GLOBAL MILLENNIAL
CAPITAL

Blockchain Technologies

Research and Insights White Paper

Public Information and Disclosure

Table of Contents

GLOBAL MILLENNIAL CAPITAL

01

Executive summary and key insights for our blockchain technologies research

Executive summary and key reflection points of our research study

The future of blockchain technologies promises significant advances which are expected to transform various industries ranging from technology applications, financial services as well as traditional industries through its use case applications. Emerging business models such as dAaps (decentralized applications), blockchain ecosystems and cryptocurrencies have emerged which provide a technological platform to various business models to emerge such as decentralized finance (DeFi), smart contracts, gaming, digital identity, development tools as well as enterprise solutions. As blockchain continues to evolve, businesses and entrepreneurs are expected to remain agile and adapt to the changing landscape to maintain competitive advantage or think outside the box and thrive in a blockchain enabled future.

The UAE is leading the way in blockchain technology adoption with initiatives such as the Emirates Blockchain Strategy 2021 and Dubai Blockchain Strategy, which aim to transform 50% of government transactions on to blockchain platforms. This has spurred significant industry adoption within sectors such as finance, healthcare, and logistics. For instance, in the finance sector, the Dubai International Financial Centre (DIFC) has launched the “Blockchain Valley” to attract blockchain startups, while banks are exploring blockchain for cross-border payments and trade finance.

Our research includes the examination of three prominent blockchain platforms—Ethereum, Polygon, and Solana. Ethereum, in particular, is known for its powerful smart contract functionality and extensive use in DeFi and NTFs, positioning it at the forefront of industry innovation with a valuation of around $400 billion. Enhancing Ethereum’s capabilities, Polygon provides Layer 2 solutions to optimize blockchain applications and improve scalability. Solana stands out for its exceptional transaction speed and low costs, creating a favorable ecosystem for developers. These platforms exemplify the transformative potential of blockchain technology and underscore the necessity for ongoing investment in this rapidly evolving sector.

Blockchain technology presents a novel paradigm for data management and transactions, challenging traditional legal frameworks and regulatory environments. As blockchain continues to evolve and integrate into various sectors, it encounters a complex set of legal and regulatory issues. These challenges stem from blockchain decentralized nature, which does not easily fit into the conventional categories recognized by current laws and regulations.

We remain optimistic about the future of blockchain enabled business models and the emergence dApps, as technology continues to challenge the status quo of traditional industries creating new markets and accelerating disruptive innovation and entrepreneurship.

Key predictions for blockchain technologies and business models

PREDICTION MARKETS

Prediction: Prediction markets are a form of collective intelligence that leverage market mechanisms to incentivize large numbers of individuals to make forecasts about future uncertain events.

Implications: Prediction markets may prove to be the first mainstream application for governance protocol for blockchain, cryptocurrencies and decentralized finance (DeFi).

PEER-TO-PEER GAMBLING

Prediction: Peer to Peer blockchain based sports gambling allows users to place bets and offers in-house odds. Any number of peer-to-peer gambling protocols can be implemented on the Ethereum blockchain.

Implications: Blockchain specifically uses a decentralized system based on coordinated independent nodes network thereby not giving any particular a centralized advantage in the process. Blockchain is used to ensure randomness or rather incapability of knowing the outcome of a bet.

CROP MARKET INSURANCE & DERIVATIVES

Prediction: Blockchain technology properties such as distributed ledger provides storage of both static and dynamic transactions, without the need for a centralized authority, along with a consensus mechanism which helps in the validation of the transactions.

Implications: In addition to crop-based insurance, a financial derivatives contract can be developed using a data feed of the weather instead of any price index.This concept can be further expanded to natural disaster insurance generally.

CLOUD COMPUTING

Prediction: In cloud computing, blockchain can create a decentralized network of nodes that share data and processing power. Enterprises can rely on a distributed network of computers that are not under the control of any one company.

Implications: The technology can be used to create a verifiable computing environment, allowing users to delegate computations and then optionally ask for proofs that specific computations at randomly selected checkpoints were done correctly, allowing for a decentralized cloud computing market.

CYBERSECURITY

Prediction: Blockchain offers a different path toward greater security. This approach reduces vulnerabilities, provides strong encryption, and more effectively verifies data ownership and integrity.

Implications: The decentralized nature of blockchain makes it particularly ideal for organizations in need of highly secure technology. With blockchain, all information stored on the network is verified before being encrypted with a cryptographic algorithm.

SMART MULTI-SIGNATURE ESCROW

Prediction: Blockchain technologies allow multi-signature transaction contracts which require a specified number of signatures out of a given set of keys to authorize the spending of funds in an automated, safe manner.

Implications: Smart multi-signature escrow allows for more granularity in the number of keys which can authorize spending of funds along with daily limits.

Key predictions for blockchain technologies and business models (contd.)

Underlying Business Models

Blockchain as a Service (BaaS)

Description: Third parties provide and manage cloud-based networks for clients to develop blockchain applications. The services include infrastructure and support to allow companies to focus on their solutions without backend complexities.
Key Players: Microsoft, IBM, Amazon, R3, Hyperledger Foundation
Revenue Stream: Subscription fee, premium features, usage-based fee

Utility Token Business Model

Description: The business model incorporates functionality into a company's operations through digital tokens that grant holders access to a company's product or service.
Key Players: Basic Attention Token(BAT), Filecoin, Biance
Revenue Stream: Token sale with ICO, token value appreciation, transaction fee, service fee, revenue distribution

Blockchain Gaming

Description: Blockchain is integrated into video games to provide players ownership and trading ability of in-game assets. It introduces the play-to-earn models where players can earn cryptos or NTFs in games.
Key Players: Nintendo, Microsoft, Sony, EA, Activision Blizzard
Revenue Stream: In-game purchases, transaction fee, advertising

Peer-to-Peer Blockchain Business Model

Description: The P2P model facilitates direct interactions between end-users without central authority. It allows digitalized and decentralized transactions and exchanges.
Key Players: Bitcoin, BitTorrent, OpenBazaar
Revenue Stream: Token sales, transaction fee, BaaS Fee

Network Fee Charge

Description: This involves generating revenue through transaction fees on blockchain networks. Every transaction processed incurs a fee, which compensates miners or validators for their work.
Key Players: Ethereum, Bitcoin, Biance Smart Chain
Revenue Stream: Transaction fee, network usage fee

Blockchain Based Financial Services

Description: This offers a range of financial products and services including DeFi, asset tokenization, lending and borrowing, and cross-border payments.
Key Players: Aave, MakerDao, Compound, Ripple
Revenue Stream: Interests, trading fee, token appreciation

02

An overview of select blockchain ecosystems and underlying technologies and key applications

Blockchain technologies key definitions and industry interpretations (1/2)

General definition of blockchain technologies

Blockchain technology is often described as a decentralized digital ledger that records transactions across multiple computers, ensuring that the transactions cannot be altered retroactively. This concept is rooted in the definition provided by Satoshi Nakamoto (2008) in the original Bitcoin White Paper, which describes blockchain as a system that "timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work." This network relies on the longest chain of blocks, serving as proof of the sequence of events and the largest pool of CPU power without the need for a central authority.

Blockchain technology's potential extends far beyond monetary transactions, as Professor Arvind Narayanan from Princeton University provides a more general definition and describes it as a distributed database that maintains a continuously growing list of ordered records called blocks, with each block containing a timestamp and a link to the previous block to form a chain.

In conclusion, these descriptions of blockchain technology highlight its decentralized, immutable, and cryptographically secure nature. These characteristics allow blockchain to revolutionize the landscape of various industries by providing a transparent and tamper proof system for recording valuable information.

Definition by practitioners of blockchain

Aside from academia, leading firms play a crucial role in defining and applying blockchain technologies to practical scenarios, as blockchain is widely recognized for its ability to provide decentralized solutions for transactions and data management. In the subsequent page you will find some of the practitioners' definitions and perspectives about blockchain technologies.

Blockchain technologies key definitions and industry interpretations (2/2)

"Blockchain technology is an advanced database mechanism that allows transparent information sharing within a business network."

- IBM

"A blockchain is "a technology that allows people who don't know each other to trust a shared record of events". This shared record, or ledger, is distributed to all participants in a network who use their computers to validate transactions and thus remove the need for a third party to intermediate."

- Deloitte

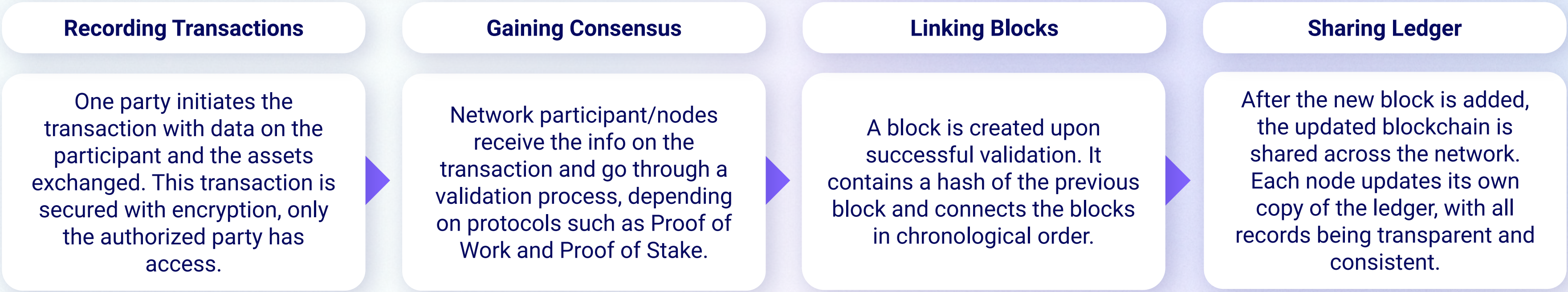
"Blockchain is a distributed ledger technology (DLT) that allows multiple parties to transfer and store sensitive information securely, permanently, anonymously, and efficiently within a decentralized network."

- Globant

"Digital, distributed, decentralized public ledger that exists across a network and facilitates the recording of transactions"

- McKinsey & Company

An overview of blockchain process flow



Recording Transactions

One party initiates the transaction with data on the participant and the assets exchanged. This transaction is secured with encryption, only the authorized party has access.

Gaining Consensus

Network participant/nodes receive the info on the transaction and go through a validation process, depending on protocols such as Proof of Work and Proof of Stake.

Linking Blocks

A block is created upon successful validation. It contains a hash of the previous block and connects the blocks in chronological order.

Sharing Ledger

After the new block is added, the updated blockchain is shared across the network. Each node updates its own copy of the ledger, with all records being transparent and consistent.

Key layers of blockchain architecture

The layers of blockchain architecture

Blockchain architecture is composed of multiple layers. This layered approach enables modular design, with enhancements and optimizations at each level without disrupting the entire system. This architecture typically starts with the foundational infrastructure, followed by core protocol that governs blockchain's operations, and includes additional layers designed to improve performance and scalability. Understanding this architecture is essential for grasping how blockchain technology supports diverse applications across various use cases.

Layer 0: Network Layer

Function: This foundational layer is all about the infrastructure necessary for blockchains to operate. It includes the physical hardware (servers, computers), and the networking protocols that allow nodes (the computers that make up a blockchain) to communicate with each other.

Examples: Technology that enhance connectivity and interoperability between blockchains, such as Polkadot's relay chains or Cosmos' Inter-Blockchain Communication (IBC) protocol, are considered part of Layer 0.

Layer 1: Protocol Layer

Function: This is the core blockchain layer consisting of the blockchain protocol itself. It defines the rules of the network, including how transactions are processed and validated, and how data is stored. This layer ensures security, consensus, and the creation of blocks in the blockchain.

Examples: Well-known blockchains like Bitcoin and Ethereum operate at Layer 1. Ethereum, for example, uses a consensus mechanism (initially Proof of Work, transitioning to Proof of Stake) to agree on the state of the network and process transactions.

Layer 2: Network Layer

Function: Built on top of Layer 1, Layer 2 solutions are designed to enhance scalability and speed without compromising the security of the underlying blockchain. They achieve this by processing transactions off the main chain (Layer 1) and later reconciling them with the main blockchain.

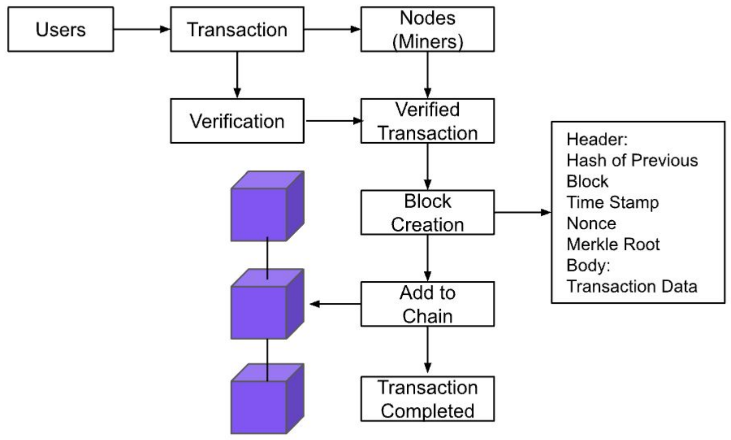
Examples: Solutions like Lightning Network for Bitcoin and Rollups for Ethereum. These technologies allow for faster and more cost-effective transactions by handling them away from the main blockchain and then settling the final state on Layer 1.

Elements and select definitions of a blockchain network

Elements of a blockchain network

Several components work cohesively to establish a decentralized and secure system within blockchain technology, including:
P2P Network, which is a decentralized network where each participant, known as a **Node**, interacts with each other without a central server. The **Ledger** is the immutable and transparent record of all transactions, consistently maintained by synchronization of all nodes. The synchronization is supported by the **Consensus Mechanism**, which is fundamental to all blockchain operations, ensuring all participants agree on the ledger's state.

The **Wallets** play an important role in the ecosystem by storing public and private keys needed to execute transactions and engage with smart contracts. The **Smart Contracts** are programs stored on a blockchain that run when predetermined conditions are met. They automate the execution of an agreement so that all participants can be immediately certain of the outcome. Security for these transactions is fortified by various cryptographic techniques. For instance, a **Hash** is a unique, fixed code derived from a hash function that helps to protect transmission of data across the cryptocurrency network. With these interconnected components, blockchain technology creates the platform for facilitating transactions and ensuring data integrity across a wide range of applications.



Types of blockchain(s) and select differentiation elements

PUBLIC BLOCKCHAIN

Completely decentralized and open to anyone, with all transactions being transparent and verifiable by all participants. It is used when trust is low among participants and transparency is crucial. The advantages include the absence of central control, robust security, permissionless participation, high transparency, and strong resilience against attacks. However, they also face challenges such as congestion during periods of high transaction volumes, slower processing speeds due to complex consensus protocols, energy-intensive operations, and regulatory uncertainty.

