



Blockchain and
Artificial Intelligence
The new payments
paradigm

May 2025

Contents

Introduction	2
The future of AI, blockchain, and Web3	4
Use cases	6
Landscape and impact	10
Conclusion	13
Endnotes	13
Contacts	14
About Blockchain & Digital Assets at Deloitte	15

Introduction

The payments sector is on the cusp of a transformative shift, driven by the convergence of blockchain technology and artificial intelligence (AI).

These powerful technologies are poised to improve payment processing, boost security, and even enhance customer experiences. However, along with these advancements come several risks and challenges that must be carefully managed to ensure secure and compliant operations.

Let's begin with AI, which is making significant strides in the payments industry. The ability of advanced AI algorithms to analyze transaction patterns in real time

enables the early detection and prevention of fraudulent activities, which may not only help to reduce the risk of fraud, but also enhance the security of transactions. Despite these capabilities, the technology itself can be exploited. For example, cybercriminals may use sophisticated AI algorithms to mimic legitimate transactions, making it challenging to distinguish between genuine and fraudulent activities. And, while AI's dependence on customer data could raise concerns regarding data privacy and

the potential misuse of information, its ability to leverage behavioral data allows for the creation of highly personalized user experiences. By analyzing spending patterns and trends, AI can forecast behaviors and offer tailored services, thereby enhancing customer satisfaction and loyalty.

Blockchain is also proving to be an important mechanism for achieving data integrity, traceability, and the security of AI systems. Blockchain offers programmatic



controls via smart contracts—self-executing agreements with conditional terms (e.g., confirmation of delivery of shipment, interest, or dividend payable dates) that trigger actions directly written into code. This inherent transparency, autonomous control operation, and efficiency eliminates the need for intermediaries, thereby increasing trust in how AI systems operate and reducing transaction costs. Moreover, the ability of smart contracts to autonomously automate and enforce agreements will become increasingly important as AI platforms develop greater agentic capability. This capability will require controls to limit and constrain the behavior of those agents, and smart contracts represent an effective method to implement such control.

Picture it. A world where gig workers receive their payments instantly through a blockchain and AI-powered platform. Smart contracts automatically verify completed tasks and release payments in real time using digital currencies or stablecoins, all while AI algorithms monitor the platform for signs and patterns of fraudulent gigs, creating a secure payment environment. Yes, the potential for AI systems to act autonomously does raise concerns about rogue AI. However, proper controls can help prevent AI agents from executing unauthorized transactions or making decisions that deviate from organizational policies and regulatory requirements.

By offering efficient, secure, cost-effective solutions, blockchain and AI could also revolutionize the cross-border payments market. Real-time transfers of digital currencies or stablecoins promise quick, low-cost transactions, while AI-powered compliance can enable adherence to regulations. Of course, preventing unsanctioned access and unauthorized transactions on blockchain platforms is crucial, but strengthening access control mechanisms can help uphold the integrity and security of the system and foster greater trust and confidence in blockchain and AI.

The integration of blockchain and AI technologies promises to bring transformative changes to the payments landscape. Despite their risks and challenges, these technologies promise to revolutionize payments by creating a safer, efficient, and user-friendly financial ecosystem.

The future of AI, blockchain, and Web3

The rise of blockchain, AI, and Web3 marks a fundamental shift toward a decentralized digital landscape that offers enhanced user control over data and digital assets.

Unlike the current Web2 paradigm, where intermediaries dominate, Web3 envisions a more equitable digital landscape where consumers own their own digital wallets, enabling them to interact directly with financial institutions and other service providers without relying on intermediaries. By eliminating intermediaries, transaction costs can be reduced, and the speed of financial interactions can be significantly increased, providing a more efficient, more transparent, and more secure transaction experience.

