between parties, often in an anonymous, trustless exchange.

Why This Is Important

Cryptocurrencies enable rapid financial or asset exchange because they do not rely on a central authority, instead, they distribute transactions across a shared network. Cryptocurrencies create speculative investment vehicles, but also enable mechanisms to accelerate business transactions and thereby enable growth.

Business Impact

Impacts of cryptocurrency include:

- Cryptocurrencies transcend national borders and make it possible for people in developing nations to access credit they otherwise couldn't. If someone is concerned about the stability of their own currency, they can buy cryptocurrency and hold it in a wallet without having to deal with financial institutions.
- Cryptocurrencies have moved from speculative investments to viable alternative currencies. While they aren't being utilized everywhere, they are being used in a number of places and they open up opportunities in their own right.

Drivers

- Cryptocurrency is now gaining attention in the financial services space because of the marketplace dynamics similar to that of equities.
- Prices of cryptocurrencies are set by supply and demand and traded across numerous exchanges. Herein lies opportunity for arbitrage, speculation and investment in a growing list of cryptocurrencies that aim to utilize the blockchain technology in some way.
- New and fragmented markets are low-hanging fruit for talented quantitative traders. Furthermore, the biggest reason for financial interest is that the investment returns, which are in constant flux, can be astoundingly high.
- For some users, the anonymity cryptocurrencies offer is what makes them so attractive. Industries where anonymity is important will also start to gravitate toward “privacy coins” or might even issue them on their own.
- The future use of cryptocurrencies will likely depend on how well they can meet the needs of users compared with other electronic payments, such as electronic bank transfers. The extent to which there is uptake of cryptocurrencies more broadly will depend on costs, incentives and convenience for users — for any payment system to succeed it needs to be convenient, accessible and stable for both consumers and businesses.

Obstacles

- Consumers are notorious for wanting multiple forms of payment, and the infrastructure needed to support day-to-day use of the cryptocurrencies is not close to being sufficiently widespread.
- Multiple payment and alternative currencies are available for banked and unbanked individuals to transact. It is clear from our research that context, fungibility (of token and wallet), cost, risk and ease of use are essential components determining adoption speed.
- Gartner consumer data also indicates a lack of broad awareness and sense of trust in cryptocurrencies. We believe that these issues may improve as cryptocurrencies are incorporated more into mainstream enterprise use and gain credibility at a national and regulatory level.
- Despite the increased level of interest in cryptocurrencies, there is skepticism among most industry experts about whether they would ever replace more traditional payment methods or national currencies.

User Recommendations

- Identify use cases, such as international payments, where cryptocurrency may be more effective than other mechanisms.
- Keep cryptocurrencies out of your business; instead, for any experimentation or proofs of concept, first convert the cryptocurrency to your currency of record as it enters your systems.
- Monitor the evolution of the regulatory environments, locally and globally, as regulators are eying each others' regulations to understand the implications of cryptocurrency experimentations.
- Update compliance and risk policies, and seek external legal advice on cryptocurrency use.
- Plan (technology and business roadmaps) for the potential integration of cryptocurrencies with mainstream mediums of exchange. For example, review changes to transaction execution, treasury management and risk systems.