HYBRID BLOCKCHAIN

A blend of public and private blockchains with flexible control mechanisms where transparency can be displayed according to specific needs. It has advantages including the combined benefits of both blockchain types and controlled selective transparency, allowing for scalability and performance optimization. It also presents challenges such as complex integration processes, potential security vulnerabilities at the intersection of public and private components, and increased operational costs associated with managing multiple blockchain environments.

PRIVATE BLOCKCHAIN

Operated by a single organization with private access and permissions, making it more centralized and efficient than public blockchains. It is used by enterprises to manage and streamline internal processes with a priority on efficiency and scalability. It has pros such as improved confidentiality, customizable features to meet specific organizational requirements, and enhanced scalability and operational efficiency due to a controlled number of participants. However, the cons include potential risks related to centralization, such as single points of failure, and limited opportunities for broad-based innovation and adoption due to restricted access.

CONSORTIUM BLOCKCHAIN

Used for business collaborations and governed by a group of organizations, focusing on the balance between decentralization and efficiency. It offers advantages like controlled decentralization, scalability, and efficiency comparable to private blockchains, and fewer regulatory concerns. However, its disadvantages include complex governance structures and challenges in interacting with other blockchain networks.

Blockchain ecosystem participants high level overview

NETWORK PARTICIPANTS

Full Nodes ensure the security and accuracy of the blockchain by validating transactions according to the established rules. Miner Nodes in the PoW system solve complex mathematical problems to confirm transactions and create new blocks with the reward of cryptocurrencies. Validator Nodes in the PoS system stake their own cryptocurrencies to validate transactions and create blocks. Together these participants maintain the network's decentralized operations and facilitate trustless consensus.

DEVELOPERS

Protocol Developers work on the fundamental aspects of blockchain and try to optimize the underlying protocols. DAPP developers build decentralized applications based on the blockchain platforms to address specific market needs. The developers contribute to the ecosystem by enhancing the blockchain's frameworks and promoting the utility and reach of this technology across various industries.

FINANCIAL STAKEHOLDERS

Exchanges serve as the platforms providing the infrastructure for trading digital assets, ensuring liquidity, and establishing market prices. Investors participate in the ecosystem through these exchanges by engaging in initial coin offerings, trading, and holding cryptocurrencies. Together the stakeholders influence the growth and market dynamics of the blockchain ecosystem.

REGULATORS AND CONSUMERS

Regulators play a crucial role in the landscape by formulating and enforcing the rules to govern the operation of blockchain technologies while consciously adapting laws and regulations to accommodate the integration of these emerging technologies. On the commercial side, enterprises benefit from blockchain's transparency and security features to improve the operation of businesses. Meanwhile, individual consumers drive demand for blockchain technologies and drive potential innovation in applications with increasingly diverse functionalities.

Blockchain technologies for enterprises and priority sectors (1/2)

Blockchain technology enhances business operations with a distributed ledger system where permissioned participants access shared information in real-time, leading to higher efficiency, trust, and reduced operational friction. Blockchain's unique attributes consensus on data validity, immutable record-keeping, and enhanced security through restricted access allow enterprises to scale various solutions.

Banks and Financial Services

J.P. Morgan's Onyx Coin System uses blockchain for real-time, multi-currency transfers and domestic / cross border settlements on a permissioned ledger.

HSBC's Gold Tokenization offers digital tokens representing fractional ownership of physical gold that is recorded on a distributed ledger, enhancing accessibility and investment flexibility in gold markets.

Technology

IBM Blockchain provides its platform with enhanced transparency and traceability in supply chains across various industries, supporting businesses in improving operational efficiencies and product authenticity.

Microsoft's Azure Blockchain is a platform that allows enterprises to build and govern networks, simplifying the formation and management of consortium blockchains.

Manufacturing

BMW Group employs blockchain in its supply chain to ensure the traceability of automotive parts and raw materials from suppliers in order to reduce the risk of fraud.

Renault is working with Microsoft and Viseo to develop a digital car maintenance book with blockchain technology that tracks each vehicle's maintenance history.

Accounting

EY Blockchain Analyzer helps EY audit teams by facilitating the collection and analysis of transaction data from various blockchain ledgers, supporting the financial audits and verifications for cryptocurrencies.

Big Four has teamed up with a consortium of 20 Taiwanese banks to pilot a blockchain-based platform which facilitates real-time auditing of public companies' financial statements

Blockchain technologies for enterprises and priority sectors (2/2)

Oil and Gas

Shell and BP's Blockchain Trading Platform Vakt: Shell and BP, along with other major entities in the industry, have developed a blockchain-based digital trading platform to reduce time spent on operations and paperwork in the energy commodity trading.

Saudi Aramco through its controlled chemicals firm SABIC, is piloting a blockchain-based digital product passport solution that enables the monitoring of 'Scope 3' CO2 emissions within supply chain and recycling processes.

Insurance

AXA's Fizzy, a smart contract-based insurance product that can be triggered when a two-hour delay is confirmed by global air traffic databases, that ensures immediate and automatic compensation without the need for manual claims processing.

Allianz has implemented blockchain technology for captive insurance programs, simplifying the management of transactions, reconciles payments, and records claims for multinational corporations.

Logistics

DHL and Accenture deployed a blockchain-based serialization prototype that tracks pharmaceuticals from the point of origin to the consumer, preventing tampering and errors.

UPS has integrated blockchain technology to streamline its logistics and freight operations, enhancing security of sensitive data and simplifying the complexities involved in international logistics involving multiple carriers and regulatory systems.

Others

Sony Global Education has developed a blockchain-based platform to secure and share student records and academic credentials. This enables educational institutions to create, store, and manage digital records of students' academic achievements.

BurstIQ uses blockchain in healthcare data management by allowing patients, doctors, and healthcare providers to access and share health data.

Blockchain ecosystems and core applications high level overview

Ethereum Blockchain

A platform for smart contracts and decentralized applications (dApps), known for its mature ecosystem that supports a wide range of applications across finance, gaming, etc.

Polygon Blockchain

Designed as a scalability solution for Ethereum, it provides faster transactions and reduced gas costs, supporting Ethereum-compatible blockchain networks with scaling solutions like sidechains, optimistic rollups, and zk-rollups.

Solana Blockchain

Hosts applications that require rapid state changes. Known for its high-speed transaction capabilities and low fees, it is ideal for applications requiring fast throughput such as high-frequency trading and decentralized exchanges.

Avalanche Blockchain

It features high scalability and customizable blockchains with its subnets that allow for tailored solutions. Enables the creation of networks for enterprise-level applications.

Base Blockchain

It has the security of Ethereum while offering lower transaction costs and better user accessibility. It simplifies blockchain application development with tools for easier deployment and integration.

Select Applications

1. DeFi
2. Smart Contracts
3. Gaming
4. Digital Identity

1. DeFi
2. Gaming
3. NFTs
4. Marketplace
5. Scalability Solutions

1. DeFi
2. High Speed Transactions
3. Media and Entertainment

1. DeFi
2. Customizable Solutions
3. Enterprise Solution

1. DeFi
2. Enterprise Solution
3. Development Tools
4. Cross Chain Application

Select economic benefits of blockchain applications (1/2)

Economic Benefit	Particulars
Cost Reduction	The blockchain expedites transaction processing, making it a uniquely efficient and cost-effective strategy that offers substantial economic advantages over conventional systems.
Enabling Tokenization	Tokenization involves the blockchain-based process of creating a digital representation of a conventional asset. These tokens could represent everything from bonds and equities to agricultural commodities or real estate.
Immutability	Once data is recorded on the blockchain, it cannot be altered or deleted. This feature protects data integrity and audit trails in sectors such as financial services, legal documents, and public records.
Speed and Efficiency	Blockchain networks can automate and streamline processes through smart contracts and decentralized operations to deliver faster services than traditional systems.

Select economic benefits of blockchain applications (2/2)

Economic Benefit	Particulars
Distributed Authority	Blockchain technology is not controlled by any single entity, as it distributes power and control among all users. This model reduces the risk of centralized failure points and promotes a democratic and equitable digital economy, especially valuable for areas such as voting systems and community governance.
Enhanced Security	The cryptographic techniques involved in blockchain technology prevents malicious actions due to the resistant nature of the connected chain. This trait is critical to applications with sensitive data such as in financial services and record keeping.
Increased Market Access	Blockchain technology lowers barriers of entry for small and medium enterprises with reduced need for large capital investments. This democratizes market access especially for industries like financial services and global trade.
Flexibility	Blockchain technology provides companies with the tools to develop highly flexible solutions tailored to specific business needs. Businesses can adjust these protocols to respond to changes in the marketplace or regulatory demands.

03

Smart contracts overview and select industry applications

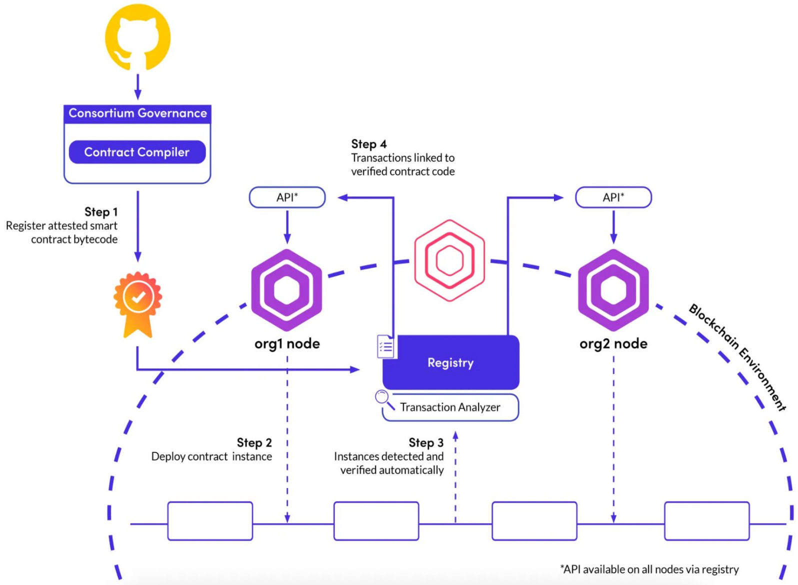
A brief overview of smart contracts for blockchain technology

A smart contract is a digital protocol built on the blockchain technology, designed to automatically execute and document events according to predetermined terms. It ensures decentralization and data integrity of transactions by eliminating the need of approval or oversight from any intermediaries, as the executions of transactions are conditional upon criterias being met just like a line of the “if/then” code sequence. Smart contact presents an alternative to traditional intermediaries and financial infrastructures with enhanced transparency and trust.

History of smart contracts

Smart contracts were conceptualized by Nick Szabo in 1994, which were envisioned as automated systems that execute predetermined conditions of a contract, aiming to reduce reliance on trusted intermediaries and minimize the potential of fraud. One of the early examples can be the vending machine. The true potential of smart contracts began to be realized with the emergence of blockchain technology, which introduced the basic contracts through protocols that governed transactions like requiring the correct private key and sufficient funds. Multi-signature transaction mechanism in 2012 further expanded the functionality and enhanced security by requiring multiple approvals before a transaction. The transformative breakthrough for smart contracts came with Ethereum in 2015. Ethereum’s blockchain acted as a world computer capable of running multiple smart contracts simultaneously and laid the ground for a new era for future developments. Currently, there are 1,051,553,823 smart contracts deployed across all available chains including Ethereum, Polygon, BNB Smart Chain, Fantom, Optimism, Avalanche, Arbitrum, and Gnosis.

Smart contracts architecture high level overview


Consortium Governance
Contract Compiler
Step 1
Register attested smart contract bytecode
API*
API*
Step 4
Transactions linked to verified contract code
org1 node
Registry
org2 node
Blockchain Environment
Transaction Analyzer
Step 2
Deploy contract instance
Step 3
Instances detected and verified automatically
*API available on all nodes via registry

Agreement Formulation: Parties agree on terms and define how the smart contract will operate, including conditions for fulfillment.

Contract Development: The contract is coded into a programming language, while ensuring the contract's security is crucial in this phase.

Deployment: The finalized contract is deployed on the blockchain, where it becomes immutable and begins monitoring for specified conditions.

Condition Monitoring and Execution: The contract automatically executes actions when its predefined conditions are met, such as transferring funds or updating ownership records.

Record Finalization: The blockchain records the completed transaction, ensuring transparency and permanent access to the agreement details.

Smart contracts select benefits and limitations overview

An overview of key benefits and limitations of smart contracts

BENEFITS

- **Efficiency:** Automated executions can streamline processes, eliminate delays and manual errors, resulting in a smoother transaction flow and increased productivity in operations, especially those involving complex and multi-party agreements.
- **Transparency and Trust:** The transactions are verifiable and visible to all parties under the environment constructed by smart contracts. The decentralized nature of blockchain also promises that no single entity has control over the entire database, which makes it impossible to alter transactions for fraudulent purposes
- **Security:** Because each record on the blockchain is linked to the previous and the subsequent ones through cryptographic hashes, it is difficult to alter any single record without modifying the entire chain.
- **Cost Reduction:** By eliminating the needs for intermediaries such as brokers, lawyers, and banks, smart contracts reduce fees associated with these services. The removal of bureaucracy and paperwork lead to leaner processes and lower costs.

LIMITATIONS

- **Rigidity**: Smart contracts are immutable, meaning when bugs or vulnerabilities are discovered post-deployment, these contracts cannot be corrected or upgraded directly.
- **Dependency on Off Chain Oracles**: Smart contracts require external data to be pushed to them, creating potential discrepancies in the timing and accuracy of information received by different nodes. This necessitates the use of oracles, introducing a compromise of decentralization and potential single point of failure.
- **Limits of Precision**: The exactitude required by smart contracts can conflict with the intentional ambiguity often used in traditional business negotiations, which may raise the costs of drafting contracts.
- **Loophole Vulnerability**: As smart contracts rely on pre-programmed condition, some parties may not act in good faith and create loopholes that are difficult to detect until damage occurs, especially for those without deep knowledge of the technology.

Smart contracts use cases and select industry applications (1/2)

REAL ESTATE

Smart contracts are revolutionizing the real estate industry by automating key processes like property transactions and lease agreements. In the domain of escrow services, smart contracts hold funds securely and release them only when all transaction terms are met. For instance, Propy utilizes smart contracts to automate property sales, ensuring transactions are executed with payments confirmed.

RETAIL

For retailers, smart contract can help digitize processes such as payment to contractors, payroll management, and real-time inventory tracking, reducing labor-intensive tasks and minimizing errors. For example, OpenBazaar utilizes smart contracts to manage transactions within its decentralized marketplace, simplifying operations for small business owners and offering them more competitive positioning in the market.