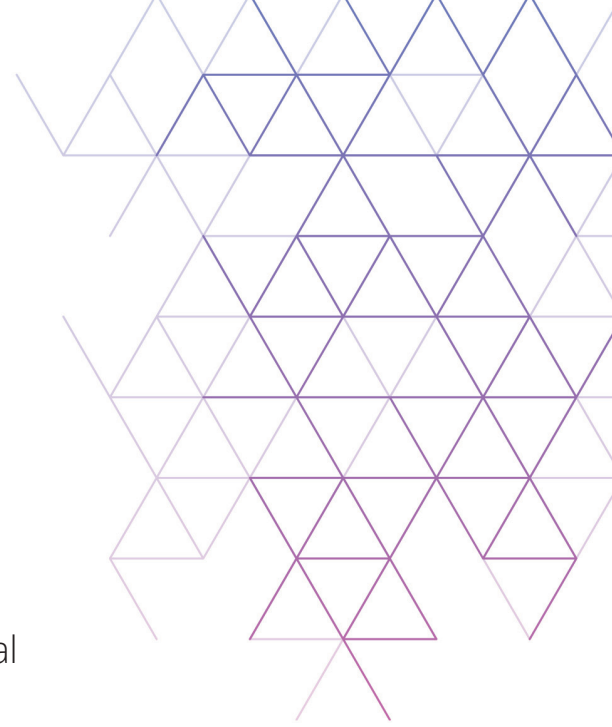
AI models that can independently make decisions and learn over time have the potential to revolutionize digital payments by dramatically enhancing efficiency and delivering highly personalized services. By leveraging AI, Web3 platforms can offer more intelligent and responsive interactions, improving user experiences and operational efficiencies on decentralized applications. The synergy between AI and Web3 could lead to true innovations such as automated financial advising, personalized content delivery, and advanced cybersecurity measures. For example, agentic AI could analyze vast amounts of financial data in real time, providing users with tailored investment advice and risk assessments, thereby democratizing access to sophisticated financial product offerings.

As Web3 continues to evolve, ensuring privacy and security remains the paramount priority, but Zero-Knowledge Proof (ZK Proof) technology offers a promising approach to some of the inherent risks associated with decentralized systems. ZK Proofs enable one party to prove to another that a statement is true without revealing any specific information beyond the validity of the statement itself. This technology can significantly enhance privacy and security in Web3 applications, allowing users to verify transactions and identities without exposing sensitive data. By incorporating ZK Proofs, Web3 platforms can manage risks related to data breaches and unauthorized access, fostering a more secure and trustworthy digital environment. For example, in financial transactions, ZK Proofs can confirm that parties meet certain criteria (e.g., creditworthiness) without disclosing detailed financial information, thus preserving privacy while maintaining trust.

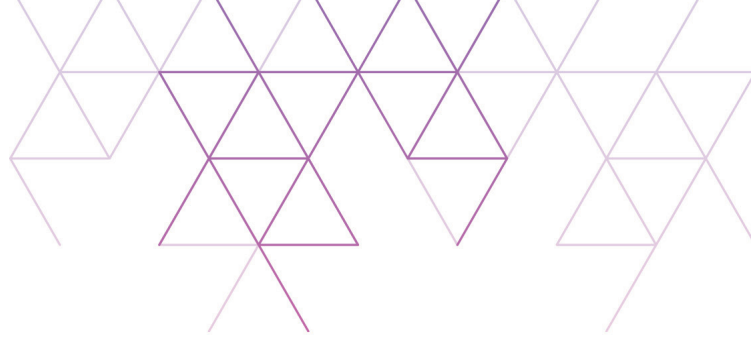
The adoption of Web3 and its associated technologies can also lead to more resilient and transparent financial systems. Decentralized finance (DeFi) platforms built on blockchain technology enable peer-to-peer financial transactions without the need for traditional banking intermediaries. This can democratize access to financial services, particularly in underserved regions where traditional banking infrastructure is lacking.

Additionally, the immutable nature of blockchain records creates transactions that are transparent and verifiable.

The convergence of Web3, agentic AI models, and privacy preserving technology is poised to transform the future of digital interactions. By empowering users with greater control over their data and digital assets, and bolstering security with advanced cryptographic techniques, these innovations have the power to create a decentralized digital ecosystem with enhanced efficiency, transparency, and highly personalized user experiences.







Use cases

AI agent for financial services

Leading cryptocurrency exchange platforms are integrating AI in various new ways to enable seamless cryptocurrency purchases and facilitate faster trades, swaps, and staking for their investors. Recently, one of the largest crypto firms launched a new product called “Based Agent.” This product allows users to create their own AI agent with access to a crypto wallet, enabling investors on a digital currency exchange to start building investment strategies based on certain parameters. These user-created AI agents can be designed to execute trades, through smart contracts, adhering to investment principles and strategies.

