2022 年 6 月 2 日

MAYER | BROWN

DIGITAL ASSETS DOWNLOAD

デジタルアセット市場の最新動向と課題

デジタルアセット及びブロックチェーンビジネスへの投資と構築 - 3 つの主要な懸念事項と注目すべき領域-

世界中の金融機関、投資家、政府機関が、デジタルアセット経済の創出に向け、膨大なリソースとエネルギーを注いでいます。 この急成長する分野では、ビジネスチャンスが増え続ける一方で、規制や法的リスクへの対応が喫緊の課題となっています。

デジタルアセットやブロックチェーンビジネスへの投資や構築を試みる事業主体にとって、最大の関心事となるのが、規制の不確実性、サイバー攻撃、IP（知的財産）保護の 3 つです。これらの分野は昨今ではどのようなビジネスにおいても重要視されていますが、特にもデジタルアセットやブロックチェーンの世界では重大な懸念事項となり得ます。

本記事では、これらの懸念の論拠、これらの懸念を踏まえて事業主体が現在講じているいくつかの措置、及びこれらの重大な懸念に関して今後特に注目すべき領域を概説します。

規制の不確実性

- **主要な懸念事項**
  - デジタルアセットに適用される現行の法規制の多くは、ブロックチェーン技術が普及する前から存在するものです。その結果、規制間での重複が生じ複雑な解釈を強いられるばかりか、ブロックチェーン技術の活用を阻害する場合もあります。
  - 加えて、新規の又は修正された法規制により、デジタルアセット事業への投資やデジタルアセットそのものが違法、無価値となり、又はそれらの運用にかかる経済的・時間的なコストが増大する可能性があります。
  - 新たな規制により、デジタルアセットやサービスに対する需要が阻害されたり、他社が競合製品を開発する契機となる可能性があります。
  - 特に最近の TerraUSD の暴落/崩壊のような市場の出来事に照らせば、規制は今後も強化され、複雑化する可能性があります。
- **現在のアプローチ**
  - 既存の規制の不確実性にもかかわらず、デジタルアセットやブロックチェーンビジネスの事業主体は、当局による法規制が適用され得ることを前提に、製品やサービスを開発・創造しています。 政府機関や規制当局は、規制と技術革新のバランスをとるべく、これらの分野全般に対する規制を更新し続けます。

– その結果、事業主体は現行の規制の枠組みの中で製品やサービスを構成し、規制の発展に即して、製品やサービスの変更、又はピボット（事業戦略の転換）を企図することになります。

- **今後注目すべき領域**

– 暗号資産の利用を一切禁止する意向を示す国々がある一方で、暗号資産を法定通貨の一種として認める国も現れるなど、各国はデジタルアセットの規制に向けて多種多様なアプローチを確立し続けています。 このことは、デジタルアセット市場の発展やこの分野への投資の流れに影響を与えると考えられます。

– 各国内における規制当局間の競合や重複も、規制の発展に影響を与える可能性があります。

– 事業主体は、市況や顧客の需要の変化に適応するのと同様に、外部アドバイザーの協力を得たうえで、規制の動向を注視し、規制の変更に対応するために製品やサービスの内容及び提供方法を調整する必要があります。

サイバーセキュリティ

- **主要な懸念事項**

– デジタルアセットやブロックチェーン上で取引される物の価値が増大し続けるにつれて、悪質な事業者がデジタルアセットやブロックチェーンネットワークを攻撃し又は混乱させるための様々な手法を生み出していくと考えられます。

– デジタルネイティブでサイバースペースのみに存在するビジネス（ブロックチェーン上で運営されているビジネスなど）は、サイバー攻撃によって壊滅的な影響を受ける可能性が高いです。

– サイバー攻撃が実際に行われた場合、銀行口座や暗号資産ウォレット情報の窃取、個人情報を含むデータ、企業秘密及び/又はその他の知的財産の窃取、デジタルアセット自体の損失が生じる可能性があります。

- **現在のアプローチ**

– 緻密に設計された分散型ネットワークでは、従来の中央集権型ネットワークに比べてセキュリティ上の利点がありますが、ブロックチェーンに発生しうるセキュリティ上の脆弱性が完全に消失するわけではありません。