IDENTITY

Digital identity management is revolutionized by smart contracts with less no more for manual checks, which speeds up transactions and reduces errors, while allowing users to maintain a consistent digital identity across various platforms. Civic uses smart contracts to offer a decentralized mechanism for identity verification, enabling users to use their verified identity in finance, healthcare, and more, without the need to repeatedly provide the same documentation.

IP

Establishing an immutable blockchain-based registry of IP rights, smart contracts provide a blockchain timestamp for creations and offer undeniable proof of ownership that is critical in protecting the rights of creators. For example, Etherscan encodes IP information directly onto the blockchain to streamline the process of rights management and enforcement.

Smart contracts use cases and select industry applications (2/2)

RISK MANAGEMENT

Smart contracts facilitate the issuance and management of various digital tokens, each designed with specific functions. For example, Filecoin's FIL token is used for payments within its decentralized storage network, and Compound's COMP tokens grant holders governance rights.

INSURANCE

Smart contracts are revolutionizing parametric insurance by automating payouts based on specific conditions, like weather events affecting agriculture. For instance, a crop insurance policy executed via a smart contract might automatically compensate farmers if rainfall levels deviate from predetermined thresholds.

FINANCIAL

DeFi services utilize smart contracts to mimic traditional financial services like loans and trading without intermediaries. These contracts automate processes and enforce rules, improving efficiency and reducing costs. For example, BarnBridge employs smart contracts to automate portfolio rebalancing, allowing users to maintain predetermined asset allocations.

GAMING

Blockchain gaming utilizes smart contracts to ensure fair and secure in-game actions. For example, PoolTogether is a game where participants stake funds in a pool that earns interest; after a set period, one winner receives the interest while others reclaim their stakes. Additionally, smart contracts facilitate fair distributions in NFT, supporting features like randomized loot drops in RPGs.

Legal and regulatory considerations relating to smart contracts (1/2)

Is a Smart Contract a Legal Contract?

Advocates argue that the public nature of smart contracts negates the need for legal oversight, as "the code is law." However, from a legal perspective, the fundamental contract elements offer acceptance, and consideration which must be present for smart contracts to be legally enforceable. In reality, most smart contracts serve as terms within traditional legal agreements. Despite some states introducing specific legislation recognizing smart contracts, these laws do not make them inherently binding but affirm that they do not lose validity merely for including automated terms.

Legal Issues

- Developer Liability: When third parties create smart contracts, they may face liability if errors occur or if the contract is used unlawfully. Developers could be held responsible for regulatory violations if they could foresee misuse of their code, as seen in cases pursued by the CFTC and SEC.
- Final Agreement Ambiguity: Traditional contracts are assessed by courts based on the final written document, emphasizing the "meeting of the minds." For smart contracts, it potentially leads to conflicts when there's a discrepancy between the written terms and the executed code. In cases involving ancillary smart contracts, courts generally view the text and code as a single unified agreement, and complexities arise when the two factors do not align.
- Complexity in Understanding and Verifying Code: The complexity in understanding and verifying the functionality of smart contract code presents challenges for non-technical parties, who often rely on technical experts to translate the terms. This highlights the need for additional legal documentation and expert validations, especially for custom smart contracts.
- Enforceability of Automated Decisions: The automation of smart contracts that executes based on fixed conditions, often overlooks the nuances and extenuating circumstances typically considered in legal decisions. This can result in disputes when automated outcomes conflict with principles of fairness or established standards.
- Adaptation to Regulatory Changes: Smart contracts are programmed with fixed rules and do not automatically adjust to new regulatory requirements or legal reforms. This static nature can create compliance issues, especially for long-term contracts that necessitate mechanisms for dynamic updates.

Legal and regulatory considerations relating to smart contracts (2/2)

Specific Regulatory Actions

Uniform Commercial Code (UCC) and Statute of Frauds:

- Written Requirement: Courts recognize that written agreements don't necessarily need to be composed in traditional prose. The UCC allows for any intentional tangible representation of an agreement, which encompasses electronic formats such as emails. This flexible interpretation enables smart contracts, which are fundamentally electronic records, to generally meet the UCC's requirement for a written agreement. While not all smart contracts may automatically fulfill this requirement, their explicit code and clear parameters typically make them suitable for clearly documenting transaction terms, particularly in cases involving the sale of goods or lease agreements. Similarly, under the Statute of Frauds, a valid writing need not be entirely in natural language prose or to be comprehensive. Courts have adopted a broad approach by considering the intent of the parties to forge a binding agreement as the crucial factor. Smart contracts that inherently define precise terms such as price and delivery details satisfy the Statute of Frauds.
- Signature Requirement: Digital signatures in smart contracts require authentication with public and private key cryptography by each party, thus they qualify as "symbol executed or adopted with present intention to adopt or accept a writing" and meets the standards of both the U.C.C. and the Statute of Frauds.

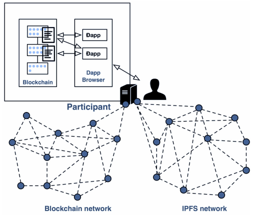
Electronic Signatures in Global and National Commerce Act (E-SIGN) and Uniform Electronic Transactions Act (UETA):

- These acts state that electronic records and signatures utilized in interstate or foreign commerce must be recognized as legally valid and cannot be denied legal effectiveness solely because they exist in electronic form. These acts define electronic records as "information processing systems, computer equipment and programs and similar technologies", and electronic signatures as "electronic sound, symbol, or process attached to or logically associated with a record" that could encompass "digital signature using public key encryption technology". Smart contracts, stored on blockchains, clearly fit within these frameworks.
- These acts also introduce the concept of an "electronic agent" as any computer program or automated procedure that perform an action or respond to electronic records without human intervention. Smart contracts classify under this definition and enhance their standing as enforceable agreements. However, is it necessary for parties to engage in a non-electronic format prior to implementing a smart contract.

04

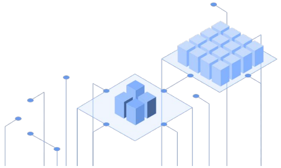
Blockchain technologies infrastructure overview and description of select use cases

A high-level overview of blockchain, cryptocurrencies and Daaps



Blockchain Dapps and Developer Applications

These applications leverage the underlying blockchain infrastructure to create functional products and services across various sectors. They are distinct from the infrastructure itself, which is agnostic of specific applications and serves a broad array of use cases. Unlike cryptocurrencies, which are generally uniform in their function as tokens or currency, blockchain applications are extremely diverse, ranging from financial services (DeFi) and supply chain management to gaming and healthcare.



Blockchain technology

Blockchain infrastructure includes core hardware and software components like protocols, consensus mechanisms, and network architecture. This infrastructure is crucial as it provides the necessary platform for both blockchain applications and cryptocurrencies to function. It differs from the other two in that it primarily focuses on the technical and operational aspects necessary for the blockchain's functioning.

Cryptocurrencies

Cryptocurrencies represent digital assets or tokens that can be used for transactions, investments, and as a means of transferring value. Currencies like Bitcoin and Ethereum are not just mediums of exchange, but also serve as incentives to encourage nodes to participate in the network and validate transactions. They rely on the infrastructure for their existence and security, but unlike applications, which are diverse in function and industry focus, cryptocurrencies are specifically designed for economic transactions and value storage.

Key properties of blockchain infrastructure technology

Blockchain technology fundamentally transforms how industries operate by leveraging its unique properties: decentralization, transparency, security, and immutability. These properties facilitate more efficient and trustworthy exchanges without centralized oversight. Through this decentralized nature, blockchain is laying the groundwork for a new era of digital interaction, where all stakeholders have a consistent and reliable audit trail, creating advancements in how businesses and individuals interact with and maintain records on a global scale.

Decentralization

By removing intermediaries, blockchain facilitates peer-to-peer transactions, reducing costs and increasing efficiency. This can disrupt industries reliant on central authorities, such as finance, where traditional banking and payment systems can be replaced by decentralized finance (DeFi) applications.

Transparency

Blockchain's transparent ledger ensures that all transactions are publicly recorded and verifiable. This can enhance trust and accountability in sectors like supply chain management, where it can provide end-to-end visibility, helping to prevent fraud and ensure product authenticity.

Security

The cryptographic nature of blockchain ensures high levels of security, making it difficult for data to be altered or hacked. This is crucial for industries like healthcare, where patient data security and integrity are paramount.

Immutability

Once data is recorded on a blockchain, it cannot be changed or deleted. This creates a reliable and permanent record, which is beneficial for legal and compliance purposes in sectors such as real estate and legal contracts (through smart contracts).

Roles and responsibilities within a blockchain network

To understand specific legal responsibilities and obligations, it is important to understand the distinct roles within a blockchain network, with each participant in the network facing unique legal challenges based on its role and activities. Here are some key roles and associated legal considerations:

Network Operator

Responsible for the overall management and governance of the blockchain network, including drafting and enforcing network rules and contracts. Its legal considerations include ensuring the network complies with applicable laws and regulations across different jurisdictions and handling information reporting and conducting thorough due diligence.

Technology Partner

Responsible for providing the technological infrastructure for the blockchain network. Its legal considerations include designing systems that comply with international standards and local regulations regarding data protection and cybersecurity, and maintaining the continuous operation of the platforms by addressing any technological faults.

Commercial Nodes

Responsible for engaging in the network for business transactions such as buying or selling goods and services. Its legal considerations include balancing the efficiency gained from data sharing with the protection of commercially sensitive information, and ensuring transactions comply with commercial laws, trade regulations, and contractual obligations.

Infrastructure Nodes

Responsible for providing infrastructure support for financial and logistical aspects, such as processing transactions or facilitating logistics. Its legal considerations include all data exchanges and transactions that meet stringent regulatory standards, and managing risks associated with infrastructure failure.

Blockchain technologies select use cases (1/4)

Asset Tokenization

Definition	Asset tokenization is the process of converting the rights to both tangible and intangible assets into digital tokens on a blockchain. This process typically involves five steps: creating the tokens that represent shares of underlying assets, implementing smart contracts to manage these tokens, distributing tokens through sales to investors, managing the assets and revenues through blockchain, and facilitating trading on the secondary market.
Use Case	Initially launched as a cryptocurrency exchange, tZero has pivoted to focus on leveraging blockchain technology to securitize company equities, particularly for those seeking private capital. By offering security tokens via its platform, tZero enables a broader spectrum of investors, including accredited and retail investors, to participate in private equity markets—a realm typically dominated by large institutions and venture capital funds.
Benefits	The benefits of asset tokenization include democratizing access to traditionally exclusive investment opportunities and enhancing market liquidity. This process is applicable across a wide range of asset classes, enabling fractional ownership in bonds, real estate, collectible art, and even carbon credits.

Blockchain Gaming

Definition	Blockchain games, often referred to as metaverse games, employ blockchain technology to elevate the gaming experience beyond traditional platforms. These games integrate smart contracts to authenticate and record in-game transactions and asset ownership, allowing players to truly own, buy, or sell digital assets like tokens or NFTs, which can be used across different gaming ecosystems.
Use Case	Axie Infinity is an innovative play-to-earn (P2E) game that revolves around adorable creatures known as Axies, which players can collect, breed, and battle. Unlike traditional games, Axie Infinity allows players to genuinely own their in-game assets as Non-Fungible Tokens (NFTs), tradable on the game's marketplace. The game's economy is driven by its native governance token, AXS, and a reward token, SLP, both of which play crucial roles in the ecosystem.
Benefits	This decentralized approach provides players with direct control and potential earning through play-to-earn model. However, blockchain games face challenges such as technical barriers for new users, scalability issues on networks like Ethereum.

Blockchain technologies select use cases (2/4)

Cross Chain

Definition	Cross-chain technology allows blockchain interoperability, seamless communication and asset transfer across disparate blockchain networks. This capability enables more complex applications, such as cross-chain decentralized exchanges (DEXs), cross-chain money markets, and multi-chain dApps, by allowing tokens to be locked or minted on one blockchain.
Use Case	Cosmos is designed as "Internet of blockchains", facilitating interoperability and secure communication across different blockchain networks. It uses the Cosmos Hub, supported by over 180 validators, to integrate various blockchains through its native token called ATOM. Key components like Tendermint for consensus and networking, and the Cosmos SDK for building custom blockchain applications, enable developers to create and connect dApps.
Benefits	At the forefront of this innovation is the Cross-Chain Interoperability Protocol (CCIP), an open-source standard that can enable a single dApp to operate across multiple blockchains, enhancing usability and reducing the need for multiple deployments.

Decentralized Finance (DeFi)

Definition	Decentralized finance (DeFi) represents a shift in the financial sector by leveraging blockchain technology to conduct financial transactions and services without centralized intermediaries. Through the utilization of cryptocurrencies and smart contracts on blockchains like Ethereum, DeFi platforms maintain a decentralized ledger that records all transactions, which can be openly verified by any user.
Use Case	Sushiswap is a decentralized exchange with a network of liquidity pools that enables users to lock assets into smart contracts, allowing others to buy and sell cryptocurrencies directly from these pools. This process facilitates direct peer-to-peer transactions without the need for a central operator. Users contribute to liquidity pools by depositing pairs of assets, such as USDT and ETH. In return, they can trade within these pools according to the platform's smart contract rules.
Benefits	This technology allows DeFi to support a wide range of applications, from asset trading and loans to complex financial products like derivatives and insurance.

Blockchain technologies select use cases (3/4)

Metaverse

Definition	Metaverse facilitates immersive experiences by blending virtual reality (VR) and augmented reality (AR) with digital economies, Blockchain ensures that all transactions within the metaverse are secure and transparent, supporting a decentralized ownership model for digital assets like virtual land and NFTs.
Use Case	The Sandbox is an example of a metaverse implemented on the Ethereum blockchain, where it creates a decentralized virtual world that participants can directly influence and monetize. Its LAND tokens are digital parcels of real estate that users own and on which they can build and manage unique gaming and social experiences. Additionally, The Sandbox uses SAND tokens for transactions within the metaverse, including purchasing LAND and interacting with user-generated content.
Benefits	This technology also integrates advanced computing and open programming standards like HTML and WebXR, laying the groundwork for a dynamic virtual world where users can work, socialize, and create freely.

Non-Fungible Tokens

Definition	NFT represents an application of blockchain technology in the digital asset space. Each NFT is a unique cryptographic token that cannot be replicated, existing on a blockchain that supports metadata and smart contracts. Unlike fungible tokens like cryptocurrencies, where each token is identical to another, each NFT has a unique identifier that makes it distinct.
Use Case	In collaboration with FIFA, Modex launched FIFA+ Collect, a platform that enables fans to own digital collectibles minted on the Algorand blockchain.
Benefits	The uniqueness allows NFTs to represent ownership of digital items like artwork, music, videos, and virtual real estate, as these tokens can be traded globally.

