THE FOUNDERS’ GUIDE TO UK CRYPTO LAW
Edited by Lisa McClory and Cessiah Lopez

CONTENTS

CHAPTER 01

CHAPTER 05

CHAPTER 06

CHAPTER 07

CHAPTER 08

DISCLAIMERS

The content in this publication is not legal, financial, or tax advice, nor a recommendation to use any particular product or service. The mention of specific organizations, technologies, or products does not imply endorsement or preference over others not mentioned. Users are responsible for seeking their own independent, professional advice based on their individual circumstances. The publishers, editors, authors, contributors, and reviewers, along with their affiliated entities and employers, do not accept responsibility or liability for any claims arising from the use or reliance on this publication. None are responsible for outdated or incomplete content. Users must verify the currency and accuracy of all information contained herein. All rights reserved.

While this guide references the UK, please note that different laws may apply in England and Wales, Scotland, and Northern Ireland. You should seek advice from suitably qualified professionals in the relevant jurisdiction.

ACKNOWLEDGMENTS

Editors

- Cessiah Lopez, Superteam UK
- Lisa McClory, D2 Legal Technology

Many thanks to Superteam UK and to all the expert contributors to this essential guide (in alphabetical order):

Contributors

- Akber Datoo, D2 Legal Technology & Co-Chair, Law Society Technology and Law Committee
- Aleksandra Wawrzyszczuk, LawtechUK and New York University School of Law
- Andrew Maguire, Littleton Chambers
- Anne Rose, Mishcon de Reya LLP
- Callum Blundell, Mishcon de Reya LLP
- Cap, Superteam UK
- Charles Kerrigan, CMS; RAK DAO
- Derya Karli, Own Protocol
- Dion Seymour, Andersen LLP
- Ian Cox, Avark Agency / Manchester Blockchain Alliance
- James Burnie, WAGMI Advisers, Gunnercooke LLP
- Joni Pirovich, DAOstar (a project of The Metagovernance Project Inc)
- Leon Hurd, CyberSandbox and Keystone Law Ltd
- Marcin Zarakowski, Token Recovery
- Maria Riivari, Avara

- Marcus Bagnall, Wiggin LLP
- Mark Pearce, Alkimi
- Matt Green, Lawrence Stephens Ltd
- Mohamed Ezeldin, Animoca Brands
- Morgan Lewis, Brabners LLP
- Omri Bouton, Outlier Ventures
- Pavan Kaur, WAGMI Advisers, Gunnercooke LLP
- Sara Hall, Walkers
- Professor Sarah Green, D2 Legal Technology

Reviewers: Daniel Maw, Christopher Brown, and Sylvia Papadopoulou of D2 Legal Technology

With special thanks to our media partners **LexisNexis UK**.

PR and Marketing Support: Jo Timmins
Design: designticket.co
Cover Design: 1984drum

Editor’s Note
Lisa McClory
9 December 2024

The idea for this *Founders’ Guide to UK Crypto Law* arose during a conversation with Cap (a) of Superteam at the inaugural BlockStart Scotland event. It followed a lively, question-filled legal discussion panel that highlighted an urgent need for solid, practical guidance for projects aiming to enter the Web3 space.

While ample guidance does exist, much of it is highly technical and not always easy for non-lawyers to digest. The purpose of this guide, therefore, is to bring together top experts in the field to cut through some of the mystery and complexity surrounding Web3 law. We aim to reduce the “ifs, buts, and it-depends” that too often characterize a project’s search for quality advice in this rapidly evolving area.

Each contributor was chosen for their depth of experience and expertise. The result is a diverse selection of topics covering law, tax, and compliance, supplemented with practical tips that readers may not find elsewhere. We hope you find it useful and informative.

This is a particularly exciting time to be innovating in the Web3 industry. The advent of AI is increasingly intersecting with Web3 applications—in on-chain analytics, algorithmic trading, and more. AI often aids blockchain by sifting and sorting data, enabling richer engagement with off-chain data sources. Conversely, blockchain can assist AI development by providing digital trust and fidelity in our increasingly complex online landscape. As we face challenges such as discerning deepfakes from reality, the interplay between AI and blockchain will only grow more important.

Soon, we’ll witness integrated applications of AI and crypto alongside robotics, smart sensors, AR, VR, and beyond. We are standing on the cusp of rapid change and innovative potential. At times, it may feel as though we’re already living in the world of *Star Trek*.

The UK has a prime opportunity to place itself at the heart of this new industry, fostering innovation and leveraging its skilled digital workforce to build groundbreaking businesses. The flexibility of the common law and the UK’s reputation as a center for dispute resolution make English law an attractive choice for encoding into smart legal contracts. Importantly, the benefits of this innovation should not be limited to traditional financial hubs. Instead, we must ensure these opportunities spread across the country, enabling fresh ideas, pioneering opportunities, and creative thinking to flourish.

We are proud to have collaborated not only with Solana Superteam UK but also with the Manchester Blockchain Alliance on this initiative. The front cover celebrates this dynamic partnership, paying homage to Manchester’s spirit of creative industry, collaboration, and collective enterprise—values that resonate strongly within the diverse and free-thinking potential of the digital economy.

As we launch this guide, we are closely following the UK's evolving approach to crypto regulation. A crypto roadmap was announced by the Financial Conduct Authority (FCA) in November 2024, following Tulip Siddiq MP's Mansion House speech, which identified fintech as one of five priority growth opportunities for the UK.[1][2][3] Globally, regulators are introducing frameworks that provide much-needed clarity and consistency for cryptoasset service providers and trading platforms.

Regulation is essential for the steady, safe growth of the cryptoasset industry. Achieving proportionality—ensuring startups can access quality advice and support—is a key challenge for regulators. Delivering clear, user-friendly regulatory frameworks swiftly is imperative for those seeking leadership in the digital economy.

Accelerators like Superteam UK are vital to this ecosystem. They bridge the gap between professional advisors and projects, and provide networks, co-working spaces, and other essential resources for growing initiatives.

This guide is intended as a starting point for builders and entrepreneurs in the UK, acknowledging the crucial role that law and regulation play. We hope it helps some projects navigate uncertainty, avoid pitfalls, and gain the knowledge needed to fulfill their potential. We envision this guide as a living document, one that will evolve over time.

Riffing a bit off our excellent chapter on Token Launch: “Things are only impossible until they're not!” – Captain Jean-Luc Picard of the Starship Enterprise.

Lisa McClory

1. AI x Crypto (Version 9.1), Outlier Ventures (Feb. 2024)
2. Cryptoasset Roadmap, Financial Conduct Authority (03 February 2024)
3. Mansion House 2024 Speech, UK Government (14 Nov. 2024)

INTRODUCTION

The UK as a Base for distributed ledger Technology, Tokenisation and Fintech
(Aleksandra Wawrzyszczuk - LawtechUK and New York University)

In 2024, there is a notable momentum building in the race for legal dominance over digitised markets, including financial services operating digital assets.

When it comes to internationally mobile transactions, digital assets are certainly leading the pack. For a borderless technology, with an eye-watering market size (revenue in the US alone in 2023 is projected US $\$ 60,150.0 \mathrm{~m}),{ }^4$ it is unsurprising that the race for jurisdictional supremacy only accelerated with the widening adoption of the technology. For example, in digital capital markets, continental European jurisdictions eagerly stepped in with legislation governing digital securities, or transactions of issuance of debt or equity on blockchain (and DLT) to establish a 'desirable' legal framework. In addition to EU-wide efforts, culminating in larger frameworks such as Regulation (EU) 2023/1114 on Markets in Crypto-Assets ("MiCA"), some individual member states took more targeted action at varying levels of granularity. The willingness to "get ahead' led France to legislate on the matter of digital securities so early in the day (2019) that it has already needed to update its PACTE Act for 2023.

Legislation is not the only way forward, however. English law may already provide the necessary tools to address most of the challenges arising in industries utilising digital assets. It successfully accommodates new technology and business innovations by incrementally developing doctrines grounded in established general rules. Thanks to the breadth and depth of its doctrinal backing. English law is highly portable: it has already been adopted as governing law in crossborder and global transactions in many contexts, ranging from maritime law to capital markets.

In order to promote the message that English law serves digital business, the UK's Ministry of Justice established the UK Jurisdiction Taskforce (UKJT) to focus specifically on promoting English law and the UK jurisdictions for the digital economy. Chaired by Master of the Rolls, Head of Civil Justice in England and Wales, and a vocal advocate for common law, Sir Geoffrey Vos, the Taskforce coalesces a multinational community to provide clarity on legal controversies under English law.

The UK Jurisdiction Taskforce describes itself as 'an industry-led initiative, tasked with promoting the use of English law and UK's jurisdictions for technology and digital innovation: ${ }^5$ It houses representatives from the Financial Conduct Authority, City of London Corporation and, importantly, the Law Commission, as well as senior practitioners and judges. Its objective, broadly speaking, is to clarify the legal position of digital assets under English law and promote the UK's jurisdictions for digital economy. The Taskforce already publishes so-called 'authoritative legal statements' that seem to perform the functions that the Law Commission wishes to delegate to the prospective panel. The purpose of those statements is also to provide

market assurance of English law's clarity, clarifying key technical issues arising in the industry, and how the English law should respond to them. ${ }^6$ Unlike the Law Commission. however, it does not make recommendations for future law reform: instead, it simply analyses the existing laws and explains them to the market.
${ }^4$ Digital Assets - Worldwide, Statista Market Forecast, (July 2024)
${ }^5$ UK Jurisdiction Taskforce (UKJT) Home, LawtechUK (Nov. 2023)
${ }^{\circ}$ High Court endorses UK.JT Legal Statement and proprietary status of cryptoassets, Linklaters (May 17, 2001).

What underpins the Taskforce's mission is the assumption that legal clarity and certainty is good for business, and English law (or common law in general) is perfectly capable of providing not only flexibility but also security of outcomes. It is hard to disagree with the assets and research that the Taskforce has produced to further its agenda. The legal statements are a result of extensive public and private consultations, drafted collectively by a team consisting of senior experts in a given area, in close dialogue with the Law Commission, with whose projects the Taskforce's work is vastly complementary. Undeniably, the Taskforce, which includes former Law Commissioner Sarah Green, has been a helpful testing bed for the Commission's intuitions. For example, the Legal Statement on Cryptoassets and Smart Contracts first suggested the creation of a new category of property of digital assets back in 2019.

But the power of the UKJT is in its judicial endorsement, which helps raise its authority among the courts and legal practitioners. If a statement receives a stamp of approval from the second most senior judge in the country, it is likely that other members of the judiciary will be more confident to adopt it. For example, the findings of the UKJT's Legal Statement on Cryptoassets and Smart Contracts were endorsed by the commercial division of the High Court in AA $\checkmark$ Persons Unknown, ${ }^7$ a case deciding the point whether Bitcoin (BTC) could be considered as property for the purposes of granting a proprietary injunction over Bitcoin. The opinion specifically cited the statement as well as specific points from its analysis of the nature of cryptoassets, further affirming the reasoning from B2C2 v Quoine, ${ }^8$ one of the first cases to apply common law of contracts and torts to cryptocurrency trading. ${ }^9$

The same rings true in a non-contentious context. Following the UKJT's publication of research on the Economic Value of Digital Securities, ${ }^{10}$ accompanied by the Legal Statement on Digital Securities" earlier this year, we witnessed the establishment and launch of Euroclear's Digital Financial Market Infrastructure.
the first central securities depository capable of handling English law securities, followed by the inaugural digital securities issuance by the World Bank under English law. ${ }^{12}$ Granted that Euroclear was represented by Linklaters, who are actively involved in the Taskforce, but the signal that this successful transaction sends to the market is immense.

The Taskforce complements the strategic vision of the Law Commission, which has done enormous amounts of work to demonstrate the value of English law as a leading jurisdiction for digital assets. Since November 2021, it has announced five projects in emerging technologies:

three reviews (digital assets, smart contracts and electronic trade documents) have been concluded, and two (conflict of laws and DAOs) are due to be delivered shortly. ${ }^{13}$ The comprehensive programme of work sends a strong signal to the market that the UK is as serious about capturing tech as it has been about traditional financial services.

Various projects across the market consistently highlight that English law:

- provides sufficient assurance to the market to instill confidence in outcomes: 'if you do x. y will happen.'
- offers sufficient flexibility to accommodate novel scenarios (reasonable management of expectations ex ante, not ex post) without compromising predictability (rules do not change haphazardly without good cause).
- if a regulatory response is required, it is always timely: as agile as technology that drives the market.
- is cheap and straightforward to comply with, eliminating any negative impact on new or potential market entrants.
- is aligned with business objectives and incentives of market participants who generate value to the economy.
- underpins the legal system, including the courts, which demonstrates deep institutional understanding of:
- technology and its potential future:
- finance and its potential future.
- exemplifies portability, facilitating multi-jurisdictional transactions and borderless application of uniform rules.
- tech-neutral and capable of guiding business activities irrespective of changing technology.

'AA v. Persons Unknown [2019] EWHC 3656 (Comm) (17 January 2020)
"B2C2 Ltd v Quoine Pte Ltd [2019] SGHCi0 3
${ }^9$ id
${ }^D$ English law and Digital Securities. Oxera x LawtechUK (Feb. 2023)
"Legal Statement on the Issuance and Transfer of Digital Securities, LawtechUK (Feb. 2023)
프 Citi acts as first Issuing and Paying Agent for World Bank on Euroclear's new D-FMI DLT platform. City. (Oct. 24, 2023);
Linklaters advises Euroclear Bank on the establishment and launch of its new Digital Securities Platform, and Euroclear Bank
and TD Securities on the inaugural digital securities issuance by the World Bank, Linklaters (Oct. 24. 2023)
${ }^{15}$ Law Commission to review how private international law applies to digital assets and other emerging technology. Law Commission (Oct. 18, 2022)

Overall, the ongoing mission to inject confidence in the English legal system within the digital assets community is beginning to show early signs of success. While it may still ring true to some that English law requires a more nuanced calculation of commercial risk than legislation, a savvy lawyer will recognise the generally sensible attitude towards digital assets from both the Law Commission and the political, legal and business community. They also tend to appreciate that English law's flexibility makes it generally more permissive towards creativity within bounds of common sense.

QUICK TAKEAWAYS FROM THIS GUIDE

If you are in a hurry and would like a quick digest of this guide, here are some of our top takeaways from the different contributors' sections:

Tokens require thoughtful design, and must be a critical component of their ecosystem. In the chapter on 'Tokenomics' (Mo Ezeldin), you can read about the importance of sustainable token economies for long-term success of your project

"If your business model involves dealing with TradFi firms or products, you will need to understand how the current system operates and work within it." To find out how, see 'Tokenisation' (Charles Kerrigan)

From James Burnie and Pavan Kaur at Gunner Cooke / WAGMI in the section on 'Token Launch':

There are some quick easy wins in terms of being able to sell into the UK. For example, classical non-fungible tokens (NFTs) sold into the UK from abroad are often unregulated.

As regulation increases globally. it is becoming increasingly important to factor in how compliance will be ensured using a cost-effective route appropriate for the project.

In order for a project to be successful, a more than purely legal approach needs to be taken. Participants have expectations regarding token launches and so using an experienced Web3 CMO to navigate these will help ensure the success of the token launch.

Poorly drafted Token Warrants can often lead to issues for a project, including oversupply of tokens > See "What is a Token Warrant" (Anne Rose and Callum Blundell) for more tips on how to avoid pitfalls

Data governance and security are an important way to build compliance into your product from the get-go > for checklists and suggestions of where to start, see 'Product, Data and Compliance by Design' (Derya Karli and Lisa McClory)

Contracts need to go digital in order to be fit for the Web3 era: but what does this mean for lawyers? Read 'Computable Contracts' (Akber Datoo)

Building a project, sure, but building a legal architecture? How should you plan that? > Read 'Navigating Legal Architectures: Building your Web3 Project on Solana in the UK' (Marcus Bagnall)

"If truly decentralised decision-making power is to be achieved or retained, significant thought should be given as to how best to guard against this sort of concentration of voting power" > Read "Decentralised Autonomous Organisations" (Professor Sarah Green) on some key English legal factors to consider when building DAOs

The Cayman Foundation is a popular offshore structure for DAOs, including operating a fully decentralised DEX > In 'Exploring Offshore Jurisdictions: Things to Think about" (Sara Hall), you can read about the importance of assessing the legal and regulatory status of the DAO's interactions with onshore users and other important things to bear in mind

- Can you automate compliance through technical standards? In 'DAO Legal and Tax Standards' (Joni Pirovich of DAOstar,) there is an introduction to the tools available to DAOs for data standardisation, allowing better interoperability with traditional legal and tax reporting frameworks
- Many projects think about financial regulation, but what about gambling regulation? > In 'Web3 Games' (Omri Bouton), we break out the main things to consider regarding Web3 Games, gambling regulation, loot boxes and more
- Great SocialFi doesn't just happen, it needs careful planning to provide a good experience for users > read top tips for projects in 'Boosting Organic Growth with SocialFi' (Ian Cox)
- How does DePIN differ from a traditional cloud computing arrangement? > The chapter on DePIN cloud infrastructure agreements (Morgan Lewis) discusses how to balance contractual terms with DePIN customers and nodes, whilst providing adequate contractual protections for the DePIN operator
- The lack of specificity over the application of law and regulation in a decentralised context poses many challenges for DeFi projects > in 'Practical Guidance for DeFi Developers', read Maria Riivari for an overview and some key practical considerations for DeFi projects when managing decentralised compliance
- When do you need to get a licence for crypto activities, and when are sanctions laws a concern? > Read Leon Hurd of Cybersandbox and Keystone Law in 'Setting up for Success (Risk Mitigation)'
- Tax administrations globally are increasing their efforts to ensure that the correct tax is paid, including HMRC recently sending "nudge letters" to review potentially undeclared tax liabilities. As information on ownership of cryptoassets continues to grow, proactive compliance is an area of importance for all project founders. In 'Tax and Accounting' (Dion Seymour) you can find a general overview and key guidance, whilst 'The 5 W's' (Mark Pearce) takes you through five 'who, what and where' questions with respect to tax and accounting factors
- The UK's new rules extending regulation of financial promotions to cryptoassets took effect in October 2023. A helpful overview is provided by Andrew Maguire in 'UK Regulation of Financial Promotions of Cryptoassets'
- How can you recover stolen cryptoassets, and what are the most important first steps to take? > In 'Tracing, Freezing and Recovery', Matt Green and Marcin Zarakowski give an overview of cryptoasset tracing and the steps involved in recovering stolen assets in the event of a hack, theft or loss.

PRODUCT DESIGN AND PLANNING CHAPTER 01
Tokenomics: Designing a Product that Powers Ecosystems and Empowers Holders (Mohamed Ezeldin - Animoca Brands)

Tokens are not just tools for governance or fundraising-they are products in their own right. Like any product, they require a suite of complementary systems to sustain them, along with thoughtful design to ensure usability, engagement, and longevity. Founders must treat tokenomics as a critical component of the ecosystem, where both the token and the surrounding products are meticulously designed to enhance user experience and value.

The Token as a Product

When thinking of tokens as products, their success hinges on three core principles:
1. Purpose and Utility:

The token must serve a clear purpose within the ecosystem. Whether it's enabling governance, incentivising user engagement, or unlocking features, the token's value is derived from its utility. A token without utility risks becoming a speculative asset, detached from the ecosystem's core goals.
2. Supporting Ecosystem:

A token cannot exist in isolation. To thrive, it requires an ecosystem of products and services that provide continuous use cases. For example:
- Gaming Ecosystems: A game token might enable ingame purchases, facilitate trading, or provide access to exclusive content.
- Governance Ecosystems: Governance tokens must be paired with robust decision-making platforms and tools for transparency.
- DeFi Ecosystems: DeFi tokens should integrate with yield strategies, staking, and liquidity provision mechanisms to retain engagement.

3. Lifecycle Management:

Like any product, tokens go through a lifecycle. Founders must plan for the long-term evolution of the token. ensuring mechanisms like staking, lockups, and deflationary pressures align with the project's growth trajectory.

Web2 vs. Web3 UX: Designing for Two Worlds

Web2 and Web3 audiences bring fundamentally different expectations to the table. In Web2, the focus is on seamless. infuitive user interfaces with minimal cognitive load. In Web3, the experience is often more technical, requiring familiarity with wallets, tokens, and smart contracts.
1. Different UX Priorities:
- Web2 UX: Prioritises simplicity, reducing barriers to entry. Users expect experiences like one-click logins, clear navigation, and customer support.
- Web3 UX: Often appeals to tech-savvy, early adopters who are comfortable with concepts like self-custody and gas fees. This audience values transparency and sovereignty over convenience.

2. Bridging the Divide:

Founders must design products that cater to both audiences. In the short term, most token interactions will be dominated by Web3-native users, but as adoption grows, Web2-style interfaces can help onboard a broader audience. Hybrid approaches, like abstracting wallet management or offering fiat onramps, can reduce friction for Web2 users while maintaining Web3 functionality.

Community Dynamics and Expectations

Tokens are deeply tied to their communities, especially in the early stages of a project. Founders must recognize and design for the inherent expectations of Web3-savvy users, who often see participation as an entitlement to rewards.

1. Reward Culture:

- Incentives: Web3 users expect tangible rewards for their participation, whether through staking, governance, or contributing to the ecosystem.
- Engagement Models: Successful projects incorporate gamification and social recognition to reinforce participation, ensuring users feel both rewarded and valued.

2. Feedback Loops:

Tokens thrive on active and engaged communities. Mechanisms like governance votes, leaderboards, and airdrops can create virtuous cycles, where participation begets more engagement, which in turn strengthens the ecosystem.

3. Short-Term and Long-Term Alignment:

Web3 communities often emphasize short-term rewards, but founders must balance this with the project's longterm vision. Strategies like vested rewards, fee-sharing models, and progressive token unlocks can align shortterm engagement with sustainable growth.

Legal and Practical Considerations

When building tokens as products and integrating them into a dual-audience ecosystem, several key legal and practical factors must be addressed:

1. Interoperability:

Building ecosystems where Web2 and Web3 products coexist requires interoperable infrastructure. Leveraging standards like ERC-20/721 for Web3 and APIs for Web2 integration ensures seamless interaction.

2. Scalability:

Projects must anticipate the demands of scaling from Web3-savvy users to broader audiences. This includes integrating Layer 2 solutions, optimising transaction costs, and ensuring UX scalability.

3. Compliance and Regulation:

Tokens as products must still comply with UK (and global) laws and regulations, including financial promotions and AML/KYC requirements. Founders should design incentives that align with legal constraints while remaining attractive to users. For more on rules, compliance and regulation in the context of token projects, please read on after 'The Bottom Line'.

The Bottom Line

Treating your token as a standalone product ensures it is more than just a speculative asset. By designing thoughtful ecosystems, balancing UX across Web2 and Web3, and catering to community dynamics, founders can build sustainable token economies that attract users, drive engagement, foster long-term success and are legally compliant.

Tokenisation

(Charles Kerrigan - CMS; RAK DAO)

The first question might be: why do a token?
A response is perhaps: 'To raise capital!'
For reasons we explain, however, this is not a good answer.
The reality is not as simple as some might think.

This is muddied by the fact that many 2017 ICOs did, in fact, issue tokens and raise capital. Perhaps the best way of thinking about this is that it is not so simple anymore. Sometimes the first people who break some rules can do so because regulators are not looking in their direction. Once rules are broken though, regulators definitely are looking in that direction.

As with everything in crypto, we have to start with some definitions. Tokenisation means different things to different people. So, the first thing you have to be clear on in your project is what you mean by tokenisation.

Tokenisation is one of the ways we see the difference between crypto and traditional finance (TradFi).

In TradFi, a token is a digital representation of a financial instrument of some sort. It could be a stock or a bond or other debt instrument. It could be cash. It could be an alternative asset like wine or physical art. But current market practice is to issue the stock or bond or whatever, then create an onchain digital representation of it. The point is that the way TradFi currently understands tokenisation is as a wrapper around an existing product and process. This is the story of the hugely successful BTC ETFs from the beginning of 2024. They demonstrated investor appetite for BTC, not through investors buying BTC direct or through exchanges, but by getting exposure to BTC through a traditional financial product, an ETF that owned BTC.

