ADGM Academy Research Centre

ADGM

zodia CUSTODY

Securing the Future:
Custody Best Practices for Web3, DAOs and Blockchain Foundations

FULL PAPER

Authored by:

Dmitry Fedotov, Dominic Longman,

Zane Suren

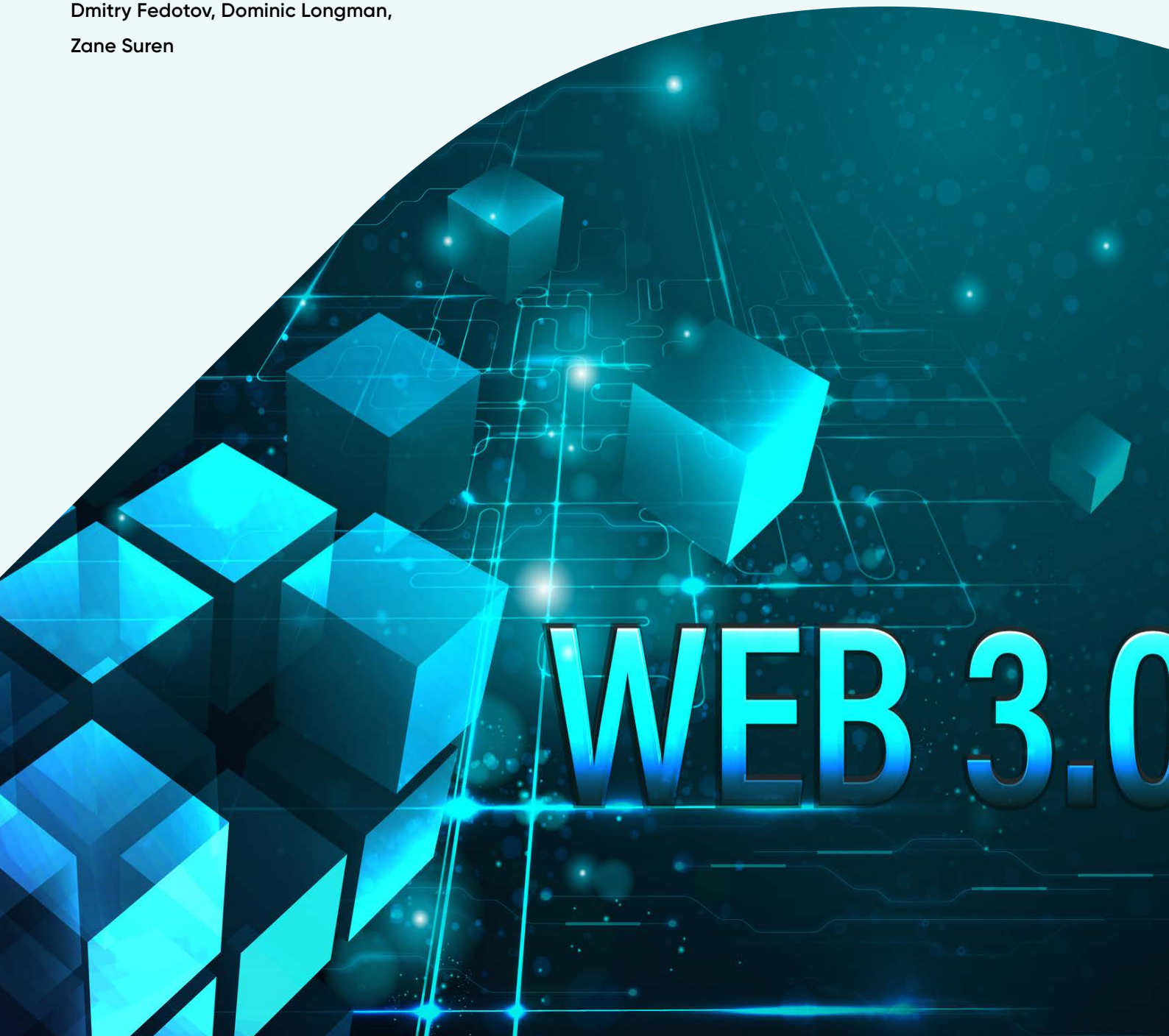


TABLE OF CONTENTS

FOREWORD

The rapid evolution of Distributed Ledger Technology (DLT), which resulted in new decentralised structures such as blockchain foundations, Decentralised Autonomous Organisations (DAOs) and Web3 entities, presents both transformative opportunities and significant challenges. As these innovative structures manage increasingly substantial digital asset treasuries, the need for robust security and clear governance frameworks becomes paramount. Secure custody is no longer a peripheral concern but a foundational necessity for building trust and ensuring the long-term sustainability of this burgeoning ecosystem.

ADGM Academy is committed to nurturing responsible innovation within a secure and transparent environment. Recognising the unique requirements of this new digital landscape, the ADGM Registration Authority (RA) pioneered the world's first comprehensive DLT Foundations framework, providing essential legal clarity and structure for blockchain foundations and DAOs. Complementing this, the ADGM Academy Research Centre plays a vital role in advancing knowledge and facilitating crucial dialogue across the industry.

This paper, a collaboration between ADGM RA, Zodia Custody and ADGM Academy Research Centre, exemplifies the critical partnership required between forward-thinking regulators and industry leaders. It delves into the core challenges of digital asset custody for blockchain foundations, Web3 entities and DAOs, offering actionable insights and outlining best practices derived from regulatory understanding and practical expertise.

Addressing the complexities of secure custody, governance, and compliance is essential for unlocking the full potential of a decentralised future. I am confident that the analysis and recommendations presented herein will serve as a valuable resource for all stakeholders navigating this dynamic field.

Mansoor Jaffar
CEO of ADGM Academy & Research Centre

1. SUMMARY

As Web3 technologies reshape digital interaction, governance and value exchange, new organisational structures—DAOs, blockchain foundations, and Web3 entities—are emerging at pace. These entities collectively manage billions in digital assets and treasuries yet face acute challenges in securing and governing these resources amidst technical complexity and regulatory ambiguity.