Blockchain technologies select use cases (4/4)

Oracles

Definition	Blockchain oracles serve as intermediaries, bridging the gap between blockchain networks and external data. The oracles enable smart contracts to access off chain data, vital for executing contracts based on real-world events and interactions.
Use Case	Chainlink serves as an intermediary in DeFi by securely relaying external data to smart contracts on blockchain networks such as Ethereum. These oracles are decentralized networks themselves, consisting of multiple nodes that validate and aggregate external data. A smart contract on the blockchain issues a request for external data, received by Chainlink nodes. These nodes use the Chainlink Core software to convert this request into off-blockchain formats that external APIs can understand.
Benefits	By functioning as data feeds, oracles provide essential information such as price feeds, weather conditions, or even the outcome of a sporting event.

Zero-Knowledge Proof

Definition	Employed with the blockchain network, ZKPs are a cryptographic method that enables one party to prove to another that they know a specific piece of information without revealing the information itself. This is particularly useful in scenarios where transaction details must remain confidential, such as in financial services or identity verification processes.
Use Case	zkSync is a Layer-2 scaling solution for Ethereum, designed to enhance transaction efficiency through the use of zero-knowledge rollups (zk-rollups). By batching multiple transactions into a single group, zkSync reduces the load on Ethereum, allowing for faster and cheaper transaction processing. Zero-knowledge proofs (ZKPs) are then employed to validate these batches without disclosing individual transaction details. Once validated, these proofs are submitted to the Ethereum mainnet for final verification.
Benefits	The effectiveness of a ZKP relies on its three key properties: completeness, ensuring that valid statements by honest provers are verifiable; soundness, preventing dishonest provers from convincing verifiers of false statements; and zero-knowledge, where verifiers gain no knowledge beyond the truth of the statement.

05

Business case studies of leading blockchain technology companies

Business Case Study: Ethereum

Ethereum – General Overview

Company name: Ethereum

- **Headquarters Regions :** Zug, Switzerland
- **Founded Date :** 30 July 2015
- **Founders :** Vitalik Buterin, Mihai Alisie, Amir Chetrit, Anthony Di Iori, Charles Hoskinson, Gavin Wood, Joseph Lubin, Jeffrey Wilcke
- **Funding and Valuation:** $3,431.65 per (ETH/USD) with a current market cap of $ 412.55B USD.

General Overview

Ethereum is a decentralized, open-source blockchain platform that enables developers to build and deploy smart contracts and decentralized applications (dApps). Launched in 2015 by Vitalik Buterin and a team of co-founders, Ethereum aims to create a global, decentralized computing platform that allows anyone to write code that controls digital value, runs exactly as programmed, and is accessible anywhere in the world.

History of Ethereum: A Brief Overview

Ethereum was conceived in 2013 by programmer Vitalik Buterin, inspired by the limitations of Bitcoin's lack of scripting capabilities for application development. It quickly gained interest for its potential as a platform to execute decentralized smart contracts and decentralized applications (dApps).

Founding and Early Vision (2015-2016)

Ethereum was officially launched in 2015 with its first live release, Frontier. Its early vision was to create a decentralized platform that would enable developers to build applications over a distributed network, without the risks of downtime, fraud, or interference from third parties.

Early Research and Breakthroughs (2016-2017)

During this period, Ethereum experienced significant growth in its ecosystem, with the development and deployment of hundreds of dApps. One of the major breakthroughs was the introduction of the ERC-20 token standard, which standardized the creation of new tokens on Ethereum's platform.

Ethereum – General Overview

Vision and Mission

The vision behind Ethereum is to decentralize the internet by replacing servers with a worldwide system of nodes, creating an environment where applications run on a peer-to-peer network that is beyond the control of any single governing entity. This "World Computer" aims to democratize the creation and execution of applications, reducing the risk of censorship, downtime, and third-party interference.

Ethereum's introduction has spurred a wave of innovation and has led to the development of new sectors within the industry, such as DeFi and NFT. Offering a platform for decentralized application development with smart contract executions, Ethereum has attracted a vast range of industry participants from startups to giant corporations.

Ethereum represents a transformative leap from traditional internet models to what is now termed the "Internet of Value." In economic terms, Ethereum can be likened to a self-sustaining economic entity, akin to a virtual country where the platform itself acts as both the marketplace and the infrastructure, while also providing the regulatory framework through its consensus mechanisms and smart contracts. It is a foundational economic system supporting a wide array of industries—from finance and art to manufacturing and logistics

Founder and Key Collaborators Profiles

Vitalik Buterin first introduced the concept of Ethereum in a 2013 white paper, envisioning a blockchain capable of executing programmable smart contracts and applications. His ongoing involvement includes spearheading significant protocol upgrades that have significantly enhanced Ethereum's functionality and efficiency.

Joseph Lubin as a co-founder who initially financed the startup with his own funds prior to Ethereum's ICO, Joseph Lubin's role was crucial in stabilizing Ethereum's early financial foundation. His later ventures, including founding ConsenSys, have played a pivotal role in expanding Ethereum's ecosystem, supporting startups, and promoting innovation within the community.

Mihai Alisie co-founded Bitcoin Magazine with Vitalik Buterin and was among the first to support the Ethereum concept. He played a crucial role in building the community and ethical framework around Ethereum, emphasizing transparency and open access.

Ethereum – Founding Team

Anthony Di Iori

Anthony Di Iori founded the Toronto Bitcoin Meetup Group, which quickly became a hub for crypto enthusiasts, including Vitalik Buterin. Recognizing the potential of Ethereum from Buterin's initial white paper, Di Iorio provided early funding and essential financial support, helping to navigate the project through its formative stages.

Jeffrey Wilcke

Jeff Wilcke entered the Ethereum project, participating in early discussions under an alias while working as a core developer for Mastercoin. Wilcke developed his own implementation of Ethereum in Google's Go language named "Go Ethereum," which has become one of the leading Ethereum clients used by developers around the world.

Charles Hoskinson

Charles was the CEO of Ethereum. He joined the Ethereum project early on, bringing strategic direction and a focus on creating sustainable business models. Before Ethereum, he founded The Bitcoin Education Project and contributed significantly to the broader understanding of cryptocurrencies.

Amir Chetrit

Early involved in the colored coins project, which laid foundational ideas for what would become NFTs, Amir joined the Ethereum team after an invitation from Buterin to review and contribute to the Ethereum whitepaper. His involvement symbolizes a direct link between early blockchain innovations and Ethereum's foundational technologies.

Gavin Wood

Gavin Wood authored the Ethereum Yellow Paper that delineates the technical framework for the Ethereum Virtual Machine (EVM), which is critical for implementing smart contracts. He also created Solidity, the primary programming language for Ethereum smart contracts, becoming foundational in the development of decentralized applications.

Ethereum – Technology Stack Overview

Ethereum operates on its own blockchain and uses a Turing-complete virtual machine called the Ethereum Virtual Machine (EVM) to execute smart contracts. The technology stack includes:

Ethereum Mainnet

This is the primary public blockchain where Ethereum operates, supporting all transactions and smart contracts executions. It is a decentralized platform where all data is verified and stored across multiple nodes to ensure security and resilience.

Ethereum Virtual Machine

This is the Turing-complete virtual machine that allows anyone to execute arbitrary EVM ByteCode. It is the place where all smart contracts operate and enabling the development and deployment of decentralized applications (dApps)

Ethereum Nodes

To interact with the Ethereum blockchain, applications connect to Ethereum nodes, which are computers running Ethereum client software. These nodes verify transactions, maintain network security, and ensure data accuracy by collectively storing and updating the Ethereum blockchain's state. Through the JSON-RPC API, applications can read blockchain data (like user balances) and send transactions (such as transferring ETH or executing smart contract functions) to interact with the network.

Solidity Programming Language

This is the primary language for writing smart contracts on Ethereum. Designed to target the EVM, it is a contract-oriented, high-level language whose syntax is similar to that of JavaScript. Solidity is statically typed, supports inheritance, libraries, and complex user-defined types among other features.

Ethereum – Serenity Upgrade

Ethereum 2.0 / Serenity

Ethereum 2.0, also known as Serenity, is a comprehensive upgrade to the original Ethereum blockchain (Ethereum 1.0). It aims to address scalability, security, and sustainability issues that have emerged with Ethereum's increased adoption. The transition introduces a shift from a Proof of Work (PoW) to a Proof of Stake (PoS) consensus mechanism. Proof of Work (PoW) and Proof of Stake (PoS) are two different consensus mechanisms. In PoW, miners compete to solve complex mathematical problems using computational power. The first miner to solve the problem gets the right to add a new block to the blockchain and is rewarded with the blockchain's native cryptocurrency. In PoS, validators are selected to create new blocks based on the number of coins they hold and are willing to stake. The more coins they stake, the higher their chances of being chosen to validate a transaction and add a block. This upgrade is executed in phases, each designed to incrementally integrate and migrate the system to another platform.

Phase 0, Beacon Chain and PoS Framework:

This is the beginning of Ethereum's transition to a PoS consensus mechanism. It introduced the Beacon Chain, a new PoS blockchain that will act as the central coordination and consensus hub of Ethereum 2.0.

Phase 1, Sharding Framework:

This phase introduces a significant structural transformation through the deployment of shard chains, aiming to amplify Ethereum's ability to process transactions and manage data more efficiently.

Phase 1.5 and 2, Merging Ethereum 1.0 and 2.0:

"The Merge" is a critical update where the existing Ethereum 1.0 blockchain integrates into the Ethereum 2.0 system, making it one of the 64 shard chains. This integration preserves the complete history and state of Ethereum 1.0, while transitioning to a more energy-efficient and scalable PoS consensus mechanism.

Phase 3, Final Touches:

This finalization phase is flexible in serving to address and resolve any remaining technical or operational issues from previous updates. The phase also emphasizes improving privacy measures and reinforcing security protocols to safeguard against any potential cyber threats.

Ethereum for Enterprise Ecosystem Overview

Ethereum For Enterprise

Enterprise blockchain applications can be built on the public permissionless Ethereum Mainnet, or on private blockchains that are based on Ethereum technology. There is only one public Ethereum Mainnet. Applications that are built on the Mainnet are able to interoperate, similarly to how applications built on the Internet can connect to each other, leveraging the full potential of decentralized blockchain. Some collaborative efforts to make Ethereum enterprise friendly have been put together by different organizations:

Enterprise Ethereum Alliance

The EEA enables organizations to adopt and use Ethereum technology in their daily business operations.

Hyperledger

Hyperledger is an open-source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, Internet of Things, supply chains, manufacturing and Technology.

Key Benefits

- Blockchain Security/Immutability - Ethereum Mainnet is secured by the interaction of thousands of independent nodes run by individuals throughout the world.
- Performance - Because private Enterprise Ethereum chains may use high performance nodes with special hardware requirements and different consensus algorithms such as proof-of-authority, they may achieve higher transaction throughput on the base layer (Layer 1). On Ethereum Mainnet, high throughput can be achieved with the use of Layer 2 scaling solutions.
- Cost - The cost to operate a private chain is primarily reflected in labor to set up and manage the chain, and the servers to run it. While there is no cost to connect to Ethereum Mainnet, there is a gas cost for every transaction which must be paid for in Ether.
- Node Permissioning - Only authorized nodes can join private chains while anybody can set up a node on Ethereum Mainnet.
- Privacy - Access to data written to private chains can be controlled by restricting access to the network, and on a finer grained basis with access controls and private transactions.

Ethereum for Decentralized Applications Overview

Ethereum as a Next Generation of Smart Contracts and Decentralized Application Platform

Ethereum intends to provide a blockchain with a built-in fully fledged turing-complete programming language that can be used to create "contracts" and to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

Commonly cited alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments ("**colored coins**"), the ownership of an underlying physical device ("**smart property**"), non-fungible assets such as domain names (“**namecoin**"), as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules ("**smart contracts**") or even blockchain-based "decentralized autonomous organizations (“**DAOs**”).

There are three types of applications on top of Ethereum, i) **financial applications** including sub-currencies, financial derivatives, hedging contracts, savings wallets, wills, and ultimately even some classes of full-scale employment contracts, ii) **semi-financial applications** where money is involved but there is also a heavy non-monetary side to what is being done; a perfect example is self-enforcing bounties for solutions to computational problems, iii) **online voting** and iv) **decentralized governance.**

Token systems range from sub-currencies representing assets such as USD or gold to company stocks.

Financial derivatives and stable-value currencies are the most common application of a "smart contract", and one of the simplest to implement in code, while the main challenge in implementing financial contracts is that the majority of them require reference to an external price ticker.

Other applications include **identity and reputation systems**, **decentralized file storage, decentralized autonomous organizations.**

Ethereum – Governance Model (1/2)

Ethereum Governance Ethereum's governance process is based off-chain, led by the Ethereum Foundation and conducted through online forums such as Discord, GitHub, Ethereum Magicians, and Zoom.

EIPP: Ethereum Improvement Proposal Process

The official process for upgrading Ethereum is called the Ethereum Improvement Proposal (EIP) process. It is based on the Bitcoin Improvement Proposal (BIP) process, which is a standardized process for submitting code changes to the Bitcoin protocol. The BIP process was in turn inspired by Python's PEP-0001 process, which outlines a governance model for improving the Python coding language. BIPs and EIPs are documents that describe new features or changes to Bitcoin and Ethereum, respectively. There are three types of EIPs.

Standards Track: Most EIPs are Standards Track EIPs, which specify code changes to Ethereum that require a hard fork, affect Ethereum's network layer or execution API, or introduce new application-level standards and contracts. Standards Track EIPs are further divided into the following categories: Core, Network, Interfaces, and Ethereum Request for Comments (ERC).

Core: Refers to code changes that require a full network upgrade to activate

Network: Refers to improvements to Ethereum's peer-to-peer network layer, also known as "devp2p".

Interface: Refers to code changes that affect Ethereum client APIs and RPC specifications.

ERC: Refers to improvements related to the Ethereum application layer. Ethereum core developers are considering a separate governance process for ERCs that is distinct from EIPs.

Meta/Process: Meta EIPs do not propose changes to Ethereum's codebase, but rather describe changes to processes (such as the decision-making process for EIPs).

Introducing Changes to Ethereum Protocol

Step 1: Propose a Core EIP:

The first step to formally proposing a change to Ethereum is to detail it in a Core EIP. This will act as the official specification for an EIP that Protocol Developers will implement if accepted.