If your business model involves dealing with TradFi firms or products, you will need to understand how the current system operates and work within it. You can find information on this by searching - Tokenisation + Investment Association.

A final few points before we move on to how this works if you are building outside the current financial system.

If you want to have TradFi firms as investors, partners, or customers for anything:
- you will need a legal opinion confirming if you are inside or outside the regulatory perimeter - i.e. if you need a licence from a financial regulator to do what you're doing;
- you will need to be incorporated in a jurisdiction that has a good reputation for regulation - many UK financial institutions have a strong preference to deal with UK based fintechs;
- you will need enough capital to be able to survive a long process of answering questions from different stakeholders.

That covers enough on tokens and business models that are inside the current financial system.

In crypto native conversation a token can refer to a number of things.

A token can simply be a message or instruction between computers. That is not what people think of as tokenisation. Tokens of this type are not recognised by the legal systems as assets. They generally therefore do not have value because they have no existence beyond the sending of the message.

So, when we talk about tokens, we are generally talking about tokens that have value or utility on a blockchain. Tokens of this type can be recognised by legal systems as assets.

This distinction is important because it goes to the question of whether a token is suitable for fundraising or not.

If fundraising is a primary use case for your token, it will trigger rules relating to securities issuance. This is why the argument about whether a token is or isn't a security is so significant. A token that is a security must be issued in accordance with securities rules and regulations. These differ jurisdiction by jurisdiction but they all have some common features. Regulators would refer to these features as relating to investor protection and market integrity.

Investor protection centres on things like making full and fair disclosures of all relevant information. Relevant information means details of the issuer, the issuer's business model, the terms of the tokens (securities), risk factors etc. Traditional forms of whitepapers are not "MiCA compliant", so there are no good precedents for new projects to use now.

In fact, recent regulation is designed to harmonise rules relating to securities and unregulated tokens to remove the ability for issuers to arbitrage between the rules. The recent European rules you will have heard referred to as MiCA essentially read across to tokens the equivalent rules that already apply to securities. A MiCA-compliant whitepaper will look more like an IPO prospectus than a traditional whitepaper for a token.

Market integrity centres on things like restrictions on frontrunning. trading on inside information, manipulating prices or order flow, and anything else that puts some investors in before worse position than others. The worst offence is for the team to make money from inside information. That is usually illegal. It also kills projects because it destroys trust.

Crypto lawyers spend a lot of time analysing the rules that classify tokens. A token that gives a holder rights like those that a shareholder in a company would get will be a security. A token that does not have those rights will not and will therefore not be subject to securities regulations. If proceeds of a token issuance will be used to furd the costs of the company that issues the token, or if the investor is buying the token to get a return, these are indications that the token is a security. Remember how different BTC is to this - no issuer, no promises, no controller beyond the community. Its value comes only from its hard-capped scarcity.

The short point here is that taking in money from a thirdparty investor is one of the most serious things that a business or project can do in the eyes of regulators so there are high barriers to entry. Broadly, third party money is an investment (in shares or tokens) made by a person who is not personally known to you. Regulators care about this for the reasons set out above, summarised as: you might lose the investors their money.

By this they mean that you might literally lose it because you get hacked through not having spent enough time or money on security, or you might misspend it, use it as your own, or any number of other problems. Regulators also care about preventing financial crime. If you take investment from a criminal, then you may be holding the proceeds of crime. Holding proceeds of crime is an offence. Returning them is money laundering. Some of these rules exist to save inexperienced projects from themselves. If you are not used to handling other people's money, you need to do a lot of work understanding your responsibilities before you do so.

The analysis so far focused on securities because those are the rules made famous by Gary Gensler. Alongside them there are similar rules and requirements for projects that pool capital. In the UK these rules require "collective investment schemes" to be licensed. In Europe, they require fund vehicles to be licensed.

The rules differ in specifics by jurisdiction but the themes are the same. In practice, this means that most tokens are now launched in core markets only initially. then expansion follows as the project scales and has the bandwidth and funds to get sign off for other countries.

There are now other ways in which you are kept on the straight and narrow. Now that CEXs are subject to strict money laundering rules and have regulators checking that they are not securities exchanges without a licence, if you want to list your token on an exchange (which investors will want for the liquidity), the exchange will also check that the token isn't a security. Investors often now also ask for the same analysis and assurance. In practice, cutting a corner by launching a token that is in breach of some regulation limits your project's ability to scale - when serious investors arrive, they do checks and find the flaw and it's a problem then.

This all means that there is some time and trouble now involved in a token issuance that is for building. The most common way in the UK now is for a project to take in equity from angels or VCs and use that for building, but also have a token in their roadmap and issue a token warrant (a right for early investors to take tokens when they are issued) to the equity investors. The token follows the set up and build.

This way also solves the other main issue that applies with token issuances in the UK now. The UK regulator has limited the ability to market tokens, including on social media. If you can't tell people about your token, you can't get liquidity or trading. These rules are called the financial promotions rules, and they are explained elsewhere in this guide.

So, what does that leave as options for tokenisation for earlystage firms?

You can tokenise the equity in a UK company without too much trouble. Rules on secondary trading of securities mean that this on its own doesn't make a market. But, sometimes projects do that to show their credentials as crypto projects.

You can be a true L1 blockchain, where the Bitcoin analysis above applies. Your token could be for security and network validation. But BTC took a long time to be valuable. And a Bitcoin fork isn't valuable these days.

You can go for "sufficient decentralisation" but that takes scale and money. Even well-known DeFi projects can have relatively few large token holders and relatively few validators. If a regulator sees this, they will argue the project is not decentralised.

You can do a pure utility token. That means not raising capital but giving features or services. As we say above, this doesn't have to be at the very start of the project.

You can do a governance token. This could be a way to engage with your community. But you need to be careful that you don't mix up governance rights that shareholders have in your company, governance over, say, technical features of your codebase.

You can do your own design of a utility token. There are some that are effectively loyalty programs, but they capture community and engagement without promising mooning returns. Some of those have then been expanded and changed to share value, but only when the project has the money and experience to handle the responsibilities that come with that.

Top crypto investors like tokens. They think they are where the value will accrue in the best projects. But they are hard to impress on tech and even harder on tokenomics. You need a true "category creation" project to win with them. So, work on your plans for tokenisation but know that tokens aren't the easy option, and they certainly aren't now free money.

What is a Token Warrant?
(Anne Rose and Callum Blundell - Mishcon de Reya)

A Token Warrant functions as a promise that gives the holder the right, but not the obligation, to purchase a set number of digital tokens at a later date, for a price that's decided upfront. The price is fixed in advance, so if the tokens do well and their value goes up, you could bag a bargain! They work in a similar way but there are key differences that set them apart from traditional derivatives, like stock warrants.

Token Warrants usually pop up when a new blockchain project is getting off the ground. When a company has an exciting new idea and starts putting it together, but before everything is up and running, it might offer token warrants to hype up potential investors and raise some cash. Token Warrants should not be confused with token incentive schemes but may be offered to team members as well as investors.

The Importance of Heads of Terms
As with any part of a funding round, it is extremely important for the company and investor(s) to work together at the outset to agree the heads of terms for the deal and, as part of that, ensure they don't overlook the terms of any Token Warrant to be issued. For example, agreeing a clear definition of "Portion" (as discussed in more detail below) from the beginning should ensure negotiations on the terms of the Token Warrant go much more smoothly.

We often find Token Warrants are sidelined in the context of larger equity or debt financing rounds, meaning important provisions regarding Token Warrants are left out when drafting heads of terms.

This can have unintended consequences for the company, for example, drafting the definition of "Portion" too widely can lead to an oversupply of tokens which pushes down the token's value.

Top Tips:
Defining the Portion of tokens that an investor is allocated - the investor friendly approach is for the investor's allocation of any given token (Portion) to be defined as a fixed percentage of the total number of tokens created. This is often set at the same percentage as the investor's equity ownership in the company at the time of an investment round. The key consideration here for the company is that future investors may demand the same treatment as early investors / token warrant holders and communities may also have a negative perception of a project with tokens heavily allocated to investors early on, which can therefore impact future funding rounds.

The more company friendly compromise would be for the Portion of token allocation to reflect the pro rata proportion of the investor's equity ownership in the company at the time of a token launch / generation event (which could be a lower percentage than if a fixed percentage is agreed to at the time of entering into the token warrant instead).

The definition of "Portion" will usually include a further definition of "Pro Rata Share" reflecting the percentage of the investor's equity ownership in the company. Be wary that where an investor has an unexercised stock warrant at the time of a token launch / generation event (and the Pro Rata Share is based on the investor's fully diluted equity ownership), this should not artificially increase the Pro Rata Share of the investor's Portion of tokens allocated. The rationale for this is that the investor may decide to never exercise the equity warrant!

Check the definition of "Excluded Tokens" - as well as a definition of "Tokens", heads of terms should define "Excluded Tokens" for example. tokens issued for development, testing or experimental purposes or pursuant to activities like staking (earning rewards by validating transactions on the blockchain), rewards or inflationary or dilutive controls.

There is no benefit to an investor being issued these types of tokens and failing to exclude them could have unwanted consequences.

Reduce ambiguity - we often see references to intellectual property and material intellectual property, but these terms should be properly defined to avoid any ambiguity. It should also be abundantly clear how certain processes, such as the service of notices, are triggered.

Lockup Provisions - companies typically want to restrict the transfer of tokens acquired under token warrants for a certain period after the token launch. For example, a lockup schedule preventing any transfers for 12 months after the token launch date, releasing 50\% of tokens from the oneyear mark then a gradual release of the remaining balance over the next year or two. Lockups can encourage cooperation between token holders, allow the broader community a fair chance to snap up popular tokens, and can include additional transfer restrictions to manage compliance risks and regulatory requirements.

Most Favoured Nations Clause - a Most Favoured Nation (MFN) clause is a provision often argued for by investors and sometimes included in Token Warrants to ensure that the investor receives equal treatment to that given to future investors. In essence, if the company grants a future investor a Token Warrant with better terms, benefits, or privileges, for example a less restrictive lockup, these must also then be extended to the earlier investor that is subject to the MFN clause.

An MFN clause is market practice in the USA, if a bit aggressive, but in the UK we have seen companies successfully push back on an MFN clause so this should ideally be ironed out at the heads of terms stage to prevent investors sneaking it into the initial (or subsequent) drafts of the Token Warrant.

Custodians - many investors will be keen to include a provision that, following any token launch / generation event (TGE), the company will partner with a high-quality custodian (a third-party which looks after the tokens) which will accept and support the tokens with secure wallet and storage services promptly following such distribution. The company should only agree to use commercially reasonable efforts in such a scenario, as otherwise it runs the risk of being strongarmed into partnering with a custodian on unfavourable terms.

Dispute Resolution - we have found that dispute resolution provisions, which enable the parties to escalate disputes to arbitration, are not as common in Token Warrants as they ought to be. While such provisions shouldn't prevent the parties from taking a dispute to court entirely (for example, claims for injunctive or equitable relief and claims relating to intellectual property rights should be reserved for the court's jurisdiction) it's often advisable, if the company is open to the alternative. to include a dispute resolution clause rather than confining the parties to pursuing claims through the courts only.

Product, Data and Compliance-by-Design (Derya Karli - Own Protocol and Lisa McClory - D2 Legal Technology)

"Compliance is your responsibility. If we find inadequate controls in your firm, we may take action against you." UK Financial Conduct Authority

Data is a vital force for Web3 applications! It performs many important tasks, including triggering smart contract functions, allowing access to permissioned resources, providing connections and information, underpinning decentralised proof of trustworthiness, identity, ownership and more.

When building a Web3 application, you are effectively building a home for all the data that will one day live within your app, and this can be a complex area with nuanced trade-offs to take into account, technical standards and legal requirements, all against a shifting backdrop of cyber risk factors. You may need to think carefully about your house's rooms and facilities to cater properly to the needs of its inhabitants!

By thinking about data governance and compliance right from the start of your product design phase, you avoid having to rewind and do an expensive rebuild when an appstore or regulator later imposes requirements. Planning around data law and security requirements also helps you to manage compliance costs later in your project.

Why is Data Security and Governance Important in a Web3 Context?

Web3 applications often act as store or record of value and may perform important functions relating to the allocation of resources or project governance. Data breach and exploitation of security flaws can result in a particularly heightened risk of financial losses, or potentially expose people to severe risks of scams, theft and identity fraud.

Due to the nature of Web3 often involving novel and innovative use of emerging technologies, whilst also pushing the boundaries of what is possible when enabling collaboration and shared networks, there are heightened security and data breach risks.

The FCA recently surveyed

consumer attitudes and behaviours towards crypto, finding that consumer awareness is now up to

, and only 1 in 10 people failed to do research before buying cryptoassets. Consumers care about security and data, as do regulators, and it is highly important that your product is built on solid foundations of good data governance practices.

Data Governance

Good data governance is an essential starting point for any robust, reliable and trustworthy product.

It is an approach to managing the availability, usability, integrity, and security of data, including establishment of policies, procedures, and standards that ensure data is properly handled throughout its lifecycle. Good data governance can not only protect against risks, but will also help to streamline operations and enable better use of automation, better scalability, and lower costs of data storage: all very important factors to get right from the outset of your project.

Effective data governance is therefore highly important to all Web3 projects and should be something that developers consider throughout the project lifecycle. Projects should define clear roles for data management, implement data classification and access controls, and ensure consistent practices.

A solid working knowledge of data law, data ethics and security best practices is important because:

- this is a regulatory obligation under the General Data Protection Regulation in the EU and the UK;
- actively embedding good data governance and security standards, including responsible data practices, will help you to build a secure and robust product, bringing good value to your ecosystem and community.

Training employees on these standards is also essential, as their understanding directly impacts an organisation's ability to safeguard sensitive information. Ultimately, robust data governance enhances informed decision-making, improves efficiency, and builds customer trust by demonstrating a commitment to security and privacy.

Types of Data

There is a key distinction between personal data and other more general kinds of data or information.

Personal data requires particular attention because data laws, such as the EU and UK General Data Protection Regulation (EU) 2016/679 provide individuals with legal protection whenever their personal data is processed. These regulations reflect the fundamental human right to privacy enshrined in human rights treaties, such as the Universal Declaration of Human Rights.

Personal data is any information that directly or indirectly identifies or relates to a natural person, including where it is an identifier that identifies a person only indirectly, or when aggregated with other pieces of information. It can include a wide range of information and generally requires special protection, e.g. name, personal ID records, user location details and so on.

EU and UK GDPR are presently pretty much the same (at the time of writing), as the UK retained a frozen version of the EU GDPR following the UK's exit from the European Union (the transition period ended on 31 December 2020). Alongside the UK GDPR, the Data Protection Act 1998 still applies in the UK, but is essentially only relevant for law enforcement and intelligence services.

As the UK is no longer in the EU, the UK's approach to data law is currently under review and a new Data Protection and Digital Information Bill ${ }^{15}$ is being proposed. This Bill will clarify and make provision for several important areas of the digital economic environment, such as electronic signatures and digital authentication, oversight of biometric data and general rules about privacy of electronic communications. These new requirements will be relevant to Web3 businesses in any number of areas.

General Data Protection Regulation

Data protection law is centred around certain core principles which seek to ensure that personal data is processed lawfully. fairly and in a transparent manner. The principles are:
- lawfulness, fairness and transparency: a general principle that organisations usually manage by creating data policies with disclosures of processing activities to people whose data is processed, and by documenting decisions around whether activities involving data are fair and lawful;
- purpose limitation: collection and processing for specified, explicit and legitimate purposes, e.g. not collecting data for one reason, and then using it for something very different and unexpected;
- data minimisation: ensuring that data is adequate, relevant and limited to what is necessary for the purposes of its processing;
- accuracy: taking every reasonable step to keep data accurate and up-to-date and deleting or rectifying any errors without delay:
- storage limitation: ensuring data is held for no longer than is necessary. Relatedly, individuals also have a legal right to request the erasure of their personal data (a 'right to be forgotten'). and in some circumstances to withdraw their consent to processing;
- integrity and confidentiality: data must be collected and processed, stored and processed securely, ensuring appropriate safeguards against accidental loss, destruction or damage.

Transparency is one of the key features of Web3 technology. This is useful because it allows people to access information directly, without relying on intermediaries, and also because it is possible to trace and recover assets in the event there is a theft or a fraud. However, this transparency is also a challenge for many Web3 projects when seeking to get the right approach to privacy and user safety. Where personal data is concerned, the notion of storing data permanently onchain, where it can be accessed openly by any node or person reviewing

15Data Protection and Digital Information Bill, UK Parliament (23 September 2024) the ledger through a block explorer app, is very difficult to reconcile with data laws, including the principle of data minimisation.

Article 25 GDPR sets out the obligation of data protection by design. This requires data controllers to implement appropriate organisational and technical measures to implement the data protection principles, including data minimisation, in an effective way, as well as integrating safeguards that meet data law requirements. This obligation applies both at the outset, when determining how data will be processed, and later at any time when data is actually being processed.

This requirement is to be interpreted in the circumstances of each type of processing. and must take into account:
- the state of the art;
- the cost of implementation:
- the nature, scope, context and purposes of data processing; and
- the risks of varying likelihood and severity for rights and freedoms of natural persons by the processing.

Article 32 GDPR also sets out specific expectations for security of data processing. This includes requirements for the pseudonymisation and encryption of personal data, as well as processes for the regular testing and evaluation of technical and organisational security measures. ${ }^{16}$ This requirement under GDPR applies alongside other network and information security obligations applicable to certain digital service providers, including online marketplaces, online search engines and cloud computing services under the Network and Information Systems Regulations 2018.
${ }^{16}$ Data Protection and Digital Information Bill (23 September 2024)

Key things to consider where your product will process personal data:
\begin{tabular}{|l|l}
\hline \begin{tabular}{l}
Data controllers must register \\
with the ICO
\end{tabular} & \begin{tabular}{l}
There is a small fee to pay and the form is easy to complete online. Details are \\
available on the ICO's website."
\end{tabular} \\
\hline
\end{tabular}

Legal obligations apply to controllers and processors of personal data, each having a different role and responsibility. This includes specific compliance steps, such as preparing a Data Protection Impact Assessment.

Decentralisation and data governance?

Be especially careful of sensitive personal data

Data protection by design and security are highly important

Ethical practices are important too

In the context of decentralised organisations, it can be difficult to define who has the role of controller or processor, and individuals may not have an easy way to establish how their data is stored, who is responsible for data governance, or where they can direct a query in the event there is any issue. Making adequate provision for data governance and security within an app's design and build is a helpful way to resolve ambiguities and prevent problems and disputes from arising.

GDPR provides particular protection to special categories of personal data which are particularly sensitive. Special category data relates to: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Processing of this type of data is only permitted under limited circumstances and you should be especially careful to consider your legal obligations where dealing with any special category data.

GDPR requires all data controllers to design their systems and processes for compliance with data protection principles.

There are specific security requirements under GDPR and this is a big part of ensuring compliance. You can find a security checklist ${ }^{18}$ on the UK ICO's website as a starting point, but this is a highly important area and requires detailed, specialist attention. You should seek professional support as required.

By associating data about wallet owners from onchain and offchain digital sources, it is possible for any third party to acquire a great deal of information about a person, their online activity and assets they hold.

Even if your app does not directly hold personal data, take care to think about the safety of users and put in place best practice measures to safeguard user data.

Artificial Intelligence Regulation

Increasingly, blockchain applications are using AI agents for smart contract execution and algorithmic trading, amongst other purposes. Developers should also be aware that new AI regulations are gradually emerging, including the EU AI Act (Regulation (EU) 2024/1689), which came into force on 1 August 2024. The AI Act creates a comprehensive framework to regulate AI systems across the EU, and also has some extra-territorial effect, e.g. where an AI system's output is used in the EU.

Where it applies, the EU AI Act will prohibit certain unacceptably high-risk AI practices, including - for example - systems that employ subliminal or purposefully manipulative or deceptive techniques with the objective or effect of materially distorting a person's behaviour in a way that is reasonably likely to cause them significant harm. Other systems are classified as high risk, including many uses of AI in a workplace setting, and some uses of biometric data. There is also a requirement to provide users with transparency that they are engaging with an AI system, where the AI system generates synthetic audio, image. video or text content (see Article 50 EU AI Act).

If your product uses AI in any area of your tech stack, ensure to check whether AI regulations may apply and take compliance steps accordingly.

Practical Data Governance through the Product Lifecycle

Web3 involves many different technologies, and the approach to data governance can vary depending on the technology involved. In this section, we cover some key things within different areas of the app build process that you need to think about from a data governance and compliance perspective.

When thinking about data governance in a Web3 context, it is helpful to be aware of the following key concepts:

```
\begin{tabular}{|l|l|}
\hline Data Classification: & \begin{tabular}{l}
Involves categorising data based on sensitivity and regulatory requirements, \\
including classification of personal data or Personal Identifiable Information \\
(PII), including online identifiers or identification numbers and other personal \\
information stored in any format, such as National Insurance records, \\
addresses, birthdates, family situations, banking information, and medical \\
histories.
\end{tabular} \\
\hline Transaction data: & \begin{tabular}{l}
Refers to users' activity across various services and accounts. This can include \\
the customer's transaction history, exchanges, withdrawals, transfers and \\
payments, including dates and amounts.
\end{tabular} \\
\hline The state of a smart contract & \begin{tabular}{l}
Refers to its current set of data and conditions at a specific point in time. This \\
includes the values of variables, balances, and any outcomes from \\
interactions with the contract. In essence, the state is a snapshot of the smart \\
```

contract's "memory" and how it behaves based on prior inputs and events.
\end{tabular} \\
\hline Analytics and metrics & \begin{tabular}{l}
Refer to the processes and tools used to measure, analyse, and interpret data \\
generated by systems, users, and transactions. These insights are used to \\
optimise performance, enhance decision-making, and monitor compliance \\
and security.
\end{tabular} \\
\hline System logs & \begin{tabular}{l}
Are records generated by software or hardware systems that document events, \\
operations, and activities within the system. In the context of blockchain and \\
crypto projects, system logs provide critical information about how dApps, \\
nodes, or blockchain platforms are functioning. These logs are essential for \\
debugging, auditing, and ensuring operational transparency.
\end{tabular} \\
\hline
\end{tabular}

Managing Product Data Flow

When designing an app, a key area to consider is the product's data flow. Overall, the aim should be to ensure data minimisation throughout the product's lifecycle, particularly where it relates to any personal data/PII.

Input data is a very important part of this, because you can encrypt data before it goes onchain and this will reduce your app's data footprint and save you a lot of compliance worries elsewhere in your project. Always hash data before putting it onchain, and ensure to use a secure hashing algorithm with adequate sources of randomness.

Transaction monitoring is not an obligatory thing to include. but it is really important for your product's internal controls. It will allow you to keep an eye on malicious or risk-related activity in your system and helps you manage risks.

Your product may require you to maintain oracle services. If so, this could be a lot of work. Consider using tools (e.g. chain.link) that help you manage data in a secure and compliant way. Think carefully about the additional work required to build your own oracle management solution and weigh up the costs and benefits associated.

There are three key areas to consider when thinking about data location:
- onchain data;
- offchain data;
- hybrid approaches.

Onchain Data

Onchain data is a cornerstone of blockchain systems, enabling transparency, security, and trustless operations. However, its costs and limitations demand thoughtful design. By strategically managing smart contract state, transaction history. and public attestations, and by carefully analysing the trade-offs of onchain storage, developers can build efficient, scalable, and compliant Web3 systems.

1. Smart Contract State

$\square$

Smart contract state represents the core variables and conditions stored on the blockchain, defining the functionality and outcomes of the contract. For example, a token contract's state might include user balances and supply limits, while a DeFi protocol might store collateral ratios and governance decisions.