AI can also significantly enhance customer service in banking by providing instant, accurate responses to inquiries; automating routine tasks; and integrating with blockchain technology to help ensure the privacy and integrity of customer data. AI-powered chatbots can handle common inquiries and tasks like account balances or password resets, improving efficiency and customer satisfaction. This will free up human representatives to focus on more complex inquiries, resulting in improved quality of service and customer satisfaction.

Integrating AI with blockchain technology allows financial services firms to offer secure and structured product offerings. By analyzing historical customer data, AI algorithms can provide personalized product recommendations suitable to a client’s risk tolerance. As a result, this integration enables personalized financial products and advice, helping clients achieve their financial goals.

Modernizing payments in the gig economy

While the gig economy continues to grow exponentially, traditional payment systems often fall short in providing timely, secure, and transparent payments to gig workers. Blockchain can transform this landscape by enabling instant and transparent transactions, eliminating intermediaries, and reducing transaction costs. For example, a blockchain-based payment platform can facilitate real-time payments using digital currencies or stablecoins, with each transaction recorded transparently and immutably on the blockchain. This not only speeds up the payment process but also enhances trust between gig workers and employers by providing a verifiable record of all transactions.

AI further enhances gig economy payments by automating contract management and helping to prevent fraud. AI-powered smart contracts can automate processes based on predefined conditions, such as releasing a payment once a milestone is completed and verified. Additionally, AI algorithms can analyze transaction patterns to detect and prevent fraudulent activities, enabling an environment of trust and security.

By leveraging the combined capabilities of blockchain and AI, a seamless and secure payment platform can be developed that provides instant payments, enhanced transparency, automated processes, robust fraud prevention, and cost reduction, ultimately benefiting both gig workers and employers.

AI-enhanced fraud detection in banking

Fraud detection presents a significant challenge for banks, as traditional methods frequently fall short in identifying sophisticated schemes. But with AI, banks can analyze vast amounts of transaction data in real time, identifying patterns and anomalies indicative of fraud. As AI algorithms continuously monitor transactions on a blockchain, integrating AI with blockchain can enhance security and transparency by flagging suspicious activities and providing an audit trail. This not only helps safeguard data integrity and prevents tampering but allows for real-time fraud detection, enhanced accuracy, and reduced operational costs through automation. automated processes.

A blockchain-based payment platform can facilitate real-time payments using digital currencies or stablecoins, with each transaction recorded transparently and immutably on the blockchain

Transforming global remittances

The global remittance market is projected to reach \$913 billion in 2025,¹ while the cross-border payments volume is projected to hit \$428 billion in 2025.² This growth is crucial for developing countries and the overall traditional remittance landscape, which is often slow and costly. The integration of blockchain and AI has the potential to revolutionize this landscape by offering benefits such as cost reduction, real-time transfers, enhanced security, improved customer experience, and automated compliance. The transparency and immutability of blockchain can not only help reduce fraud risks, but a blockchain-based platform can also facilitate real-time transfers of digital currencies or stablecoins, enabling quick and cost-effective transactions.

AI further advances the remittance process through automation. AI-powered chatbots can provide 24/7 customer support, AI algorithms can detect and report fraudulent transactions, and AI can automate compliance checks, confirming transactions adhere to regional and local regulations. For example, a worker in the United States can send \$500 to their family in the Philippines using a blockchain and AI-powered platform, processing the transfer in real time with minimal fees. The recipient can then convert stablecoins to local currency or use them directly to make purchases in the local markets.

Expanding accessibility to health care payments

From insurance claims to patient billing, the life sciences and health care industry faces significant challenges in managing payments. With traditional systems often plagued by inefficiencies, delays, and high administrative costs, it's time to turn to new technologies.

By integrating blockchain and AI, health care providers can improve the financial health of both patients and providers by enhancing security and transparency, helping reduce the risk of fraud, reducing administrative overhead, and enabling timely payments.

A blockchain-based platform can facilitate direct payments from insurance companies to health care providers using programmable smart contracts that can automate the execution of payments based on predefined conditions, such as verification of services rendered. And ZK Proofs can be employed to keep patient data confidential while still allowing for the verification of claims, thus enhancing both security and compliance. Additionally, AI can improve the process by automating administrative tasks and enhancing accuracy, such as automatically verifying insurance claims, detecting fraudulent activities, and confirming compliance with regulations.