Step 2: Present your EIP to Protocol Developers:

Once a Core EIP, for which community input is gathered, is presented to Protocol Developers, it is proposed for discussion on an AllCoreDevs call. It is likely some discussions will have already happened asynchronously on the Ethereum Magician's forum or in the Ethereum R&D Discord.

Ethereum – Governance Model (2/2)

Ethereum Improvement Proposal Workflow

After an EIP is submitted it goes through a life cycle of technical reviews, research, and discussions including:

Draft – An EIP is merged by an EIP Editor into the EIP repository when properly formatted

Review – An EIP author marks an EIP as ready for and requesting Peer Review.

Last Call – An EIP that is done with its initial iteration and ready for review by a wide audience.

Accepted – A core EIP that has been in the last call for at least two weeks and any technical changes that were requested have been addressed by the author.

Final – An EIP that core developers have decided to implement in various clients (Geth, Nethermind, etc.) and is scheduled for release in a future hard fork, or has already been released in a hard fork.

Ethereum Governance Stakeholders

There are various stakeholders in the Ethereum community, each playing a role in the governance process, including:

Ether holders: these people hold an arbitrary amount of ETH.

Application users: these people interact with applications on the Ethereum blockchain.

Application/tooling developers: these people write applications that run on the Ethereum blockchain (e.g. DeFi, NFTs, etc.), or build tooling to interact with Ethereum (e.g. wallets, test suites, etc.).

Node Operators: these people run nodes that propagate blocks and transactions, rejecting any invalid transaction or block that they come across.

EIP Authors: these people propose changes to the Ethereum protocol, in the form of Ethereum Improvement Proposals (EIPs).

Validators: these people run nodes that can add new blocks to the Ethereum blockchain.

Protocol Developers (a.k.a. "Core Developers"): these people maintain the various Ethereum implementations (e.g. go-ethereum, Nethermind, Besu, Erigon, Reth, at the execution layer or Prysm, Lighthouse, Nimbus, Teku, Lodestar at the consensus layer).

Community Consensus and Disagreements

While some EIPs are straightforward technical improvements with minimal nuance, some are more complex and come with tradeoffs which will affect different stakeholders in different ways. Since Protocol Developers have no way to force people to adopt network upgrades, they will generally avoid implementing EIPs where the contentiousness outweighs the benefits to the broader community.

Ethereum – Select Particulars of ETH’s Token Model

Ether (ETH) is Ethereum’s native cryptocurrency. It is used to pay for transaction fees and computational services, crucial for executing interactions and running decentralized applications (dApps). ETH incentivizes ongoing development and participation within the ecosystem, aligning the interests of developers and users with the health and expansion of the Ethereum platform. This role ensures ETH remains central to Ethereum’s operational and economic model, driving network engagement and technological progress.

Ethereum Token Model

ERC-20: The Standard for Fungible Token: interchangeable tokens, with each unit identical in value and function, making them ideal for creating digital currencies and assets. This standard underpins many of the digital currencies and tokens used in a variety of decentralized applications.

ERC-721: The Standard for Non-Fungible Tokens: provides a framework for non-fungible tokens, which are unique and individually identifiable. This standard is critical for digital collectibles and art, enabling the representation of ownership over these distinct assets.

ERC-1155: A Multi-Token Standard: enhances transaction efficiency by allowing a single contract to manage multiple types of tokens, both fungible and non-fungible. This versatility is especially beneficial in gaming and decentralized finance, where different asset types frequently interact within the same ecosystem.

Ethereum Economics

Ethereum's economic framework is designed to balance scalability, security, and decentralization, often referred to as the blockchain trilemma. The network's native cryptocurrency, ETH, is not just a medium of exchange but also a vital component of Ethereum's security protocol, especially with the transition to proof of stake (PoS) in Ethereum 2.0. Ethereum Economics also encompasses the platform's approach to transaction fees (gas fees), its monetary policy, and the mechanisms for issuing new ETH into the system, which together influence the network's liquidity, usability, and overall value.

Ethereum – Key Investors and Funding Rounds

Key Investors and Funding Rounds

Ethereum has a substantial market cap, making it one of the leading cryptocurrencies. The project was initially funded through a public crowdsale (ICO) on 22, July 2014, raising around $18.3 million with 60000000 ETH sold at an average price of $0.31. Since then, Ethereum has continued to attract significant investment from individuals and institutions, reinforcing its position as a foundational layer of the blockchain ecosystem.

Ethereum's market cap is closely tied to its diverse and evolving revenue streams. Ethereum's network revenues are projected to rise significantly from $2.6 billion annually to as high as $51 billion by 2030. This growth is primarily driven by several key revenue components including transaction fees, Miner Extractable Value (MEV), and Security as a Service (SaaS).

Ethereum Foundation, a non-profit organization that supports Ethereum and its related technologies, received support from 16 known investors with a total funding amount of $18.4M.

- **Seed and Pre-Seed Rounds:** Winklevoss Capital, KR1
- **Venture Rounds:** Flux Capital, Alexis Berthoud, Breyer Labs, Placeholder, David J. Namdar
- **Initial Coin Offering:** George Burke, Kenneth Bok, Karnika Yashwant
- **Secondary Markets:** Zachary Snader, 8 Decimal Capital, Arbi Khodagholian, Block Ventures, MKT

Business Case Study: Polygon

Polygon – General Overview

Company name: Polygon

- Headquarters Regions: Camana Bay, Cayman Islands
- Founded Date: 2017
- Founders: Jaynti Kanani, Sandeep Nailwal, Anurag Arjun
- Funding and Valuation: Polygon's (MATIC) price of $0.534908 per token, with a market cap of $5.29 billion

General Overview

Polygon (formerly Matic Network) is a protocol and framework for building and connecting Ethereum-compatible blockchain networks. Its primary goal is to address the scalability issues of the Ethereum blockchain by providing solutions for faster and cheaper transactions.

History of Polygon: A Brief Overview

Polygon (formerly Matic Network) is a blockchain platform which aims to create a multi-chain blockchain system compatible with Ethereum. Polygon is used in decentralized applications (dApps) such as Defi, DAOs, and NFTs.

The Matic Network was launched in 2017 by four Mumbai-based software engineers: Jaynti Kanani, Sandeep Nailwal, Anurag Arjun, and Mihailo Bjelic. In February 2021, the project was rebranded as Polygon Technology.

In December 2021, Polygon acquired the Mir blockchain network for 250 million MATIC tokens, with the tokens having a value of around $400 million at the time of the deal.

In February 2022, Polygon raised $450 million by selling MATIC tokens in a round led by Sequoia Capital India including Tiger Global and Softbank Vision Fund. In November 2022, JPMorgan Chase & Co executed its first live trade on a public blockchain, using Polygon and modified Aave. By February 2023, the blockchain was doing business with large companies such as Starbucks and Mastercard, with Fortune noting it had been relatively unaffected by the 2022 cryptocurrency crash compared to other companies. The Fox Network began working with Polygon on a blockchain project in 2023. TIME in 2023 named Polygon Labs one of the Time100 Most Influential Companies of the year.

Polygon – Founding Team

Sandeep Nailwal

Sandeep Nailwal brings extensive experience in software development to Polygon. His role involves the oversight of Polygon's daily operations and the strategic planning for its long-term scaling solutions.

Jaynti Kanani

Jaynti Kanani, serving as the CEO of Polygon, originally a data scientist, has a rich history in blockchain scalability solutions. His expertise was pivotal in the initial development of Polygon's core architecture

Mihailo Bjelic

Mihailo has a MSc in CS from the University of Belgrade. Prior to joining the Web3 industry in 2017 and co-founding Polygon, he worked on AI/ML projects for the auto industry and several startups.

David Z

David is the Co-Founder and CTO at Polygon Labs. Obtaining MSc in Telecommunication Engineering, he further pursued big data and cybersecurity at MIT.

Jordi Baylina

Jordi is in charge of technical development of the Polygon Hermez zkRollup and engages in zkEVM implementation to scale Ethereum. He has a background in Electronics Communications Engineering.

Antoni Martin

Antoni is the Co-Founder and Business Development Lead. He previously worked at Deutsche Bank as an Intrapreneur Initiative for Digital Asset Platform development.

Brendan Farmer

Brendan is the Co-Founder and CEO of Polygon Zero, focusing on zero-knowledge cryptography. He has a background in Math and Philosophy, and is the co-founder of Mir.

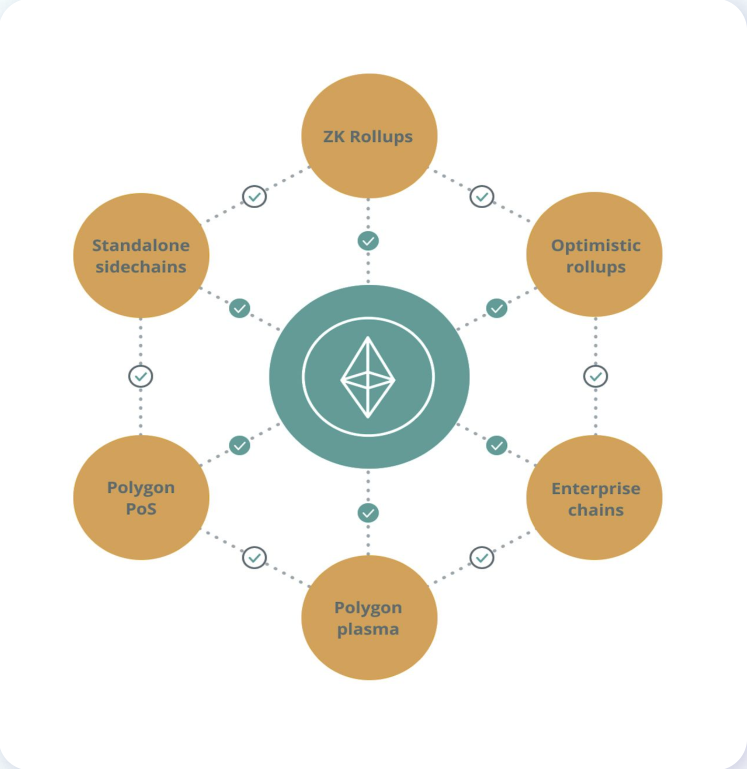
Daniel Lubarov

Daniel is the Co-Founder of Polygon Zero. He studied computer science at Harvey Mudd and was a soft engineer at Google prior to founding Mir Protocol.

Bobbin Threadbare

Bobbin is the project lead for Polygon Miden, a STARK-based general-purpose ZK rollup. He was a core ZK researcher at Facebook's Novi and lead development for Winterfell.

Polygon – Technology Stack



General Overview

Polygon is a blockchain platform operating as a layer-2 scaling solution which aims to create a multi-chain blockchain system maintaining full compatibility with Ethereum protocols and tools. As with Ethereum, it uses a proof-of-stake consensus mechanism for processing transactions on-chain. This compatibility allows integration and interaction with Ethereum's existing decentralized applications (dApps) and smart contracts.

- **Standalone Sidechains**

  Polygon utilizes a network of side chains that are separate but parallel blockchains linked to the main Ethereum chain via two way bridge. These sidechains help to offload the transaction load from Ethereum, enhancing speed and reducing costs.

- **Plasma**

  Plasma chain is considered a child chain of Ethereum mainnet and is designed for high security but are less suited for complex operations. It sends periodic state committments to Ethereum and uses fraud proof to arbitrate disputes.

Polygon – Technology Stack

Proof of Stake (PoS)

Polygon's main chain operates on a PoS consensus mechanism, allowing for faster and more energy-efficient processing of transactions compared to Ethereum's traditional proof of work system.

zk-Rollups

It scales by bundling numerous transactions into a single one, with validity proof that confirms the correctness of all transactions in the batch without revealing their contents.

Optimistic Rollups

It functions similarly to zk-Rollups but with a fraud-proof mechanism that assumes transactions are valid unless proven otherwise.

Enterprise Chains

Customized blockchain solutions for corporate use that provide both the advantages of Polygon's scalability and Ethereum compatibility.

Transactions and Transaction Fees

Polygon significantly enhances Ethereum's capabilities by addressing key issues of transaction speed and cost. It achieves up to 65,000 transactions per second, a contrast to Ethereum's 14 to 30, due to its layer-2 scaling solutions. Transaction costs on Polygon are markedly lower, often just a fraction of a cent, compared to Ethereum's fees, which can soar to $15 to $80 during peak times.

Technologies like zk-Rollups and optimistic rollups can manage transaction loads efficiently. These measures speed up transactions and keep costs minimal, attracting more dApp users and developers.

Polygon SDK

Provides a software development kit that enables developers to build and connect Ethereum-compatible blockchain networks easily. This tool is pivotal for creating diverse multi-chain ecosystems.

Polygon – Technology Roadmap

The technology roadmap for Polygon is centered on enhancing its capabilities as a leading layer-2 scaling solution for Ethereum. It aims to improve transaction speed and reduce costs through continuous technological advancements. Polygon compensates network validators through transaction fees and staking rewards, using its native token, MATIC. Transaction fees on Polygon are significantly lower, and they adjust according to network congestion to ensure affordability and efficiency.

Polygon Chain Development Kit (CDK):This toolkit allows developers to build Ethereum-compatible decentralized applications as Layer 2 solutions by simplifying the creation and maintenance of side chains and Layer 2 protocols.

Aggregation Layer: This sophisticated framework unifies liquidity across the Polygon ecosystem. It facilitates cross-chain transactions, improving the fluidity and interoperability.

Polygon Miden Rollout: Miden emphasizes zero-knowledge proofs, utilizing a custom virtual machine designed to optimize privacy and transaction throughput.

Enhanced Protocol Architecture in Polygon 2.0: This focuses on integrating zero-knowledge (ZK) technology to achieve unlimited scalability and unified liquidity. The upgrade will address the inherent scalability challenges faced by Web3 technologies, streamlining the addition of new chains and improving user experiences.

Type 1 Prover Integration: Polygon Labs has partnered with Toposware to introduce the Type 1 upgrade to the zkEVM, enabling any EVM chain to transition into a ZK Layer 2 and connect with the AggLayer.

Polygon – Governance Model (1/2)

Blockchains are distributed, open protocols with no single point of control. Polygon operates three pillars of governance, specifically i) protocol governance ii) system smart contracts governance and iii) community treasury governance.

Protocol Governance facilitates decentralized maintenance and development of the Polygon tech stack. For Polygon protocols, we distinguish two main components necessary for long-term maintenance, development, and governance: the PIP framework and a decentralized community to sustain it.

At its core, the PIP framework is currently defined by two main documents:

- PIP-1 10 acts as the axis mundi around which all other elements of the PIP framework orbit. It provides a structure for PIPs in all tracks, describing general content requirements, as well as outlining the progression flow each PIP may take before it is implemented.
- PIP-8 8 is an advisory implementation framework. It details all of the different moving parts of the Polygon PoS architecture and how an upgrade to each of those parts may be facilitated by the PIP framework.