To comply with data minimisation, developers should store only essential variables directly in the contract and offload non-critical data to offchain storage. Using event logs instead of state updates can significantly reduce gas costs while maintaining transparency, as events do not contribute to contract storage. Additionally, implementing robust access control mechanisms ensures that only authorised users or entities can modify sensitive state variables. Regular optimisation of smart contracts, such as batching multiple updates into a single transaction, can further reduce storage costs and improve scalability.

Transaction history encompasses a detailed, immutable record of all user activities, such as token transfers, staking operations, and smart contract interactions. While transaction history ensures traceability and accountability, developers must anonymise data to prevent exposing sensitive user information. Storing minimal metadata-such as transaction amounts, timestamps, and wallet addresses-rather than including personal identifiers or extraneous details is critical for compliance. Aggregating transaction data or summarising interactions can also help minimise storage requirements while maintaining verifiability. For example, rollups or batching mechanisms can summarise hundreds of transactions into a single onchain update, reducing costs and improving blockchain throughput. Cryptographic techniques like Merkle proofs or zero-knowledge proofs (ZKPs) can be employed to validate offchain transaction details onchain without compromising user privacy.

3. Public Attestations

Public attestations provide verifiable proof of actions, claims, or ownership recorded on the blockchain. Examples include identity verification, proof of ownership for NFTs. or certifications of data integrity. While public attestations enhance trust and transparency, they can inadvertently expose sensitive information. To align with data minimisation principles, developers should rely on hash-based attestations where only a cryptographic hash is stored onchain, and the underlying data is kept offchain. This approach ensures that the data remains verifiable without exposing its contents. Leveraging privacy-preserving technologies like ZKPs allows users to share selective information for verification without revealing unnecessary details.

Decentralised Identifiers (DIDs) and Verifiable Credentials are also effective solutions, enabling offchain storage of attestations while maintaining onchain verifiability.

4. Cost-Benefit Analysis of Onchain Storage

Storing data onchain provides immutability, transparency. and decentralisation but comes at a high cost, especially on networks like Ethereum. To minimise costs, developers should store only essential data directly onchain and use offchain systems like IPFS or Arweave for large or sensitive datasets. For example, instead of storing the metadata of an NFT directly onchain, developers can store a hash that points to its offchain location. Layer 2 scaling solutions like zkSync or Optimism are valuable for reducing storage costs by handling most data processing offchain and submitting only summarised data to Layer 1. Periodic data pruning can help archive outdated or inactive data offchain while retaining a root hash for future validation. When designing systems, evaluating lower-cost blockchains for less critical data storage can further optimise operations. Balancing these considerations ensures efficient use of onchain storage without compromising functionality or compliance.

- Private User Information

Storing personal data offchain is essential to comply with privacy regulations like GDPR and to sefeguard users from identity theft or breaches. To protect private user information, projects should use encrypted databases and ensure robust access control mechanisms. By offloading this data to secure storage, only references or hashed pointers to the data need to be stored onchain, maintaining compliance without compromising user privacy.

- KYC/AML Documentation

Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements necessitate the storage of detailed user verification documents, such as government-issued IDs or proof of address. Storing these large, sensitive data sets offchain reduces costs and prevents unnecessary exposure on the blockchain. Using decentralised identity frameworks, such as Decentralised Identifiers (DIDs). allows projects to store KYC/AML data securely offchain while enabling selective onchain verification for compliance checks without revealing sensitive information.

- Large Datasets

Blockchain systems are not designed to handle large datasets such as media files, logs, or complex analytical reports. Storing such data offchain on platforms like IPFS or Arweave reduces costs and ensures scalability. For example, an NFT project might store high-resolution images or videos on IPFS, while retaining only the IPFS hash onchain to link the data for verification.

- System Configuration

System configurations, such as application settings, network preferences, and smart contract deployment parameters, are better stored offchain for flexibility and security. This ensures that changes to configurations can be managed dynamically without requiring costly onchain

updates. Storing configuration files in secure, centralised systems or encrypted offchain databases is a practical solution for managing this type of data.
- Analytics and Reporting Data Analytical insights and reports, such as user behaviour metrics, transaction patterns, or performance logs, are typically too voluminous for onchain storage.

Projects can store these data sets offchain in dedicated data warehouses or analytic platforms like Google BigQuery or AWS Redshift. By integrating these fools with blockchain data, projects can perform advanced analytics and generate reports without burdening the blockchain's storage.

Hybrid Solutions

The following hybrid approaches can offer developers a choice when balancing different concerns of data privacy. vs security and efficiency:
- Merkle Proofs for Data Verification

Merkle proofs allow developers to verify offchain data integrity without storing the full dataset onchain. A Merkle tree generates a cryptographic root hash from multiple pieces of data, enabling verification of any single piece by comparing its hash to the root. For example, a supply chain dApp can store transactional data offchain while using Merkle proofs onchain to validate individual records.
- IPFS Integration Patterns

IPFS (InterPlanetary File System) is a decentralised file storage system ideal for offloading large files while maintaining onchain verifiability. Projects can store metadata, images, or other bulky content on IPFS and reference the file using its unique hash onchain. To ensure data persistence, developers can use services like Pinata or Filecoin to maintain file availability on IPFS.
- Zero-Knowledge Proof Implementations

Zero-knowledge proofs (ZKPs) enable the verification of offchain data without revealing the underlying information. For example, ZKPs can confirm that a user has passed a KYC check without exposing their personal details. By integrating ZKP frameworks like zk-SNARKs or zk-STARKs, developers can enhance privacy while maintaining compliance and trust in their systems. (e.g. ZK ID ${ }^{19}$ and zkTLS^{20} solutions for onchain compliance).
- Layer 2 Scaling Solutions

Layer 2 solutions such as Optimism, Arbitrum, or zkSync process transactions and data offchain while periodically posting summaries or proofs on the Layer 1 blockchain. This approach reduces storage and transaction costs significantly while retaining the security and trust of the main blockchain. For example, a DeFi protocol can manage user balances and interactions offchain on a Layer 2 network, submitting only essential final state updates onchain.

Tools and Compliance Management

Efficient data management and compliance tools are vital for Web3 builders to handle data securely, streamline operations, and meet regulatory requirements. Developers can enhance system performance, ensure scalability, and minimise risks by leveraging specialised tools for data management, monitoring, and compliance automation. This section provides an overview of key tools and strategies for compliance management in blockchain projects.

Data Management Tools

- Blockchain Indexers and Query Layers Blockchain indexers and query layers simplify accessing and analysing onchain data. Tools like The Graph, Etherscan APIs, and Alchemy Enhanced APIs allow developers to efficiently query transaction histories, smart contract states, and logs without interacting directly with the blockchain's raw data. These tools enable real-time insights and significantly reduce the complexity of data retrieval, making them essential for analytics, compliance reporting, and debugging.
- Database Compliance Capabilities: Databases must support data encryption, role-based access control, and audit logs to ensure compliance with regulations like GDPR or CCPA. Platforms such as Google Cloud SQL and AWS offer built-in compliance features.
- Monitoring and Alerting Systems

Monitoring and alerting tools ensure blockchain systems remain secure and operational. Tools like Prometheus, Grafana, and New Relic provide real-time tracking of system health, resource usage, and anomalies. These tools are invaluable for detecting failed transactions, excessive gas usage, or potential breaches. Alerts can be configured to notify developers immediately when irregular patterns are identified, enabling faster resolution of critical issues.

- Compliance Automation

Compliance often requires periodic reporting of transaction histories, user data usage, and system performance. Automated tools like Chainalysis, Elliptic, or Blocknative generate reports for anti-money laundering (AML) compliance, tax reporting, and regulatory filings. These systems reduce manual effort and minimise errors, ensuring timely and accurate submissions.
${ }^2$ ZK Identity: Why and How (Part). OxPARC (last visited 03 December)
${ }^{20}$ Oracles vs, Web Proofs: A Comparison. vLayer (23 September 2024)

- Audit Trail Maintenance

Audit trails are essential for tracking system changes, user activity, and data interactions. Immutable logs maintained through blockchain or external systems like Splunk or Graylog ensure traceability and accountability. Developers should design systems to log all critical events, such as smart contract upgrades, access attempts, and configuration changes, to create a comprehensive audit trail for compliance and debugging.

- Data Access Logging

Data access logging tracks who accessed sensitive data, when, and for what purpose. This is critical for maintaining user privacy and complying with regulations like GDPR and HIPAA.

Logging solutions such as AWS CloudTrail or Azure Monitor allow developers to implement robust access logs for offchain storage systems. These tools also support alerting for unauthorised access attempts, helping to mitigate risks in real time.
- Incident Response Procedures

Incident response procedures outline steps to address and resolve security breaches, data loss, or system failures. Developers should integrate automated systems to detect anomalies and initiate predefined response actions. Tools like PagerDuty or Opsgenie help coordinate responses, while blockchain-specific incident response frameworks can implement mechanisms like smart contract "pauses" to prevent further damage during an exploit. Regular testing and simulation of response procedures ensure readiness for real-world incidents.

Post-Quantum Security and Technical Standards

Although this guide gives an introduction to some of the data governance and security considerations when building compliance into your product, this is a fast-moving area with many aspects to explore further, including smart contract security and also the risks of quantum algorithms.

Quantum, particularly when combined with AI, is a known upcoming threat to encryption technology, and it is expected that the encryption landscape could materially change at any time, and certainly by 2035.

The pace of algorithmic development is increasing, and the timings of technological breakthroughs are unpredictable. This is a present and not just a theoretical issue, and updates to the NIST security standards are in progress, due for publication in Q4 2024. This is a big and growing area of focus. Effective risk management includes making provision for disaster response and recovery processes in the event of a brute force attack on your PKI (Public Key Infrastructure).' Follow NIST ${ }^{21}$ and keep a close watch on standards updates as a priority for your product security.
${ }^2$ NIST Internal Report 8547 (Initial Public Draft). National Institute of Standards and Technology (November 2024)

Computable Contracts (Akber Datoo - D2 Legal Technology and Co-Chair, Law Society of England and Wales Technology and Law Committee)

We are on an inevitable journey towards data-orientated contracts, with a meaningful representation of the written contractual terms in a manner that follows a consistent, predictable and structured data format. This paves the way for automation in an increasingly digital world, with a promise of business value through smart legal contracts in sight.

The format of contracts that best suits human to human communications requires a radical overhaul if contracts are to be fit for the coming Web3 era.

Organisations increasingly operate through processes and systems (both of which may be efficient and organised, or not!) and this reaches its pinnacle in respect of global, decentralised autonomous organisations (DAOs).

The role of agreements is to document a commercial understanding that is important, perhaps because two parties have divergent commercial interests and cannot trust one another. However, smart legal agreements operate in a world where resource governance can be hardwired into protocols and smart contracts, and shared networks provide a trustengine that shifts the role of contracts into something more machine-led. Contracts need to be capable of being split down into clear logical statements so that a smart contract action can be triggered, (or at least something sufficiently structured to be capable of being reliably plotted on an AIdriven probabilistic journey towards that binary classification). We often forget that in traditional (analogue) contracts, there are many areas of contractual imprecision, such as allowance for reasonableness or contractual discretion. These exist intentionally and fulfil a crucial role in traditional contracts. because parties cannot know at the outset all of the variables that might affect their relationship during its course, and rather than precisely drafting for all possible sets of circumstances (which would of course be impracticable and uneconomical), the parties set out tramlines to ensure that categories of unexpected happenings are dealt with according to specified processes.

Global information networks present a change to the core essence of collaboration, which is that protocols allow sufficient sophistication of automaticity that they enable strangers to enter into structured, rule-based arrangements with one another at scale.

Up to now, this has never been possible because we did not have programmatic assets, or any way of sharing a store of information that was robust against one party with access simply changing the records. BTC, ETH and other subsequent network innovations changed all of that. In this data-powered world, the trade-off for friendly bargaining, gentleman's agreements, discretion and contractual comfort-language is objectivity, speed, efficiency, global scale - which equates to power.
The oft-cited comparison to the industrial revolution rings true: smart contracts and networks bring the same sort of velocity and power to transactional processes as did the invention of steam and the combustion engine.

Much in the way that the invention of writing powered the global expansion of not just knowledge, but also collaboration and coordination (Yuval Noah Harari - Nexus), so contracts are the lawyer-code that up to now has allowed human-to-human organisations and structured collaborations of all kinds to proliferate.

In the digital future, data will necessarily be the medium through which contracts are powered. To move from current paper and MS Word-based contracts to those which allow for the automation and application of the data elements, meaning must be given to the structured data variables and allowable values of those variables. Huge advancement in AI technology allows humans to glimpse inside the intricate web of smart contracts and aids explainability (if it is correctly configured to do so). AI can sort unstructured data into insights suitable for ingestion by smart legal agreements, thereby expanding information networks' access to the universe outside of the code-environment.

This is an exciting time for the evolution of the legal profession into a new format that allows forward-thinking lawyers to interact and engage with these powerful ecosystem-based networks, to evolve the craft of contractual drafting into something new and tech-enabled. This evolution in human ability to collaborate is crucially essential if we are to meet the challenges around resource shortage, climatic disruption, war and instability of the present era. The role of lawyers is about to change for the better. We can finally focus on solving the societal and business problems, rather than the legal component of such problems.

Navigating Legal Architectures: Building your Web3 Project on Solana in the UK (Marcus Bagnall - Wiggin)

The Solana blockchain offers UK developers a high-speed, low-cost platform that's ripe for innovation. Whether you're tokenising real-world assets, crafting DeFi protocols, launching NFT art collections, developing cutting-edge games, building decentralised exchanges (DEX), or creating identity authentication systems, understanding the legal architecture is crucial. By carefully considering your legal architecture, you lay a strong foundation that supports innovation, growth, and compliance.

The Web3 legal landscape can seem as complex as the technology itself. But fear not-this chapter demystifies the legal structures available, tailoring insights specifically for UKbased projects on Solana. We'll explore entity types, structural considerations, project-specific suggestions and offer guidance to balance ambition with pragmatism.

Remember, the right legal structure doesn't just protect you from piffalls; it propels your project forward. It's about crafting a framework that aligns with your vision, resonates with your community, and withstands the scrutiny of regulators and investors alike.

Choosing the Right Legal Entity: Laying the Foundation

The UK's legal system provides a variety of entity types suitable for Web3 projects. Selecting the appropriate one is like choosing the right programming language-each has its strengths and quirks.

Private Limited Company (Ltd) - the developer's favourite A Private Limited Company is the go-to choice for many startups, and for good reason:

- Corporate identity: A Private Limited Company enables the project to enter contracts, own assets, and hire employees under a legally recognised entity. This professional structure is essential when dealing with partners, regulators, or customers. Additionally, Ltd companies can issue shares to incentivise key personnel or reward early contributors.
- Limited liability: Shareholders' liability is limited to the capital they have invested. This separation of personal and corporate assets is essential in Web3, where regulatory uncertainty and rapid technological changes pose inherent risks. If the company fails or faces legal challenges, personal assets of founders and investors remain safe.
- Investor appeal: The Ltd structure is familiar to venture capitalists, angel investors, and institutional backers. It provides governance transparency and clear ownership rights, making fundraising more accessible. Shareholders benefit from established legal protections, ensuring their investments are safeguarded.

Ideal for: Projects seeking external investment and rapid scaling. If you're planning to raise funds, a Ltd company is often the smoothest path.

Limited Liability Partnership (LLP) - collaboration central

An LLP combines partnership flexibility with limited liability protection:

- Flexible profit distribution: Unlike companies, LLPs allow partmers to determine how profits are distributed, regardless of their ownership stake. This is beneficial in scenarios where contributions vary significantly-for example, one partner provides capital while another contributes tech skills or business development.
- Tax transparency: LLPs are tax-transparent entities. meaning profits are taxed as personal income for partners rather than at a corporate level. This avoids double taxation seen in companies, where profits are taxed first as corporate income and then as dividends for shareholders.
- Collaborative vibes: LLPs are often used in professional services or collaborative ventures, making them suitable for blockchain developer collectives, consultancies, or research consortia. Each partner contributes according to their expertise or resources, fostering a cooperative environment.

Ideal for: Teams where members contribute differently but want shared control, like consulting firms, developer collectives, or joint ventures between established entities.

General Partnership - simplicity with a side of risk

Easy to set up but comes with unlimited liability:

- Minimal formalities: Setting up a general partnership is quick and requires minimal legal paperwork. Partners can begin operations almost immediately, making it suitable for short-term or exploratory projects.
- Shared liability: Partners share profits and liabilities equally unless otherwise agreed. However, each partner is personally liable for all debts and obligations, which can lead to significant personal risk if the venture incurs losses or faces legal claims.

- Quick exit: General partnerships can be dissolved relatively easily, making them a low-commitment option for temporary ventures.

Ideal for: Small projects or temporary collaborations with trusted partners, perhaps in the initial exploration or proof-of-concept phase of a Web3 idea.

Trusts - guardians of assets

Trusts hold assets for beneficiaries:
- Asset shielding: Trusts can hold tokens, intellectual property, or other critical assets separate from your operational entity. This separation shields assets from operational risks, such as litigation or insolvency, ensuring their availability for beneficiaries.
- Privacy and control: Trusts can offer anonymity for beneficiaries. Trusts can also be structured to enforce specific governance rules, such as distributing royalties or allocating tokens according to specific rules.
- Complex but effective: Establishing a trust involves some legal complexities, including drafting trust deeds and appointing trustees. Managing the trust requires ongoing oversight, which can be expensive and time-consuming. But for projects with valuable assets, it can be worth it.

Ideal for: Projects needing to safeguard assets, perhaps in NFT or gaming projects where IP rights are paramount or to protect valuable assets in a non-Web3 component of a project.

Tailoring Legal Structures to your Web3 Project

One size doesn't fit all in Web3. As Web3 projects are diverse, the legal structure that works for one may be unsuitable for another. Each project type has unique operational, legal, and regulatory considerations, requiring a tailored approach to entity formation, governance, and compliance. Your project's nature influences the optimal legal structure.

Real-World Assets (RWA) - Tokenising the Tangible

Legal Challenges: Ensuring token ownership represents legal ownership of the physical asset requires bridging the gap between blockchain technology and traditional real and personal property laws. Contracts must explicitly define rights, liabilities, and remedies, ensuring enforceability in both digital and physical realms. Regulatory complexities arise if the asset is fractionalised or tokenised into securities. Without clear legal frameworks, token holders may lack enforceable claims to the underlying assets.

Regulatory Compliance: Depending on the jurisdiction, tokenising RWAs may require adherence to property laws, securities laws, and financial regulations. For example. platforms tokenising real estate need to ensure compliance with land registration requirements in the relevant country. Failure to comply with these laws could invalidate tokenholder rights or expose the project to enforcement actions.

Example: A Solana-based platform tokenising real estate could use a UK company for development, if the real estate is in the UK then the structure could involve relevant UK entities holding title to land, and an offshore structure to issue tokens, facilitating compliance with requirements under UK laws and offshore crypto regulations.

Decentralised Finance (DeFi) - navigating regulatory rapids

- Regulatory Scrutiny: DeFi projects often intersect with financial services regulations related to securities, derivatives, lending, or trading. Depending on the jurisdiction, tokens or activities might fall under complex frameworks regarding cryptoasset services, financial services and money laundering regulations. Projects operating without regard for these regulations face significant enforcement risks and reputational damage.

- Compliance Programs: Implement robust KYC/AML policies and transaction monitoring, even in unregulated environments. This not only builds trust with users but prepares the project for potential future regulatory shifts. Early adoption of compliance measures positions the project as trustworthy and resilient to regulatory evolution.

Example: A UK-based team develops a lending protocol on Solana. Governance tokens are issued by an offshore entity, navigating favourable regulatory conditions while keeping development operations separate.

Non-Fungible Tokens (NFTs) and Gaming - protecting creativity and play

- IP Rights: Intellectual property ownership is critical in NFT and gaming projects. Ambiguities in IP rights can lead to disputes, eroding user and creator trust. Agreements must clarify the ownership of digital art, in-game assets, and user-generated content. Smart contracts can automate royalty payments but must align with applicable laws.
- Consumer Protection Laws: Digital goods and services, such as in-game purchases or NFT sales, are subject to consumer protection laws. Platforms must ensure transparent pricing, refund policies, and compliance with consumer protection regulations. Non-compliance risks reputational damage and enforcement actions.

Example: An NFT marketplace ensures artists retain rights through smart contracts and legal agreements. A UK company manages the platform, enforcing IP rights and ensuring compliance with UK consurrer laws.

Decentralised Infrastructure - building the backbone

- Operational Considerations: Decentralised infrastructure projects, such as those focusing on storage or compute, involve network participants who may operate globally. Clear legal frameworks must govern participant relationships and data usage. Without these frameworks, disputes between network participants could disrupt operations.
- Token Economics: Projects must ensure compliance with laws governing utility tokens versus securities. Misclassifying a utility token could lead to enforcement actions, fines, or investor claims. Proper classification protects the project from regulatory risks.

Example: A decentralised storage network on Solana uses a UK company to develop software, while tokens are issued by an offshore foundation to support network decentralisation.

Location, Location, Location: Team and Market Considerations

Where your team operates from, and the market you're targeting, can significantly influence the legal and operational architecture of your Web3 project. Each of these factors comes with specific legal and practical considerations that affect compliance, tax efficiency, and operational viability.

Team Location - The Heartbeat of Your Project

- Employment Laws: UK employment contracts must adhere to statutory requirements, including working hours, minimum wage, holiday entitlements, and statutory benefits like sick pay. Misclassifying employees as contractors to avoid these obligations can result in penalties, lawsuits, or reputational damage. Comprehensive contracts with clear terms of engagement and IP assignment clauses are essential to protect both the company and employees. Noncompliance with employment laws can disrupt operations and lead to costly legal disputes.
- Tax Residency: Corporate tax residency is typically determined by the location of the company's central management and control. Regular board meetings held in the UK. with directors making key decisions locally. can establish UK tax residency. However, if critical decisions are made elsewhere, it could shift tax residency to that jurisdiction, creating dual taxation risks. Ensuring clarity about where the company is liable for corporate tax and help avoid unexpected tax bills.
- Global Teams: A distributed team introduces operational complexity, including compliance with diverse local employment laws, handling cross-border payments, and navigating tax liabilities for remote workers. Time zone differences and language barriers can also affect productivity and team cohesion. Employer-of-record services or local entities can simplify compliance with foreign employment regulations.

Tip: Efficiently managing a global workforce reduces administrative burdens and ensures compliance with local laws. For globally distributed teams, consider setting up entities in key jurisdictions or using employer-of-record services to manage payroll and compliance. Be mindful of the costs and administrative overhead involved.

The Paper Trail: Essential Documents

Setting up your project isn't just about code- it's about contracts.

Pre-incorporation Documents - laying the groundwork

Founders' Agreement: This document establishes clarity among the founding team. It outlines the roles. responsibilities, equity splits, and IP assignments among the founding team. It's crucial to establish expectations and prevent disputes. It also addresses what happens if a founder exits or fails to meet their obligations. Key clauses include decision-making processes, vesting schedules for equity, and dispute resolution mechanisms.

Non-Disclosure Agreements (NDAs): NDAs safeguard sensitive information shared during early-stage discussions. Protects sensitive information during discussions with potential partners, investors, or team members before formal agreements are in place. It should specify what information is considered confidential, the duration of the confidentiality obligation, and remedies for breaches.

Corporate Governance Documents - steering the ship
Articles of Association: A foundational document that sets out the rules for running the company. It defines the rules for decision-making, share issuance, and director powers. Customisation is essential for Web3 projects to address unique governance needs, such as token voting rights or alternative dispute resolution mechanisms.

Shareholders' Agreement: This agreement supplements the Articles by defining the rights and obligations of shareholders. It covers areas like decision-making authority, minority protections, exit strategies, and how disputes between shareholders are resolved. It protects investors' and founders' interests. especially as the company grows and you bring on external parties and investors.