Together, these technologies can help to reduce the risk of fraud by securing sensitive information, automating complex decision-making, reducing human intervention, and enabling faster claims processing in the health care industry.



Deep dive: Enhancing the travel booking and payment process



Overview

The travel industry has experienced a remarkable resurgence post-pandemic, partly driven by a collective desire to explore and reconnect, and partly by corporations encouraging more face-to-face meetings with clients. In fact, the travel and tourism sector is projected to contribute approximately 10%³ of the global GDP in 2025, marking a return to pre-pandemic levels of travel and marking a significant five-year increase of nearly 100%.⁴ Despite the growth of travel websites, the process of booking travel remains tedious. However, by integrating AI and blockchain technology, the entire booking process could fundamentally change.

Typically, travelers go through a cumbersome, stressful process of allocating specific budgets for flights, hotels, and activities, utilizing various payment methods such as real-time payments, Automated Clearing House (ACH) transfers, wire transfers, or credit cards. But, by leveraging the capabilities of large language models (LLMs), which are pre-trained on extensive data sets and outperform traditional search engines, these AI models can make travel booking simpler, efficient, and more user-friendly.

The impact of blockchain and AI on travel payments

AI agents have the capability to autonomously perform tasks assigned by humans. For example, a user could instruct

their personal AI agent to book a flight and hotel in Spain for five nights with a budget of \$3,000. To accomplish this, the AI agent would need secure access to the user's funds, which is where Web3 and blockchain technology come in.

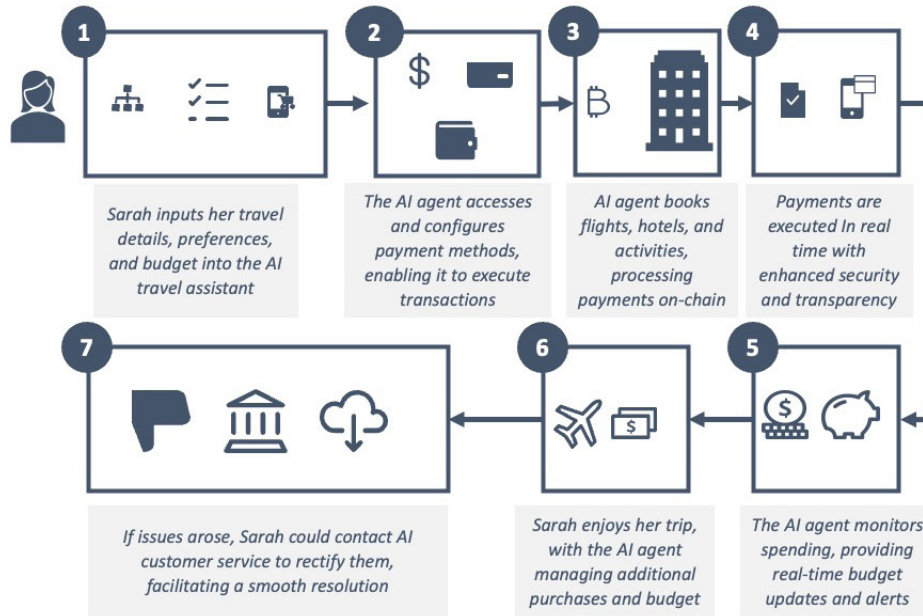
In this new and improved booking experience, a user would deposit stablecoins/cryptocurrency into an embedded wallet or link their existing digital wallet to the booking platform. From there, AI agents can spend the user's stablecoins/cryptocurrency to book travel on their behalf by leveraging a Web3 client layer for seamless on-chain transactions. Then, to maintain security and privacy protocols throughout both on-chain and off-chain processes, the transaction must be approved by the user before execution.

On-chain smart contracts prevent AI agents from exceeding predetermined budgets and avoid double bookings by alerting AI to limit spending, helping users stay within their financial limits and avoid booking conflicts. Additionally, AI can leverage data to optimize travel bookings to find the best deals and rates and provide a more personalized travel experience. And, since blockchain creates an immutable audit trail, verifiable evidence for receipts and reimbursements can be provided, even when a trip is canceled, thereby increasing confidence and accountability in the booking process.

Figure 1: Detailed User Journey in a Travel Use Case

AI travel booking: Sample payment overview

This life cycle illustrates a user, Sarah, using an AI travel assistant to book, manage, budget, and plan her vacation. The AI agent manages the details of the trip and connects her payment through a blockchain payment provider.