This white paper explores the evolving landscape of digital asset custody. It outlines the major risks—from smart contract vulnerabilities and governance attacks to regulatory uncertainties—and underscores the growing importance of institutional-grade custodianship. The paper illustrates how best-in-class solutions such as cold storage, multi-party computation (MPC), and multi-signature wallets can safeguard assets and enable operational resilience.

In parallel, the paper details a pioneering regulatory framework, including the world's first DLT Foundations regime, which provides DAOs and blockchain foundations with limited liability and legal personality—bridging the gap between decentralised models and traditional legal systems.

Through a shared lens of regulation and industry practice, the paper concludes with a call to action: to ensure long-term sustainability, Web3 projects must embrace secure custody, rigorous governance, and forward-thinking regulation. Only by doing so can the ecosystem truly secure its future—one that is decentralised, compliant and resilient.

2. **INTRODUCTION:** THE RISE OF WEB3 ENTITIES, BLOCKCHAIN FOUNDATIONS AND DAOS

As the digital landscape evolves towards Web3, characterised by decentralisation and user ownership enabled by blockchain technology, new organisational structures like Decentralised Autonomous Organisations (DAOs), Blockchain Foundations, and diverse Web3 platforms are emerging and managing significant digital assets. However, the very nature of digital assets – where control often resides solely with the holder of cryptographic private keys – introduces unique and substantial risks. High-profile incidents involving lost keys, rendering hundreds of millions inaccessible, or smart contract vulnerabilities leading to catastrophic losses underscore a critical problem: safeguarding these assets can be complex and fraught with peril. For DAOs managing community treasuries, foundations stewarding protocol development funds, and Web3 platforms handling user assets, the lack of robust security and operational controls can lead to irreversible financial damage, loss of trust and operational failure. Furthermore, navigating the ambiguous legal status and compliance requirements associated with these novel structures presents significant challenges. Therefore, specialised digital asset custody solutions are not merely optional conveniences but essential infrastructure. They solve the core problems of securing private keys against loss or theft, managing operational complexities, enabling compliant participation in the ecosystem, and providing the necessary controls for effective governance and treasury management.

Web3 – often described as the next evolution of the Internet – promises a decentralised, user-empowering digital ecosystem built on blockchain technology. Where Web2 encourages far greater participation than the original static webpages of Web1 by asking users to take part in ecommerce, blogging or social media, it was nevertheless not designed for native ownership of digital assets. Instead Web3, which encompasses cryptocurrencies, decentralised finance (DeFi), non-fungible tokens (NFTs), and decentralised autonomous organisations (DAOs), is giving us all a greater stake in how decisions are made, data is managed and assets are owned.

Unlike traditional Web2 platforms controlled by centralised entities, Web3 platforms leverage distributed ledgers to give users direct ownership of data and digital assets. DAOs, in particular, have emerged as novel governance structures: internet-native organisations, often coordinating large communities and significant treasuries based on token holders and transparent smart contract rules rather than centralised leadership. This model enables collective decision-making and resource management on a global scale, paving the way for new "blockchain foundation" entities, typically non-profit bodies established to foster the growth and development of specific open-source protocols and their ecosystems. The rise of Web3 and DAOs has been rapid, underlining their growing significance in the digital economy.

Multiple indicators point to Web3's rapid growth and future potential. Estimates for the global Web3 market vary, reflecting its dynamic nature. One analysis[1] valued the market at USD 2.25 billion in 2023, projecting growth to USD 33.53 billion by 2030 at a Compound Annual Growth Rate (CAGR) of 49.3% from 2024 to 2030, driven by factors like demand for data privacy and advancements in internet technology. Other reports suggest different scales, highlighting the challenge of precisely quantifying this rapidly evolving sector.

Broader blockchain adoption trends are similarly striking: the overall blockchain technology market, according to MarketsandMarkets Research, is projected to grow from USD 20.1 billion in 2024 to USD 248.9 billion by 2029, reflecting a robust CAGR of 65.5%[2] as investments in blockchain continue to accelerate. Beyond market size, the proliferation of Web3 projects and DAOs underscores their momentum. Beyond market size, the proliferation of Web3 projects and DAOs underscores their momentum. While precise historical figures are difficult to ascertain consistently, data aggregators like DeepDAO show the significant scale these entities manage. As of early 2025, the total value held in tracked DAO treasuries was approximately USD 14.6 billion, though this figure fluctuates significantly with market conditions, having reportedly exceeded USD 42 billion earlier in 2024. This volatility highlights the treasury management challenges these organizations face. Despite fluctuations, major DAOs like Mantle and Uniswap continue to hold billions in their treasuries , illustrating the substantial capital pools involved. Such growth trajectories and capital pools illustrate how significant Web3 and DAO ecosystems have become in a short space of time.

In essence, the idea of Web3 aims to redistribute power, value and control from centralised intermediaries to communities of users. Participants can directly own digital assets, vote on protocol decisions via governance tokens, and share in the upside of network growth. This paradigm shift – often likened to the early Internet in its transformative potential – has attracted interest from startups, tech giants, and governments alike.

However, this rapid innovation has also unfolded against a backdrop of significant legal and operational uncertainties. Historically, DAOs and similar decentralised structures have faced ambiguity regarding their legal status, how they can own assets, enforce decisions, and shield participants from liability – key pain points hindering wider adoption and institutional trust. High-profile industry events, such as the collapse of FTX in late 2022, further underscored the severe consequences of inadequate governance and custody practices, alarming participants and reinforcing the critical need for robust solutions. Recognising both the immense potential and

1 https://www.grandviewresearch.com/press-release/global-web-3-0-market
2 https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html

the inherent risks, forward-thinking regulators are seeking to provide frameworks that foster responsible innovation. ADGM, for example, guided by its mission to cultivate a trusted and progressive financial centre in the capital of the United Arab Emirates, has engaged deeply with the industry to understand and address these specific challenges. The very features that make Web3 powerful – decentralisation, smart contract reliance, community control – also introduce new vectors for failure, particularly concerning the safeguarding of assets.