Employment and Contractor Agreements - building the team

Director Service Agreements: These agreements formalise the relationship between the company and its directors. They detail roles, responsibilities, confidentiality, and remuneration, including equity or token allocations. Clauses may also address conflicts of interest and termination procedures.

Employment Contracts: For staff based in the UK, these contracts must comply with employment laws, including minimum wage, leave entitlements, and dismissal rights. They should also include IP assignment clauses, ensuring any work product created by employees belongs to the company.

Contractor Agreements: Clearly defined agreements with contractors are essential, especially in global Web3 teams. These documents specify the scope of work, deliverables, payment terms, and ownership of any IP created. They should also address the contractor's status as an independent entity to avoid misclassification.

Intellectual Property Documents - protecting your creations

IP Assignment Agreements: These agreements transfer ownership of intellectual property created by founders, employees, or contractors to the company. Without this, the company might not legally own key assets, which could deter investors or lead to disputes.

Trademark Registrations: Protects your brand name, logo, and other identifiers from being used by others diluting your brand or creating confusion in the market. In Web3, this is particularly important for project names, platforms, and token branding.

Patent Applications: If your project involves novel technical solutions (e.g., unique consensus algorithms or cryptographic methods), filing patents can provide exclusive rights and give you a competitive edge. The application process can be lengthy and complex, requiring thorough documentation.

Commercial Agreements - engaging with the world
Terms of Service and Privacy Policies: Essential for any platform interacting with users to protects the company from user disputes and ensure compliance with legal requirements. Terms of Service define user rights and obligations, while Privacy Policies ensure compliance with data protection laws like GDPR. These documents should address liability limitations, user data usage, and dispute resolution.

Licensing Agreements: These agreements are critical if your project involves licensing IP, such as that required for software. It can be used to generate revenue streams and prevent misuse of your IP or software. They specify the terms of use, royalties, and restrictions on sublicensing or modifications.

Partnership Agreements: Collaboration with other projects or entities requires clearly defined partnership terms to ensure all parties have a shared understanding of the collaboration and mitigates risks of disputes. These agreements typically cover roles, revenue-sharing. joint IP ownership, and exit strategies.

Intercompany Agreements - connecting the dots
Service Agreements: Define the services provided between entities, such as a UK DevCo providing development or operational support to an offshore foundation. These agreements should include fee structures, performance metrics, and dispute resolution mechanisms. These are critical to establishing clear roles and ensuring intercompany transactions meet regulatory and tax requirements.

IP Licensing Agreements: Define the services provided between entities, such as a UK DevCo providing development or operational support to an offshore foundation. These agreements should include fee structures, performance metrics, and dispute resolution mechanisms.

Practical Guidance and Recommendations

Building on Solana in the UK is an adventure worth embarking on, but with an eye on the legal compass.
1. Start simple, think big - lean structures with growth potential
Begin with a straightforward UK Ltd company to minimise costs and administrative burdens. This structure is wellunderstood, easy to set up, and suitable for early-stage projects focusing on development. As your project grows, you can consider adding offshore entities or more complex structures to address specific needs like token issuance or international expansion.

Tip: Avoid overcomplicating your structure at the outset. Complexity adds costs and can divert attention from building your product.
2. Protect your intellectual property - safeguard your creations
Ensure all IP created by founders, employees, and contractors is owned by the company with clear IP assignment agreements. Register trademarks and consider patents if applicable. Protecting your IP not only secures your competitive advantage but also enharces your project's valuation in the eyes of investors.

Tip: Regularly audit your IP assets and ensure that all necessary protections, registrations and renewals are up to date.
3. Engage early with professionals - invest in expertise Consult legal professionals experienced in blockchain and crypto to receive tailored advice. Similarly, consult accountants and tax advisors to optimise your structure for tax efficiency and compliance. These experts can help you navigate regulatory changes, draft robust contracts, and prevent costly mistakes.
Tip: Consider joining industry groups or networks where you can access shared resources and recommendations for trusted advisors.
4. Stay informed and adaptive - the only constant is change The Web3 legal landscape is evolving rapidly. Keep abreast of developments in regulations, best practices, and industry standards. Participate in industry events, webinars, and forums. Engage with the broader Solana and Web3 communities to stay connected and informed.
Tip: Assign someone on your team to monitor regulatory updates and assess their impact on your project.
5. Budget wisely - plan for the road ahead Create a realistic budget that accounts for legal and compliance costs. While it's tempting to minimise expenses, skimping on legal matters can lead to greater costs down the line. Balance the need for compliance with your resource constraints. Prioritise essential legal work and consider phased approaches to implementing more complex structures.
Tip: Explore grant programs, accelerators, or incubators that may offer legal support as part of their services.
6. Embrace transparency - build trust through openness Operate with transparency in your governance, tokenomics, and compliance efforts. This builds trust with users, investors, and regulators. Publish clear terms of service, privacy policies, and disclaimers. Be upfront about risks and how you're addressing them.
Tip: Consider open-sourcing parts of your codebase to foster community engagement and demonstrate commitment to the Web3 ethos.
7. Leverage the Solana ecosystem - strength in community The Solana ecosystem offers resources, partnerships, and support. Engage with Solana-focused developer groups. forums, and events. Collaborate with other projects to share knowledge and potentially pool resources for common legal challenges

Decentralised Autonomous Organisations (Professor Sarah Green - D2 Legal Technology)

A Decentralised Autonomous Organisation (DAO) is an entity or organisation represented by rules encoded as a computer program, typically on a blockchain. Unlike traditional organisations, DAOs operate without centralised leadership, relying instead on smart contracts and collective decision-making.

Key Characteristics

Decentralisation: No central authority; decision-making is distributed.

Autonomy: Operates based on smart contracts, executing actions automatically when conditions are met.

Transparency: Transactions and decisions are recorded on a blockchain, visible to all members.

Governance

DAOs facilitate a communal approach to governance, in contrast to conventional arrangements that rely on a centralised authority or management team. This means of decision-making is often conducted by the distribution of governance tokens. These tokens can be issued in fungible or non-fungible form and have the effect of granting voting powers or rights to those who hold them. In turn, governance smart contracts provide a means by which those members of a DAO who hold the governance tokens in question can propose and vote on operational and architectural decisions. Similar governance smart contracts can also be set up in order to make treasury decisions, to manage the issuance, distribution and buyback of tokens (where applicable), and to register new members.

Community Governance: Members vote
on proposals and decisions using governance tokens.

Whilst decentralised decision-maiking can be highiy beneficial in meeting the objectives, and matching the ethos, of organisations and their founders, it comes with potential drawbacks, all of which should be borne in mind at the outset. For instance, token-based governance of the sort described above might mean that the making of decisions is slower and less efficient than in a traditional organisation,in which decision-making is more concentrated, or has a single point of focus. Particularly in the early days of a DAO's existence, during its set up phase, when there are many decisions to make, decision-making may be limited to a small group before rights are distributed over time in what becomes, effectively, "progressive decentralisation." An inherent risk of a structure of this kind is of course the potential for the concentration of power in any individual who retains or accumulates large numbers of tokens with corresponding voting power. If truly decentralised decisionmaking power is to be achieved or retained, significant thought should be given as to how best to guard against this sort of concentration of voting power.

In Legal Terms, what is a DAO?

It is important to recognise that, as a matter of English law, there is no discrete legal concept of a DAO. As a consequence, there exist important questions about the proper legal characterisation of any particular DAO, and, consequently, the relationships between various participants in such arrangements. This means that there is less certainty about the content of members' legal rights and obligations than there would be in a conventional entity that has a recognised legal form. One option, however, is for a DAO to adopt traditional, legally-recognised organisational structures, such as a limited company, a partnership model, an offshore trust or foundation. It is also possible to adopt a DAO-specific legal entity (which have recently been introduced in some jurisdictions), or a combination of several of these options. The entity chosen could either be coextensive with the DAO, or alternatively used only for a specific function, such as to employ developers, or to hold off chain property. This is known as "wrapping". It is crucial to note, however, that if the DAO is only partially "wrapped" in a legal entity, this might give rise to questions about the nature of the relationship between the legal entity and the non-wrapped part of the DAO. and about the legal characterisation of the elements that co not form part of, or come under, the wrapper. Where a legal entity has been adopted in any capacity, the legal entity or entities in question will be subject to the usual legal, tax and regulatory requirements of the jurisdiction in which they are set up.

Where a DAO has taken no active steps to set up a legal entity: that is, and/or where no thought has been given to the members" collective legal status, any legal intervention that is required will need to start by working out retrospectively what the legal status of the arrangement is.

This can be a difficult (and therefore costly) exercise. especially if the DAO does not fit easily within existing structures that can arise as a matter of law, such as general partnerships or unincorporated associations. What a particular DAO is from a legal perspective will determine much about the way it is treated by the law, including the rules for its operation, the liability of its participants, and how it can interact with the real world concepts of contracts. property, and tax. DAOs that have taken active steps to include a recognised legal entity within their structure are therefore very different from those that have not. Wrapped DAOs therefore arguably have a greater ability to transact in the "real world" and to do so in a way that allows their members to predict the consequences of those transactions. It may be necessary, for instance, to characterise the legal relationship between various actors within a DAO to determine who is liable if something goes wrong.

What happens, for example, when actions by or on behalf of the DAO give rise to liability in tort (such as negligence), or if there are any regulatory breaches or criminal conduct? If and when this happens, the law will need to establish who or what is responsible for the actions of the DAO. Such an analysis could conclude that all or certain participants within a DAO are part of a general partnership or unincorporated association, or alternatively to have a contractual or agency relationship with other parties. This could mean that individual participants have personal liability for the actions of the DAO. For example, in a general partnership, all partners are jointly liable for the debts and obligations of the partnership. If, however, a DAO has used as a wrapper a formal legal entity such as a company with a "legal personality" separate from that of its participants, the answers to the questions posed here are likely to be more straightforward because the DAO itself will shoulder much of the burden since, as a legal person, it can hold property. enter into contracts and sue and be sued in its own name.

Practical Steps to set up and use a DAO
1. Define the Purpose of your particular DAO

Determine what you want to achieve with the DAO (e.g.. funding, governance, development).
2. Choose the Blockchain Platform

Factors to consider:
High-speed transactions?
Mature ecosystem with numerous DAO tools?
Lower transaction costs?

3. Develop Smart Contracts

Use frameworks like OpenZeppelin or platforms like Aragon. DAOstack, or Snapshot to create and deploy smart contracts.
4. Distribute Governance Tokens

Decide how tokens will be distributed:
Initial offering (e.g., ICO, airdrop).
Performance-based rewards.
5. Engage Your Community

Build and grow a community of contributors.
Use platforms like Discord and X for communication.
6. Launch and Govern

Open the DAO for proposals and voting.
Allow the community to participate in decision-making and resource allocation.
Smart contracts can have vulnerabilities. Conduct audits regularly.

Exploring Offshore Jurisdictions: Things to think about (Sara Hall - Walkers)

Many businesses use offshore vehicles as part of their overall structure, such as Kraken, Coinbase and Bitfinex, and many community led projects have successfully developed a thriving ecosystem using one or more offshore vehicles. Maker DAO, Aave, Arbitrum and Worldcoin are well known global examples but there are hundreds more.

The principal reason to consider choosing offshore is because many activities which would be regulated in an onshore jurisdiction - such as token issuance or the operation of a fully decentralised DEX - are either outside the scope of regulation or lightly regulated in several of the offshore jurisdictions. In addition, several of the offshore jurisdictions have a government policy of actively supporting digital asset businesses and are able to shape their laws relatively quickly as technology develops. There are also skilled service providers who are passionate about Web3 such as directors, lawyers, accountants, and governance experts who can support the smooth running of the ecosystem. And there are specific kinds of companies which lend themselves to Web3 businesses governed by DAOs such as the Cayman foundation or the British Virgin Islands (BVI) company limited by guarantee.

Before following the well-frodden path of setting up a Cayman foundation, with a BVI token issuer, however, it's important to consider some "up front" factors and to take tax and regulatory advice as a first step. One of the first things to consider is where the people who are making strategic decisions will be based. This is because onshore activity such as onshore board meetings may inadvertently cause the operations to be "on-shored" - thus defeating the purpose of setting up offshore. It's also important to consider budget and which particular jurisdiction might work best from a cost/ benefit perspective.

A Cayman foundation is offen seen as the most prestigious of the foundation companies offshore. Setting up and running a Cayman foundation therefore comes at a cost which many new start-ups and scale-ups are not immediately able to meet. A jurisdiction such as the BVI which has lower costs might be a good alternative.

Founders should be aware that a handful of activities if conducted by an offshore entity for profit may require the entity to have adequate "economic substance" in the specific jurisdiction where the profits are generated (though the alternative is to make the entity tax resident onshore). Before executing on a proposal, it is therefore important to take legal advice on all aspects of the project, including the proposed income generating elements, to ensure there are no showstoppers or additional unexpected costs.

It's also important to consider if and how the founders (and investors) are going to earn revenues from the overall project. Many offshore ecosystems will be the brainchild of one or more talented developers who have set up their own company. It is this company that often sells services to the offshore ecosystem, and profits can be earned by founders and investors in the form of dividends. Finally, the offshore ecosystem will always be accessed by people onshore - and so every project will need to budget for assessing whether its interactions with onshore users are going to be restricted by onshore regulation (and if so, how to achieve compliance).

DAO Legal and Tax Standards (Joni Pirovich - Regulatory Interoperability Lead, DAOstar (a project of The Metagovernance Project, Inc)

As worldwide regulations about DAOs evolve, and without standardisation of key information about DAOs and our interactions with DAOs or blockchains, the industry cannot easily interoperate with traditional means of legal and tax reporting.

DAOstar is the standards body for DAOs, with over 80 of the world's largest DAOs and DAO tooling providers, and was convened with the spirit of maturation through data standardisation.

DAOstar's standards, DAOIPs - or DAO Improvement Proposals - are available here: https://github.com/metagov/ daostar/tree/main/DAOIPs

A DAOIP is a design document providing information to the DAO ecosystem, or describing a new feature for DAOs or their processes or environment. Each DAOIP author is responsible for building consensus within the community and documenting dissenting opinions.

DAOs should firstly have regard to DAOIP-2 which describes the key data fields about a DAO that should be displayed by a DAO: https://github.com/metagov/daostar/blob/main/DAOIPs/ daoip-2.md. Compliance with DAOIP-2 would be similar to sharing basic information with the registrar of limited liability companies in a jurisdiction, so that the entity information can be easily searched by the public.

DAOIP-8 sets out the recommended security data fields that a DAO should present to the public, and can be found here: https://github.com/metagov/daostar/blob/main/DAOIPs/ daoip-8.md.

DAOIP-9 focusses on a DAO's legal communications. The goal of DAOIP-9 is to define a clear and easy method for communicating legal information to and from online communities-whether a DAO or other form of entity-that may or may not be recognised as legal or tax persons but that do have an onchain presence. DAOIP-9: Legal Communications:
https://github.com/metagov/daostar/blob/ main/DAOIPs/daoip-9.md

Finally. DAOIP-10 is about the presentation of tax information by DAOs, and is modelled from the OECD's Crypto-Asset Reporting Framework with modifications for the idiosyncrasies of DAOs. DAOIP-10 is awaiting publication, at the time of writing this report.

TOKEN TYPOLOGIES CHAPTER 02

Web3 Games
(Omri Bouton - Outlier Ventures)

The convergence of video games and blockchain technology has now been hailed for some time as one of the most promising areas of Web3 convergence - one that has the potential to bring more people into Web3 and help the industry achieve the growth and scale it has been striving for.

In this guide, the term Web3 games covers a broad range of implementations, such as: i) fully onchain games, where the game logic runs entirely on the blockchain; and ii) games that integrate cryptoassets to a lesser degree (for example, NFTs for in-game assets).

Web3 games bring unique regulatory challenges that are often overlooked. Many developers focus on compliance with financial services and anti-money laundering (AML) laws and rightly so - but there is more to consider.

For example, if you plan to issue tokens or NFTs before launching the game to raise funds, and/or if your game allows for the in-game trading of cryptoassets (including NFTs), then your game will likely fall under the scope of antimoney laundering regulation (for more, please see "Setting up for Success - Risk Mitigation" and "Token Launch" elsewhere in this guide).

Conversely. if users can buy "qualifying cryptoassets" through your game, then that would likely be deemed as an invitation or inducement to engage in investment activity under the Financial Promotions regime (for more, please see the section on financial promotions elsewhere in this guide).

In addition to the considerations outlined above, one unique regulatory challenge arising from the convergence of blockchain and gaming is gambling regulation - which forms the focus of this chapter, as other regulatory topics are already addressed in separate sections.

Before we delve further into the different types of gambling activities, it is important to highlight two key aspects of gambling regulation: its extra-territorial scope and the lack of harmonisation across jurisdictions.

Firstly, UK gambling regulation applies extra-territorially. This means that even if your business is not based in the UK, offering a game that falls within the scope of the UK Gambling Act to UK players will subject you to its requirements. Secondly, holding a gambling licence from a jurisdiction outside the UK does not grant you the right to offer gambling activities to UK players. Each jurisdiction operates independently, and a licence issued elsewhere is not recognised as valid for activities within the UK.

Intro to Gambling Regulation

In the UK, offering 'gambling facilities' without a licence from the Gambling Commission (the competent authority) is illegal. Breaching this law can lead to fines, imprisonment, or both.

Under the UK Gambling Act 2005 ("Gambling Act"), gambling is defined as:
- Gaming;
- Betting: and
- Lotteries.

However, securing a gambling licence is difficult, expensive, and often doesn't align with the goal of Web3 game developers. Therefore, it's critical to know whether your game might be considered gambling so you can adjust its design to avoid this classification.

With that in mind, let's look at the main gambling activities.

Gaming

Gaming is likely the most relevant gambling activity for Web3 games. Therefore, we have spent some more time breaking down the definition so as to try and provide as much guidance as possible.

Gaming is defined as "playing a game of chance for a prize" - here is what this means:

Playing

The Gambling Act explains that a person is considered to be 'playing" a game of chance simply by participating in the game, regardless of whether they are playing alone or with others. Importantly, the law doesn't require players to pay or risk something of value to bring the game under gambling laws. A free game with a prize can still qualify.

Game of chance

A "game of chance" is broadly defined, and includes games that combine elements of both chance and skill. games where chance can theoretically be eliminated through exceptional skill, and even games that are simply presented as involving an element of chance.

In my experience, this is one area founders may accidentally get wrong. because the definition of "game of chance" is intentionally broad, and not limited to games that are wholly based on chance.

For example, if your game includes randomised item drops (like in Mario Kart) or unpredictable challenges, it's likely a game of chance. On the other hand, if the game is purely skill-based, where the better player always wins, it's more likely to fall outside the meaning of "game of chance" and be deemed as a "game of skills".

In essence, if a skilled player doesn't always achieve better results than an unskilled one. your game likely involves chance.

Prize

A "prize" under the Gambling Act is defined as "money or money's worth" - essentially, something capable of having monetary value.

In traditional video games, in-game items are typically confined within the game environment and cannot be freely traded or sold. This is further reinforced by End User Licence Agreements (EULAs), the contracts between game providers and players, which often prohibit users from selling their accounts or monetising in-game assets. Therefore, in traditional video games, in-game items and currencies are unlikely to qualify as something capable of having monetary value (or a "prize"), because players are generally unable to extract these "assets" from the game and trade them for money.

The Gambling Commission confirmed this view in relation to loot boxes, stating that:

"Where in-game items obtained via loot boxes are confined for use within the game and cannot be cashed out, it is unlikely to be caught as a licensable gambling activity:"

However, Web3 games often integrate cryptoassets-such as fungible tokens used as in-game currencies, non-fungible tokens (NFTs) representing in-game assets, or other blockchain-based items-which are inherently transferable.

While developers could theoretically design non-transferable cryptoassets (for example, 'soulbound' tokens), this would go against one of the main premises of Web3 games: the ability for players to truly own their in-game assets and use or trade them freely outside the game environment.

Unlike traditional in-game assets. Web3 assets built on blockchain infrastructure are inherently more likely to be classified as a "prize" under the Act. As a result, if a Web3 game includes elements of chance, it is likely to fall within the scope of the Gambling Act.

Therefore, if your game incorporates cryptoassets, ensure that the mechanics for awarding prizes are entirely skillbased and devoid of any elements of chance.

Betting

Betting is defined as placing or accepting a wager on the outcome of an uncertain event, the likelihood of something occurring or not, or whether a specific statement is true. In essence, any situation where a player risks something of value on an uncertain outcome is likely to qualify as betting. In the context of Web3 games, cryptoassets-due to their inherent value-can be considered a wager under this definition.

This concept extends beyond traditional betting and is especially relevant to Web3 fantasy sports games. These games often involve prediction-based mechanics, such as forecasting which teams or players will perform best in realworld competitions, with point systems or rewards tied to these predictions.

If you are developing a Web3 fantasy game, such as a fantasy football platform, it is crucial to evaluate whether the game could fall under the definition of betting, and you will likely need to adjust the game's design to avoid regulatory pitfalls (for more, please see the Prize Competitions section below).

Lotteries

Lotteries are defined as arrangements where participants pay to enter, and prizes are awarded entirely by chance. A key feature of lotteries is the combination of a payment-to-enter mechanism and randomised prize distribution.

In the context of Web3 games, requiring players to hold a specific NFT to participate is likely to be regarded as a form of payment, given that NFTs are typically purchased. Furthermore, as with gaming, cryptoassets-such as tokens or NFTs-are likely to qualify as prizes due to their inherent monetary value.

Some mechanics and features that could be classified as lotteries include:

- Lootboxes: Where cryptoassets (e.g., tokens or NFTs) are awarded randomly through the opening of lootboxes.
- Randomised Prizes: Mechanics where players pay (e.g.. in cryptocurrency) to spin a wheel for prizes, or where prizes are distributed based on chance within gameplay. such as randomised drops from defeating enemies or items scattered randomly on a game map.
- Token Staking with Randomised Rewards: Where players stake tokens and receive rewards distributed on a randomised basis.

Therefore, if you plan to include any of these mechanics, or any feature where prizes are allocated by chance and participation involves payment, it is essential to recognise that it will likely qualify as a lottery. Offering such features without proper authorisation could result in a breach of the Gambling Act. Therefore, you will need to make adjustments to the design of the 'game' and to how you offer it to avoid that (please see the Free Draws section be ow).

Out of Scope: Free Draws \& Prize Competitions

Unlike the activities discussed earlier, Free Draws and Prize Competitions fall outside the scope of the Gambling Act and can therefore be offered without the need for a licence.

However, it is crucial to ensure that your offering aligns with the legal definitions of Free Draws or Prize Competitions (which are purposefully narrow) to avcid unintentionally falling under the Gambling Act.

Free Draws

A free draw is a type of promotional activity where participants are not required to pay to enter.

There are two types of free draws:
- Entirely Free Entry: where all entries must be free of charge (keeping in mind that requiring holding an NFT to participate will likely not qualify as a 'free entry').
- Paid and Free Entry Routes: where there is both a paid and a free entry option. However, if you include a paid entry route, you must ensure that:
- Participants can choose to enter without paying.
- The free entry route is no more expensive and no less convenient than the paid route (effectively, you cannot provide preferential or faster entry methods for paid participants while requiring free entrants to go through a more time-consuming or complicated process).
- The free entry route is prominently displayed and promoted at the same level as the paid route.
- The choice between free and paid routes is clearly communicated to participants.
- The system used to allocate prizes treats entries from both routes equally, without favouring one over the other.

Prize Competitions

A prize competition is an activity where the outcome depends entirely on participants' skill, judgement, or knowledge.

To qualify as a prize competition, the skill, judgement, or knowledge required must:
- be sufficiently challenging to deter a significant number of people from entering: and
- prevent a proportion of participants from winning a prize.