– これらの脆弱性には、暗号鍵に係るセキュリティの不備や、ソフトウェアコードのセキュリティテストが不十分であることなどが含まれます。

– そのため、デジタルアセットビジネスは、ブロックチェーンによる構造的なセキュリティのみに依存してはならず、物理的形式とデジタル形式の双方から、複数の重複するセキュリティ対策を講じる必要があります。 また、定期的にネットワークの監査を行い、最新の脅威に対応するためにコードとセキュリティ対策を更新する必要があります。

- **今後注目すべき領域**

– ブロックチェーン技術やデジタルアセットを利用した取引総額が増加するにつれ、サイバー攻撃を行う者とブロックチェーンネットワークの利用者とは、より複雑な態様で戦い続けることになると考えられます。

– 各事業主体とブロックチェーンの利用者は、ブロックチェーンとデジタルアセットへのサイバー攻撃を防ぐために、幾重にも重なる防御メカニズムを開発又は設定する必要があります。

知的財産

- **主要な懸念事項**

– 事業主体がメタバースにおいて、NFT やデジタルブランドなどの IP やデジタルアセットを形成した場合、その IP の保護又は管理に失敗するリスクがあります。

– これらの財産に対する法的権利が明確に規定され又は記録されていない場合、事業主体はデジタルアセット IP における価値を維持するための法的手段を持たない可能性があります。

– 同様に、消費者は、NFT と紐づく権利の性質及び範囲について正確な理解を欠いたままこれを購入する可能性があります。

– ブロックチェーン上の IP 関連活動（スマートコントラクトによるブロックチェーン上の IP の権利の販売など）は、IP の盗難や不正利用、誤用や詐欺によるブランドへの損害、事業の市場価値の損失などのリスクを有します。

- **現在のアプローチ**

– デジタルアセット IP の作成又は使用を希望する事業主体は、新規又は既存の IP の権利を付与する前に、慎重にコスト・ベネフィット分析を行う必要があります。

– 事業主体はまた、この IP に関連する法的保護の内容を精査して、付与又は留保される権利の内容を明確化し、IP 侵害への法的措置の実効性を確保する必要があります。

- **今後注目すべき領域**

– デジタルネイティブアセットの権利と利用方法を規定する法律の改正動向を注視するべきです。

– IP をめぐる訴訟・紛争がどのように発展していくか、既存の又は将来の裁判例の動向を注視する必要があります。

– 法執行機関が消費者保護のためにどのような施策をとるかを注視する必要があります。

Mayer Brown は、The Legal 500 United States 2021 の Fintech 部門において、トップグループ (Tier 1) に選ばれています。

For more information about the topics raised in this Legal Update, please contact the members of the Mayer Brown Digital Assets, Blockchain and Cryptocurrency group.

David Beam
Partner, Washington DC

Matthew Bisanz
Partner, Washington DC

Joe Castelluccio
Partner, New York

Kota Fujii
Foreign Associate, New York

Rohith George
Partner, Northern California

Matthew Kluchenek
Partner, Chicago

Christopher Leach
Partner, Washington DC

Andrew Olmem
Partner, Washington DC

Christina Thomas
Partner, Washington DC

MAYER | BROWN

June 2, 2022

DIGITAL ASSETS DOWNLOAD

MARKET UPDATE AND KEY ISSUES REPORT

Investing in—or Building—a Digital Assets or Blockchain Business? Three Key Concerns and Areas to Watch

Financial institutions, investors and governments around the world have devoted massive resources and energy to the digital assets economy. As business opportunities in this rapidly growing sector continue to multiply, the challenges and risk have also increased.

For any business investing in or building a digital assets or blockchain business, three of the biggest areas of concern are regulatory uncertainty, cyber attacks and IP protection. These areas are critical in any business but are particularly challenging in the digital assets and blockchain world.

Described in this update are some key reasons for these concerns, some steps businesses are taking now in light of these challenges and key areas to watch in these critical areas.

REGULATORY UNCERTAINTY

Key Concerns

- Most current regulatory regimes governing digital assets predate blockchain technology. As a result, there are overlapping, complex and sometimes contradictory regulations that apply to digital assets.
- In addition, new or modified regulations could make the investment in a digital assets business or the assets themselves illegal, worthless or too costly or burdensome to operate.
- New regulations could stifle demand or need for a digital asset or service or incentivize competitors to develop different products.
- It is likely that regulation will continue to increase in the future, especially in light of market events such as the recent crash/collapse of TerraUSD.