ADGM's approach, developed in consultation with industry stakeholders, focuses on providing tailored legal structures, including distinct legal personality and limited liability, uniquely supporting blockchain foundations and globally distributed DAOs alongside other Web3 entities, thereby tackling these historical ambiguities head-on. Specifically, securing the rapidly growing treasuries and governance assets held by these organisations presents unique custody hurdles. Understanding these vulnerabilities, and the emerging best practices and regulatory solutions designed to mitigate them, is essential for building trust and sustainability in the Web3 ecosystem. The next section examines several of the most critical security and custody challenges facing these ventures in detail.

3. COMMON SECURITY AND CUSTODY CHALLENGES

Despite its promise, the Web3 landscape faces **significant security and custodial challenges** that must be managed for the ecosystem to mature. Unlike traditional systems where established legal and technical safeguards have been carefully developed and adopted, Web3's decentralised nature shifts much of the responsibility (and risk) to a reliance on the robustness of code within smart contracts and puts the onus for securing assets onto their owners and users. Several significant risk categories have emerged:

Smart Contract Vulnerabilities

Web3 applications often rely on smart contracts – pieces of self-executing code written on blockchains – to hold funds and enforce rules. A flaw in this code can be catastrophic, since "code is law" in these systems. One infamous example is The DAO hack of 2016[3] The DAO was an early Ethereum-based investment DAO that raised over **$150 million in ether (ETH) A coding vulnerability allowed attackers to steal roughly 3.6 million ETH, valued at approximately USD 50-60 million at the time , representing about a third of the total funds raised.** The exploit involved recursively draining funds from the DAO's smart contract via a loophole in its withdrawal function. [4]This specific vulnerability, known as a recursive call or reentrancy attack, allowed the attacker to repeatedly withdraw funds before the initial transaction updated the balance. The incident became legendary and was so severe that the Ethereum community intervened by hard-forking the blockchain to restore the stolen funds – a controversial decision that ultimately split the network into two (becoming Ethereum and Ethereum Classic). This case underscored how a single bug can undermine an entire decentralised organisation. Ensuring rigorous smart contract audits and formal verification has therefore become a critical priority, as any oversight can lead to an irreversible loss of user assets.

Governance Attacks

Decentralised governance – where token holders vote on proposals – is core to many DAOs. However, governance mechanisms themselves can be manipulated if not carefully designed. A stark demonstration was the **Beanstalk Farms** [5]exploit in April 2022. Beanstalk, a decentralised stablecoin protocol, had a governance system where a two-thirds supermajority could fast-track proposals. Attackers used a flash loan (an uncollateralised, instantaneous loan) to **acquire a majority of Beanstalk's governance tokens temporarily,** then approved a malicious proposal to siphon out funds. The attacker leveraged two malicious proposals (BIP-18 and BIP-19), passed using an 'emergencyCommit' function that bypassed standard voting delays, reportedly exploiting unaudited code. In seconds, the protocol's reserves – valued at approximately USD 181-182 million – were drained to the attacker's wallet. netted roughly USD 76-80 million in profit after repaying the flash loan, with the stolen funds subsequently laundered via Tornado Cash,. leaving the community devastated. This incident highlights that decentralisation is not a panacea – if one actor or a malicious group of actors working together can accumulate sufficient voting power (even temporarily), it can override the collective will. Robust safeguards like proposal time delays, quorum thresholds and limited treasury access are needed to prevent such governance failures.

Key Management and Custody Risks

In Web3, holding the private keys to a digital asset wallet equates to holding its assets. This grants users sovereignty over funds, but it also means that **lost or stolen keys can result in irretrievable losses** since no central authority can reverse unauthorised transactions. Both individuals and organisations have learned this the hard way. For example, QuadrigaCX[6], once Canada's largest crypto exchange, imploded when its CEO died unexpectedly – he alone knew the passwords to wallets holding about **$190 million** of clients' cryptocurrency, which became

3 https://www.gemini.com/cryptopedia/the-dao-hack-makerdao#section-origins-of-the-dao
4 https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto
5 https://en.wikipedia.org/wiki/Cryptocurrency_and_crime#:~:text=In%20early%202022%2C%20the%20Beanstalk,It%20was%20initially%20unclear
6 https://en.wikipedia.org/wiki/Cryptocurrency_and_crime#:~:text=Gerald%20Cotten%20%20founded%20QuadrigaCX,158

inaccessible upon his death. Subsequent investigations by the court-appointed monitor revealed significant irregularities, including evidence that the CEO had created fake accounts and transferred substantial customer funds to personal accounts on other exchanges. The circumstances led to widespread speculation and requests to verify the CEO's death. Similarly, DAO treasuries secured by multi-signature wallets are vulnerable if keyholders lose their keys or are compromised. These incidents emphasise the need for robust custody solutions (such as distributed key management and Hardware Security Modules) to protect digital assets against human error and malfeasance.