Simple multiple-choice questions or questions that allow a second attempt rarely meet this standard, as they are not deemed challenging enough. ${ }^{22}$
${ }^{22}$ Free Draws and Prize Competitions. Gambling Commission (23 October 2024)

Design With Regulation in Mind

The last thing you want is to invest significant resourcestime, money, and effort-into developing a project, only to later discover that it cannot be legally offered. To avoid this, it's essential to consider gambling regulations early in the development process and design your game to steer clear of activities that may fall within the definition of gambling. Prioritising skill-based mechanics, where applicable, can be an effective way to achieve this.

Carefully evaluate your project to identify any design elements that could bring it under the scope of gambling regulation.

To get started, ask yourself the following key questions:
Does entry to the game require payment?
(Remember that requiring players to hold an NFT could be regarded as a form of payment.)

Are rewards distributed based on chance?
(Randomised rewards or prize allocations are highly likely to fall under gambling regulations.)

What determines the outcome of the game loop?
(Is the outcome entirely skill-based, or does it involve an element of chance? For example, if the game loop is repeated multiple times, would the outcome vary due to chance?)
Please keep in mind that this is only a starting point to help you identify game elements that might increase the likelihood of your project falling within the scope of gambling regulations.

Ultimately, consulting a lawyer who specialises in this area is the most reliable course of action. While this might feel burdensome-especially when you're juggling multiple challenges in your project-it is a critical investment, particularly in today's regulatory climate.

For instance, Sorare, one of the most prominent Web3 games, is currently facing legal action from the Gambling Commission. This highlights the increasing scrutiny on Web3 games and underscores the importance for businesses operating in the UK, or offering games to UK users, to either ensure they fall outside the scope of the Gambling Act or fully comply with its requirements.

A Practical Tip

Resist the temptation to rely on financial incentives to drive engagement. Based on my experience, projects that focus heavily on financial rewards tend to attract speculators and traders rather than genuine players. These communities often abandon the project when the tokenomics falter, leaving the ecosystem unsustainable.

Instead, prioritise creating a game that offers a genuinely enjoyable and engaging experience. Players who are drawn in by great gameplay are far more likely to stay loyal. If your game includes cryptoassets (tokens, NFTs, or otherwise), limit their distribution to skill-based mechanics to align with this approach. By focusing on fun and skill-based design, you can build a sustainable and dedicated player community and as always, please consult a lawyer!

SocialFi: Boosting Organic User Growth with SocialFi (Ian Cox-CEO and Founder, Avark Agency / Manchester Blockchain Alliance)

SocialFi has become the latest buzzword in Web3, with many brands and products incorporating it into their strategies. At its core. SocialFi focuses on creating engaging, rewarddriven experiences that overcome the design limitations of traditional Web2 apps and social media platforms. By integrating SocialFi, communities are incentivised to interact with an app or plafform, produce content about the product and community experiences, and boost the ecosystem's reach through organic word-of-mouth.

No Project in Web3 will succeed without a Solid User Base

Community building lies at the heart of success, serving as a dependable way to expand the user base and enhance user acquisition. By launching gamified SocialFi campaigns that motivate users to engage and share publicly, brands can lay the groundwork for future success. This strategy generates buzz and momentum while establishirg a sustainable foundation to support the ecosystem and fuel ongoing product development.

Great SocialFi campaigns don't happen by chance. Success requires a careful balance of strategy, visual design, and storytelling. A well-defined strategy ensures campaigns resonate with the target audience, while exceptional design makes the experience intuitive and visually engaging. Meanwhile, strong storytelling gives campaigns emotional depth, making them relatable and inspiring users to connect with the brand on a deeper level. Together. these elements help create a campaign that captivates users and fosters loyalty.

Turn User Interaction into Valuable Insights...
The platform's flow is typically designed to be simple, making it easy for users to get involved. However, the challenge lies in maintaining engagement. Delivering a sense of accomplishment and creating a feedback loop that motivates users to return and share the platform is critical. Ultimately. the goal is to build a legion of super users-individuals who are rewarded for their time and energy and who, in turn, share ownership of the brand. This is the future of Web3 business: building ownership through community.

Campaigns can progress in "seasons," with each season lasting roughly six weeks. At the end of each season, new features are introduced to sustain engagement and growth. The abundance of metrics available allows for continuous testing. evaluation, and improvement. Developing "super users" is especially valuable. These are the users who rank highest on leaderboards and progress charts, and they can be engaged as testers and ambassadors for your product. They naturally roll into the main platform, becoming an extension of your community and team.

A Loyal Fanbase is your Key to Web3 Success
Gamified platforms highlight the importance of creating experiences that users can actively engage with. The power of a dedicated fanbase should never be underestimated, particularly when launching a product or token. These loyal users can-and should-be rewarded for their efforts in building brand awareness.

Steps projects can take to ensure a successful SocialFi strategy with regard to both legal and best practice factors include:
- ensure you have clear guidelines for community members around good behaviour and expectations. Take time to ensure you block bots from taking part and keep channels clear for genuine users only. The community moderation team will be vital when ensuring proper engagement in any open discussion channels;
- consider adapting your brand to be more open and allow users to use certain brand assets in permitted ways to create shared videos, assets and images. You will need to consider your intellectual property licences and think about what parts of your brand you would like to protect and what could be opened up to community usage. You could create a brand pack and acceptable use guidelines, too:
- If you are giving key governance roles to community members, ensure they have the right skills to take on any responsibilities:
- when collaborating with other brands, use a collaboration agreement to ensure you have clear legal arrangements, including in respect of IP rights;
- be conscious of marketing and advertising laws, including local restrictions on the advertising of crypto-tokens, and take advice on compliance early on in your project.

DePIN (Morgan Lewis - Brabners LLP)

Web3 advocates often state that we should all be concerned about how there is an oligopoly over the second generation of the internet and that Web3 presents an opportunity for the power and control to be wrestled from the few and given to the many.

The development of cloud infrastructure has revolutionised the way governments, businesses and individuals access and use technology. The use of an internal server room and a personal home computer (with its accompanying pc tower under the desk) are now no longer used by the masses and have to a degree become a mark of a tech laggard. However, the supply of the underlying cloud infrastructure can certainly be understood to be an oligopoly due to being dominated by Amazon Web Services (AWS), Microsoft Azure, and Google Cloud.

Rightly so, advocates for and providers of decentralised alternatives are quick to point out that such an oligopoly is cause for grave concern. This is because its failure would be catastrophic given the pervasive nature of cloud infrastructure and the fundamental impact it has on nearly all aspects of our day to day life. Surely something so critical to the smooth working of the modern world should not rest upon a foundation of a small handful of powerful companies. At best this small group could hold the world to ransom on price and at worst a sudden full or partial failure of the operations of one of these providers would see entire industries grind to a halt.

DePINs seek to replace the rows and rows of servers located in data centres with the nodes of a decentralised, blockchain or encryption-based system, with the nodes typically being rewarded for the use of their computational power by the network.

At this point it is worth outlining a general disclaimer that I provide to any business seeking to disrupt an industry by using new or innovative technology.

It is a natural consequence of working in a disruptive manner with new or innovative technology that the legal and regulatory backdrop is often not very clear, meaning that any such business needs to be prepared to adapt and change as the legal and regulatory landscape develops. Unfortunately for any such business it means that lawyers like myself often respond with "it depends", "we will have to wait and see" or "I don't know" when answering their enquiries. In order to navigate this uncertainty it is wise to focus on "what" is actually happening in the supply of a product or service rather than get too bogged down in the "how" it is happening. Doing so will allow you to draw from:

- existing laws and regulations for guidance as to how the legal and regulatory landscape is likely to develop; and
- any contractual arrangements that are somewhat similar in nature as inspiration for how to structure any new or novel type of contractual arrangement.

The contractual framework for the operation of a DePIN differs from that of traditional cloud infrastructure predominantly as a result of the fact that the infrastructure is not owned and the services are not being directly provided by the operator of the DePIN.

Firstly operators of a DePIN will need to ensure that the contracts they enter into with their customers (for access to and use of the DePIN) are put together with the understanding that the DePIN's infrastructure is not owned by the operator of the DePIN. Specific points to note here are that the operator of the DePIN should refrain from giving any warranty that it owns the DePIN or the infrastructure and should ensure that it is permitted to utilise the services of subcontractors (and be permitted to amend these subcontractors without any requirement to notify or receive the approval of the customer).

Further, customers are likely to have concerns about the scalability, reliability and security of a DePIN when compared with traditional cloud infrastructure. Any operator of a DePIN therefore needs to ensure that a correct balance is struck within any contract that assuages the customer's concerns but does not over-promise the DePIN's capabilities.

The operator of a DePIN will be unable to provide the same levels of guarantees as a household name cloud services provider in these respects and therefore it is likely that the customer's worries will need to be relieved via educating the customer on the "security by design" nature of DePIN and the operators plans for scalability and reliability (instead of by the customer imposing onerous contractual damages on the operator).

Additionally, one thing that should not be missed in any sales pitch is the fact that a balanced contract can in fact be entered into with the operator of the DePIN. and not one predetermined to favour the cloud services provider (as is the way with AWS, Microsoft Azure and Google Cloud standard terms).

Secondly the operator of a DePIN should enter into subcontractor type agreements with the owners of the nodes on the DePIN in order to utilise each node for the purpose of the provision of services by the operator. Given the number of nodes within a DePIN this should be facilitated by requiring the owner of each node to agree to a standard set of terms when downloading/installing the operator's software that will give the operator access to the computational power of the node.

From my experience, the operators of a DePIN have been proactive in putting contracts together with node owners (i) to outline how access and use of the node's computational power will work in practice and (ii) to set out the mechanism for how the reward (i.e. the consideration element of the contract) is earned.

However, what is often overlooked is including sufficient protection for the operator of the DePIN to reflect the fact that access and use of each node's computational power is critical to the operator being able to provide a service to its customers. This means that the contract should include guarantees/warranties that would typically be given by a cloud service provider to their customer via their standard terms, but in this instance be given by the owner of any node for the benefit of the operator of the DePIN.

Further thought should also be given to whether this contract should include additional obligations on the owner of any node to reflect the obligations placed upon the operator of the DePIN to assuage the scalability, reliability and security concerns of the operator's customers (as outlined above). These might include:
- guarantees surrounding availability of access to the node's computational power:
- detailed information security requirements; and
- additional protections to ensure the sharing of any personal data is done so in manner that is compliant with GDPR/UK GDPR (and if needed the inclusion of an international data transfer agreement or the standard contractual clauses as approved by the EU. where the node is

located outside the UK or EEA). This is still true even if the data shared with the node is encrypted (irrespective of whether the node has the capability to decrypt the data or not).

Finally, given that the contracts with the owners of the DePIN's nodes will need to be entered into prior to the operator of the DePIN agreeing a contract with a customer (as it should take place as part of the set-up of the DePIN), the operator needs to retain the ability to amend its contract with the owner of each node without obtaining their approval. This will allow changes to be made based on the obligations that any operator commits to via its contract with any future customer. This could be done by the contract including an express right for the operator to amend the contract at will (although this may be unenforceable in some circumstances and jurisdictions) or by updating the contract/terms and requiring the owner of each node to re-accept the new contract terms when they next login or access the software dashboard (that is typically used to manage the node's role within the DePIN).

Practical Guide for DeFi Developers (Maria Riivari - Avara)

Decentralised Finance (DeFi) has rapidly grown into a diverse and complex ecosystem, presenting unique challenges and opportunities. This chapter explores DeFi in three key parts: first, it examines jurisdictional considerations and the current regulatory landscape in the UK. Second, it provides practical guidance for protocol developers, focusing on legal considerations for creating and operating permissionless smart contract protocols. Finally, it offers a simple toolkit for front-end developers, addressing critical factors for navigating running interfaces within the DeFi space based on current industry practices.

Part 1. UK Regulation \& Perspectives on DeFi

One of the challenges with modern internet and blockchain systems from a legal perspective is their inherently global nature. In contrast, laws are jurisdiction-specific and do not operate seamlessly across borders. As a rule, it is not straightforward to identify whether a particular DeFi project falls under one or another jurisdiction due to its decentralised and cross-border nature; despite extensive global discussions and consultations, currently there remains little clarity on whether, and to what extent, phenomena categorised as "DeFi" are subject to regulation.

Currently in the UK DeFi operates largely in an unregulated space, with the UK legal framework for DeFi still evolving as regulators strive to balance fostering innovation with ensuring consumer protection and financial stability. Key legislation relevant to this area. discussed elsewhere in this guide. includes the Financial Services and Markets Act 2023, which introduces provisions for regulating cryptoassets, including stablecoins, under existing financial rules. ${ }^{23}$ The FCA plays a critical role in overseeing crypto promotions and enforcing compliance with anti-money laundering (AML) regulations, signalling a growing regulatory focus on DeFi platforms. However, unique challenges such as decentralised governance, pseudonymity, and the lack of traditional intermediaries create uncertainties about the application of current UK laws.

Future guidance is expected to address these gaps, particularly as DeFi projects are likely to increase engagement with traditional financial markets. This evolving regulatory environment highlights the need for clarity and adaptability to manage the complexities inherent in decentralised financial systems.

That said, it should not be forgotten that certain activities (which are unlikely anyway to fall under what would be understood as "DeFi") which fall under the regulatory framework in the UK include:
- Custody of Assets: Providing custody services for digital assets, such as managing digital wallets or safeguarding private keys, is subject to regulatory scrutiny. The FCA oversees firms offering these services to ensure the protection of customer funds and compliance with antimoney laundering (AML) regulations.
- Facilitation of Fiat-to-Crypto or Crypto-to-Fiat Transactions: Activities involving the exchange between fiat currencies and cryptocurrencies are regulated under the UK's AML and counter-terrorism financing (CTF) laws. Firms facilitating these transactions must register with the FCA and implement robust AML/CTF controls. The FCA has taken enforcement actions against firms failing to comply with these regulations, highlighting the importance of adherence to AML requirements.
- Stablecoin Issuance: Whilst not fully regulated in the UK today. the UK government has recently announced plans to regulate stablecoins under a unified regulatory framework, ensuring they maintain stable value and are appropriately backed by assets. Tailored rules will address their issuance and use, aligning with global standards like the European Union's Markets in Crypto-Assets (MiCA) ${ }^{24}$ Regulation. The framework, set for early 2025, aims to balance innovation with consumer protection and financial stability while positioning the UK as a competitive hub for digital assets. ${ }^{25}$

${ }^{23}$ Financial Services and Markets Act 2023

${ }^{24}$ Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-assets. 2023 O.J. (L 150) 1

${ }^2$ Keynote Address at the Tokenisation Summit; UK Government Approach to Tokenisation and Regulation. UK Government (25 November 2024)

This brings us to an important development in the European regulatory landscape. Whilst of course not applicable in the UK, MiCA, which has been announced to serve as the inspiration for the future UK regulations, addresses DeFi in Recital 22. This recital clarifies the regulation's applicability to decentralised services:

"This Regulation should apply to natural and legal persons and certain other undertakings and to the crypto-asset services and activities performed, provided or controlled, directly or indirectly, by them, including when part of such activities or services is performed in a decentralised manner. However, where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation."

This section can be interpreted to mean that MiCA covers services involving intermediaries, even if some operations are decentralised. In contrast, services that are entirely decentralised, operating without any intermediaries, are excluded from MiCA's scope.

This distinction is important for understanding how DeFi platforms may be regulated under MiCA. Unfortunately trying to define "decentralisation" is like trying to herd cats - good luck getting everyone on the same page. One attempt to shine light on the scope of this carve out came from the Danish Financial Supervisory Authority (DFSA) who emphasised that significant criteria must be met for an offering to be considered truly decentralised. Therefore, this carve-out, while promising, leaves room for interpretation and highlights the importance of understanding the nuanced distinctions between decentralised and centralised operations when navigating the regulatory environment. If there's one thing to take away from this carve-out, it's that decentralisation can really impact a project's regulatory status, especially if it's fully achieved.

Additionally, it should be noted that HM Revenue \& Customs (HMRC) has been particularly active in addressing the tax implications of DeFi activities, such as lending and staking of cryptoassets. Recognising the complexities and ambiguities within existing tax frameworks, HMRC initiated a call for evidence in July 2022 to gather insights from stakeholders on the taxation of DeFi transactions. Building upon the feedback received, HMRC launched a formal consultation in April 2023, proposing legislative changes to better align the tax treatment of DeFi activities with their economic substance. ${ }^{26}$

Part 2. A Compass for DeFi Protocol Developers

Rather than dwelling too much on the rapidly changing status quo of DeFi regulatory developments in the UK, the following two sections seek to focus on providing practical ideas for developers to navigate this evolving landscape. Specifically, we discuss permissionless protocol networks. In this context, "permissionless" refers to the ability of anyone to interact with a protocol's smart contracts, either through a user interface or directly on the blockchain.

It is important to note that legal risks are highly situation, fact, and context-specific, making individual assessments crucial.

From a legal perspective, developers typically have no direct connection or contractual relationship with the end users of the DeFi protocols; they operate in a mere conduit role, solely providing the framework for these decentralised interactions. While we explore topics related to user interfaces in Part 3 of this Chapter, it is important to consider the distinction between protocol development and interface development. Some organisations engage in both, making all considerations relevant to their operations. However, maintaining conceptual clarity about these activities is crucial for understanding the developer's position and responsibilities as they can help delineate legal and operational boundaries. What follows seeks to offer "food for thought" on what might make a difference in terms of various legal risks in designing DeFi protocols.

1. Prioritise Security

The protocol's security is your best security. Building on new technologies is inherently challenging, especially in selfcustodial systems where the stakes are high.

While many factors may be beyond developers' control, prioritising security is crucial-not only to ensure system integrity but also to protect users. Beyond the ethical imperative, the practical reality is that security lapses can increase the risks for developer organisations, including legal ones. Even if developers are not fundamentally liable, managing these risks can be time-consuming and stressful. Investing in security is not just about doing the right thing: it is also a sound long-term strategy, aligning with the broader goal of building a fair and secure decentralised financial system.

[26] The Taxation of Decentralised Finance Involving the Lending and Staking of Cryptoassets; Call for Evidence, UK Government (27 April 2023)

Trade-offs are often unavoidable, particularly in the early stages of development. It should be recognised that creating robust systems requires balancing numerous complex factors and navigating difficult choices between competing risks. Just as Rome wasn't built in a day. industry practices evolve as systems mature, providing more reliable security standards over time. Security is a key reason decentralisation often exists on a spectrum, particularly in early stages. Initial considerations may involve compromises, such as incorporating upgradeability features or temporarily retaining admin keys. These measures can sometimes be justified to ensure the system's security is reasonably validated and provide additional safeguards to protect end users from potential losses. While there is no one-size-fits-all approach to managing these challenges, demonstrating that decisions were made with security as a guiding principle can significantly benefit developers in the long run.

2. Champion Documentation

Transparency is fundamental to building trust in DeFi, which inherently benefits from its ability to eliminate information asymmetries through open and accessible systems.
Developers can embrace this principle by providing clear and comprehensive documentation that explains their protocols, highlights potential risks, and makes relevant data readily available.

DeFi comes with various risks, including vulnerabilities in smart contracts, unique interoperability challenges related to bridges and oracles, and broader economic risks like market volatility. By proactively disclosing these risks as they pertain to their specific project, developers not only empower users to make informed decisions but also reduce the likelihood of disputes or issues that could undermine the project's reputation.

High-quality, credible, and accessible documentation benefits both users and the ecosystem. For users, it fosters informed decision-making and builds trust. For the broader DeFi community, it encourages collaboration, innovation, and development by other contributors, ultimately strengthening decentralisation and expanding the ecosystem.

3. Address the Degree of Control

DeFi is built on the principle of decentralisation, but this concept encompasses varying degrees and interpretations. In addition to what has been discussed above about decentralisation itself, developers might consider the following points when designing protocols:

- Mutability vs. Immutability: Striking the right balance between flexibility and security is often a key consideration in deciding whether a smart contract could be made immutable. Immutability is often regarded as beneficial because it can be seen to introduce a degree of separation between the actions of the developer deploying the DeFi protocol and the permissionless activity that may occur afterward by other users. The idea is that this separation might help reduce the likelihood of developers being perceived as owners or controllers of a system, potentially mitigating liabilities.
- Resilience Through Decentralisation: It has been argued that one goal of decentralised systems seeks to minimise single points of failure. By reducing reliance on specific individuals or entities, protocols can aim to function more effectively and distribute risks across the network. A resilient system may be more aligned with decentralisation principles, enhancing robustness and trust in the network.

Part 3. DeFi Interface Developer Cheat Sheet

Permissionless access to DeFi allows users to engage with networks and protocols in various ways, and the interfaces themselves vary widely-some focus on specific functionalities, while others cater to broader DeFi needs, creating a range of user experiences.

The regulatory uncertainties surrounding DeFi also extend to interfaces. A distinction is, however, is that interface providers often have a closer connection to end users, unlike the decentralised blockchain networks they interact with or the developers that wrote the code of the network. However, this connection does not necessarily impose liability on developers for user interactions or the underlying smart contracts. Nonetheless, it is a critical consideration that could play a significant role in mitigating legal risks.

There is no one-size-fits-all solution for DeFi interfaces, but the following toolkit outlines areas that developers may consider. It reflects practices observed across various DeFi front-ends and highlights aspects that may be relevant depending on specific circumstances. While many points are rooted in general principles for online platforms, they can be adapted to address the nuances of DeFi.

Aspect
Considerations

Security
Security is a critical concern for DeFi interfaces, which are common attack vectors. Many interfaces focus on implementing robust measures to protect users and systems.

Terms of Use

Some interfaces adopt detailed terms to outline user responsibilities, limit liability, and address specific risks.

Privacy Policy
Important to provide a clear privacy policy that complies with data protection laws and explains data collection and usage.

Clickwrap Agreements
Some interfaces use clickwrap agreements requiring users to actively accept terms and the privacy policy, improving the argument that users understood and agreed to key terms.

Decentralised Hosting
Hosting on decentralised platforms (e.g., IPFS) is an approach some developers take to align with DeFi's principles and enhance resilience.
\begin{tabular}{|c|c|}
\hline Geoblocking & An option considered by some front-ends is geoblocking to restrict access from jurisdictions with regulatory or legal concerns. \\
\hline VPN Blocking & Some interfaces include tools for monitoring blockchain transactions or flagging/ blocking certain wallets based on risk factors from connecting to the interface. \\
\hline User-Friendly Design & Interfaces often emphasise user-friendly designs to reduce mistakes and enhance user experience. A well-informed user is less likely to encounter issues. Moreover, in the event of a dispute, developers are more likely to successfully rely on the argument that users were empowered to make informed decisions based on the comprehensive information provided and accepted by the user. \\
\hline User Support & While many DeFi projects rely on community-managed resources (e.g., Discord), some interfaces consider offering dedicated support channels to address user needs. \\
\hline Warnings \& Notifications & Some interfaces include warnings or notifications to alert users about potential risks, such as transaction fees, failed connections, or security concerns. \\
\hline Fiat On/Off-Ramps & Interfaces that facilitate fiat on/off-ramps may highlight that the end user typically engages directly with the exchange provider, which may be regulated. Developers should consider clarifying these relationships and undertaking due diligence on the requirements on these providers. \\
\hline Promotions & Where promotions are involved, developers may assess regulations governing promotional activities, particularly in jurisdictions with strict advertising rules \\
\hline Third-Party Materials & Developers may want to address how third-party content or integrations (e.g., incentive programs, fiat gateways, analytics tools) are presented, with disclaimers that clarify the interface provider's role and limit liability for third-party issues. \\
\hline
\end{tabular}

This list aims to guide DeFi interface developers by offering an overview of many industry practices and key considerations. Each project is unique, with varying jurisdictional connections, and developers should carefully assess the relevance of these points in the context of their specific circumstances and the evolving regulatory landscape. It is also important to continue innovating and developing new best practices, as there is still much to explore and improve in this rapidly evolving space.