USER FLOW EXPLAINED

- 1** Sarah visits the OpenAI marketplace, selects an AI travel agent, and completes the purchase using her preferred payment method. The AI agent is linked to her Web3 identity, making all interactions and transactions transparent and verifiable on the blockchain.
- 2** Sarah opens the AI agent's settings and links her digital wallet. Smart contracts are created to manage these payment methods, enabling secure and automated transactions. The AI agent verifies the payment methods.
- 3** Sarah inputs her travel details, including dates, destination, and budget, into the AI agent's interface. The AI agent presents Sarah with a personalized travel plan that fits her preferences and budget.
- 4** Sarah reviews and approves the travel plan presented by the AI agent. The AI agent executes the bookings, making payments through blockchain-enabled transactions. Sarah receives real-time notifications of each booking and payment confirmation.
- 5** While traveling, Sarah uses the AI agent to make additional purchases, such as buying merchandise or booking leisure activities. Sarah receives real-time updates on her spending and remaining budget.
- 6** If Sarah approaches or exceeds her budget limit, the AI agent notifies her and restricts further spending. All budget management activities are tracked on a decentralized ledger, enabling transparency and accountability.
- 7** Sarah arrives at her hotel and discovers an issue with her booking, such as a duplicate reservation. She contacts customer service, which accesses the blockchain records to verify booking details and quickly rectify the mistake.

AI regulations

AI systems present unique regulatory challenges that require a comprehensive and nuanced approach. One primary consideration is data privacy and security, governed by stringent regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These laws set standards for the collection, storage, and processing of personal data to safeguard individual privacy within AI systems. Ensuring data anonymization and implementing robust security measures are crucial elements of these regulatory requirements and help protect against data breaches and unauthorized access.

The ethical use of AI, along with bias mitigation, is also a critical regulatory consideration. Transparency and accountability are essential to building trust in AI systems, with regulations potentially requiring AI systems to provide clear, understandable explanations of their decisions to help ensure that AI operates fairly and does not perpetuate biases present in the training data, ultimately helping promote fairness and prevent discrimination.

Furthermore, clear accountability guidelines and liability frameworks are essential to address the outcomes of AI-driven decisions, particularly in critical sectors such as health care and finance. Interoperability and compliance between AI and blockchain systems is crucial, as these systems must work seamlessly together while adhering to relevant regulations.

Landscape and impact

AI and blockchain technologies promise to streamline payments operations, enhance security, and offer personalized customer experiences. However, they also present new risks and regulatory challenges that must be navigated carefully to enable secure and compliant operations.

Risks

Fraud risks

According to the Federal Trade Commission (FTC), fraud has been on the rise in recent years: “People reported losing \$10 billion to scams in 2023, \$1 billion more than 2022, and the highest ever in losses reported to the FTC.”⁵ Despite AI’s capabilities in detecting and preventing fraud, the technology can be exploited by cybercriminals who use sophisticated AI algorithms to mimic legitimate transactions, making it challenging to distinguish between genuine and fraudulent activities. Blockchain’s transparency can also be a double-edged sword as it may expose transaction patterns that could be exploited by malicious actors.

Identity risks

Identity theft cost Americans more than \$189 billion in 2022.⁶ Blockchain’s reliance on cryptographic keys for identity verification can lead to significant risks if these keys are lost or stolen. Similarly, AI systems that use biometric data for identity verification must ensure that this data is securely stored and processed to prevent identity theft.

Rogue AI risks

The potential for AI systems to act autonomously raises genuine concerns about rogue AI. If not properly controlled, AI agents could execute unauthorized

transactions or make decisions that deviate from organizational policies and regulatory requirements. Weaknesses in access control mechanisms, as well as risks surrounding the misuse of AI or the amplification of existing inherent biases, could compromise the integrity and security of the payments system.

Systemic risks

AI systems, especially those integrated with blockchain technology, have the potential to become deeply embedded within the financial infrastructure. This integration can lead to systemic risks where a failure or malfunction in one AI system can have cascading effects throughout the entire financial system. For instance, an AI algorithm responsible for transaction processing might inadvertently introduce errors or biases that propagate through the blockchain, affecting numerous transactions and stakeholders. Such systemic risks can undermine the stability of the financial system, leading to widespread disruptions and loss of trust among users.