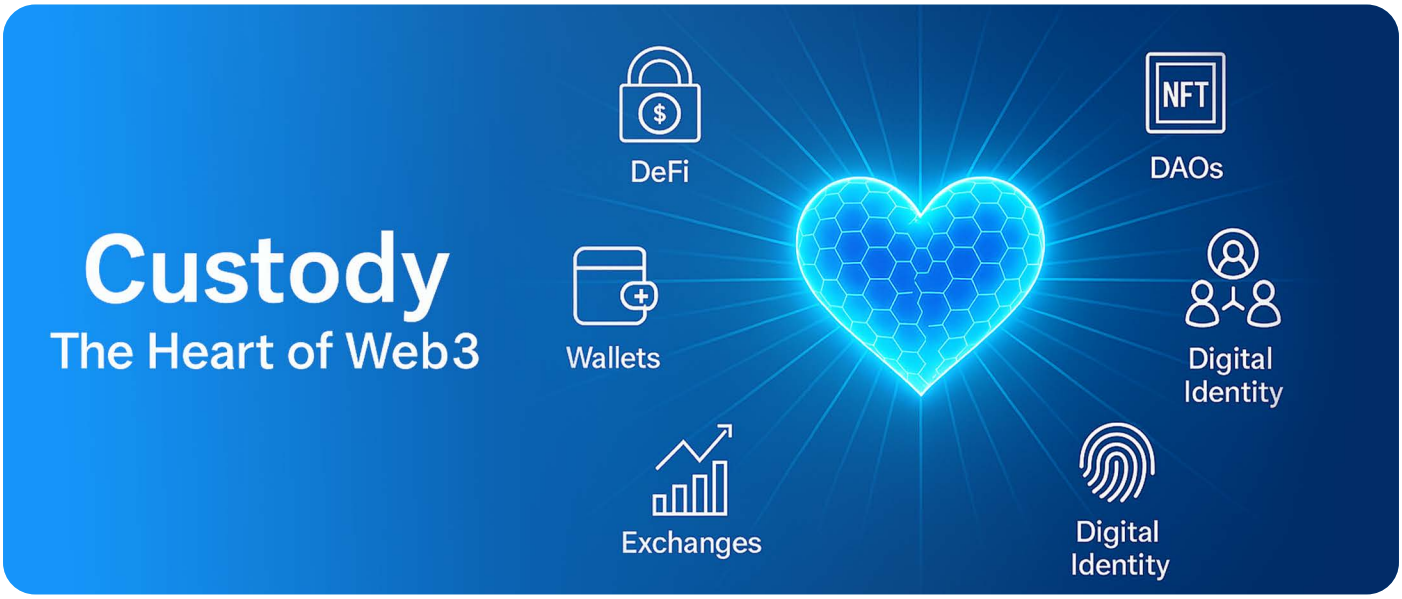
Operational Custody Challenges

Beyond external threats and individual key loss, the inherent nature of these decentralised entities introduces distinct operational custody challenges. Effectively coordinating essential security procedures, such as transaction signing via multi-signature wallets, can be complex and slow when signatories are geographically dispersed, operate across different time zones, or have varying levels of technical expertise. Implementing rigorous key lifecycle management protocols – encompassing secure generation, distribution, backup, rotation, and recovery – is also significantly more challenging without centralised security personnel. This is often compounded by a lack of dedicated internal resources or specialised operational security expertise within the DAO or foundation itself, potentially increasing vulnerability to human error or process failures.

Regulatory and Legal Uncertainties

The regulatory environment for Web3 and DAOs remains uncertain and varies widely from jurisdiction to jurisdiction, posing compliance challenges. Existing laws were not designed for ownerless, decentralised organisations, leading to ambiguity about how rules apply. A prominent example arose in 2022 when the U.S. Commodity Futures Trading Commission (CFTC) took action against Ooki DAO. In this first-of-its-kind enforcement action, the CFTC successfully argued that Ooki DAO could be treated as an «unincorporated association» comprised of token holders who voted on governance proposals. Following a default judgment, the court held the Ooki DAO itself liable as a legal 'person' under the Commodity Exchange Act for operating an illegal trading platform and unlawfully acting as an unregistered Futures Commission Merchant (FCM), including failing to implement required KYC/AML procedures. This ruling, which included a monetary penalty and mandated the shutdown of the DAO's website, set a significant precedent. It demonstrated that DAOs are not immune to regulatory action and raised concerns about the potential for liability to extend to participating token holders under the unincorporated association theory, although this aspect remains debated. Meanwhile, global approaches to cryptocurrency and digital assets vary widely – from outright bans to collaborative regulatory sandboxes – creating a patchwork of rules that complicates cross-border operations. Moreover, without formal legal status, a DAO cannot easily enter contracts or bear legal obligations, heightening uncertainty. **Regulatory risk** has thus become a major concern for Web3 projects.

4. THE ROLE OF INSTITUTIONAL CUSTODIANS IN WEB3



Digital asset custodians sit at the **heart of Web3**. Without certainty over the security and safety of digital assets, enterprises and multinational institutions, who have fiduciary duties and are responsible for managing clients' funds or holding their assets, would simply be unable and unwilling to open up their businesses to the potential risks posed by this emerging industry.

Institutional-grade custodians including those like Zodia Custody, which are invested in and backed by leading financial institutions such as Standard Chartered, Northern Trust, National Australia Bank and Emirates NBD, put safety and security at the centre of everything they do. However, it is not only financial institutions which need support in managing digital assets. As we have seen above, many types of token holders, including Web3 businesses, DAOs and blockchain foundations, increasingly have treasuries needing secure management and custodial services. In the early days of cryptocurrency institutional-grade custody providers and solutions were not available. Now, as the industry grows and matures, such organisations are looking for external providers rather than relying on self-custody solutions as they may have had to do in the past.

The importance of security, compliance and operational resilience

Alongside the essential requirement of security, regulatory compliance and a robust focus on operational resilience are necessary components in safeguarding digital assets for Web3 projects. Institutional-grade custodians place a strong focus on governance and risk oversight as well as using the latest in custody technology to ensure that clients' funds are managed and stored safely.

Providing best-in-class enterprise custody solutions

Today's digital asset custody solutions have been designed to be fit for purpose for the world's largest global financial institutions and enterprises. A variety of best practices and trusted security measures have been developed[7] including cold storage, multi-signature key management, sharding and multi-party computation.

7 https://www.aima.org/sound-practices/industry-guides/digital-asset-custody-guide.html

Custodians also often offer further protection through institutional-grade insurance, with leading digital asset crime and cyber policies put in place to protect clients from the risk of scams, fraud and rugpulls (a type of scam where the developers of a project abandon it, usually after hyping it up to attract investors, and then sell their tokens, leaving investors with worthless assets).