SETTING UP FOR SUGGESS AND RISK MITIGATION

(Leon Hurd - Cybersandbox and Keystone Law Limited)
CHAPTER 03

Overview of Anti-Money Laundering (AML), Sanctions and Compliance Law

The fragmented nature of regulatory regimes in the UK means that it can be challenging to ascertain every single regulatory and/or legislative framework with which you need to ensure compliance. As a rule of thumb, in the context of cryptoassets and blockchain, when seeking to mitigate against financial crime risks and adhering to important regulatory standards, the core frameworks that ought to be considered are:

- The Money Laundering. Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs)
- Authorisation under the Financial Services and Markets Act (FSMA)
- Electronic Money Regulations (EMRs) and the Payment Service Regulations (PSRs)
- Sanctions Regime under the Sanctions and Anti-Money Laundering Act (SAMLA) and various implementing Orders
- The Financial Promotions Regime (covered elsewhere in this guide)
- Data Protection/GDPR (covered in the Product, Data and Compliance by Design section)

AML registration with the UK Financial Conduct Authority (FCA)

The MLRs are an important tool in the combatting of financial crime and money laundering. The MLRs were extended to certain types of cryptoasset businesses in January 2020, pursuant to which: (i) "cryptoasset exchange providers"; and (ii) "custodian wallet providers" (both as defined in 14A of the MLRs) are required to register with the FCA for supervision of their AML processes.

Many cryptoasset service providers 'CASPs'/Exchanges will, therefore, need to comply with the registration requirement in order to deliver services into the UK. To successfully apply for registration, applicants will need to demonstrate robust AML controls including the following:

Risk Assessment:
- A comprehensive business-wide risk assessment
- Individual customer risk profiling
- Geographic risk considerations

Customer Due Diligence (CDD):
- Verification of customer identity
- Enhanced due diligence for high-risk customers
- Ongoing monitoring of transactions

Operational Controls:
- Appointment of a Money Laundering Reporting Officer
- Staff training programs
- Suspicious activity reporting procedures
- Record-keeping systems

There is a substantial amount of guidance around what constitutes a custodian wallet provider or an exchange. It is not uncommon for a business to believe that it is not caught within the definition under Regulation 14A because for example, it purports to only provide self-custody wallets when in fact as part of its broader business there may actually be custodian services attached which bring it in scope.

Similarly, a cryptoasset business might provide ancillary services which bring it in scope: for example, a crypto remittance business that might as part of its services include an exchange service to enable customers to change USDT to ETH before remitting the ETH. It is imperative that legal advice is obtained on the entire business model and customer journey to ascertain whether registration is required.

FSMA establishes the regulatory perimeter, that is the boundary which delineates between regulated activities for which FCA authorisation is required, and unregulated activities for which FCA authorisation is not required (although other legal and regulatory rules may also apply).

Broadly speaking, the need for authorisation is likely triggered, subject to applicable exclusions and exemptions, where you are: (1) conducting specified activities, (2) involving specified investments. (3) by way of business, and (4) from or in the UK.

Currently, cryptoassets are not expressly included in the definition of specified investments for the purposes of regulation under the specified activities regime (note however that they are included as 'qualifying cryptoassets' under the financial promotions regime), however, the FCA has by way of guidance created a taxonomy by which some cryptoassets are capable of being treated akin to specified investments and consequently capable of falling within the regulatory perimeter if there are specified activities undertaken in respect of them (i.e. traditional financial services such as arranging deals in investments, managing investments, advising on investments etc.,) by way of business in or from the UK. To achieve this, the FCA categorises cryptoassets into regulated and unregulated tokens:

- Regulated tokens - primarily security tokens and emoney tokens:
- Unregulated tokens -primarily utility tokens and exchange tokens.

The FCA supports a substance over form approach and will classify a token as a security token, and consequently capable of being caught within the perimeter, if they:

- Have characteristics similar to traditional securities;
- Provide rights like ownership, repayment of money, or profit share:
- Are transferable and tradeable on capital markets.

Similarly, the FCA will deem a token to be an E-Money Token if they:

- Meet the definition of electronic money under EMRs;
- Maintain stable value pegged to fiat currency;
- Are used for payment.

Some stablecoins might fall within this definition and it is understood that there are future plans to include stablecoins within the definition of e-money under the EMRs. The FCA's crypto roadmap published on 25 November 2024 states that the FCA aims to consult on its regulatory approach to stablecoins in Q1/Q2 2025. ${ }^{27}$

Unregulated Tokens remain outside the perimeter when they:

- Are primarily used for exchange;
- Don't provide rights similar to regulated investments;
- Function as utility tokens for accessing services.

From a compliance perspective, it is essential that careful analysis is undertaken to correctly classify tokens. When considering whether a business is engaging in authorised activity, the FCA will look beyond any superficial labels that are given to an activity and will look at the substance of what is happening to determine whether regulated activity is being undertaken. They will, for example, closely examine whether a token is indeed a utility token or whether in fact it is behaving as a security, and may ask probing questions about the operation of the business to help with their assessment.

Advice should always be obtained as to whether authorisation is required as the position is not always clear. There is, for example, substantial case law around the meaning and application of the different statutory criteria for determining whether authorisation is required.

Where authorisation is required, you may need to engage services of compliance consultancies and law firms to prepare the various documents needed for an authorisation application, such

as policies and procedures, a detailed business plan and detail on key personnel and how they satisfy FCA requirements.
${ }^{27}$ Cryptoasset Regulation Roadmap. Financial Conduct Authority. (last visited 27 November 2024)

The authorisation process can be lengthy and will usually take a minimum of 6 months if everything goes smoothly. It is also important to note that you cannot undertake authorised business before obtaining authorisation as this is a criminal offence under FSMA; this can sometimes be alleviated by the introduction of temporary licence regimes, but again careful assessment is required to determine what activities can be done while authorisations are being sought.

Electronic Money Regulations / Payment Service Regulations

The question of whether activities are subject to regulation under the EMRs and/or the PSRs largely depends on whether the cryptoassets, supported by the business/platform, meet the legal definition of "electronic money" (e-money). Activities relating to the transfer of e-money are regulated under the PSRs; operating a platform which facilitates the transfer of emoney from one person to another is likely to fall in scope and require a Payment Institution (PI) licence by virtue of it being money remittance which is a payment service under the PSR.

A cryptoasset business will require an Electronic Money Institution (EMI) licence if it is issuing "money", this would be the case where it is issuing tokens which meet the definition of e-money. There is currently much discussion around whether stablecoins meet the definition of e-money and there are legislative plans to bring stablecoins within the definition of e-money and, consequently, within scope of the EMR and PSR.

Careful consideration should be given to the types of tokens that are supported by a platform, particularly where the businesses services include the issue or transfer/remittance of tokens.

There are many similarities between an authorisation application under FSMA and an application for an EMI or PI licence and advice should be obtained - by reference to a detailed review of the business and customer journey - to assess whether (and which) licences are required and the content of the application.

Sanctions

Individuals and legal entities who are within or undertake activities within the UK's territory must comply with UK financial sanctions that are in force; therefore, overseas companies operating in the UK are caught. UK incorporated entities are subject to UK requirements relating to sanctions and the prevention of terrorist financing irrespective of where they are operating. This applies regardless of the regulatory/ compliance status discussed above: however, it is worth flagging that additional requirements apply to firms within the scope of the regulatory regimes referred to above. There are a wide range of economic sanctions imposed by the UK on various

countries/political regimes and specialist advice should always be obtained if there are concerns about whether business activities might breach sanctions.
Businesses should be particularly mindful of sanctions imposing asset freezes on designated persons (individuals and entities). Broadly. asset freezes imposed by the UK operate to prohibit:

- making funds or economic resources available, directly or indirectly, to, or for the benefit of, a designated person or to a person who is owned or controlled directly or indirectly by the designated person;
- dealing with the frozen funds or economic resources. belonging to or owned, held or controlled by a designated person or to a person who is owned or controlled directly or indirectly by the designated person:
- engaging in actions that, directly or indirectly, circumvent the sanctions prohibitions.

As a matter of good and robust financial hygiene, businesses should implement AML and sanctions policies which set out the procedures and policies in place to ensure that users are adequately screened, and that sanctions and broader money laundering risks are mitigated. From the UK perspective, this approach should also be taken by blockchain/cryptoasset businesses. To support this view, guidance on the regulatory expectations in respect of crypto firms was given in a "Joint statement from UK financial regulatory authorities on sanctions and the cryptoasset sector" (March 2022). Some key expectations to note are:

- where blockchain analytics solutions are deployed. ensuring that compliance teams understand how these capabilities can be best used to identify transactions linked to higher risk wallet addresses;
- updating business-wide and customer risk assessments to account for changes in the nature and type of sanctions measures;
- ensuring that customer onboarding and due diligence processes identify customers who make use of corporate vehicles to obscure ownership or source of funds;
- ensuring that customers and their transactions are screened against relevant updated sanctions lists and that effective re-screening is in place to identify activity that may indicate sanctions breaches.

Businesses should also look for red flag indicators that suggest an increased risk of sanctions evasion. These may include:

- the use of tools designed to obfuscate the location of the customer (e.g. an IP address associated with a virtual private network or proxy) or the source of cryptoassets (e.g. mixers and fumblers);
- transactions to or from a wallet address associated with a sanctioned entity, or a wallet address otherwise deemed to be high-risk, based on its transaction history or that of associated addresses, or other factors;
- transactions involving a cryptoasset exchange or custodian wallet provider known to have poor customer due diligence procedures or which is otherwise deemed high-risk.

There are also some special reporting duties for cryptoasset exchange providers and custodian wallet providers which require them to report to OFSI where they know or suspect a person is a designated person or has committed sanctions offences.

It is always sensible to obtain legal or regulatory advice around the implementation of policies and procedures to address sanctions and broader AML/financial crime risks. There is a lot of value in carrying out this exercise robustly as demonstrating good governance and processes is an important aspect of most licensing and authorisation applications.

UK REGULATION OF THE FINANCIAL PROMOTION OF CRYPTOASSETS
(Andrew Maguire - Littleton Chambers)
CHAPTER 04

Cryptoassets have been the subject of increased scrutiny during the last couple of years, with both the Government and the FCA having previously expressed concern about 'the wild west' of crypto promotions, within the context of increased regulation taking place in other jurisdictions. On 26 November 2024, the FCA has published its "roadmap", which outlines planned FCA policy publications for cryptoassets where the FCA are seeking feedback and the content they are expected to cover, concerning the regulation of crypto: see crypto roadmap.

On 7 June 2023, the UK Parliament passed the Financial Services and Markets Act 2000 (Financial Promotion) (Amendment) Order 2023, which brought cryptoassets within the scope of the regulatory framework which regulates the marketing of financial products in the UK. This legislation amended the Financial Services and Markets Act (Financial Promotion) Order 2005 ('FPO'), extending it to cryptoassets with effect from 8 October 2023. The FPO defines the investments and activities captured by the financial promotions regime as well as related exemptions.

A key component of financial regulation is the control over the manner in which investment products are marketed and promoted to the general public, by the Financial Conduct Authority's authorisation of firms marketing regulated products to the general public. In more recent times, scams perpetrated via social and digital media have increased exponentially. The UK Government has been keen to ensure that the regulatory framework is fit for purpose and relevant to the recent technological developments.

Section 21 of the Financial Services and Markets Act 2000 ('FSMA") provides that a person must not, in the course of business, communicate an invitation or inducement to engage in investment activity or to engage in claims management activity unless the promotion has been made or approved by an authorised person or it is exempt. This article does not deal with claims management activity which is a separate topic.

Therefore, a financial promotion is defined as any communication that either invites or induces a person to engage in investment activity that is communicated in the course of a business: see s. 21 of FSMA and FCA's Perimeter Guidance Manual ('PERG') at PERG 8.1.1. [emphasis added]

Guidance on the FCA's interpretation of the financial promotion restrictions and the applicable exemptions from the regime is contained in chapter 8 of PERG, which is intended to represent the FCA's views. Although not strictly binding on the courts, in practice, it is usually of persuasive effect to judges determining financial promotion regulatory issues, as recent case law has shown. This Guidance applies to persons who need to know whether their communications are subject to, or comply with, s. 21 of FSMA; namely, whether their activities, in making or helping others to make financial promotions, are regulated activities. The scale of the risk is underscored by the fact that a breach of s .21 is a criminal offence, carrying a penalty of imprisonment for up to two years and or an unlimited fine or both.

In considering whether any communication relating to financial promotions is captured by the prohibition in s. 2.1 of FSMA, the following five questions ought to be considered:
(i) is a communication being made or caused to be made?
(ii) is the communication an invitation or inducement to engage in investment activity? (iii) is the communication made in the course of a business?
(iv) does the communication originate from outside the UK and, if so, is it capable of having an effect in the United Kingdom?
(v) does the communication fall within one of the exemptions contained in the FPO?

If the communication satisfies the first four questions listed above, and there is no applicable exemption, then the financial promotion will have to be communicated or approved by an authorised person in compliance with the applicable financial promotion rules (depending on the type of investment product).
A number of exemptions exist, namely that either:
(i) the person is authorised under FSMA in accordance with section 31 of FSMA; or
(ii) the content of the communication has been approved by an authorised person that is a permitted approver in accordance with the FCA rules; or
(iii) the communication is covered by an exemption pursuant to the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005, as amended; or
(iv) there is (currently) a time limited exemption for certain crypto asset businesses who are registered with the FCA under the Money Laundering. Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ('MLR 2017'); as from 8 October 2023.

The guidance in PERG8 provides useful insights into the question of whether any communication is likely to be held to be an invitation or inducement to engage in investment activity. such as the following random examples: web links: advertisements; communications by employers to their employees; invitations to attend meetings or to receive telephone calls or visits, investment trading methods and training courses; advertisements inviting contact with the advertiser; image advertising; performance tables; company statements and announcements.

In addition, PERG8 provides guidance on what it means to communicate financial promotions: in practice. a person will need to have taken active steps to make the communication. which will be a key question of fact. The FCA take the view that a person is making a communication where they give material to the recipient or are responsible for transmitting the material on behalf of a person. Thus, if a person knowingly were to leave a copy of a document where it is likely that people will pick up such copies (who may seek to act on the information contained in those documents), that person will be communicating the content of that document.

PERG8 also distinguishes between a communication which is made to another person, such as if it is addressed verbally or in legible forms and a communication which is directed at one or more persons if it is addressed to persons generally, such as a television broadcast or a website: this distinction becomes important when the issue of exemptions is being considered.

The requirement, in s.21(1) FSMA, that only invitations or inducements communicated in the course of a business are regulated is not restricted to those carrying out regulated activities. Therefore, anyone who carries on a business that is not a regulated activity, should be careful when making communications, that may amount to financial promotions, if they seek to persuade or invite others to engage in investment activity.

Restrictions cover both written and oral communications. However, the exemptions in the FPO draw distinctions between real time and non-real time and solicited and unsolicited communications.

This is because consumers are believed to be more likely to be influenced into buying a product as a result of highpressure sales tactics during unsolicited telephone or face to face, real time discussions, so that such activities are thus subject to greater regulation.

The territorial scope of the financial promotions regime in the UK will depend on issues such as the location of both the communicator and the recipient of the promotion. In general, any promotion with the UK link, be that an incoming or outgoing communication, will be caught. Such restrictions will apply its promotions to recipients located in the United Kingdom, subject to exemptions, and under section $21(3)$ of FSMA any promotions originating outside the UK will also fall within the restriction, if they are capable of having an effect in the United Kingdom.

Financial promotions by authorised persons are not subject to the financial promotion restriction in s.21. However, authorised persons must ensure that any financial promotion they communicate must comply with the relevant financial promotion rules. The financial promotion

approval gateway introduced in 2023, replaced the previous regime under FSMA that allowed an authorised person to approve the financial promotion of an unauthorised person for the purposes of s.21. Under the new gateway a financial promotion requirement automatically applies to all authorised firms that have not applied for and be granted approval permission by the FCA. Under s.21, the content of the financial promotion can only be approved by an authorised person who either:
(i) is a permitted approval in relation to the financial promotion; or
(ii) falls within the scope of an approver permission exemption, as set out in the FSMA 2000 (Exemptions from Financial Promotion General Requirement) Regulations 2023, which allows an authorised person to approve its own financial promotion without requiring permission.

The many exemptions to financial promotion restrictions are too wide-ranging and varied to accurately set out in this brief article, as there are over 70 . Specialist regulatory advice ought to be obtained from expert lawyers in relation to such exemptions: particularly given that a wrong decision in regards whether an exemption applies or not could have literally catastrophic consequences to the individual and the entire business.

Some examples of decision making, in corporate activity. regarding whether a financial promotion is being communicated, arise in the following circumstances, especially where outside investment is being sought which give rise to all such communications being compliant with the regulatory regime: press presentations; the publication of company annual reports and accounts; the distribution of analysts research reports in the marketing of an initial public offering: the publication of a prospectus for listed securities: companies promoting either the buyback of its shares for holding in treasury or the sale of treasury shares: communicating with employees regarding employee share schemes; or unlisted companies promoting investment in its business to private equity funds.

Financial promotions, involving consumers, cover a wide range of material including stationery, shop fronts, faxes, leaflets, newspaper advertisements, emails, text messages, hyperlinks. sponsored links and banner advertising. websites, TV and radio commercials and increasingly communications via digital and social media; such as blogs, microblogs such as X , social networks such as Facebook, LinkedIn, Google+, forums, image and video sharing platforms such as YouTube and Instagram.

An illegal financial promotion is one communicated in breach of s 21 . For example, an unauthorised influencer communicating a financial promotion without approval from an appropriate authorised person and where no FPO exemption applies.

An example of an invitation might be as simple as: "Invest in [A] Ltd's share sale by completing the attached application form". An example of an inducement might be: "[A] Ltd's growth to date has been spectacular and that growth is expected to continue".

Therefore, the following examples would be likely to breach the applicable rules and be in essence criminal behaviour:

(i) an influencer is directly compensated by a firm and issues posts encouraging followers to use the firm's services;
(ii) an influencer is not currently employed by a firm but is promoting a firm's services to generate revenue from a relationship with the firm in the future:
(iii) an influencer is promoting the services of a firm on a social media platform in a bid to acquire more views and attention for their content. They are then directly compensated by the social media platform for the views they acquire:
(iv) an influencer is promoting the services of a firm but only to try to acquire more followers and likes. They will then use the increased followers and likes to ask for a higher fee in future brand deals with firms;
(v) person A is promoting chatroom B which they run to promote investment products. They have a commercial relationship with firm C who sells investment products;
(vi) person A is promoting investment products on a social media platform to lead people to a chatroom centred around investing that they run or are involved in running. They gain a monetary benefit from the success of the chatroom, for example by selling courses about investing;
(vii) an influencer promotes the services of a firm through an affiliate link. When a consumer clicks the link and purchases the product the influencer will be directly compensated for their purchase.

Activities that are less likely to be captured by the regulatory regime are myriad, such that it is almost impossible to generalise, as the wording of each communication would need to be considered in isolation. However, some random high-level examples of communications are as follows:
(i) those which are purely profile raising and which do not identify and promote particular investments or investment services may not an Scale by percentage tation or inducement of any kind. Examples of this include where listed companies sponsor sporting events or simply put their name or logo on the side of a bus or on an umbrella;
(ii) statements of fact about a company's performance or activities may not, in themselves, be inducements to engage in investment activity even if they may lead persons to decide to buy or sell the company's shares. However, statements which speculate about the company's future performance or its share price may have an underlying purpose or intent to encourage investors to act.

These few examples starkly demonstrate that seeking expert advice is prudent, as compliance with s. 21 is mandatory; there is no "best endeavours" defence available: the underlying policy requirement is for firms to unconditionally comply with the legal framework. This may require the obtaining of expert advice, if any doubt arises as to the lawfulness of a proposed communication. Increasingly, in the crypto space, such compliance is increasingly sought by potential investors, many of whom will be aware of the calamities that have arisen in the unregulated crypto market.

TAX, VAT AND ACCOUNTING

Dion Seymour - Andersen LLP;
Mark Pearce - Alkimi

CHAPTER 05

Important note: The content in this section, including any rates and thresholds mentioned, changes very quickly and is highly subject to variation based on individual circumstances. This is a guide for general information purposes only and it is extremely important to engage a professional advisor for advice on your particular circumstances.

All guidance in this section, including any details of rates, refers only to the position in England and Wales on the date of publication of this guide. Please seek specific guidance on Scotland and Northern Ireland, where relevant to your project.

Why should I read this?

The UK tax system is constantly being reformed and is still very vague on how tax should apply to digital assets or "crypto".

This section summarises some of the key issues that founders will need to consider when launching a crypto project. The following section by Dion Seymour provides more detail on the key topics but readers should bear in mind that there are currently over 17,000 pages of tax legislation that are constantly being changed and updated so it is vital that founders take advice from a suitable professional.

Failure to comply with your tax responsibilities can lead to various sanctions including, at their most extreme, a prison sentence. It is each person's responsibility to file their tax returns correctly and ignorance is not considered a defence.

Who am I?

The first question that founders need to ask themselves is the nature of the entity that is going to run the project. In the UK there are three main options, a company, a partnership or as an individual.

A company?

Establishing a company is the most common option. It is relatively simple and cheap to establish a company in the UK. A company is a separate legal entity, which is run by directors who are subject to various powers retained by shareholders (for example shareholders often have the power to appoint and remove directors). This can allow founders to appoint experts to help run their company but with the protection that they can remove those directors in the future if necessary.

While it is possible for people living in the UK to establish companies in a number of jurisdictions the UK has detailed anti-avoidance rules that will often bring profits of foreign companies established or managed by UK residents within the scope of UK taxation. Founders wishing to establish companies outside the UK should ensure they take detailed advice both in the UK and the intended county of establishment so they can be confident of understanding all the tax and regulatory requirements that will apply to them.

Founders of UK crypto companies should also consider with their accountants whether they can take advantage of various tax incentives or rebates such as EIS/SEIS, R\&D credits or VAT recovery.

A partnership?

Partnerships can, themselves, take various forms such as general, limited or limited liability partnerships. If a partnership is set up outside the UK there are often even more choices available and, again, separate advice will need to be sought. Many, but not all, partnerships are taxed similarly to companies or individuals so this guide will focus predominately on these two options.

An individual?

It is not a legal necessity for an individual to run a project as a company or in a partnership. If a project is the brain-child of one person then it is possible for that person to manage the project as an individual or sole-trader. While being a soletrader might incur the least initial legal and accounting costs a person acting as a sole-trader could face a number of difficulties quite quickly. The major concern for many founders is the potential liabilities that may apply to individuals that might not necessarily apply to companies. It is possible for people acting as sole-traders subsequently to incorporate their business but this may incur more costs than were saved by not incorporating initially.

Where am I?

The UK generally levies taxes based on the location (or situs in legal parlance) of both the relevant person and the source of taxable return. For individuals living in the UK they will generally be regarded as UK resident for taxation. The UK has a fairly prescriptive statutory residence test, which allows individuals to calculate whether or not they are UK resident. ${ }^{28}$ Individuals born outside the UK should consider their domestic tax regime as well as any relevant double tax treaties. ${ }^{29}$ Companies are generally resident where they are incorporated but non-UK resident companies can be taxed in the UK if they are managed from the UK or have a permanent establishment in the UK.

Where is my crypto?

As for the situs of crypto, the UK's default position is that crypto is situated where the person owning the crypto is resident. It is arguable if this is completely accurate. especially when one considers cold wallets and closed networks, but serves as a statement of general principle. ${ }^{30}$

What tax is charged?

To determine what tax is charged it is necessary to consider whether a receipt is income or capital gain in nature. There is no definitive test for all scenarios that can exist but as a general rule income is often regular in nature or deriving from a trade while capital gain is often realised on the sale of an asset. Common forms of income include salaries, contractor payments and rewards such as might arise from staking. The sale of an asset or the conversion of one type of an asset to another is more usually capital.

The distinction between income and capital gain is less relevant for companies as they are subject to corporation tax rather than income or capital gains tax. The distinction is, though, important for certain reliefs and rebates so your accountant should keep accurate records of whether a return is income or capital.