Decentralized Community

The PIP framework allows a clear and transparent way to propose and implement changes to the PoS chain. The following initiatives currently help foster the decentralized community:

- **The Polygon Community Forum 8** provides an open space for network participants to discuss ideas, propose and develop solutions, and deliberate on issues.
- A dedicated **Discord PIP channel** allows for async discussion of governance issues.
- **Polygon Protocol Governance Calls 10** are a space to discuss highly-technical developments of the Polygon PoS chain, held every 4 weeks.

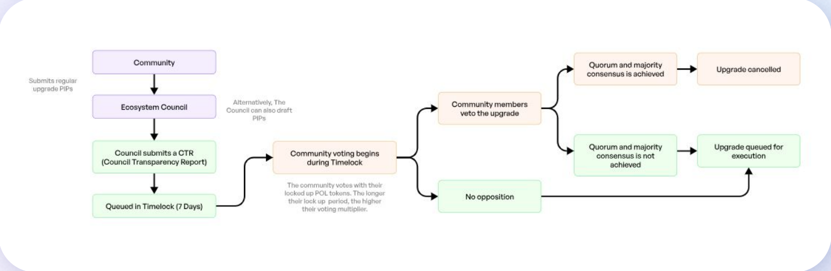
System Smart Contracts Governance facilitates the upgrades of protocol components that are implemented as smart contracts. The process of upgrading system smart contracts will begin with a Polygon Improvement Proposal (PIP).

Voting Power

To align incentives and introduce conviction-based governance, a vote escrow system is currently under exploration.

Voting Process

A window for community voting opens whenever an upgrade is queued for the timelock by the Council. The upgrade is automatically executed after the timelock has ended. However, if the quorum is met for majority opposition, then the upgrade is cancelled.



Submits regular upgrade PIPs
Community
Ecosystem Council
Alternatively, The Council can also draft PIPs
Council submits a CTR (Council Transparency Report)
Queued in Timelock (7 Days)
Community voting begins during Timelock
The community votes with their locked up POL tokens. The longer their lock up period, the higher their voting multiplier.
Community members veto the upgrade
No opposition
Quorum and majority consensus is achieved
Upgrade cancelled
Quorum and majority consensus is not achieved
Upgrade queued for execution

Polygon – Select Particulars of Polygon's Token Model

MATIC, Polygon's native cryptocurrency, is essential for transaction fees and governance within the network. MATIC serves as the payment medium for transactions and computational services on Polygon's scaling solutions. Its supply is capped at 10 billion MATIC tokens, creating a scarcity that can drive value as demand increases from network growth and usage. Its role in staking, governance, and transaction payments ensures its continuous circulation within the ecosystem, supporting its valuation and utility in the long term.

Gas Token

MATIC is used when you conduct any transaction or use an application built on Polygon PoS, to pay a small fee in MATIC and use Polygon PoS.

Network Security

Polygon employs a proof of stake mechanism that uses staked MATIC to reach consensus on the network. By staking MATIC, one can secure Polygon PoS and earn rewards. In this system, validators are disincentivized from engaging in any malicious behavior.

Tokenomics Revamp – POL

Polygon, a layer-2 network built on top of the Ethereum blockchain, is planning to revamp the tokenomics of matic, its native token as of 2023 with the introduction of POL.

POL aims to be a "hyperproductive token," similar to "productive tokens" which can be used by validators to secure a network and reap benefits. POL can be used by validators to secure multiple chains. Different chains can offer roles including accepting transactions and block generation, creating zero-knowledge proofs, and participating in data availability committees.

Migrating MATIC tokens to POL will be achieved by sending the MATIC tokens to a designated smart contract. This smart contract will handle the conversion process automatically, converting the deposited MATIC into an equivalent amount of POL. The initial supply of the token will be capped at 10 billion, and most of these tokens will be reserved for transitioning MATIC to POL.

Polygon – Key Investors and Funding Rounds

Key Investors and Funding Rounds

As of now, Polygon has a substantial market cap, reflecting its strong position in the blockchain ecosystem. The project raised funds through private and public token sales, including an initial exchange offering (IEO) on Binance. Polygon attracted investment from 49 investors with a total funding amount of $451M. Below are some of the investors with most of them participating in the ICO:

- **Seed and Pre-Seed Rounds:** Coinbase Ventures, Shinhan Venture Investment, ZBS Capital, MiH Ventures, Mark Cuban
- **Initial Coin Offering:** Crowd Venture Capital, Steadview Capital, Kevin O'Leary, Ryze Labs, Celsius Network, Cashican People LLC, Softbank Vision Fund, The Spartan Group, Galaxy Digital, Coinfund, Accel, Union Square Ventures, Dragonfly, Tiger Global Management, Finality Capital Partners, Republic Capital, Workplay Ventures, Variant, Dune Ventures, Sound Ventures, Peak XV Partners
- **Secondary Markets:** Upchain Capital, High Naut Capital.

SOLANA

Business Case Study: Solana

Solana – General Overview

Company name: Solana

- **Headquarters Regions :** San Francisco, USA
- **Founded Date :** March 16, 2020
- **Founders :** Anatoly Yakovenko, Greg Fitzgerald, Raj Gokal
- **Funding and Valuation:** $ 161.87 per (SOL / USD) with a current market cap of $ 75.14B USD

General Overview

Solana is a third generation blockchain platform that was launched to address some key limitations of earlier blockchain systems, notably scalability and speed. With the unique hybrid consensus mechanism that combines proof-of-stake and proof-of-history, the network can process transactions at speed up to 710000 transactions per second theoretically. This makes Solana one of the fastest blockchain networks in existence.

History of Solana: A Brief Overview

Foundational Years (2017-2020)

Conceived by Anatoly Yakovenko, Solana emerged from a 2017 white paper introducing Proof of History (PoH), a novel method for recording time in distributed systems. Officially launched in March 2020, Solana showcased its capability early on by processing 10,000 transactions in under a second in prototypes and running its first public testnet by mid-2018.

Expansion (2020-2023)

Solana's growth accelerated with its mainnet launch in 2020, followed by significant financing, including a $20 million round led by Multicoin Capital. By 2021, Solana had become a key platform for NFTs and DeFi projects, reaching a peak price of $260. The following years saw strategic partnerships with major tech companies and continuous network growth, highlighted by the launch of major projects like Circle's EURC stablecoin in 2023.

Solana – Founding Team

Vision and Mission

Solana's architecture supports a wide array of functionalities, from smart contracts to decentralized finance (DeFi) applications and non-fungible tokens (NFTs), without the need for additional scaling solutions. This single-layer approach contrasts sharply with other blockchains that rely on multiple layers to achieve scalability. Solana's method reduces the complexity and potential bottlenecks associated with layered scaling, offering developers a straightforward platform for building and deploying dApps. Solana faces challenges such as potential for centralization due to the high computational demands placed on its validators. Nevertheless, the innovative use of PoH provides a framework for time stamping transactions in a decentralized manner. This technology underpins Solana's ambition to compete with centralized payment processors like Visa, combining higher transaction throughput with lower fees to facilitate broader adoption.

Founder and Key Collaborators Profiles

Anatoly Yakovenko

Principal architect and co-founder. After earning a computer science degree from the University of Illinois, Anatoly led several high-stakes projects focused on operating system development at Qualcomm. Later roles at Mesosphere and Dropbox saw him innovating in distributed systems and data compression technologies.

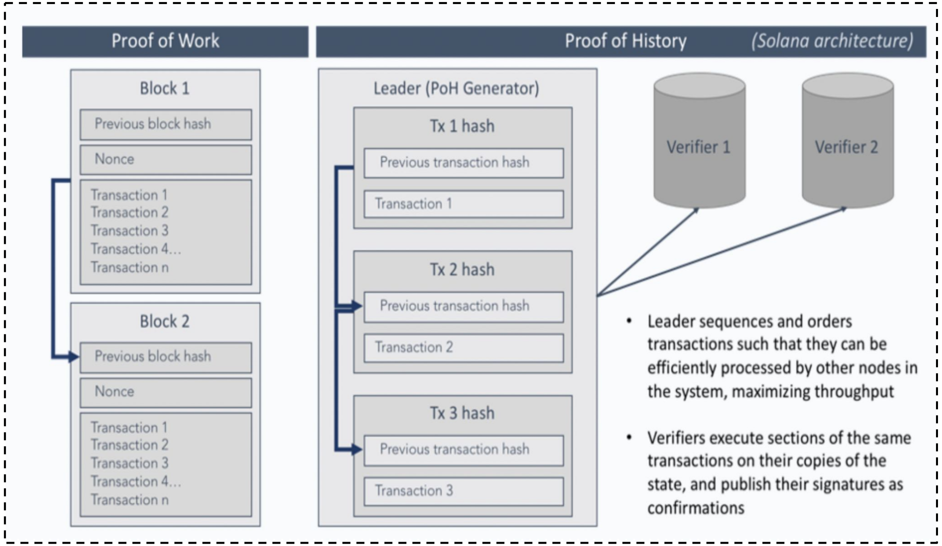
Greg Fitzgerald

Co-founder and CTO. Greg brings a deep background in operating systems and embedded systems from his time at Qualcomm. His expertise spans from developing a bidirectional RPC bridge between C and Lua for the BREW operating system to launching the ARM backend for the LLVM compiler toolchain.

Raj Gokal

Co-founder and COO. Raj oversees the strategic operations of Solana Labs. A graduate of The Wharton School at the University of Pennsylvania with a Bachelor of Science in Economics, Gokal has a diverse background spanning from venture capital as an associate at General Catalyst Partners to entrepreneurial ventures, including founding a wearable healthcare device startup, Sano.

Solana – Overview of Proof of History (PoH)



- Leader sequences and orders transactions such that they can be efficiently processed by other nodes in the system, maximizing throughput
- Verifiers execute sections of the same transactions on their copies of the state, and publish their signatures as confirmations

Proof-of-History (PoH)

A unique consensus mechanism integral to Solana's architecture, devised by Anatoly Yakovenko. It is designed to enhance the integrity and efficiency of the blockchain by providing a verifiable order of events. PoH is not just about recording events but establishing a chronological order in a decentralized environment. The Verifiable Delay Function ensures time has indeed passed between recorded events. It requires a specific number of sequential computational steps to complete, but once done, the outcome is easily verifiable by others. VDF ensures no participants can forge the chronological sequence of events, providing defense against various types of attacks on the network’s temporal structure.

Unlike PoW, which demands extensive computational effort, and PoS, which requires validators to stake cryptocurrency, PoH relies on the security provided by the chronological order of events. PoH provides immediate finality of blocks, meaning once data is entered into the Solana blockchain, it cannot be altered, contrasting with the probabilistic finality of PoW and PoS. It also lowers the demands on network bandwidth and storage, as each block only stores minimal data, essentially the hash from the previous block and its own timestamp.

Solana – Governance Model

Solana's Proposal Process for Governance

Solana's governance model is designed to foster a collaborative and secure development environment, with the proposal process for introducing new features, changes, or improvements within the network's ecosystem. Proposals serve as the design document that outline changes to the Solana environment. They provide a rationale, document potential impacts, and serve as a historical record of Solana's evolution. Proposals help scale new contributors, facilitate community awareness about changes, and act as blueprints.

A proposal is needed in cases including but not limited to: changes to the validator structure, modifications to RPC interfaces, adjustment to consensus mechanism, significant updates to proposal itself

Here are two types of proposals:

- **Standard Proposals:** These affect the majority of the Solana ecosystem, including changes to the network protocol, transaction validity, and other elements that impact interoperability across Solana implementations.
- **Meta Proposals:** They focus on processes surrounding Solana rather than the protocol itself, such as changes to decision making process

Proposal Lifecycle

Idea: The author of proposals discuss the idea with Solana core community, to vet originality and viability.

Draft: Formal document is forged and submitted as a pull request for community review.

Review: The proposal undergoes a thorough review on GitHub, where core contributors and community members provide feedback.

Accepted: Once garnered enough support, accepted proposals may either be implemented immediately or queued for future implementation.

Living: Some proposals are meant to be continually updated and thus are categorized as living, such as SIMD-1.

Stagnant: Proposals that do not see activity for six months are marked as stale and may be closed, though they can be reopened if renewed consensus emerges.

Withdrawn: If a proposal is withdrawn by the author, it is considered finalized in this state. Any revival of the idea is treated as a new proposal.

Solana – Governance Model

Implementing SPL for DAO Management on Solana

Solana's SPL Governance framework is a system developed by Solana Labs as part of the Solana Program Library, designed for the management and operational efficiency of Decentralized Autonomous Organizations (DAOs) on the Solana blockchain. SPL Governance provides a set of features that empower DAO members to create, vote on, and implement proposals that execute instructions. These proposals can govern anything from fund allocation to program upgrades and administrative changes within the DAO itself. The flexibility of the system accommodates both simple multisig scenarios and comprehensive DAO management tasks.

Key Components of SPL Governance

- **DAO and Realm Configuration:** The program distinguishes between a DAO and realms within it, where a realm can be seen as a configuration environment or subset of the DAO, tailored to specific governance needs. Although multiple realms can exist within a single DAO, typically, a DAO operates within a single realm.
- **Proposal Mechanism**: Proposals serve as the mechanism through which changes are suggested and decided upon. Members create proposals that are voted on by the DAO community; if passed, the proposals' instructions are executed according to the democratic outcomes of these votes.
- **Governance Account Structure**: The structure is hierarchical, beginning with the Realm account, which defines the community and council mints for voting. Under this are the Governance accounts, which set specific rules for proposal creation and voting processes, and finally, the Proposal accounts, where actual governance decisions are made.
- **Deployment Flexibility**: DAOs can choose between using a shared instance of the SPL Governance program for convenience or deploying their own instance for greater control and customization. This flexibility supports a range of organizational sizes and needs, from smaller community projects to large, complex organizational structures.

Solana – Technology Stack

01

TOWER BFT

Functioning similarly to the Practical Byzantine Fault Tolerance (PBFT) system, Tower BFT exploits the synchronized timing mechanism of PoH, prioritizing network liveness while maintaining a high degree of consistency. In this system, validators are able to observe and analyze the timeouts committed by other network validators directly from the ledger. This direct observation allows each node to independently verify the state and commitments of other nodes without the need for peer-to-peer communication.

02

TURBINE

Turbine is Solana's block propagation protocol to enhance the speed and efficiency of data transmission. This multi-layered approach segments the network into distinct layers of nodes, where each node is tasked with passing on ledger entries to a select group of nodes in the subsequent layer. By limiting the number of direct communications each node manages, Turbine addresses the scalability trilemma related to bandwidth.