Cold Storage

Cold storage is a solution designed to protect holders of digital assets against theft and unauthorised access since cold wallets are held offline reducing cybersecurity risks. Today's institutional-grade cold wallets allow clients to store digital assets securely but with near-instant 24/7 availability. For Web3 clients who want security but also need to rapidly access funds whenever they need them, perhaps for staking or other Web3-based activities, these types of custody solution allow access to assets in air-gapped cold wallets instantaneously. An air gapped wallet is a hardware wallet disconnected from the Internet and generally never plugged into a computer. Instead, they communicate by passing microSD cards back and forth or by scanning QR codes.
This added layer of security is well suited to digital asset storage solutions which need multiple signatures to initiate or complete a transaction.

Hardware Security Modules (HSMs)

Hardware Security Modules (HSMs) primarily protect against the risk of compromised cryptographic keys and sensitive data, which can lead to unauthorized access, data breaches and other security incidents. Clients' private keys are stored in HSMs held in secure data centres. HSMs are tamper-proof servers that require multi-signatory verification to access and move digital assets. They are designed to repel any unauthorised attempt to break into them and are independently certified to validate this design principle. Using co-located facilities also minimises risk by adding a further layer of operational resilience. Holding the master keys within a custody solution in an escrow account or using a trust structure also adds extra layers of security and resilience in the unlikely event of a failure by the custodian.

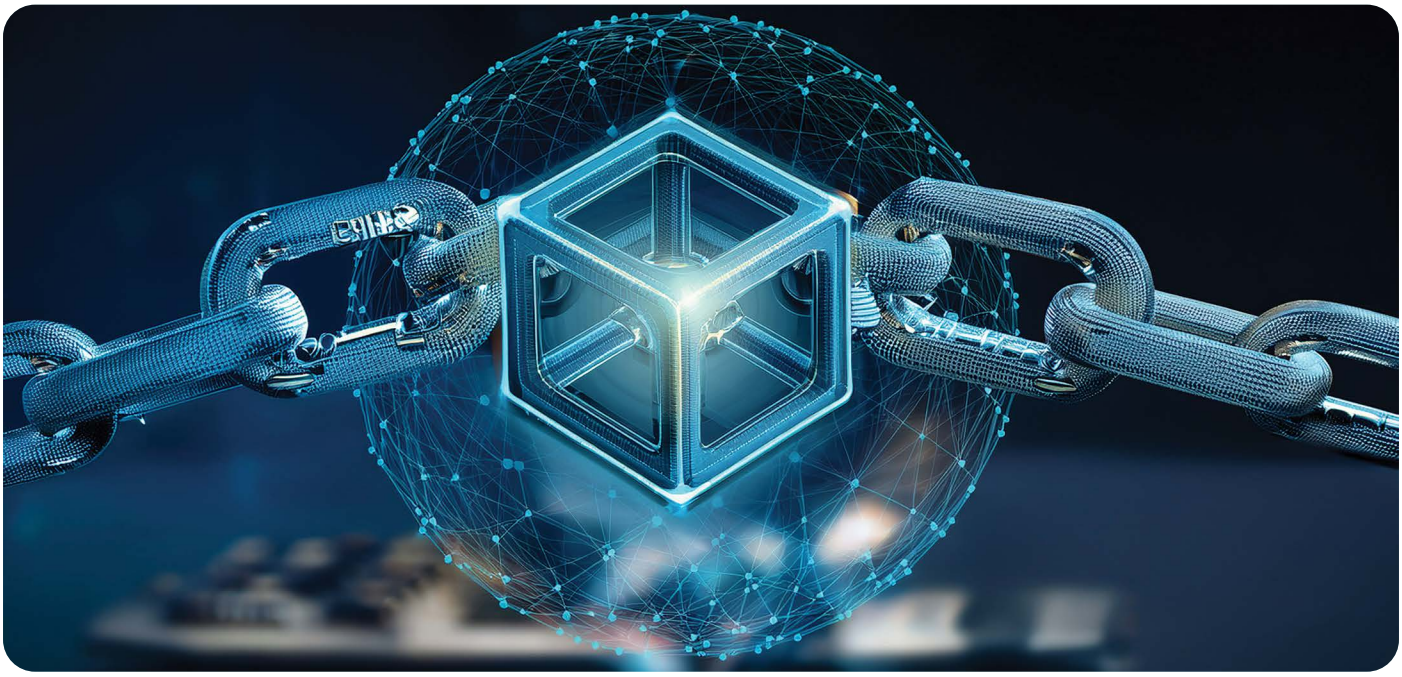
Multi-signature Wallets

Multi-signature wallets (also known as multi-sig) eliminate single points of failure and protect against key theft and key loss. Using multi-signature wallets offers increased security since it requires multiple parties or devices to approve a transaction. A multi-sig wallet uses multiple private keys and a transaction can only be executed if a certain number of these keys are used to sign it. Multi-signature wallets allow distributed control over funds. This makes them very suitable for scenarios where multiple individuals or entities need to manage assets jointly, such as in DAOs or Web3 corporations.

Sharding and Multi-Party Computation (MPC)

When data is spread out, the risk of a single point of failure is reduced, making it more challenging for unauthorised users to access sensitive information. Multi-Party Computation (MPC) technology is designed to address this risk by splitting the client's private key into 'shards' and distributing portions of the original private key to as many trusted parties as required. When the asset needs to be moved, the users coordinate as part of a signing scheme so there is no single point of failure. This reduces the risk of hacking and the threat of human error or theft.

5. ADGM'S REGULATORY FRAMEWORK



Addressing the significant regulatory and legal uncertainties highlighted earlier, which pose major hurdles for blockchain foundations, DAOs and Web3 projects, ADGM, an international financial centre based in the UAE, has taken a pioneering step. In 2023, ADGM introduced the world's first comprehensive regulatory framework specifically designed for DLT (Distributed Ledger Technology) Foundations. This innovative regime aims to provide blockchain protocols, DAOs, and various Web3 initiatives with a much-needed, purpose-built legal structure, bridging the gap between the decentralised ecosystem and traditional legal systems. This framework operates within ADGM's independent jurisdiction, which is based on English common law, providing a familiar legal framework for international entities.