For individuals, there is a significant difference currently between the tax rates that can apply to income (up to 45% at the time of writing) and capital gains tax (up to 24\%). As such, determining whether a return is income or capital can lead to a significant difference in the tax due.

It is also worth noting that inheritance tax might be charged if you own assets on death, such as direct crypto holdings or shares in a company, or if you make certain lifetime transfers of assets. Inheritance tax is not likely to be relevant to many founders so this guide does not consider this further.

Finally, other, discrete taxes might apply in specific circumstances. For example, if you employ staff or pay yourself a salary then national insurance contributions may fall due. Certain contracts you enter into may be subject to VAT and if you incorporate a business you may be able to reclaim any VAT that you have spent.

When is tax charged on my crypto

Income tax

If you receive a salary, including a bonus, then your income tax is likely to be deducted by the paying company before you receive the income through PAYE. PAYE is often a "best guess' as to your tax liability and when you come to complete your tax return you may find that there is some more tax to pay or, alternatively, a tax repayment owed to you. However, this is not something you need to calculate until it is necessary to file your tax return. Other forms of income will need to be declared in your tax return.

Capital gains

Capital gains are also declared in your tax return so it is important to know what is a chargeable disposal for capital gains tax purposes. In essence, the conversion of any asset to another asset is a chargeable disposal that may give rise to a gain or a loss. These gains or losses must be calculated in GBP meaning that you may also need to consider fluctuating exchange rates to ascertain whether a disposal gives rise to a profit or a loss.

HMRC regards all crypto as being a separate asset meaning that changing from one crypto token to another token should be recorded as a disposal. It is the subject of much academic debate but this could even apply whether you go from a token such as ETH to a wrapped version such as WETH. Below is a simplified, illustrative example showing how much detail founders should record, which hopefully highlights the need for accurate book keeping from the outset.

[28] Guidance Note for Statutory Residence Test (SRT) (RDR3), UK Government (22 January 2020)

[29] Tax Treaties, UK Government (28 July 2014)

[30] CRYPTO22600 - Cryptoassets for individuals: Capital Gains Tax: determining the location of exchange tokens, HM Revenue & Customs (21 August 2023)

Date	From	To	From value	To value	GBP-USD	Total Gain
06.04 .24	GBP	USDT	$£ 10000$	$\$ 12,000$	$1: 1.2$	0
13.06 .24	USDT	ETH	$\$ 12,000$	$\$ 12,000$	$1: 1.13$	$£ 620$
22.08 .24	ETH	\$Founder	$\$ 18,000$	$\$ 18,000$	$1: 1.25$	$£ 3,780$
07.12 .24	\$ Founder	\$BTC	$\$ 90,000$	$\$ 90,000$	$1: 1.15$	$£ 63,860$
14.02 .25	\$BTC	\$USDT	$\$ 80,000$	$\$ 80,000$	$1: 1.2$	$-£ 11,594$
05.05.25	\$USDT	GBP	$\$ 80,000$	$£ 72,727$	$1: 1.1$	$£ 6,061$
TOTAL						

The important point to note here is that even though from a USD perspective there was no gain or loss on the 13 June 2024 transaction, because the GBP:USD exchange rate had changed since 6 April 2024 a taxable gain was still realised.

Corporation tax

Each company will have its own accounting period after which it will need to file accounts (usually 12 months after the end of an accounting period) and pay tax (usually 9 months after the end of the accounting period).

UK companies may wish to consider aligning their accounting period to the UK tax year (6 April to the following 5 April) but if, for example, the company is heavily US focussed it may wish to align it more to the US tax year (1 January to 31 December).

Overview of Tax and Accounting for Crypto Projects (Dion Seymour - Andersen UK)

1. The UK crypto tax landscape

There is no "crypto tax" law. Cryptoasset transactions are nonetheless taxable. Existing tax laws and principles must be applied to cryptoassets in the same way as they do to other assets.

There are a number of different taxes that may apply to you and your business. The main taxes that you will need to consider are Income Tax (IT). Capital Gains Tax (CGT) Corporation Tax (CT) and Value Added Tax (VAT).

IT, CGT and CT are called "direct taxes" as the tax is charged against income, capital gains or profits arising from a particular activity (e.g. employment income, investment gains or trading profits). VAT, by comparison is known as an "indirect" tax because it is charged on "consumption" (i.e. on the goods or services being "consumed" and not the activity).

HMRC publishes tax guidance (called manuals) to help taxpayers understand what they must do. However, multiple manuals covering different taxes and a targeted cryptoasset manual means that assessing one's tax position can feel like searching for a needle in a haystack. That said, the manuals are very helpful in understanding HMRC's opinion on topics, although it is just HMRC's view, and there may be alternative positions.

An online platform for engaging with HMRC, covering registration to submitting tax returns, is available through the Government Gateway at Gov.UK. This can be used for all the main taxes, including IT, CGT, CT, and VAT. It is important to note that there are deadlines for registration with HMRC, and if these are not met, HMRC may charge penalties.

2. Important dates

You are responsible for the completion of and ensuring that tax returns are submitted on time and are accurate. The system is generally referred to as "self-assessment" as you assess the due tax and report (and pay) that to HMRC. HMRC operates a "process now, check later" approach to taxation.

This means that HMRC does not actively check each and every tax return, however, they do undertake compliance reviews to ensure that tax returns for individuals and businesses are complete and accurate.

2.1 Income and capital gains tax

IT and CGT self assessment (SA) is a way of reporting income/profit/gains and paying tax to HMRC. This is for individuals and also applies to the self-employed or a partner in a partnership. Any capital gains from selling cryptoassets must also be included in the SA return. Anyone earning income outside of PAYE or CT must complete an SA tax return.

The key dates for SA tax returns are:

- 5 October - register for SA for the first time
- 31 October - submit paper tax return
- 31 January - submit online tax return

2.2 Corporation tax

To register as a company, one must also submit an annual return to Companies House and an annual tax return to HMRC. CT self-assessment is relevant for companies, and the key dates for CT Self Assessment are based on the periods in the accounts, also called the accounting period. The submission date for the CT tax return, called the CT600, is 12 months after the end of the accounting period. There is a separate deadline to pay the CT bill, which is usually 9 months and one day after the end of the accounting period.

2.3 VAT

You must register your business if it makes "Vatable" supplies exceeding £90,000.

If your business makes supplies that are in the scope of VAT and the taxable turnover for the last 12 months goes over $£ 90,000$ or you expect your taxable turnover to exceed $£ 90,000$ in the next 30 days, registration must be completed within 30 days of the end of the month when the threshold was exceeded.

The effective date of registration is the first day of the second month after exceeding the threshold.

You also need to register if the business is based outside the UK and supply any goods or services to the UK.

Unlike CT or IT, which are annual returns, VAT periods are quarterly, and the VAT refurn needs to be submitted by the end of the following month.

Several VAT accounting schemes are available, such as the flat rate scheme, which can simplify the calculation of VAT, and the Annual Accounting scheme, which requires a VAT return to only be submitted once a year. There are conditions applied to the schemes and these may not be suitable for all businesses.

3. UK regulated start-ups

A UK regulated start up is one that has the necessary registrations with the FCA (and other relevant regulatory bodies). The UK company is permitted to conduct its business and crypto transactions in the UK.

3.1 Trading v. investment

The first matter to assess is whether the company is investing or trading in crypto.

Often, when cryptoassets are bought and sold, this is described as "trading". However, the term has a different meaning when it comes to taxes. For direct tax, there is a difference between trading (buying and selling crypto) and the meaning of trading for tax purposes.

For tax purposes, trading is a "venture in the nature of trade." This is an old phrase from case law that describes, essentially, a business. That does not mean that trading in crypto is also a "venture in the nature of trade." This is important as profit from a business can have different tax implications.

Typically, the buying and selling of crypto will be treated as an investment activity. Any profits from transactions are known as chargeable gains and are liable to corporation tax. with losses being offset against the gains.

However, where the company is actively trading in cryptoassets with a sophisticated level of operation, such as personnel, algorithmic bots etc. and a clear profit motive, it may be treated as a financial trader.

This is important to note when it comes to loss relief. Whilst chargeable gains and trading profits are both taxable to corporation tax (i.e. the same tax rate), there is a difference in how losses are treated for corporation tax. Trading losses can offset against both capital gains and other trading profits arising in the same period, or be carried forward for offset in future periods. Capital losses can only be offset against capital gains, and where they exceed available gains in a given period, they are carried forward to offset against future capital gains only.

Transaction fees will be considered within any cryptoasset transactions as these will be treated as an allowable cost where they are for the acquisition or disposal of an asset for the business.

3.2 Accounting

Companies must complete financial statements each year for submission at Companies House under accounting standards. These are due to be filed with the registrar 9 months following the company's year-end.

UK accounting standards (FRS) consider most cryptoassets to be an "intangible asset" which is a "non-monetary" asset. Whilst many users might consider cryptoasset to be cash or investments. treatment as an intangible asset creates unique issues for accounting purposes that need to be considered.

This includes the cost basis for including as an asset, tracking unrealised and realised gains on the disposal of cryptoassets. whether assets can be revalued (if there is a sufficient active market and liquidity) and how often revaluations take place.

Unless a business disposes of cryptoassets immediately on receipt, there is likely to be a gain or loss that crystalises on disposal. This, along with the cost basis for intangibles, also needs to be recorded.

It is therefore important to consider suitable software to track onchain movements both for accounting purposes and tax calculations, and matters can escalate in complication quickly.

Any goods or services purchased using cryptoassets would be recorded at the value of those assets at the time of disposal. Where these are incurred for business purposes. they are deducted from income in order to calculate the level of profits that are subject to corporation tax.

To transfer cryptoassets there is typically some form of "gas" fees (fees paid to validators of transactions on the blockchain). The gas fees are payable in cryptoassets (usually in the same cryptoasset as the transaction), and this, too, is a disposal (i.e. any gain or loss in the crypto needs to be recognised). However, the gas fee would be a tax-deductible expense for the business.

Aside from accounting principles, it is highly recommended that businesses consider the value held in cryptoassets, as well as the liquidity of the business. Where cryptoassets are received from services performed, those cryptoassets are valued for accounting and tax purposes at their market value at the time of receipt. When markets suffer, if the liquidity is held in cryptoassets, the business may be required to make disposals for fiat, which could make it difficult to settle taxes due.

3.3 VAT

To date, limited guidance has been released from HMRC on the implications of VAT on cryptoassets. However, the CJEU (Court of Justice of the European Union) was one of the first courts to consider the implications of tax on cryptoassets. In the case of C-264/74 Skafteverket v David Hedqvist, the CJEU considered that exchanging Bitcoin for fiat currency (and visa versa) was considered to be an exempt supply on the basis that it was a supply of financial services. It should be noted that only Bitcoin was considered presenting uncertainty if there is no fiat currency involved (i.e. cryptoasset to cryptoasset transactions) the treatment would be the same.

VAT is charged on the supply of goods and services with VAT liability following the activity. Cryptoassets, such as SOL, are neither a good nor a service in their own right. Therefore, a business selling cryptoassets would not add VAT to their sale as they are not a good (i.e. they do not have a physical form). They would, however, add VAT to the charge for providing that service.

For VAT to apply, there must also be a clear link to the customer and the service being provided. Where a business undertakes mining the activity does not constitute an economic activity as there is not a sufficient link between the service and the consideration (the fees that have been received) for providing that service as there is no clear customer.

A great example of the complexities that can arise when applying existing VAT principles to cryptoasset transactions is the application to NFTs. As NFTs can cover a wide range of uses this means identification of what is being supplied must be considered on a case-by-case basis. Some EU jurisdictions have stated that the supply of a 'jpeg' NFT is a service and, if that is correct, it follows that the treatment would follow the rules of electronically provided services (ESS). For B2C transactions, this would require the seller to register for VAT in their customer's location. Of course, many NFT projects do not know where the seller is located. Some jurisdictions, such as Spain, will treat all sales as to Spanish customers unless evidence can be provided to the contrary. There has been a mixed approach from HMRC in some cases adopting a similar position in Spain and in others (incorrectly) treating the NFT as a security and exempt from VAT!

Whilst NFT jpegs may have had their day. NFTs have multiple use cases not least to represent real world assets (RWAs) or intangible property. This means that not all NFT sales should be considered as providing a service. As VAT follows the liability of the goods or services, selling RWAs that are VATable in the "real world" should also be VATable if they are tokenised. There is no clear guidance from HMRC on whether or not this is the case.

For the UK business, it is important to consider the VAT consequences of their NFTs' attributes at the design stage -as it may be possible to secure more certainty or efficient VAT outcome with some changes. There may well be other indirect taxes, for example, NFTs representing real estate or shares in a UK company owning real estate as Stamp Duty Land Tax (SDLT) or Stamp Duty Reserve Tax (SDRT) may be due.

4. UK unregulated start-ups using offshore regulated entities

The current UK regulatory landscape means that many web3 start ups are unable to carry on their business in the UK. A common regulatory solution is to set up an offshore entity in a more favourable regulatory environment to undertake the crypto transactions, even if the people running the business are not offshore.

However, a common misconception is that if a company is established outside of the UK there can be no tax liability in the UK. This is incorrect. A UK resident individual or company is subject to UK tax on their worldwide income and gains.

4.1 Out of the fire and into the frying pan - 100 years of anti-tax avoidance

Whilst the regulatory solution may be simple, this usually catapults the business and/or its founders into complex tax issues, the types of issues that have been traditionally reserved for large well-funded multinational groups, not bootstrapped start-ups!

The UK has 100 years of anti-tax avoidance rules and case law that prevent such persons from creating offshore companies in low or no tax jurisdictions, with little or no substance (i.e. no local people functions), and parking profits there with a view to avoiding UK tax.

Broadly, these anti-avoidance rules will deem the income. gains or profits (depending on which set of rules apply) to belong to the UK resident person on an arising basis (i.e. even if not distributed).

The main anti-avoidance rules to consider include:
- Transfer of Assets Abroad (ToAA)
- Profit Fragmentation (PFrag)
- Controlled foreign companies (CFC)
- Transfer pricing (TP)
- Intangible fixed asset (IFA) regime.

Whilst the rationale for offshoring is not tax avoidance, these rules nonetheless apply, and can lead to taxation in the hands of an unintended party or double taxation without relief.

In addition, care needs to be given to the board composition of the offshore company and its engagement of UK employees or contractors so as to ensure that it is not brought into the UK by virtue of establishing corporate residence or a branch in the UK.

4.2 Common traps and pitfalls

The anti-avoidance rules and their interaction are complex and turn on the smallest of facts. At their simplest, the most common issues include:
- The creation of a non-UK company by a UK resident individual will trigger the ToAA rules. These rules will deem the income of the offshore company to belong to that individual and subject to UK income tax (currently up to 45%) on them personally, even if no dividend is distributed.
- Where a UK company creates a subsidiary in a low or no tax country to undertake its income generating activities it will be a CFC. Its profits will be deemed to belong to its UK parent and subject to UK CT (known as the CFC charge). Costs incurred in the UK parent are not deductible against this allocation. This can lead to double taxation.
- Where an offshore company has a majority of UK resident directors or only UK resident directors, it will likely be UK tax resident and subject to UK CT.
- Where an offshore company has offshore directors, but UK resident employees, a UK branch will be created and profits attributable to the UK activities subject to UK CT.
- Where an offshore company has offshore directors and no UK employees, but has a service agreement (and potentially a licence agreement, depending on where IP is owned), with a UK

DevCo, profits will need to be attributed to that DevCo on an arm's length basis either under the TP rules, PFrag rules or IFA regime.

4.3 Special types of offshore entities and DAOs

Decentralised Autonomous Organisations (DAO) have become an increasingly popular community led method of organisation. There has yet to be any published guidance from HMRC as to their view on the tax treatment. The Law Commission considers that DAOs are a novel organisational structure often likened to existing legal forms such as a general partnership or unincorporated association. The tax treatment is, therefore, uncertain. Characteristics may lead to the conclusion that the DAO is a general partnership, in which case profits attributable to its UK members (the partners) would be chargeable to income tax. However, it could be concluded that the DAO is a form of unincorporated association, in which case the activities would fall into scope of corporation tax.

Due to the uncertainty of legal form and, therefore, tax treatment, many projects will set up a special type of offshore entity or structure to establish a legal wrapper and create tax certainty. Typically these offshore legal entities will be "orphaned". This is typically a not-for-profit entity in that it cannot distribute its profits to its members and include the Cayman foundation company, the Swiss Association, the Panama foundation, a company limited by guarantee, a purpose trust, amongst others.

In addition to the anti-avoidance rules highlighted above, the creation of such structures can lead to severe inheritance tax consequences for UK based founders, if not structured correctly. Interestingly, provided structured correctly many if not all the above mentioned anti-avoidance rules may be blunted due to the decentralised nature and ambitions of the project.

4.4 200\% penalties

Where HMRC successfully identifies unpaid tax through the use of offshore structures, the penalties, absent formal written tax advice, will be 200\% of the underpaid tax!

5. Paying the founders / team in tokens

5.1 Earnings in crypto

Businesses can pay their employees in cryptoassets. This is a disposal for the company, and any gain or loss needs to be accounted for. Consideration needs to be given to the value being paid to employees, as the number of tokens that may need to be sent to employees to satisfy their net pay may change between the payroll processing date, and the payment date.

If employees are being paid in stablecoin denominated in a different currency (e.g. USDC), the exchange rates also need to be considered. In addition, the business must withhold PAYE and pay employees' and employers' National Insurance Contributions (NICs).

UK businesses are also required to operate a workplace pension for employees. More information on this can be obtained from the pensions regulator.

If a company is paying token incentives to employees, the tokens they pay to employees are likely to be taxable and would be processed through the payroll. Under these circumstances, the business will need to retain broadly 50% of the cryptoassets they wish to pay the employee and either fund the PAYE / employees' NIC out of any fiat currency held or convert the cryptoassets into fiat currency.

Where the company is receiving tokens from a DAO structure under a service agreement, careful planning is required to match cryptoassets receipts (i.e. service fee income) with payments in cryptoasset to employees (i.e. a deductible expense) to minimise exposure to the volatile movements in the valuation of these assets.

5.2 Founder/team token planning

Some projects will seek to launch their own native token. The tokenomics will usually provide an allocation to the founders and initial start up team. It may be possible for those founders and team to effectively mitigate the IT consequences described above and only be subject to tax, CGT, if and when they sell their tokens. This would require the founders/team acquiring their token rights very early on before any agreements with third parties have been made establishing a market value - under an agreement such as a simple agreement for future tokens (SAFT), although they have many other names.

Provided no independent value has been created (i.e. no SAFTs with third parties have been agreed or executed establishing a price per token), it may be possible to use a cost based valuation to determine the price the founders/ team should pay for their tokens. This would take all costs to date associated with the token, divided by the expected total token supply plus an arm's length mark up = a price per token. The founders / team must pay this for their token allocation. A special election needs to be made by the employer to protect the CGT treatment on the sale should HMRC successfully challenge the valuation. It is recommended to obtain an independent valuation.

Even though the founders/team acquire their token rights under the SAFT, it is possible to include forfeiture clauses whilst retaining tax benefits described. Such clauses mean that if an employee leaves before all their tokens unlock, any unlocked tokens may be forfeited.

A token bonus or incentive scheme requires careful planning.

5.3 Sale of tokens

For those who have received tokens, the difference in the token's value at the time of acquisition (receipt) and subsequent disposal will be charged to CGT.

A common misconception is that tax is only due when you sell cryptoassets for fiat currency. This is not true. Tax is also due when crypto is exchanged from one crypto to another; for example, an exchange of SOL to BONK would be classed as a "taxable event". The amount of tax due is calculated in reference to what is called either the "pooling rules" or "section 104".

These rules apply to all cryptoassets and create a "pool" for each cryptoasset you have. If you have SOL with some different accounts or wallets, the rules consider that these are all in one, with other cryptoassets also having their own pool. Therefore, the holding of SOL and BONK would be considered separately. The rules create an average cost for the token used to calculate any gains or losses.

The tax calculation can become more complex as the number of transactions and different cryptoassets that are owned increases. Additional rules, such as the same-day. 30day rules, also apply that add further complexity.

Remember: tax can arise whenever tokens are disposed of, whether or not cash is received, such as when one cryptoasset is exchanged for another.

6. HMRC enquiries

HMRC has a dedicated crypto team and already receive data dumps from exchanges and other cryptoasset service providers. HMRC will then use other means to open an investigation such as statements on a project's or individual's X or discord.

HMRC enquiries can be lengthy and require careful handling. In addition to any unpaid tax, interest and penalties can also be added. Penalties depend on "customer behaviour" and can be up to 100% of the underdeclared tax. which can increase to up to 200\% where offshore links exist.

It is well known that crypto can be traced and owners identified. Tax administrations globally are increasing their efforts to ensure that the correct tax is paid. Recently. HMRC sent "nudge letters" to those that they considered had potentially undeclared tax liabilities, and the information on ownership of cryptoassets continues to grow.

The Crypto Asset Reporting Framework (CARF) is a new reporting framework from the OECD that requires cryptoasset exchanges to provide details of cryptoasset transactions to tax administrations. CARF is being introduced into approximately 60 jurisdictions around the world.

HMRC has released the draft regulations for CARF, which will be put into force in the UK from 1 January 2026. This will provide HMRC with more information than ever before on cryptoasset owners.

Cryptoasset exchanges in the scope of CARF, will be required to put systems in place to gather the required information on their customers. This must include gathering selfcertifications from all customers and recording all transactions for each cryptoasset for the information to be aggregated and submitted to HMRC.

TRACING, FREEZING AND RECOVERY - WHEN CRYPTO ASSETS ARE STOLEN
(Matt Green - Lawrence Stephens and
CHAPTER 06

The misappropriation of crypto assets is common and often versed as an operational risk. Whether:
(i) via hacking like phishing, ransomware, state sponsored operations or data thefts;
(ii) through social engineering operations like fake investment platforms or romance scams; or
(iii) from insider threats like rogue employees, developers or even rug pull scams,
it feels helplessly difficult to recover the funds. Lack of a centralised intermediary to report your loss to, pseudonymity and near-instant transactions to anywhere in the world, are unfortunately also strong enablers for criminal activity.

To be clear, recovery is real, court sanctioned and expected.
If assets are gone, time is of the essence. Report this to your lawyer and or private blockchain investigation firm immediately. and provide transaction hashes, asset type and quantum. Always report the incident to law enforcement as a matter of good practice and obtain a crime reference number.

Furthermore, as a Web3 builder or platform operator, you play a pivotal role in addressing stolen crypto assets, particularly if your project becomes a conduit for illicit activity.

For centralised platforms that custody crypto assets. applicable regulations often require you to collect KYC data from users and actively detect and prevent misuse. If stolen assets are traced to your platform, you must be prepared to respond promptly to legal notices, freeze affected accounts, and provide disclosure as mandated by court orders.

For decentralised and non-custodial projects, while you cannot freeze or seize assets, you can still contribute by providing transparent access to transaction data, educating users about risks, responding to legal notices, and implementing monitoring tools to detect illicit activity. Proactive cooperation with investigations not only reduces legal risks but also strengthens trust in your platform's integrity.

Cryptoasset Tracing

The usual goal of criminals is to as soon as possible convert stolen crypto assets to fiat currency and launder the money outside of blockchain networks. Off-ramping into fiat can take place only through centralised service providers (e.g. crypto exchanges), which have ability to freeze and seize stolen funds. Therefore, your first step should be to identify the movement and location of the assets up until such centralised intermediaries are determined. This can be done thanks to the very nature of blockchain technology.

Most blockchains serve as public, immutable ledgers, making the movement of cryptoassets directly visible onchain. By stealing crypto assets and transacting with them further, criminals leave tamper-resistant trail of evidence, which may be used to find them and bring them to justice. In order to do that, it is therefore crucial to combine onchain transaction data with offchain information (like KYC data, or wallet ownership) to identify the individuals or entities behind receiving or transacting addresses. This can be achieved by using blockchain analytic tools available on the market, which not only visualise transaction flows but also enhance them with offchain data, such as attributing specific addresses to cryptocurrency exchanges or other centralised service providers.