Sample Vendors

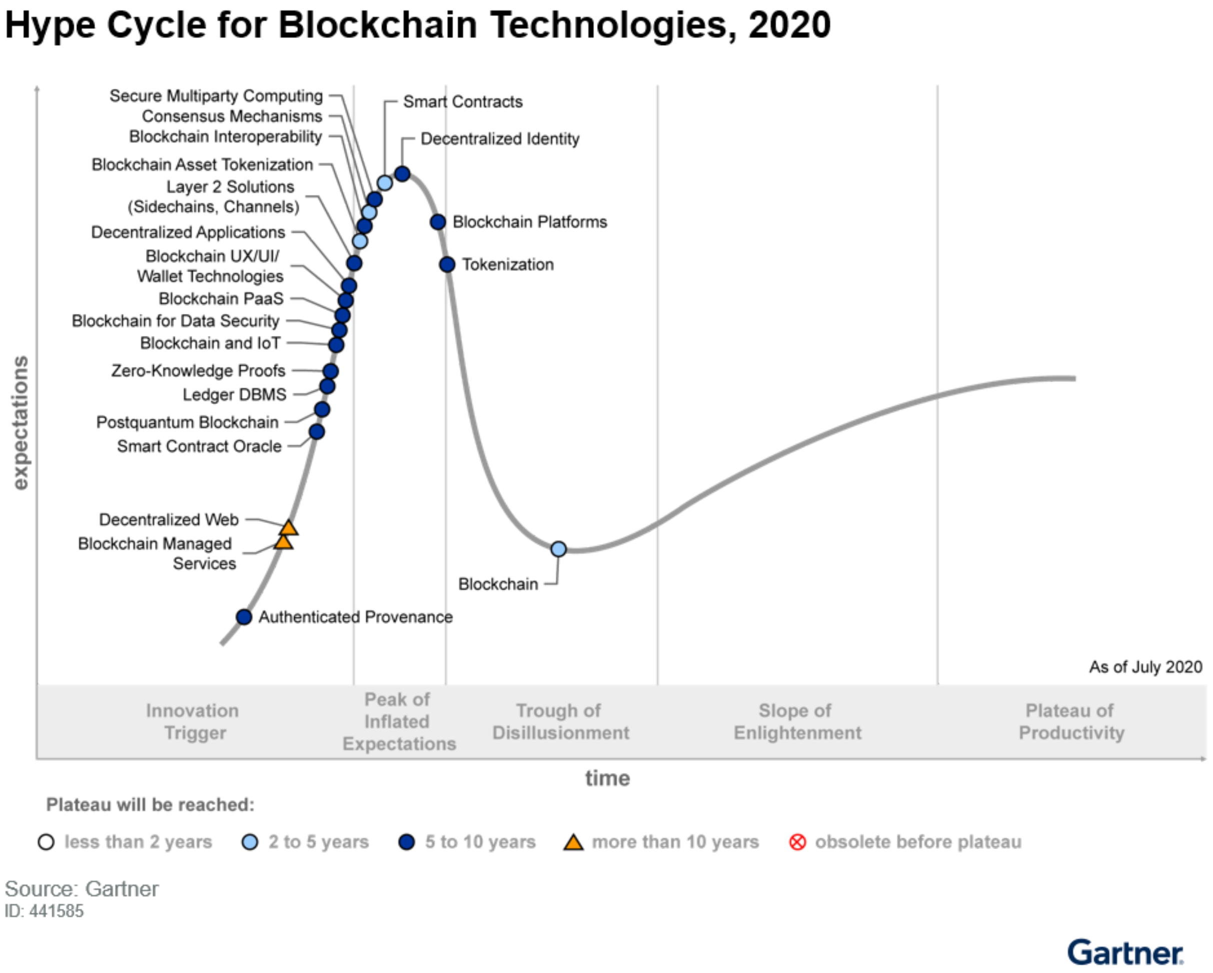
Bitcoin.com; Block.one; Dogecoin; Ethereum; Litecoin; NEM; Ripple; Stellar; Tether; Zcash