At the core of the DLT Foundations Regulations 2023[8] is the creation of a new, bespoke legal entity: the DLT Foundation. This structure directly addresses the unique requirements of blockchain-based organisations, offering several key advantages:

Tailored Legal Structure and Token Governance: Unlike generic corporate forms, the DLT Foundation is explicitly designed for organisations operating on blockchains. This allows projects to register and, where applicable, issue tokens within a well-defined regulatory scope – for example, clarifying the treatment of utility tokens. By codifying token-based operations and governance principles into law, the framework provides Web3 teams with a transparent and predictable rulebook, reducing the ambiguity that has hindered similar initiatives elsewhere.

8 https://www.adgm.com/dlt-foundations

Recognition of Decentralised Governance: A critical feature of the ADGM framework is its explicit recognition of on-chain governance mechanisms. A DLT Foundation can be legally constituted to operate via smart contracts and token-holder voting, giving legal weight to decentralised decision-making processes. While allowing flexibility (e.g., no mandatory bylaws), the framework mandates essential governance structures: a Council (minimum 2, maximum 16 members) responsible for management and a Guardian responsible for ensuring compliance with the Foundation's objectives. This structure ensures a balance between decentralised operation and accountability. Furthermore, the framework accommodates the global nature of these communities by not imposing physical residency requirements for council members.

Legal Personality and Limited Liability: The DLT Foundation structure provides the crucial benefit of incorporation: limited liability, shielding participants (such as token holders or developers) from personal liability for the foundation's obligations. The foundation itself possesses a distinct legal personality, meaning it can own assets, enter into contracts, and incur obligations in its own name. The regulations specify that token holders are not liable for the Foundation's obligations merely by virtue of holding tokens. This directly addresses the risks highlighted by cases like the CFTC action against Ooki DAO[9], offering legal certainty.

This distinct legal personality is not merely an administrative formality; it unlocks vital operational capabilities, particularly concerning the security of assets. Crucially, it empowers the DLT Foundation to formally contract with regulated institutional custodians, entering into legally binding service agreements for the safeguarding and management of its digital asset treasury. This provides a secure, accountable, and legally recognised structure for asset protection, resolving a key ambiguity faced by unincorporated decentralised entities and facilitating access to the institutional-grade security required to protect substantial value. It's important to note that the DLT Foundation framework is designed for entities undertaking 'DLT Purposes' (such as deploying DLT or issuing tokens). ADGM's DLT foundations are not permitted to carry on activities that would require a separate financial services permission from ADGM's Financial Services Regulatory Authority (FSRA) without obtaining such authorisation.

By providing this level of tailored clarity and legal certainty, ADGM has positioned itself at the forefront of regulating decentralised structures, succeeding where earlier, less comprehensive attempts in other jurisdictions saw limited uptake. The framework effectively creates a bridge, allowing decentralised networks to interact more seamlessly with the traditional legal and financial system while preserving their core ethos. Recent developments underscore ADGM's growing role, including the establishment of the Stacks DLT Foundation, the TON DLT Foundation and other major protocols within the framework. ADGM is also collaborating with Solana Foundation and Polygon Labs aimed at developing international disclosure standards for the blockchain industry.

ADGM's initiative DLT Foundation framework demonstrates that thoughtful, forward-thinking regulation can be a powerful enabler of innovation, rather than a hindrance. By setting clear standards for transparency, governance

9 https://www.cftc.gov/PressRoom/PressReleases/8715-23

and accountability, frameworks like the DLT Foundations regime foster the trust and institutional confidence necessary for the Web3 sector's sustainable and secure growth.

6. BEST PRACTICES FOR SECURING WEB3 ENTITIES AND DAOS

Ensuring strong governance, secure custody solutions and compliance

Web3 entities and DAOs are new organisational structures that understandably undergo a high degree of scrutiny from the media, as well as from potential investors, partners and clients. Reliable custody lies at the heart of trust in such organisations. Digital asset custodians have matured enormously since the birth of cryptocurrency and now offer solutions that have coalesced around a set of industry best practices which are equally suitable for both crypto-native organisations, as they are for heavily regulated financial institutions.

Governance best practices: Segregation of business lines & segregation of duties

Custodians such as Zodia Custody were deliberately created by Standard Chartered to operate as a standalone business to segregate custody as a business line distinct from trading and other services. Digital asset custodians' service offerings should also practice good governance and segregate duties across the different users who are responsible for managing assets.

Crypto assets themselves should be separated into segregated cold storage address wallets for each client while cryptographic master keys are generated in an offline environment and stored in HSMs. Officers and auditors from the company should witness and document the generation of master keys. These master keys exist so that wallets can be reconstituted from encrypted wallet seeds protected by the master key in the event that a client loses access to their wallet.

Secure Custody

Best practices in custody involve a high degree of due diligence. Having robust cyber security policies in place is a basic requirement including conducting regular pen tests, offering bug bounties, ensuring certification renewals, and frequent software testing.

To make master keys more secure, it is best practice to store shards of the master key in vaults with high levels of round-the-clock security located in jurisdictions that have robust regulatory regimes for digital assets. Withdrawals should also follow stringent cold storage restore protocols to bring funds back online including multi-factor authentication, transaction intent digital-signing, software-based security enforcement and other operational checks and balances.

Compliance

Compliance is a market requirement for digital asset custodians whether they are operating in Web3 or in traditional finance Without it, digital assets would simply not be accessible to traditional financial institutions or consumers. The TradFi market relies on digital assets firms being able to marry the regulatory lessons and security processes common to a traditional financial market - which has matured over many decades - to the newer, faster, and more transparent digital asset ecosystem. The scope of compliance requirements for digital asset custodians is broad and multi-layered, encompassing not only financial crime prevention but also operational resilience, consumer protection and data privacy.