Such tools are used to trace crypto assets and conduct blockchain investigations by law enforcement, private crypto recovery companies but also by crypto asset service providers (e.g. crypto exchanges). The latter use such tools also to regularly monitor processed transactions and assess risks of money laundering and terrorist financing.

Criminals are well aware of the traceability of their onchain transactions and employ various techniques to obfuscate their activities and complicate tracing efforts. These methods include using mixers or tumblers to mask transaction origins, transacting through multiple services-often with accounts opened under fake identities or via money mules-and leveraging cross-chain bridges to move assets across blockchains. While these tactics create additional complexity, tracing and overcoming such obstacles is often achievable with the right analytical tools, expertise, and persistence.

When stolen assets are held in unhosted wallets, there is generally little that can be done to freeze or seize them, apart from ongoing monitoring and flagging as stolen in different databases and networks. This renders such assets "tainted," making them virtually untouchable for legitimate service providers.
An exception to this rule is stablecoins-digital assets pegged to fiat currency, such as USDT and USDC. Issued centrally by Tether and Circle, respectively, these stablecoins include

functionalities in their underlying smart contracts that allow the issuers to blacklist (freeze) wallets and even burn and re-mint tokens to another wallet. In such cases, the goal of tracing is to gather sufficient evidence to enable law enforcement or courts to request stablecoin issuers to blacklist the stolen assets and reassign them to their rightful owner.

Proceeds of Crime Letters and Procedure

Once you know the location of the assets and their pathways. the first step is a legal letter, to put the cryptocurrency exchange or service provider on notice that they have received the proceeds of crime, and to detail how they must treat those assets. Failure to comply is likely to be a criminal offence in most jurisdictions. This draws a line in the sand, and ensures those exchanges are aware of the fraud and their roles going forward.

That letter will include a blockchain analytics report to show the movement and location of funds, including any mixing services if appliable. It will also request balances at the relevant address (or account where funds are pooled ${ }^{37}$) to ensure pursuing funds is commercially viable. The letter also requests certain disclosure relating to their customers who took receipt of the funds, and to prevent any withdrawals from the respective addresses/ accounts. The exchange usually seeks a Court Order compelling them to do so.

Court procedures can broadly be divided into two parallel processes, Process 1 being a substantive claim, outlining the claim for, amongst other things, deceit and restitutionary claims (making someone whole) against the bad actors and Process 2 being interim reliefs, like injunctions to prevent the assets from being dissipated. Process 2 is run to ensure Process 1 is fruitful and to mitigate risks.

Identifying the Defendants

The process starts by relying on "persons unknown" jurisdiction. ${ }^{32}$ meaning that categories of currently unknown defendants can be included in proceedings.

The first defendant will be a category defined by their actions, which may include a person who used a social media account, hosted a platform, or at least deprived an address of certain assets, being DI. This jurisdiction applies where you can serve the defendant with legal documents. ${ }^{33}$ in this instance via an NFT^{34} to the receiving address to which the stolen funds were paid, or otherwise.

The second category of defendant is the person/persons who are recipients of the traced funds and are customers of the cryptocurrency exchanges identified in the blockchain analytics report, here called D2. These parties remain unknown until the cryptocurrency exchange provides details under Process 2.

The other defendants are the relevant cryptocurrency exchanges whose customers are D2, and are not alleged to have committed any wrongdoing. They are included to ensure they provide disclosure of D2 (and D1 if possible) and to comply with the freezing of funds. So long as these exchanges can take receipt of Court documents, whether by email, NFT to the relevant address

or otherwise, they can be included. Registrations in faraway jurisdictions, or claims of decentralisation do not defeat this process. Similarly. exchanges unwilling to provide their corporate structure can be included as another category of persons unknown, being those parties who control, operate, manage and or own that exchange. ${ }^{35}$ In any event, these exchanges are the vital touchstone of the case, and demask D2.
${ }^{31}$ Pircozzadeh v Persons Unknown and Others [2023] EWHC 1024 (Ch) particularly paragraphs 8 and 26
${ }^{32}$ Bloomsbury Publishing Group Ltd v News Group Newspapers Ltd [2003] EWHC 1205 (Ch), see paragraph 21 and and CMOC Sales \& Marketing Ltd v ${ }^{33}$ Person Unknown \& Ors [2018] EWHC 2230 (Comm) (26 July 2018) at paragraph 9
Tippawan Boonyaem v Persons Unknown Category (A) \& Ors [2023] EWHC 3180 (Comm) and by comparison Mooij v Persons Unknown (February 2024) EWHC 814 (Comm) considering Cameron v Liverpool Victoria Insurance Co Ltd [2019] UKSC 6
${ }^{36}$ Fabrizio D'Aloia v. (1) Persons Unknown (2) Binance Holdings Limited \& Others [2022] EWCH 1723 (Ch) (June 24, 2022)
LMN v Bitflyer Holdings Inc and others [2022] EWHC 2954 (Comm)
AA v Persons Unknown \& Ors, Re Bitcoin [2019] EWHC 3556 (Comm) (13 December 2019)

Freezing Funds and Disclosure
Process 1 allows for a claim against the Defendants broadly as above. Process 2 includes a Court application made without notice on D1 and D2, for, amongst other things, (i) the specific treatment of the traced funds as property ${ }^{36}$ (in equity or otherwise), including to demarcate, ringfence and prevent the withdrawal or conversion of those funds (ii) a freeze over all of D2's assets worldwide and (iii) identification details of D2, including any documents or information used for onboarding at the exchange, and any transactions details in a specified period. We are able to rely on disclosure even where information is fake, where the email address is designed for a one-time use, or manipulated identification documents are used.

Once the documents are served on D2 (now identifiable individuals), they are entitled to give evidence at a return date in Court. Most do not, as they are money mules uninterested in giving evidence in formal proceedings. That is the cost of operation. At this stage, funds should be frozen at exchanges, and Process 2 is largely complete.

Recovering Funds
Process 1 continues, and the defendants will have a number of days to file a defence in Court. In most instances they fail to do so. and the victim can apply for default judgment (the defendants have run out of time) or summary judgment (broadly there is no reasonable grounds for defending the claim). This is a win on paper.

As to enforcement, ${ }^{37}$ the judgment can be used to seek recompense from the exchanges, who have D2's assets frozen. Another Court order will compel the exchanges to hand over the funds, and a recovery is made. If the funds have been cashed out, the disclosure should provide for the D2's bank details too, and banks can assist.

This is a very simple outline of how these processes might run, and things can become more complicated depending on the fact pattern. However, this process can be quick, cost effective and prevents bad actors relying on pseudonymisation, being located offshore, or appearing to not exist at all.

Receiving Proceeds of Crime and Letters Requesting Freezing

If you run, operate, manage, control or own a cryptocurrency exchange, are a service provider which deals with cryptocurrencies, including Web3 projects, and receive the proceeds of crime, even unknowingly, you may still be liable under proceeds of crime legislation.

Transaction monitoring services are extremely useful in mitigating risks of processing and custodying the proceeds of crime and should be used as a matter of good practice.

In the event you are aware that you are processing. custodying or dealing with the proceeds of crime in any way, you must deal with them carefully. If you receive a letter alleging receipt of the proceeds of crime, you must act as if you have done so.

Broadly you should not allow the assets to be withdrawn, converted or transacted, and inform a member of law enforcement without delay, called an authorised disclosure. It is vital to check the rules around dealing with the proceeds of crime in your relevant jurisdiction. You must also not tip off the party who has provided those assets.

It is best practice to note instances of dealing with proceeds of crime without delay.
\$3LMN v Bitflyer Holdings Inc and others [2022] EWHC 2954 (Comm)
\$3AA v Persons Unknown \& Ors, Re Bitcoin [2019] EWHC 3556 (Comm) (13 December 2019)
${ }^{57}$ Joseph Keen Shing Law v Persons Unknown \& Huobi Global Limited (unreported. 26 January 2023)

YOU'RE OFF TOKEN LAUNCH

(James Burnie and Pavan Kaur - WAGM Advisers, Gunnercooke
CHAPTER 07

Traditionally, token launches have been seen as a global phenomenon, the idea being to play a numbers game to generate as much income from the launch process as possible. However, such an approach has become increasingly illegal, with rules and licensing restrictions both in terms of the place (i) where tokens are sold from and (ii) where tokens are sold to. Furthermore, in order for a token launch to be truly successful, it is vital to look beyond legal considerations and. for example, curate a well-developed and functioning community that supports the token.

Legal: Boring until it isn't! A UK token launch: for startups, a thing of the past

The act of selling a token from the United Kingdom (UK) triggers a requirement to register with the FCA under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. Currently, there are around 50 firms registered with the FCA, against a backdrop of a failure rate of around 90% among those firms that have applied. Whilst, with the right advisors, the process for becoming FCA registered is clear and achievable, it is generally not an appropriate first step for a start-up to become registered. Rather, it is more usual to sell into the UK from an offshore jurisdiction - and, whilst a consideration of offshore jurisdictions is outside the scope of this guide, it is worth noting that tax considerations have an integral role to play in determining what jurisdiction to sell into the UK from.

Selling into the UK: getting it right matters

Once the token issuing entity is set-up, the next question is what jurisdictions the token can be sold to. In this respect, different countries have brought in different regimes in order to protect their populations. For example: in the EU, this has taken the form of MiCA; in the UK, it takes the form of the financial promotions regime; and in the USA (whilst the position is currently unclear), it generally takes the form of treating the majority of cryptoasset activity as falling within the existing securities rules. Whilst these are the most wellknown regimes, it is worth noting that most new regimes ranging from Kazakhstan to Botswana to Mauritius generally have restrictions on selling to their general population unless local legal and requirements are met.

Traditionally, a "who cares?" approach has been taken to these developments, the assumption being that nothing will actually happen if these marketing rules are broken however, this approach is coming under increasing pressure. There are, of course, the well-publicised moves by the SEC in the USA to take jurisdiction over any cryptoasset enterprises that interact with US persons (that may include persons with a US passport even if not in the US). In the UK, we are also seeing the FCA flex its muscles, as indeed a failure to comply with UK requirements is a criminal offence, punishable by an unlimited fine and imprisonment for up to 2 years. The "criminal offence" element here is particularly important, as it means that all service providers to a project, such as banking partners, are handling the proceeds of crime if cryptoassets are sold in breach of the UK financial promotion rules. As such, the FCA has the ability to simply make a public statement that a project is in breach of the UK rules (called a consumer warning), and the effect will be that many service providers will no longer be prepared to support the project for risk of sanction. Furthermore, in more extreme cases, we have seen the FCA and other regulators co-ordinate to bring an end to projects considered particularly harmful.

It is worth noting that the FCA is taking a broad interpretation regarding what is meant by selling into the UK - and generally any communication in English needs to be considered carefully. As such, even if the intention is not to sell into the UK, care needs to be taken to ensure that appropriate barriers are in place to block communications from being viewed or accessed by persons in the UK. This includes making sure that, for example, appropriate disclaimers are in place to make it clear that a communication is not intended for the UK market in all social media posts.

Selling into the UK: the thing of the future.
Given the evolving landscape, token sales becomes a numbers game from a legal perspective. In this respect, whilst we have seen the UAE often held out as a jurisdiction to sell into due to its traditionally relatively lax approach, in practice this is limited as the hype of what can be achieved in sales simply does not meet the reality. This causes projects to look elsewhere. The EU, which was also previously lax in the sense that certain licences were relatively cheap and easy to obtain, is now moving into a more aggressive regime under MiCA, which brings with it added uncertainty.

What is certain is that the EU will become more expensive however, we note that with the right structuring, it is possible to sell tokens into the EU without requiring a MiCA licence, and so well-informed projects will be able to manage costs. Given, therefore, the UK is one of the largest crypto economies globally, and the relative cost of accessing the UK will become relatively cheaper as other jurisdictions become more expensive, it is likely that the UK will increasingly become a vital part of the product road-map for successful projects.

Against this background, the UK is likely to become a more attractive jurisdiction to sell into. In this respect, it is worth noting that not all cryptoassets are within the scope of UK financial promotions regime: tokens are not in scope if they are unregulated tokens (on which see below) and either (i) non-fungible or (ii) non-transferable. As such, unregulated NFTs are generally not subject to any restrictions on selling into the UK.

Tokens are unregulated where they do not constitute emoney or securities. The definition of e-money is relatively narrow, and so does not cover most of the stablecoins that currently exist, however this may change as a new regime for regulating stablecoins used for payment services is coming into force. The definition of security in the UK is relatively tightly defined, by reference to a specific list of so-called "specified investments". Most of the time, it will be clear whether a cryptoasset is a "specified investment", as for example tokenised equity and bonds are clearly security tokens. Where it gets more complex is in relation to cryptoassets where the holding of such gives a right to a variable income, as this may imply that the cryptoasset is a "collective investment scheme" (or in less formal language, a "fund").

Whilst we are seeing a rise in the use of security tokens, currently the majority of the liquidity for cryptoassets is in unregulated tokens (i.e. not e-money nor securities), and so generally start-ups are focussed on selling unregulated cryptoassets into the UK. In this respect, there are a range of options available for selling unregulated tokens into the UK depending on budget and the intended reach for the token. These range from using exemptions (which in very broad terms limit participants to e.g. fund managers and companies with assets over GBP 5 million), to listing on a UK exchange that can make promotions on its own behalf (and thereby indirectly promote the cryptoasset). and lastly to obtaining sign off of promotions by firms with the appropriate FCA authorisation to provide such sign off (which are relatively few in number).

It is worth noting that when selling into the UK, other than doing so on the basis of relying on one of the limited exemptions, a proper user interface build for UK consumers is required, for example there is a 24 hour cooling off period and an appropriateness assessment that must be complied with, as well as limits on the ability to use certain marketing techniques - for example incentives such as "refer a friend" campaigns are prohibited.

The universal passport that is the UK legal system

Whilst the complexity of the UK rules should not be underestimated, they do have the advantage of clarity. It is also worth noting that different regulators are taking note of regimes in other jurisdictions, and in this respect, we note that the UK legal and regulatory regime, being one of the first global movers to regulate Web3, is often used as a starting point for other jurisdictions looking to regulate the industry. In this respect, it is notable that UK opinions are often, for example, accepted by non-UK exchanges as giving a solid indication of the likely regulatory treatment of cryptoassets in their jurisdiction, even if not technically on-point.

It is also worth noting that UK law, being internationally recognised as robust and well-equipped to deal with the Web3 industry, is often the law of choice when contracting, even if none of the parties involved have a UK nexus. As such, the UK is a logical part of the international roadmap for token projects seeking to develop a solid international reputation.

Whilst regulation is generally jurisdictional-specific, marketing campaigns are generally global in nature. As such, in this section we take a more jurisdiction agnostic approach.

All token marketing campaigns worldwide must now consider compliance at every step, though it is not as daunting as it sounds. Incorporating legal disclaimers when seeking to promote your token, alongside aligning communications with your terms of business, will materially support your business' long-term interests. This is a standard operating procedure across all regulated industries.

While your venture is building its own unique brand identity and community culture, it is important to take a considered approach in order to have a robust model that will withstand future developments. In this respect, it is worth noting that regulators globally are starting to take an interest in how Web3 projects are marketed, and so businesses are beginning to adopt best practices to future-proof their position. In this respect, we have seen firms having to defend historic marketing to regulators when seeking (for example) to obtain licences to operate, and so getting your marketing wrong, even if at an early stage, can cause real damage to the future prospects of a business.

1. Community Management

Your community, although not necessarily mutually exclusive. is divided into two groups: commercial users and token holders (investors). Combined, they form your largest stakeholder group (in terms of numbers of individuals) and should be treated with a level of importance and care that recognises this fact.

Contrary to popular belief, community management is different to community growth with one requiring a very different set of skills to the other. Community management is the day-to-day oversight of your Telegram / Discord presence.

Effective community management combines frequent and transparent communication with the implementation of robust moderation and security policies for all team members within this division. Think of it like a well-oiled cog that's a fundamental part of a larger machine. your business operations.

Community management is imperative to treasury management.

Alongside policies, giving your Head of Community. Community Managers, and Ambassadors professional training therefore comes with high recommendation as, beyond the brand championing, they need to be equipped to identify the warning signs of a security breach, and respond effectively to Fear, Uncertainty \& Doubt (FUD).

Outsourcing your community management team may be a quick way to "get the job done", though it is generally not recommended in the long term as this approach can impose expensive fixed costs (as opposed to having SAFT agreements with Ambassadors for example), be robotic-like in nature and fail to create authenticity in the brand.

The question you should ask yourself continually as a founder is. what are we doing to show our existing and prospective token holders that we care about what we are building? So, what approaches should you take to growing your community?

2. Community Growth

As part of your go-to-market strategy. you will have identified your target audience and competitive landscape, all of which is in alignment with your tokenomics, corporate structure and regulation. By leveraging the below tools with an overarching pragmatic, risk-based approach, you can seek to grow a vibrant community.

i. Influencers

While influencer campaigns are arguably one of the most popular ways to grow your community across social media and community channels, engaging with them is not without reputational risk. The FCA has recently cracked down on 'Finfluencers', as they are labelled, and regulators globally show no sign of slowing down their efforts to protect the interests of the industry.

Founders can manage this reputational risk through implementing robust performance screening that delves into previous campaign metrics, including how organic their audience is. Day-to-day management of influencers can include implementing various KPIs and creating campaigns that align with your public relations and media outreach strategy.

In addition, engaging with an experienced lawyer to ensure 'well written' contracts are in place, and 'dos' and 'dont's' guidance is shared with each influencer is another solid preventative measure founders can take.

As a general rule, seeking to engage with influencers that are relevant to your vertical and that you genuinely believe are needed for what you are building may be a more sustainable approach that goes a long way with your community. After all, if your largest stakeholder group witnesses the development of a long-term relationship with a well-known name in the industry. sentiment in your project can become increasingly positive.

ii. Public Relations \& Media Outreach

Press is not a "grow a big community quick' tool. Rather, press is a long-term investment to increase the touch points through which retail can learn about and access your brand.

While you may seek to purchase sponsored packages directly from Tier 1 outlets to get the word out about a rewards scheme or milestone, gaining earned media is often seen as the more 'sophisticated' approach and a great way of building credibility.

It is important you work with an external provider that understands the nuances of public relations, has an expansive network of journalists, and has proven readership success.

iii. Market-Makers

Market-makers are essential to ensure that there is a buyer and seller of your token on a centralised exchange, and as such are essential to keeping volatility at bay. As a highly requested service provider, it is well documented that market-makers can manipulate markets and dump tokens on unsuspecting investors.

Founders often find themselves in a precarious position, wanting to rely on these entities to gain traction yet remaining unsure of their intentions. To avoid being left with your tail between your legs, it is important to consider the following:

- Engaging with an experienced, independent advisor who can act as a knowledge base on your behalf in conversations with market-makers, for example if presented with complex financial instruments, such as options and loans. A lack of understanding surrounding such topics could lead to long-term financial burdens.
- Having expectation management conversations with market-makers early on can help you in selecting a party that aligns with your interests. For instance, how often are they willing to check

in with you and discuss performance? Do they have a live dashboard facility where you can track trading activity? What are their compliance processes? Do they have adequate systems and controls in place that prevent them from market manipulation? Do they come with good recommendations?

To navigate the complexities of market-making. you must stay vigilant and well-informed. It is crucial to choose reputable partners, carefully review contract terms, and maintain constant communication with the market-maker. By understanding the risks and benefits, you can make informed decisions and protect your project.

Shooting for the moon in the beginning stages of listing your token with Tier 1 exchanges is no longer a viable approach to take. Creating a clearly defined listing strategy with your external advisor that honours the value in organic growth may be a more sustainable outlook, and one that prevents the token landing into a crisis, impacting your treasury and reputation.

It is also worth noting that certain exchanges will enable access to certain jurisdictions, and so this is worth thinking about as part of your go-to-market strategy.

iv. Whitepaper

The whitepaper is the most important promotional material that you will create in your token launch journey. Catered to prospective investors, it should contain detailed information on your commercial strategy, technical implementation strategy and token economy. As its contents are composed of multiple disciplines, it is important to create a refined process to align everyone in your executive team and create a singular tone of voice that resonates with the target audience.

As well as a mandatory legal disclaimer, adding research that backs up your value proposition, and is correctly cited, will aid in creating a well-rounded document for public consumption.

Naturally, your value proposition may evolve over time, and so it is important that when creating your whitepaper, the wordage recognises this, thus allowing room for both malleability in the business and managing the expectations of investors.

v. FAQ

Supplementing the whitepaper, a robust FAQ of at least 50 questions and answers can be created to strengthen communication around the value proposition and highlight the depth of consideration given to all areas of interest to investors.

The FAQ should be transparent, informative and easily digestible. As a relatively inexpensive way of creating meaningful content that will take investors through the token launch and beyond ICO, it is a valuable trick to explore.

vi. Media Training

First time crypto founders may see significant value in undergoing training to learn how to communicate with prospective investors via the media. This applies to any appearance, ranging from a YouTube collaboration with an influencer to a public speech at a high-profile event.

If you understand the habits of the demographic group which you are purporting to communicate with and are prepared on how to answer the "harder' questions from retail, you can create a clear narrative with an aim to "convert' listeners into active participants of your ecosystem, whether that be as an

If you understand the habits of the demographic group which you are purporting to communicate with and are prepared on how to answer the 'harder' questions from retail, you can create a clear narrative with an aim to 'convert' listeners into active participants of your ecosystem, whether that be as an investor, commercial user or follower.

Let's face the Music and Dance

Given the complex multi-faced nature of marketing, it is easy to spend a lot and achieve little. Or even worse, land yourself in regulatory hot water. As such, it is important to ensure that GTM is fully thought through well in advance of a token launch. Because whilst dancing to a bull market is fun, there may be trouble ahead...

THE IMPORTANGE OF COMMUNITY AND WEB3 ACCELERATORS
(Cap - Superteam UK)
CHAPTER 08

Throughout this guide, we have provided snapshots of the many areas where projects need to cut their way through the fangled forests of legal and regulatory factors in order to get to a successful launch, break new ground, innovate and create.

In some areas of this guide, there might be simple do's and don'ts. In other areas, it is more a question of being competent in spotting areas, such as data protection, AML and financial promotions, where thorny issues could entrap your project. Being literate in the main principles and concepts that underpin each area will allow you to separate out the key questions and communicate most effectively with advisors. Increasingly, technical ability in successfully managing legal and compliance factors will be an essential skill for projects. Projects that deal well, not just with tech, but also with compliance and regulatory strategy, will also benefit from a further moat and competitive advantage. The fact that this area has some level of entry complexity is not just to be seen as a hurdle to jump over, but also protection that once you have made this investment of time and energy, it will be far harder for competitors to keep up.

In this regard, as projects are starting out but also as they grow, there is huge strength in being part of a powerful community. As the landscape continues to develop and mature, surrounding yourself with likeminded innovators who are finding creative ways to overcome sectoral challenges can be a huge source of support. The Web3 ethos has always been concentrated around the ideals of the open-source community ethos - if there is a challenge. there is nothing that we can't build to overcome it. Some of the best multidisciplinary minds in the world find themselves in Web3, in no small part due to the everchanging complexity and challenge of every aspect of this industry. Whatever key principles exist, whatever market norms or traditional ways of doing things, they can be questioned, reimagined and redesigned.

Being around like-minded innovators to share a space, collaborate and learn is an exciting part of your journey. The Superteam UK member group provides this environment, allowing you to access an everyday opportunity to collaborate with peers at the cutting edge of the digital economy.

So whether you are planning a GTM or at a more advanced stage of your project, but still aiming to stay well clear of any hot water, an important first step is to connect with your local Superteam UK community to access support, resources, and guidance.

Superteam accelerators and community will be both the catalyst and the safety net that helps you achieve your vision and ambitions in this exciting and dynamic new industry.