Customer privacy and data risks

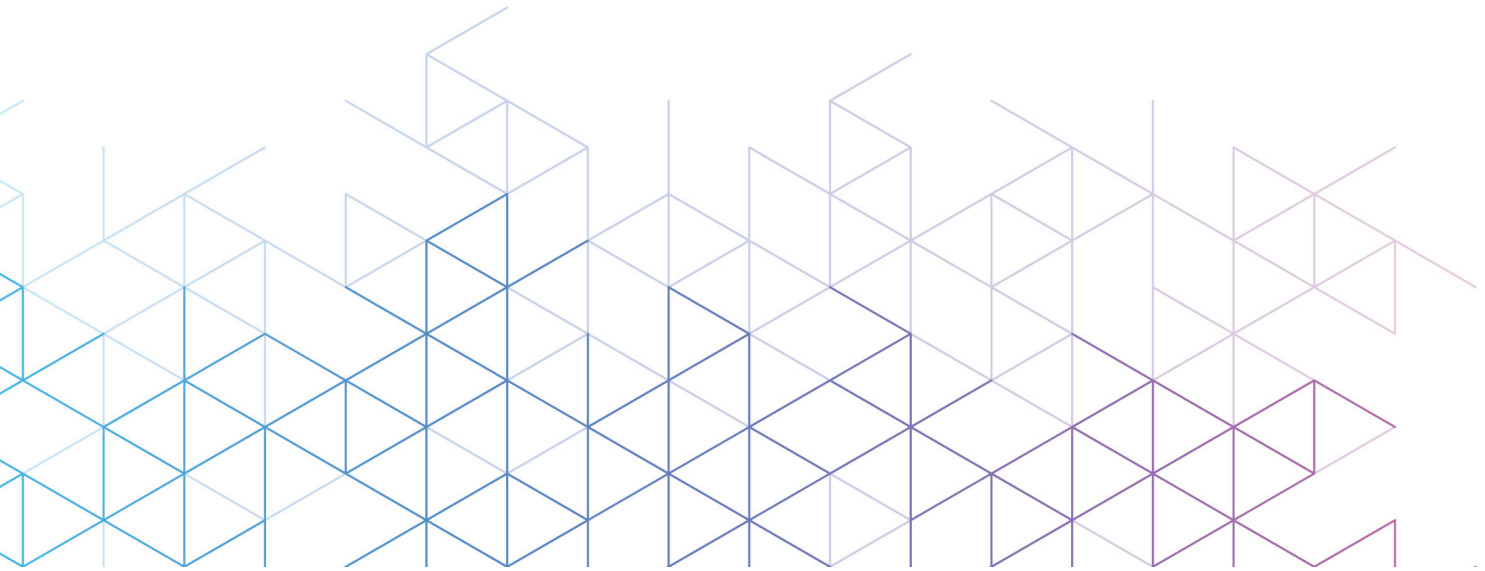
AI payments systems often rely on vast amounts of customer data to function effectively, which can present significant privacy and data security risks. For example, rogue AI could potentially misuse or mishandle sensitive customer information, leading to data breaches or unauthorized

access. Additionally, AI algorithms could inadvertently expose personal data through predictive analytics or data aggregation, compromising customer privacy. Implementing robust data protection measures and complying with privacy regulations is crucial to addressing these risks and maintaining customer trust.

Autonomous decision-making risks

An autonomous AI payments system can occasionally exhibit unpredictable behavior. For example, it might execute transactions or enforce policies that are not aligned with regulatory requirements or organizational goals or that deviate from predefined parameters by prioritizing efficiency over compliance. This unpredictability highlights the need for robust monitoring and control mechanisms to confirm adherence to policies and regulations. Integrating human oversight, by confirming that agentic AI performs as intended, can help manage risks, prevent significant financial losses, avert legal repercussions, and protect against reputational damage.





Regulatory landscape

AI regulations

Regulatory bodies are increasingly focused on the ethical use of AI, emphasizing transparency, accountability, and fairness. The European Union's GDPR and the proposed Artificial Intelligence Act set stringent requirements for AI systems including data protection, risk management, and human oversight. In the United States, the FTC has issued guidelines on the use of AI, emphasizing the need for transparency and fairness in AI-driven decision-making processes.