Key areas of compliance for digital asset custodians often include:

- **Legal and regulatory authorisation:** Custodians must be properly licensed or registered with relevant authorities in each jurisdiction where they operate. This includes meeting capital, governance and operational requirements and being subject to ongoing supervision.
- **Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Sanctions:** Robust AML/CTF frameworks are essential, including customer due diligence, transaction monitoring and sanctions screening. Custodians must be able to identify and report suspicious activity, even when dealing with pseudonymous blockchain addresses and self-hosted wallets.
- **Consumer protection:** Custodians are typically required to segregate client assets from their own, provide transparent client disclosures, and maintain robust processes for asset recovery in the event of insolvency or operational failure.
- **Data protection and privacy:** Compliance with local data protection laws is mandatory, including secure handling of client information and clear privacy policies.
- **Governance, risk, and internal controls:** Effective governance structures, including compliance committees, regular independent audits and experienced compliance officers are essential for oversight and accountability.
- **Bribery, corruption and conflicts of interest:** Zero-tolerance policies for bribery and corruption, mandatory conflict of interest disclosures and regular employee training are required to ensure integrity and trust.

Custodians must foster cultures where employees can safely report concerns or breaches, supported by clear whistleblowing policies.

Compliance in the broader Web3 context

Web3 compliance introduces novel challenges distinct from traditional finance, primarily driven by decentralisation, pseudonymity and a rapidly evolving regulatory landscape. In response, regulators are developing innovative approaches to address these distinctive characteristics:

- Regulators are implementing "travel rule" compliance requirements in alignment with FATF guidelines to address pseudonymity concerns in Web3 transactions, ensuring appropriate transparency while balancing privacy considerations;
- Several regulatory bodies are developing frameworks to legally recognise Decentralised Autonomous Organisations (DAOs), establishing clear liability structures within these novel governance models; and
- Jurisdictions worldwide are creating token taxonomies to help inform the application of regulation, whilst others have adopted "regulation by enforcement" approaches in the absence of comprehensive frameworks.
- These regulatory adaptations reflect the ongoing evolution of compliance requirements in the Web3 ecosystem, necessitating proactive engagement from market participants to ensure sustainable, pragmatic growth and institutional adoption.

Ensuring long-term sustainability and trust

Building long-term partnerships founded on shared values with entities like digital asset custodians will be key to the success and sustainability of Web3 initiatives. Custodians sit at the heart of the marketplace positioning them as a type of honest broker able to understand both institutional and crypto-native clients' needs as well as regulatory and policy concerns.

As global markets transition into a DLT-based environment, the development of quality standards and industry benchmarks is much needed to help all sides implement technology more rapidly and know who to trust. Standards governing robust and interoperable platforms will be key for the governance of the blockchain ecosystem. They will help Web3 projects and their clients to navigate the complexities of the different network models and facilitate a marketplace where a variety of engagements can take place unilaterally or multi-laterally without compromising on security or compliance.

As lynchpins of the ecosystem, custodians are also well-placed to engage with and support regulators and policymakers to resolve some of the uncertainties that exist today in this transition between Web2 and Web3. They are likely to play a significant role in promoting harmonisation across national and international levels and can help Web3 players achieve greater trust from regulators since security and safeguarding are intrinsic to their business model.

7. LOOKING AHEAD: THE FUTURE OF CUSTODY AND SECURITY IN WEB3

Secure, trusted custodial solutions for digital assets lie at the core of Web3's future success. These solutions must not just be secure but also be designed to keep pace with technological changes in this rapidly evolving industry. Some of the key trends shaping the future of custody include:

Innovation in decentralised governance

One innovative idea that could improve decentralised governance is the notion of embedding compliance rules into tokens themselves. This could solve, for example, the hurdle that some tokens are not available to investors in certain jurisdictions due to varying regulatory regimes.

AI is also reshaping how decisions are made in blockchain systems, particularly in areas like consensus and governance. By combining AI with decentralised systems, blockchain networks can operate more efficiently, for example by optimising blockchain consensus mechanisms. AI can help reduce energy usage and speed up validation by adjusting parameters based on real-time network conditions. This optimisation particularly supports more advanced governance models, such as DAOs.

Smart contract security

Since the security of smart contracts is so central to trust in Web3, developers and Web3 companies are formalising best practices to ensure that smart contracts are operationally resilient. Key tools include the use of smart contract audits and bug bounties (where rewards are offered to blockchain developers or security researchers for discovering and reporting vulnerabilities or bugs in their smart contracts). The rise of DeFAI (Decentralised Finance powered by AI) is also pushing decentralised finance into a new era, where intelligent systems analyse data and execute transactions. AI can add a new layer of efficiency and functionality to smart contracts but also comes with its own risks around data privacy, compliance and scalability, making the need for smart contract security audits even more paramount.

Treasury management

The decentralised nature of cryptocurrencies, combined with their volatility, makes effective treasury management an essential yet complex task. Relying heavily on one cryptocurrency can expose Web3 projects such as Foundations or DAOs to significant volatility risks. As reliable assets pegged to a fiat currency or basket of assets, stablecoins can play a key role here, as can diversifying portfolios to encompass a broader set of assets. One of the primary risks in crypto treasury management is the loss of private keys. Multi-signature wallets and cold storage add additional layers of security. Implementing robust internal controls is also essential to prevent errors and fraud. Custodians can assist with establishing protocols for transaction approvals, regular audits and control mechanisms to ensure transparency and accountability.

Future opportunities for digital asset custodians in a tokenised world

As Web3 and tokenisation grow, they present custody providers with enormous potential to innovate. Current areas of growth include the rise of stablecoins, which are transforming payments and global trade with a range of innovative use cases, as well as the increasing convergence of cryptocurrencies, digital assets and blockchain with other frontier technologies such as AI, IoT devices and smart cities.

Machine learning and AI will play a key part in a tokenised world with the lines between a commercial transaction and an investment asset potentially becoming more blurred in future. Blockchain-based AI is being used for tasks like fraud detection, payment processing, and optimising supply chains while Blockchain and DLT initiatives are moving beyond finance into applications across healthcare, creative industries, the energy sector and beyond.