Current Approach

- Despite existing regulatory uncertainty, businesses are developing and creating products and services with an understanding that regulations—in some form—will apply to them. Governments and regulators have a strong incentive to continue developing regulations for all areas of this sector.
- As a result, businesses are structuring these products and services within the outlines of current regulatory regimes and planning for product and service modifications or pivots as regulations evolve.

Key Areas to Watch

- Countries will continue to take different approaches to establishing regulations—while some countries have threatened to ban cryptocurrencies, others have recognized crypto assets as a legal form of currency. This will impact the development of markets and the flow of investment in this sector.
- Competition among regulators within countries may also play a role in how regulations develop.
- With the help of advisors, businesses should keep a close eye on regulatory developments in order to modify or pivot product and service offerings to comply with regulatory changes (in the same way a business would to adapt to changes in market conditions or customer demand).

CYBERSECURITY

Key Concerns

- As the value transacted in digital assets and on blockchains continues to increase, bad actors will be incentivized to invent more creative ways to steal, disrupt and attack digital assets and blockchain networks.
- Businesses that are digitally native and exist exclusively in cyberspace—such as businesses operating on blockchains—can be catastrophically affected by a serious cyber attack.
- When these threats materialize as an attack or breach, they can result in theft of bank account or crypto wallet information, theft of data, theft of trade secrets and/or other intellectual property, and loss of digital assets themselves.

Current Approach

- While well-designed decentralized networks have some inherent security benefits over traditional centralized networks, there are still security vulnerabilities that can arise in blockchains.
- These vulnerabilities can include deficient security around cryptographic keys and insufficient security testing of software code.
- As a result, digital assets businesses should not rely only on the structural security promised by blockchains—they must have multiple overlapping security measures in both physical and digital form. They also need regular reassessment of networks to update code and security measures to respond to the latest emerging threats.

Key Areas to Watch

- As the value transacted using blockchain technology and digital assets increases, cyber attackers and blockchain networks will continue to battle with increasingly sophisticated tools.
- Institutions and individuals will need to develop overlapping mechanisms to make successful cyber attacks on their blockchains and digital assets less likely.

INTELLECTUAL PROPERTY

Key Concerns

- As businesses create valuable IP and digital assets in the metaverse—including NFTs and digital brands—there is risk in failing to properly protect or manage that IP.
- If legal rights for these valuable assets are not clearly defined and recorded, businesses may not have protections in place to maintain the value in their digital assets IP.
- Consumers may, likewise, be misled regarding the nature and extent of the rights they are purchasing in connection with such NFTs.
- IP-related activities on blockchains—such as selling rights to IP on a blockchain through smart contracts—can increase the possibility of IP theft or misappropriation, damage to brands through misuse and fraud, and loss in market value of the business.

Current Approach

- Businesses that want to create or use digital assets IP must undertake a careful cost-benefit analysis before granting rights in new or existing IP.
- Businesses must also assess the legal protections related to this IP, carefully define the rights granted and reserved in connection with digital assets and confirm their ability to enforce and defend their IP rights.

Key Areas to Watch

- Look for updates to laws that more clearly define the rights and uses of these types of digitally native assets.
- Watch the court systems for disputes over IP rights and how they evolve; these types of cases are already showing up in courts and lawsuits.
- Expect law enforcement to increase its efforts to combat fraud on behalf of consumers.

Mayer Brown was ranked Tier 1 in Fintech by Legal 500 USA 2021.

For more information about the topics raised in this Legal Update, please contact the following members of the Mayer Brown Digital Assets, Blockchain and Cryptocurrency group.

David Beam
Partner, Washington DC

Matthew Bisanz
Partner, Washington DC

Joe Castelluccio
Partner, New York

Kota Fujii
Foreign Associate, New York

Rohith George
Partner, Northern California

Matthew Kluchenek
Partner, Chicago

Christopher Leach
Partner, Washington DC

Andrew Olmem
Partner, Washington DC

Christina Thomas
Partner, Washington DC