Blockchain regulations

Blockchain technology is subject to various regulatory frameworks, depending on its application. For instance, the Financial Action Task Force (FATF) has issued guidelines on the use of blockchain for anti-money laundering (AML) and counter-terrorist financing (CTF) purposes. In the United States, the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) regulate blockchain-based financial instruments and digital assets. Additionally, the Office of the Comptroller of the Currency (OCC) has provided guidance on the use of blockchain in banking.

Products and services regulations

The regulatory landscape also dictates the types of products and services that can be offered using AI and blockchain. For example, AI-driven robo-advisors must comply with investment advisory regulations, while blockchain-based payment platforms must adhere to AML and CTF requirements. To avoid legal and financial repercussions, organizations must ensure their AI and blockchain solutions are designed and implemented in compliance with relevant regulatory requirements.

Potential benefits

Enhanced security

AI's advanced algorithms can detect and prevent fraudulent activities in real time, while blockchain's immutable ledger helps to ensure the integrity and security of transactions. Together, these technologies can help provide a robust defense against cyberthreats and fraud.

Operational efficiency

AI-driven automation can streamline various aspects of payment processing, from identity verification to compliance checks, reducing operational costs and improving efficiency. Blockchain's ability to eliminate intermediaries further enhances efficiency by reducing transaction times and costs.

Personalized customer experiences

AI's ability to analyze vast amounts of data enables organizations to offer personalized financial services, tailored travel recommendations, and customized investment advice to enhance customer satisfaction and loyalty.

Transparency and trust

Blockchain's transparent ledger fosters trust among stakeholders by providing a clear and immutable record of transactions. This is particularly beneficial in capital markets where transparency is crucial for maintaining investor confidence.

Innovation and new business models

The integration of AI and blockchain opens up new opportunities for innovation and the development of novel business models. For instance, AI-driven chatbots and virtual assistants enhance customer support and engagement. And, thanks to the programmable nature of stablecoins and tokenized money, these can be utilized by future AI agents to execute smart contracts and complete transactions.

Risk management

Fraud

Despite AI's capabilities in detecting and preventing fraud, cybercriminals may use sophisticated AI algorithms to mimic legitimate transactions. Blockchain's transparency can also expose transaction patterns. ZK Proofs can verify transactions without revealing sensitive information allowing legitimate transactions to be processed while maintaining privacy. Programmable smart contracts enforce stringent rules and multi-signature requirements, adding additional layers of security.

Identity

Blockchain's reliance on cryptographic keys and AI's use of biometric data for identity

verification can lead to significant risks if compromised. ZK Proofs enable identity verification and authorization access without exposing personal information or revealing a user's actual cryptographic key or biometric data, providing security even if keys or biometric data are compromised. Additionally, Web3 solutions can improve security by spreading identity verification across multiple nodes, making it less likely for a single failure to cause problems.