Custodians' service offerings are evolving to encompass new products more tailored to these non-financial enterprises as well as offering new value-added services like the development and application of smart contracts, token vetting, or enabling interoperability between different DLT networks and protocols.
Having built up a level of trust and after investing in the development of safe and effective key management solutions, digital asset custodians are well placed to facilitate market connectivity and interoperability, positioning themselves as key players and bridges to Web3. As time goes on, they will increasingly become value-adding partners not only by leveraging new technologies to enhance their service offerings but fundamentally by remaining core drivers of trust in Web3's future.

8. CONCLUSION: A SECURE, COMPLIANT, AND DECENTRALISED FUTURE

The emergence of Web3 entities, DAOs and Blockchain Foundations represents a significant evolution in digital interaction, ownership, and governance. These innovative structures hold immense potential but face critical hurdles, particularly in the secure custody and management of their digital assets. The examples of costly exploits and regulatory uncertainty underscore that robust security, and clear frameworks are not optional extras but foundational necessities for long-term viability and trust.

Successfully navigating this landscape requires advanced technology, robust governance, and enabling regulation. Institutional-grade custodians provide the specialised security infrastructure – utilising cold storage, sophisticated key management like MPC and multi-sig, and operational resilience – essential to safeguarding assets against increasingly complex threats. Simultaneously, Web3 entities, DAOs, and Blockchain Foundations must implement rigorous internal governance processes and adhere to best practices for treasury management and operational security, ensuring decentralised decision-making does not equate to vulnerability.

Furthermore, proactive and clear regulatory frameworks, such as the pioneering DLT Foundations Framework established by ADGM, play a crucial role. Such regimes provide the legal clarity and certainty needed to bridge the gap between the decentralised world and established legal systems, fostering innovation within secure boundaries and encouraging institutional confidence.

The path forward lies in continued collaboration. The insights shared in this paper, stemming from the combined perspectives of a forward-thinking regulator (ADGM's Registration Authority) and an industry leader in institutional custody (Zodia Custody), exemplify the partnership required. Dialogue between technologists, platform builders, users and regulators is vital for developing practical standards and addressing challenges collectively.
The call to action is clear: for Web3 projects, DAOs, and Foundations, prioritising institutional-grade custody solutions and embedding strong governance practices from the outset is paramount. For policymakers, fostering innovation through clear and supportive regulatory environments is key. By embracing secure custody, rigorous governance and collaborative innovation, we can collectively build a decentralised future that is not only transformative but also secure, compliant, and trustworthy – truly securing the future for these vital ecosystem participants.

ACKNOWLEDGEMENTS

This paper was developed in collaboration between ADGM Registration Authority, ADGM Academy Research Centre, and Zodia Custody.

ADGM

ADGM[10] is an international financial centre that brings unique value to the emerging economy of Abu Dhabi and the broader region. Established in 2015, ADGM has significantly enhanced Abu Dhabi's stature as a leading financial centre and business hub, bolstering its role as a key player in the Falcon Economy. It serves as a vital strategic link between the growing economies of the Middle East, Africa, South Asia, and global markets.
ADGM Registration Authority

The ADGM Registration Authority[11] is responsible for the registration, incorporation and licensing of legal entities in ADGM and supports with all government-related services. Providing a range of activities to facilitate market entry, growth and the emergence of a vibrant and sustainable business community, the Authority guides and supports companies through the application and set-up of ADGM-registered entities.

ADGM Academy Research Centre

The ADGM Academy Research Centre[12] brings together an ecosystem of academics, financial industry practitioners, government and technology experts to unlock the shared potential to improve the financial environment in MENA and beyond. The financial industry continues to transform at a rapid pace with new technologies, disruptors, threats and opportunities appearing all the time. Independent research is crucial to be able to understand and utilise this transformation for the benefit of your business, your customers and society in general. The Research Centre provides that understanding through insights developed in collaboration with the academic community.

Zodia Custody

Zodia Custody is a leading institution-first digital asset custodian backed by Standard Chartered in association with Northern Trust, SBI Holdings, National Australia Bank and Emirates NBD.

Zodia Custody implements the requirements of the 5AMLD and applies the same standards as Standard Chartered relating to AML, FCC, and KYC. It implements the requirements of the FATF Travel Rule. Zodia Custody Limited is registered in the UK with the FCA as a crypto asset business under the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017. Zodia Custody (Ireland) Limited is registered with the Central Bank of Ireland as a VASP under Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended). Zodia Custody (Ireland) Limited was established in Ireland in August 2021. Zodia Custody (Ireland) Limited is registered with the CSSF in Luxembourg as a Virtual Asset Service Provider in accordance with article 7-1 (2) of the law dated 12 November 2004 on the fight against money laundering and terrorist financing, as amended. Zodia Custody (Hong Kong) Limited is registered with the Registry for Trust and Company Service Provider with License Number TC009245 under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO), Cap. 615 in respect of its custodial activities in digital assetss.

10 https://www.adgm.com/
11 https://www.adgm.com/registration-authority
12 https://www.adgmacademy.com/adgma-research-centre

ADGM ACADEMY RESEARCH CENTRE

Innovating Knowledge, Empowering Change

The **ADGM Academy Research Centre**, part of ADGM Academy, unites academics, financial practitioners, government, and technology experts to drive innovation and enhance the financial landscape in the UAE, MENA region, and beyond. As the financial sector evolves with new technologies, disruptors, and opportunities, independent research is vital to harness these changes for the benefit of businesses, customers, and society. Through collaborative insights with the academic community, the Research Centre delivers the expertise needed to navigate and capitalise on this dynamic transformation.

Stay up to date with ADGM Academy Research Centre.

adgmacademy.com research@adgm.com

FOLLOW US
ON OUR SOCIAL NETWORKS

Level 20, Al Maqam Tower, ADGM Square, Al Maryah Island, PO Box 111999 Abu Dhabi, UAE
الطابـق 20، بـرج المقام، مربعة أبوظبي العالمي، جزيرة الماريـه، ص ب 111999، أبوظبي، الإمارات العربية المتحدة

T +971 2 333 8500 adgmacademy.com

adgmacademy.com