03

GULF STREAM

It serves as a transaction forwarding protocol. By allowing validators to forward transactions directly to the expected leader before they become due for processing, Gulf Stream eliminates the need for a mempool, where transactions typically linger awaiting confirmation in other blockchains. This reduces confirmation times significantly and optimizes the overall transaction processing workflow, enabling Solana to handle up to 100,000 transactions per second.

04

SEALEVEL

Sealevel is a parallel smart contracts runtime that enhances the network's efficiency and scalability. Unlike other platforms that operate on single-threaded execution, such as Ethereum, Sealevel is built to handle thousands of contracts simultaneously through its hyper-parallelized transaction processing engine. Instead of executing transactions within the virtual machine itself, Sealevel utilizes the Berkeley Packet Filter (BPF) bytecode for execution on hardware natively.

Solana – Technology Stack

Pipelining

A CPU design optimization that enhances Solana's transaction processing capabilities. This technique allows the Solana network to handle up to 50,000 transactions simultaneously by distributing the workload across various stages of its four-stage pipeline.

Cloudbreak

It structures network participation into parallel chains for increased transaction processing capacity as Solana's optimized account database. It facilitates concurrent reads and writes across a RAID 0 configuration of SSDs, eliminating memory as a bottleneck in transaction speeds and scalability. This architecture allows for real-time, Ahead Of Time (AOT) transaction execution by pre-fetching necessary data as soon as transactions are observed.

Archivers

Archivers maintains data integrity and availability by offloading storage duties from validators. These nodes, which do not participate in consensus, are designed to handle extensive amounts of data, storing petabytes in a decentralized manner while remaining lightweight. Solana employs Proofs of Replication (PoRep) to periodically verify that Archivers hold the data they are tasked with.

Transaction and Transaction Fees

Solana transaction fees are usually less than $0.001. These fees are charged for processing transactions, which may contain one or more instructions executed by validators. The fee structure includes a base fee of 5,000 lamports per signature. A fixed proportion of each transaction fee, initially set at 50%, is burned, removing it from circulation, while the remainder compensates the validator. This mechanism helps maintain the scarcity and value of the SOL token, contributing to the network's long-term economic health.

Prioritization Fees

Solana offers the option of paying prioritization fees to accelerate the processing of transactions for users needing faster confirmation times, calculated based on the transaction's compute unit limit and the current compute unit price.

Rent

Rent is recurring charged for storing data on-chain that ensures data associated with Solana accounts remains available on the blockchain. Accounts must hold a minimum balance, proportional to the space they occupy, to be exempt from rent.

Solana – Technology Roadmap

Recent Update

The recent release of a mainnet beta update, v1.17.31, is specifically designed to alleviate ongoing network congestion. This update included key improvements such as differentiating staked versus non-staked packets for better traffic management, implementing Quic to use “smallvec” for aggregating chunks and saving allocations per packet, and adjusting the BankingStage Forwarding Filter. Additionally, the update tightens stream controls for staked nodes and adjusts quality of service (QoS) measures to treat super low-staked nodes similarly to unstaked ones. These adjustments are part of a series of planned updates, with more comprehensive enhancements expected in the upcoming v1.18 release, which will further address network efficiency and congestion issues.

Upcoming Features

Token Extensions: Early 2024 will see the introduction of token extensions to Solana with token creation directly at the program level. This development will include features like confidential transfers for privacy with optional auditability, transfer hooks for invoking custom programs during token transfers, and a metadata pointer to establish authoritative sources for token metadata verification.

Firedancer and Additional Validator Clients: Announced at Breakpoint 2023, Firedancer, a complete rewrite of the Solana validator client by Jump, is currently live on the testnet. This new validator client optimizes networking, runtime, and consensus components, with early benchmarks showing capabilities of processing over 1 million transactions per second per core on commodity hardware. The introduction of Firedancer, alongside other projects like Jito-Solana, Sig, and TinyDancer, signifies a move towards diversifying client software to improve network resilience.

Solana – Select Particulars of Sol’s Token Model

Sol is Solana’s native cryptocurrency that has a role in transaction fees and governance within the network. With an initial total supply capped at 500 million tokens, SOL's scarcity is poised to enhance its value as network adoption and demand escalate. SOL is integral to staking, where users can participate in network consensus, enhancing security and stability, as well as governance, allowing holders to vote on future upgrades and decisions.

Circulating Supply

Sol currently has a total supply of 579,377,833, with 79.9% in circulation and 20.1% non-circulating. The circulating supply of SOL encompasses the total amount available for transactions across exchanges, decentralized exchanges, and wallets, including both staked and unstaked SOL. Staked SOL that is unlocked allows for active participation within the staking ecosystem, though it enters a 'cool-down' period post-delegation to a validator, restricting withdrawal for 2-3 days. The non-circulating supply consists of SOL locked in stake accounts, primarily from investments or grants, with specific unlock dates. A significant portion of non-circulating SOL is managed by Solana Labs or the Solana Foundation and is actively redelegated among validators to ensure network decentralization and performance.

Inflation Schedule

Solana has a current inflation rate of 5.182%. The rate was originally at 8% and decreases at an annual rate of 15%, aiming to reach a final inflation rate of 1.5%. This inflation strategy ensures that stakers are compensated for securing the network, effectively making non-stakers pay stakers through inflation. To counteract the inflation effects, 50% of each transaction fee is burned to reduce Sol’s overall supply, while the other half rewards the validators. This balance between inflation and fee-burning helps maintain economic stability as network grows to ensure validators stay incentivized as staking rewards gradually decrease.

Solana – Key Investors and Funding Rounds

Key Investors and Funding Rounds

The Solana project raised funds through several private sales and a public token auction, securing investments from major venture capital firms and institutional investors. It has a total funding amount of $319.5M across 13 rounds with 48 investors. Here are some of the investors:

- **Seed and Pre-Seed Rounds:** AngelDao, The Spartan Group, LongHash Ventures, Lemniascap, GSR, ZMT Capital, Kosmos Ventures, Blockwall, AGE Crypto Asset Investment Fund, BlockTower Capital, Blockchange Ventures, Kevin Rose, Reciprocal Ventures, Slow Ventures, Lyndon Rive, Foundation Capital, Distributed Capital, Multicoin Capital, NGC Ventures, Passport Capital, LYVC, Ramtin Naimi, 500 Global, Chris McCann.
- **Initial Coin Offering:** To Kenz Capital, Buck Stash Genblock Capital, Collab+Currency, Alameda Research, 1kx, Memetic Capital, Blockchange Ventures, CoinFund, Genesis One Capital, Multicoin Capital, CoinShares, SeaX Ventures, ParaFi Capital, Ryze Labs, Polychain, L1D, Jump Trading, Crowd Venture Capital, COIND, CMS Holdings, Cashican Pople LLC, Andreessen Horowitz
- **Secondary Markets:** Reade Seiff, SAWA.

06

Key challenges and opportunities towards the goal of mass adoption of blockchain technologies

Select challenges in the mass adoption of blockchain technologies (1/2)

TRUST AND GOVERNANCE

Blockchain redistributes trust from centralized authorities to cryptographic systems and a complex network of protocols, leading to complexities in governance. Users need to trust the integrity of the blockchain's technological and procedural frameworks, which govern their transactions and data, despite not necessarily understanding the detailed workings of these systems.

POTENTIAL SOLUTIONS

Transparent Algorithm Audits: Develop and implement routine audits of blockchain algorithms and protocols, conducted by independent third parties.

Smart Contract Templates: Provide standardized, open-source smart contract templates that have been legally vetted and are easy to customize and audit.

Implement Hybrid Governance Models: Combine elements of decentralized and traditional governance structures to enhance trust, such as establishing a governing body composed of representatives from various stakeholder groups within the network.

ENERGY CONSUMPTION

Blockchain technology, particularly through Bitcoin mining, is a significant energy consumer due to the intensive computational work required for maintaining its decentralized ledger. The process, known as proof of work, requires numerous computers to consume large amounts of electricity. This has led to environmental concerns, as the carbon footprint of these operations can be massive.

POTENTIAL SOLUTIONS

Transition to Greener Consensus Mechanisms: Shift from energy-intensive proof of work to more sustainable mechanisms like proof of stake, potentially reducing energy consumption by over 99%.

Use of Renewable Energy Sources: Encourage mining operations to relocate to areas with abundant renewable energy sources, such as geothermal or hydroelectric power.

Select challenges in the mass adoption of blockchain technologies (2/2)

INTEROPERABILITY

Most blockchain networks operate in isolation, unable to communicate or share data effectively with one another. This limitation hinders the widespread adoption and utility of blockchain technology, especially in sectors like finance, which could greatly benefit from enhanced interoperability for data exchange and transaction processing across different blockchain platforms.

POTENTIAL SOLUTIONS

Use of Bridges: Employ blockchain bridges that connect two incompatible blockchains, allowing for the transfer of data and assets. These bridges can be either trust-based or trustless.

Adoption of Interoperability Standards: Establish and adopt industry-wide standards that define how blockchains interact. This would ensure that different technologies can communicate with each other without the need for custom solutions.

SECURITY AND PRIVACY RISKS

Blockchain's decentralized architecture inherently complicates compliance with data privacy regulations like GDPR and CCPA. The identification of data controllers and processors becomes ambiguous because multiple nodes across different jurisdictions participate in data processing without a central oversight. Despite the use of public-private key encryption that offers anonymity, data analysis can de-anonymize these keys and link them back to individuals. Lastly, blockchain's immutability directly conflicts with legal mandates such as the GDPR's right to erasure, where modification or deletion of personal data should be possible.

POTENTIAL SOLUTIONS

Mutable Append-Only Structures: Innovate blockchain designs to incorporate mutable structures where data can be redacted or anonymized retrospectively without altering the integrity of the ledger.

Regulatory Sandboxes: Engage with regulators to create blockchain-specific regulatory sandboxes that allow for real-world experimentation of blockchain applications under regulatory oversight.

05

Blockchain technology common legal and regulatory considerations

Blockchain technology common legal and regulatory issues (1/2)

Blockchain technology presents a novel paradigm for data management and transactions, challenging traditional legal frameworks and regulatory environments. As blockchain continues to evolve and integrate into various sectors, it encounters a complex set of legal and regulatory issues. These challenges stem from blockchain's decentralized nature, which does not easily fit into the conventional categories recognized by current laws and regulations. While some governments are spearheading the adoption of blockchain, many national and regional regulators are adopting a wait-and-see approach. They prefer to explore and understand blockchain's implications before moving forward with additional legal and regulatory requirements or guidance. The lack of regulatory certainty and evolving legal and regulatory position is challenging for market participants, and it is necessary that they continually assess their participation in blockchain networks. The following are some of the most common compliance-related issues that arise with the use of blockchain technology. However, these issues vary depending on the specific use case, jurisdiction, and industry-specific rules and regulations.

JURISDICTION

Blockchain can operate across borders, making it subject to multiple, sometimes contradictory or overlapping, laws in various jurisdictions. Due to the decentralized nature, determining the applicable regulatory framework for any part of a blockchain operation can be complex. This may require alignment with multiple international laws and regulations.

TECHNOLOGY NEUTRAL REGULATORY REGIME

Regulatory licensing and compliance regimes are typically not drafted with the intention of regulating specific technologies. Rather, the usual intent is to regulate the activities that the technology helps facilitate. However, neutral drafting can make it difficult to interpret how regulation should apply, and which participants should be included. It is, therefore, necessary to carefully assess the nature and activities of a blockchain network and its participants to determine their appropriate place within the regulatory landscape.

GOVERNANCE AND LEGAL DOCUMENTATION

The utility-like nature of a blockchain platform means that it is necessary to properly document the relationship between the blockchain network, the network operator (if any), and its participants through legally enforceable contracts. It is important to establish a clear and robust governance model concerning interactions among participants in the network.

Blockchain technology common legal and regulatory issues (2/2)

The model should also set out clearly the applicable terms and conditions to the blockchain platform, e.g. the mechanisms by which the network operator may implement changes to the network or the requirements around its participation. Objective and fair criteria should be set to govern access to the network and suspension or termination of participants from the network.

LIABILITY

Blockchain technology introduces new types of risks such as data breaches, system failures, or malfunctions; all of these require a clear definition of liability. Understanding and preparing for such liabilities is crucial for all participants. Therefore, the allocation and attribution of risk and liability related to the blockchain network and its transactions must be carefully assessed. This includes any errors, failures, or malfunctions, which must be clearly documented at each layer of network participation.

PERSONAL DATA PRIVACY

One of the key unique selling points of a blockchain system is that once data is stored, it cannot be altered easily, if at all. This immutability clearly has implications for data privacy, particularly when the data involved includes personal information or metadata sufficient to reveal an individual's personal details. Data protection regulation may require that personal data be kept up-to-date and accurate or deleted at the discretion of the individual. However, the immutability of a blockchain system may not be consistent with such requirements.

SMART CONTRACTS

Smart contracts aren't always or necessarily legal contracts in the traditional sense, despite the word 'contract'. Whether smart contracts are considered to be legal contracts is a question of whether the elements of a legal contract are present. In essence, smart contracts are self-executable computer codes and as a result, their use may present enforceability questions when analyzed within the traditional "legal contract" definition. However, some smart contracts themselves are being structured as legal contracts and therefore have the full force of law. In such cases, it will be necessary to understand how they meet the pre-conditions for contract formation in different jurisdictions, as well as how they will be construed and interpreted by a court or arbitral body in the event of a dispute.

Jurisdictional issues when using blockchain technology (1/2)

While there are international regulations which seek to address conflicts of laws, such as the European Union's Rome I and Rome II Regulations and the United Nations Convention on the Use of Electronic Communications in International Contracts, interpretation of these texts for cross-border projects can be complex. In addition, regulatory regimes can be even less harmonized and different regulators take very different views on the territorial applicability of their local regulators in relation to cross-border business.

KEY JURISDICTIONAL QUESTIONS WHEN ESTABLISHING A BLOCKCHAIN NETWORK

- The legal structure of the blockchain network such as a legal entity, company or partnership.
- The number of network operators, ownership and control of the network as well the participants in the network.

LEGAL DOCUMENTATION

Clear legal documentation on all aspects of the blockchain network, e.g. the legal structure, liability and governance, is essential for clarity. Furthermore, it is important to ensure that the following is considered and covered within the scope of any blockchain network's legal documentation. Here are some of the key requirements when evaluating the legal documentation:

1. Legally enforceable rulebook / terms of use for blockchain participants, including review of the civil law sanctions.
2. Key contracts for each participant to sign with a network operator and/or network owners, including key terms and conditions.
3. Key rights and obligations of participants and governance model of each set of rights and the structure thereof.
4. Antitrust considerations, ownership/licensing and/or other intellectual property rights.
5. Exit and termination rights structuring including ownership of data, confidentiality of its members along with key provisions.