Gartner Recommended Reading

Bitcoin Goes Mainstream: What It Means to You

Appendixes

Figure 2. Hype Cycle for Blockchain Technologies, 2020

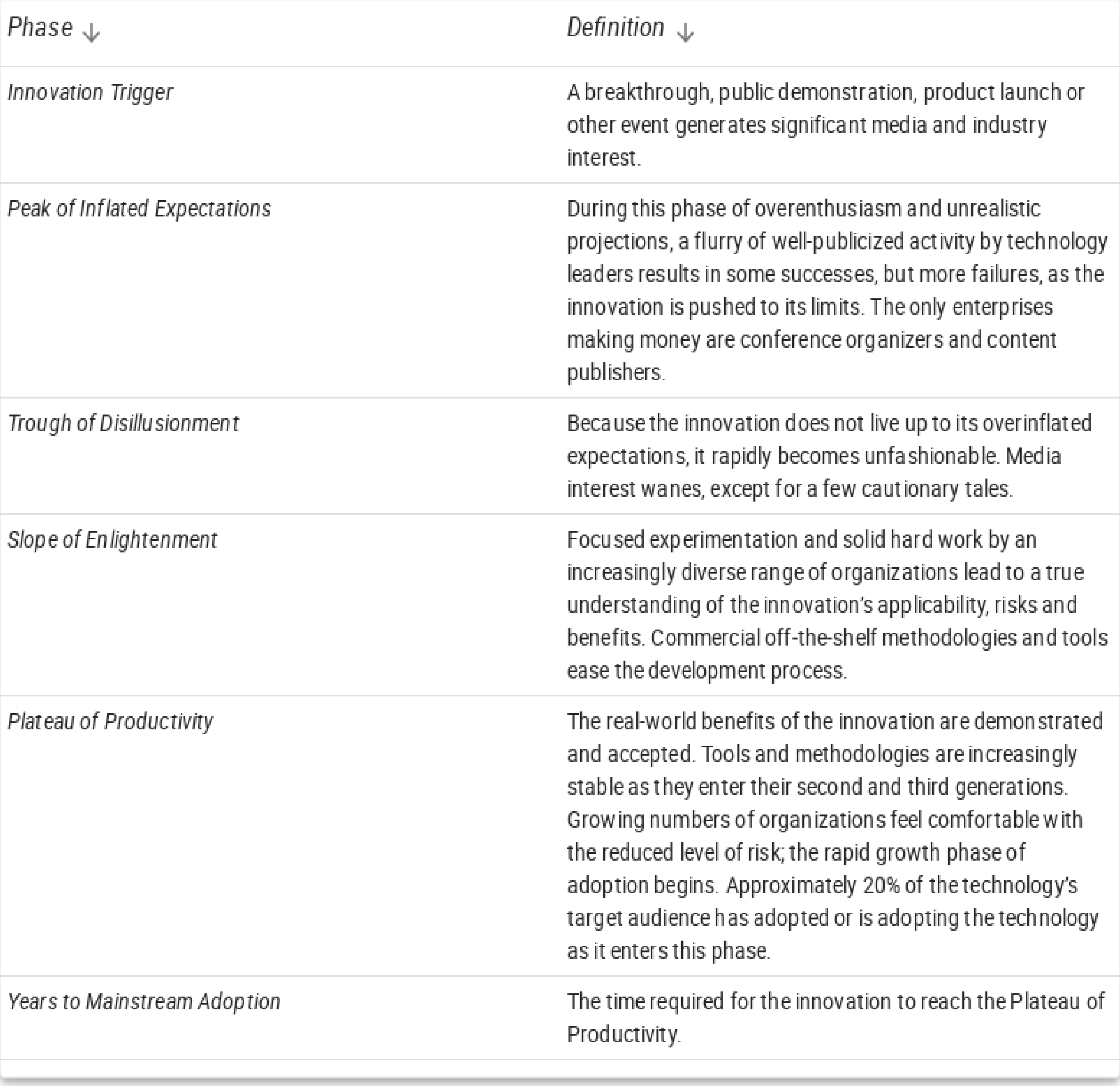


Source: Gartner
ID: 441585

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 (July 2021)