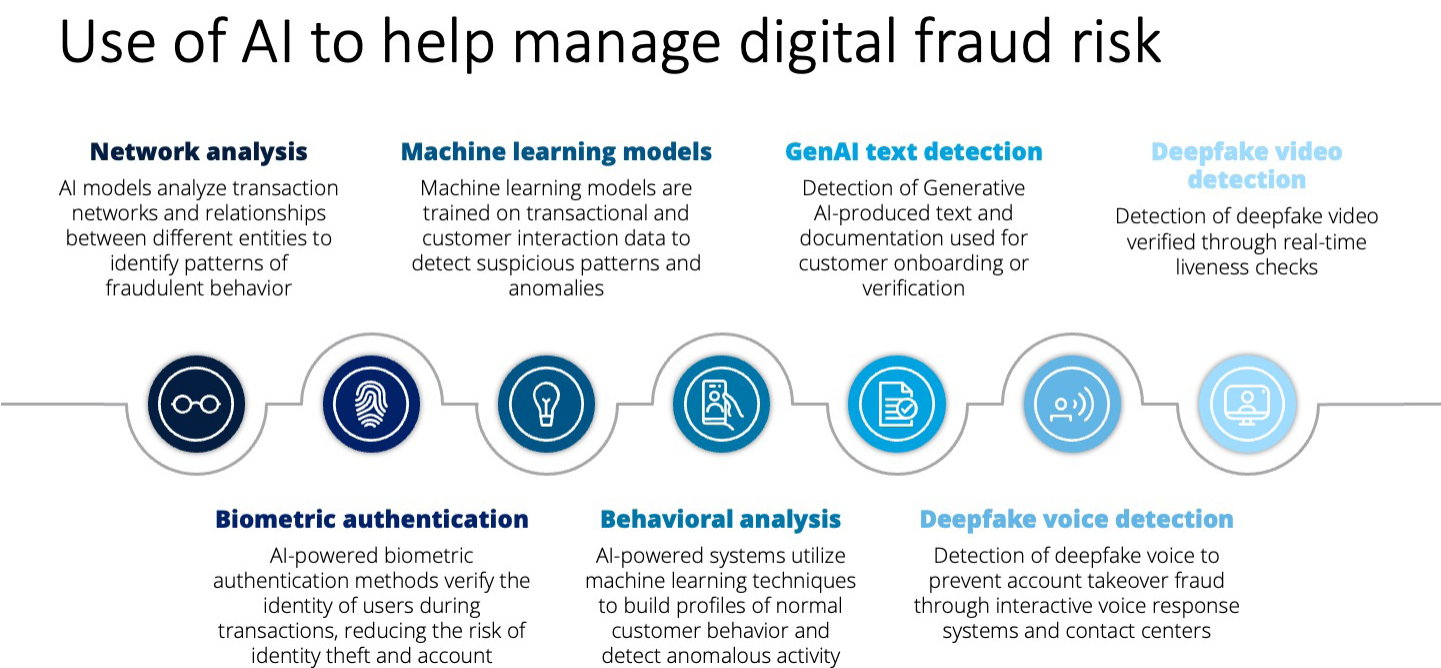
Rogue AI

Autonomous AI systems raise concerns about unauthorized transactions. To address this, programmable smart contracts can embed control mechanisms directly into AI's operational framework, enforcing predefined rules and constraints. ZK Proofs provide an additional layer of verification

confirming AI actions are authenticated and authorized without compromising sensitive information.

ZK Proofs, Web3 solutions, and programmable smart contracts can be leveraged by organizations looking to create a secure and compliant environment for AI and blockchain in payments, and to manage inherent risks and enhance transaction security.

Figure 2: AI tools that have been implemented to help manage digital fraud risk



Conclusion

The future of AI, blockchain, and Web3 is promising, with the potential to revolutionize countless sectors by enhancing efficiency, security, and user control while creating a more decentralized, transparent, and secure digital landscape. Realizing this potential requires addressing regulatory challenges and ensuring robust compliance frameworks to safeguard against emerging threats. By striking the right balance, these technologies can unleash their transformative power, all while helping to protect the interests of individuals and society at large.



Endnotes

¹ Statista, "Value of remittance flows globally," August 2024.

² Juniper Research, "Digital cross-border remittances to reach \$428 billion in 2025," press release, June 2021.

³ Doyinsola Oladipo, "Travel industry to contribute record \$11 trillion to global GDP in 2024," Reuters, September 3, 2024.

⁴ UN World Tourism Organization, "International tourist arrivals recover pre-pandemic levels in 2024," excerpt from World Tourism Barometer 23, no. 1 (January 2025).

⁵ Lesley Fair, "Facts about fraud from the FTC—and what it means for your business," Federal Trade Commission (FTC), February 9, 2024.

⁶ Federal Bureau of Investigation (FBI), Internet crime report, 2022.

Contacts

Roy Ben-Hur

Managing Director

Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
rbenhur@deloitte.com

Tim Davis

Principal

Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
timdavis@deloitte.com

Agha Khan

Senior Manager

Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
aghakhan@deloitte.com

Brendan Murray

Advisory Senior Consultant

Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
bremurray@deloitte.com

Mansi M Patel

Advisory Analyst

Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
mansimpatel@deloitte.com

Reagan Meek

Advisory Analyst

Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
remeek@deloitte.com

Madison McCaw

Advisory Analyst

Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
mmccaw@deloitte.com



About Blockchain & Digital Assets at Deloitte

At Deloitte, our people work globally with clients, regulators, and policymakers to understand how blockchain and digital assets are changing the face of business and government today. New ecosystems are developing blockchain-based infrastructure and solutions to create innovative business models and disrupt traditional ones. This

is occurring in virtually every industry and in most jurisdictions globally. Our deep business acumen and global industry-leading Audit & Assurance, Consulting, Tax, and Risk & Financial Advisory services help organizations across industries achieve their various blockchain aspirations. [Learn more](#)





This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.