For a decentralized environment, it may be difficult to identify the appropriate set of jurisdictional requirements that apply to a given blockchain platform. As nodes on a decentralized platform can be located anywhere in the world, networks often cross jurisdictional boundaries. At the simplest level, every transaction could potentially fall under the jurisdiction(s) of the location of each and every node in the network. This could result in the blockchain needing to be compliant with an unwieldy number of legal and regulatory regimes.

Jurisdictional issues when using blockchain technology (2/2)

ANTITRUST LAW VIOLATION

There may be antitrust risks arising from blockchain collaboration models (e.g. consortium) being viewed as:

- Disfavoring competitors, such as by excluding them, offering discounts to select partners, or punishing competitors using alternative private currencies.
- Abuse of dominance such as pulling a significant share of the market into a closed ecosystem, causing disadvantage to competitors and consumers.
- Collusive conduct such as fixing or manipulating prices to gain competitive advantage.
- Entering into collusion amongst significant members within a blockchain consortium, leading to manipulation of services offered to smaller entities and preferential confirmation of transactions etc.

ANTI-MONEY LAUNDERING, KYC, AND SANCTIONS

Blockchain network participants, particularly network operators, should consider the following risks and put in place appropriate systems and controls to mitigate them:

- Non-compliance with applicable AML/KYC regulations or sanctions requirements.
- Anonymity of transactions and identities on the blockchain.
- Lack of rigor in conducting “Know your supplier” checks.
- Payment to/from parties or countries on the sanctions list or with “politically exposed person” status.
- Deploying distributed applications that accept or transmit value without necessary controls and compliance programs.
- Lack of surveillance and monitoring activities to detect and prevent inappropriate activities; or perform trend analysis of patterns.
- Determining who should bear overall responsibility for AML/KYC functions.

TAX CONSIDERATIONS

The blockchain network may be subject to taxation in many jurisdictions.

Thoughtful analysis should be undertaken to make sure that the network understands where it is subject to taxes or other informational reporting.

Select intellectual property considerations for blockchain networks

INTELLECTUAL PROPERTY CONSIDERATIONS

IP considerations in a blockchain network will depend on the nature of the specific blockchain in question, including its purposes, the relationship between the blockchain participants, the underlying software (e.g. open-source) and whether the underlying IP is intended to be commercialised. The importance of protecting IP comes as an extension of addressing trade secrets, confidential information and other proprietary rights potentially contained in the data shared on or linked to a blockchain. The following are core legal concerns and questions for blockchain network participants considerations and questions around IP in blockchains:

Each type of IP (e.g. patents, trademarks, copyrights, trade secrets) has its own ownership rules (e.g. the work for hire doctrine in copy right which applies to certain jurisdictions). Parties will need to consider each type of IP right that would be created in respect of a supply-chain blockchain network. IP rights vary in each jurisdiction. Therefore, jurisdictional details need to be considered together with the governing law of the blockchain agreement.

Depending on the structure of the blockchain, the IP in the blockchain can be the property of one or various parties (e.g. joint ownership, through this is not always straightforward and should be carefully considered within the context of the specific blockchain in question). For example, IP in the blockchain could be owned by the company behind the platform (or its shareholder/investor), the developer, the founding consortium members, the node operator, or the participants who contribute know-how and data in order to develop the platform. This assessment may become more complex when using open-source software built by communities of developers.

Developers and IP owners will have to determine their IP strategy, including who owns what, and protection on all levels. Vendors will likely want to capitalise on any other commercial benefits to be generated from the blockchain, including commercialisation of the underlying dataset by way of licensing-out the underlying IP. Especially in public blockchains based on open-source software, this can be challenging, but creating mechanisms to identify who created and who owns what (e.g. time-stamps) should be considered. In addition to considerations on the ownership of the IP in the underlying blockchain, another important question relates to whether the blockchain can be used to record ownership, use and remuneration of IP licensing/transactions.

08

Blockchain technologies select industry use cases and key benefits

Blockchain technologies select industry use cases and key benefits

BANKING AND FINANCIAL SERVICES	Blockchain Technologies Solution	Benefits
KYC Compliance: Traditional KYC processes are cumbersome, often taking 30-50 days to complete. The repetitive efforts involved are subject to high compliance costs and substantial penalties for noncompliance, thus resulting in increased operational risk and inefficiencies.	The solution leverages cryptographic security to reduce manual verification and ensures the integrity and confidentiality of the data. By employing distributed ledger technology, the blockchain-based KYC registry and automation system enable real-time, automated updates and synchronization of KYC data across all banks. With the help of smart contracts, transactions are executed only when all KYC and AML requirements are met.	Reduced KYC costs and duration, enhanced fraud detection, streamlined compliance across banks, secure record keeping
International Trade: International trade involves complex, lengthy, and costly negotiations with significant risks. Traditional banking systems that facilitate these trade deals are outdated, making trade finance inaccessible for many companies, with nearly 70% lacking access to trade finance services.	The solution involves a platform built on the Hyperledger Fabric framework, which employs distributed ledger technology to streamline the international trade process. This platform provides synchronized and real-time transaction data accessible to all network participants, with smart contracts automatically executing transactions based on predefined conditions.	Enhanced trade finance access, automated and secure transaction verification, accelerated transaction speed, minimized counterparty risk

Blockchain technologies select industry use cases and key benefits

BANKING AND FINANCIAL SERVICES	Blockchain Technologies Solution	Benefits
Microfinance: Traditional financing methods are inadequate for small food retailers in developing countries, leading to challenges in accessing microloans. High costs, slow transaction times, and a lack of transparency can impede the growth of small-scale vendors and farmers.	The blockchain platform automates the entire loan process from initial application to fund disbursement and repayment. It leverages machine learning to analyze purchasing data and predict creditworthiness, enabling lenders to confidently extend microloans.	Enhanced microloan access, automated loan processing, secure and transparent record-keeping, real time credit assessment
Transforming Energy Trading: Trading commodities like natural gas and electricity through numerous intermediaries leads to delayed transactions and increased costs. Existing systems struggle with inefficiencies from redundant back-office processes like confirmations and reconciliations. Moreover, the current market structures also face credit risks due to slow settlement times and high collateral requirements.	Blockchain revolutionizes energy trading by automating and streamlining all phases of the transaction process. Smart contracts enable real-time, automated trade confirmations and physical settlement, which reduces human intervention and error. Blockchain has the potential to transform the trading of all commodities by enabling equivalence and interoperability across different asset classes.	Automated transaction process, reduced credit and operational risk, cross commodity trading flexibility

Blockchain technologies select industry use cases and key benefits

CONSUMER AND SUPPLY CHAIN	Blockchain Technologies Solution	Benefits
Consumer Goods Transparency: There is increasing demand from consumers for product origins and quality. The concerns about food safety and ethical standards drive the need for clear and verifiable information. This transparency challenge requires companies to offer more precise and trustworthy data to meet consumer expectations.	The solution involves utilizing blockchain to track the journey of consumer goods from production to retail. This technology provides a transparent, immutable ledger where data such as harvest date, processing, packaging, and shipping details are securely recorded. Each product item is assigned a unique digital identity that is accessible via QR codes, allowing consumers to verify the product's source and handling history using their mobile devices.	Increased consumer trust, improved sales of verified products, reduced risk of counterfeit goods, targeted marketing opportunities
Combating Conflict Minerals: The global trade in high-value goods such as diamonds, cobalt, and lithium faces persistent ethical and sustainability challenges. Conflict minerals are often extracted under dire human rights conditions, fueling violence in vulnerable regions. Additionally, environmental concerns arise from unsustainable mining practices that harm ecosystems.	Utilizing blockchain technology, an immutable digital ledger provides a solution for tracing the lifecycle of high-value goods from extraction to sale. Features such as high-definition photographs, unique serial numbers, and comprehensive details like the item's origin, processing, and transportation data are logged. The incorporation of smart contracts automates compliance processes to ensure the transactions only proceed if all predefined ethical and ESG criteria are met.	Verified ethical practices, regulatory adherence, improved sustainability tracking, transparency drives customer loyalty

Blockchain technologies select industry use cases and key benefits

CONSUMER AND SUPPLY CHAIN	Blockchain Technologies Solution	Benefits
Cold Chain Integrity in Pharmaceuticals: Blockchain helps ensure the integrity of temperature-sensitive pharmaceuticals during transport. Traditional methods often fail, resulting in significant product loss due to temperature excursions. Blockchain, combined with IoT technology, offers a more reliable solution for monitoring and maintaining the necessary conditions throughout the supply chain.	Blockchain technology is paired with IoT sensors to track critical parameters such as temperature, humidity, and location throughout the shipping process, enabling precise control over the conditions essential for the safe transport of temperature-sensitive pharmaceuticals.	Enhanced product safety, reduced financial loss, streamlined logistics operations
Sustainable Supply Chain Verification: Businesses today are under increasing pressure to prove their sustainability claims due to growing consumer awareness and stricter regulations. Verifying the sustainability of long and complex supply chains is particularly challenging for entities towards the end of the chain.	Blockchain, combined with digital tokens, is used to trace and verify the origin and sustainable credentials of raw materials like palm oil. By creating a digital twin of the physical product, which records every detail from growth conditions to processing and shipment, blockchain ensures that all sustainability data remains immutable and transparent.	Improved sustainability reporting, enhanced supply chain transparency

Blockchain technologies select industry use cases and key benefits

INTELLECTUAL PROPERTY MANAGEMENT	Blockchain Technologies Solution	Benefits
Asset Registry for Real Estate: Tracking real estate transactions is complex and fraught with potential for fraud. Properties must be registered when bought, sold, inherited, or mortgaged. Traditionally, these records are maintained in centralized systems, which can be difficult and costly to update and verify.	Blockchain can create a decentralized and tamper-proof registry for real estate. Each property can be tagged with a unique digital identifier on the blockchain, where all transaction histories, including sales, transfers, and inheritances, are immutable and easily verifiable.	Enhanced accessibility of property records, streamlined property transactions, reduced risk of property fraud
Royalty Payment in the Music Industry: The music industry struggles with ensuring fair compensation as digital consumption grows. Traditional systems lack transparency and efficiency, leading to significant losses for artists due to mismanagement and piracy.	Blockchain enables the storage of cryptographic hashes of digital music files, associating them with the creators' identities. Smart contracts on the blockchain can automatically enforce royalty payments as per the terms agreed upon by all parties involved, directly from consumer to artist.	Fair compensation assurance, reduced administrative cost, enhanced transparency in licensing, support for innovative revenue model

Blockchain technologies select industry use cases and key benefits

HEALTHCARE	Blockchain Technologies Solution	Benefits
Fragmentation and Inefficiency in Data Management: In the healthcare sector, managing and exchanging patient information is often hindered by disjointed record-keeping systems, which leads to incomplete or conflicting medical records and patient consent forms. This not only compromises the quality of patient care but also poses significant challenges in maintaining the confidentiality and integrity of health data.	Patient Consent and Health Data Exchange: Utilize blockchain to maintain comprehensive, longitudinal health records, ensuring patient control over their data through verifiable consent mechanisms. Clinical Trial Management: Integrate blockchain with electronic data capture systems to automatically aggregate, replicate, and distribute clinical data among researchers and practitioners. Outcome-Based Contracts: Implement blockchain-backed contracts that associate clinical outcomes with healthcare costs.	Comprehensive health records, streamlined clinical trials, personalized patient care, transparent cost management, reliable medical supply chains
Drug Traceability and Integrity: The pharmaceutical industry, particularly in the distribution of temperature-controlled drugs such as vaccines, confronts several inefficiencies that jeopardize drug efficacy and patient safety. These include inventory losses due to mismanagement, lengthy investigations to determine root causes, and logistical redundancies.	Blockchain platform provides a unified system for traceability. This platform records each transaction or handling event across the distribution journey on a ledger, which offers an immutable audit trail of environmental conditions and handling processes.	Enhanced drug safety monitoring, comprehensive audit trails, increased supply chain integrity

References and report citations

The investment white paper report has been prepared using internal analysis as well as information sourced from various sources. Here are some of the links for the report references and citations that were used as part of the preparation of the research report:

i. https://stayrelevant.globant.com/en/insights/sentinel-report/globant-sentinel-report-blockchain/

ii. https://www.cbinsights.com/research/report/blockchain-trends-2022/

iii. https://www.ibm.com/topics/blockchain

iv. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf

v. https://widgets.weforum.org/blockchain-toolkit/legal-and-regulatory-compliance/index.html

vi. https://www.ark-invest.com/big-ideas-2024

vii. https://www.cbinsights.com/research/report/blockchain-technology-companies/

viii. https://www.mckinsey.com/industries/financial-services/our-insights/web3-beyond-the-hype

ix. https://aws.amazon.com/what-is/blockchain/?nc1=h_ls&aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc

x. https://geekflare.com/blockchain-business-model/

xi. https://www.grayscale.com/research/reports/the-state-of-ethereum

xii. https://etc-group.com/blog/special-reports/the-investment-case-for-ethereum/

i. https://www3.weforum.org/docs/WEF_Building_Value_with_Blockchain.pdf

ii. https://ethereum.org/en/whitepaper/

iii. https://ethereum.org/en/roadmap/

iv. https://polygon.technology/papers/pol-whitepaper

v. https://cointelegraph.com/learn/polygon-blockchain-explained-a-beginners-guide-to-matic

vi. https://www.kraken.com/learn/what-is-polygon-matic

vii. https://4pillars.io/en/articles/complete-guide-to-polygon-tech--business-insights/public

viii. https://coincodecap.com/polygon-tokenomics-the-beginning-of-matic-explained#:~:text=Polygon%20(MATIC)%20is%20a%20layer,of%20DeFi%20tools%20and%20applications

ix. https://polygon.technology/blog/polygon-2-0-protocol-vision-and-architecture

x. https://solana.com/docs

xi. https://solana.com/solana-whitepaper.pdf

xii. https://kriptomat.io/cryptocurrency-prices/solana-sol-price/what-is/

xiii. https://figment.io/insights/solana-tech-stack-overview/

xiv. https://www.ibm.com/blockchain/use-cases/

Global Millennial Capital Investment Research Team

Andreea Danila

GENERAL PARTNER

Henry Sun

INVESTMENT ANALYST (INTERN)

Disclaimer:
This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice. The statements and data contained herein may contain certain forward-looking statements relating to the beliefs of the Global Millennial Capital Ltd. investment research team. These forward-looking statements are, by their nature, subject to significant risks and uncertainties. The opinions expressed are in good faith and while every care has been taken in preparing these documents, Global Millennial Capital Limited makes no representations and gives no warranties of whatever nature in respect of these documents.