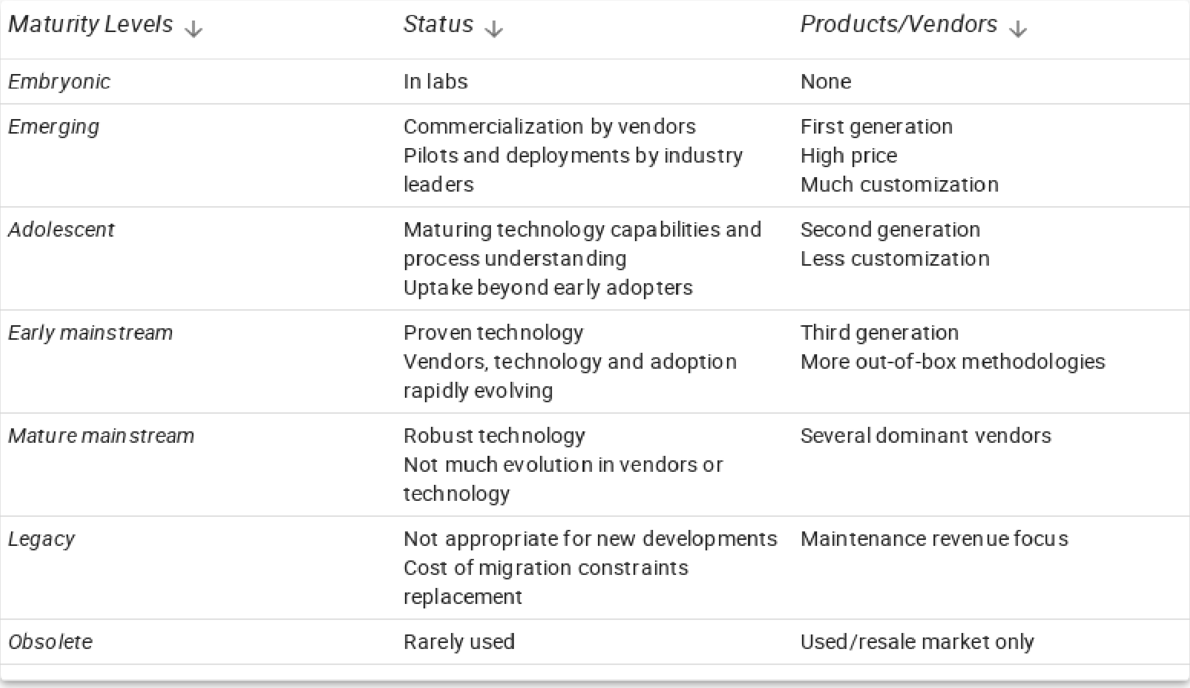
Table 3: Benefit Ratings

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 (July 2021)

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 (July 2021)

Evidence

[1] See Blockchain Trials show Business Executives Drive Focused Solutions to Production

[2] In a World First, El Salvador Makes Bitcoin Legal Tender, Reuters.

[3] See Bitcoin Goes Mainstream: What It Means to You. See slides 9-12 on CBDCs and Slide 19 on money movement work by legacy payment companies.

[4] See DeFi, CeFi and How Blockchains Interoperate: Case Study in Carbon Trading

[5] Azure Blockchain Service Retirement, Microsoft.

[6] IBM Blockchain Is a Shell of Its Former Self After Revenue Misses, Job Cuts: Sources, CoinDesk.

Document Revision History

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

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

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

What You Need to Know About Blockchain DeFi

Assessing the Optimal Blockchain Technology for Your Use Case

Bitcoin Goes Mainstream: What It Means to You

DeFi, CeFi and How Blockchains Interoperate: Case Study in Carbon Trading

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

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

Garbage In, Garbage Forever: Top 5 Blockchain Security Threats

Table 1: Priority Matrix for Blockchain, 2021

Benefit	Years to Mainstream Adoption			
	Less Than 2 Years	2 - 5 Years	5 - 10 Years	More Than 10 Years
Transformational	Stablecoins	Consensus Mechanisms Cryptocurrencies Decentralized Identity DeFi Nonfungible Tokens (NFT) Smart Contracts	Blockchain and IoT Blockchain Interoperability Blockchain Platforms CeDeFi/CeDeX Decentralized Web Smart Contract Oracle SMPC	
High		Blockchain Wallets Decentralized Exchanges	Authenticated Provenance Decentralized Applications Layer 2 Solutions Tokenization	
Moderate			Blockchain PaaS Zero-Knowledge Proofs	
Low				

Source: Gartner (July 2021)

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 (July 2021)

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 (July 2021)

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 (July 2021)