

Conceptual Framework for Legal & Risk Assessment of Blockchain Crypto Property (BCP)

The New Property on the Block

The age of tokenized ecosystems has begun – the shift from centralized to decentralized blockchain-based creation and transfer of assets is ongoing. Our current world is full of different asset classes ranging from money (in a narrow sense) to gold, real estate, securities, rights and others, many of which are difficult to physically trade or subdivide. Distributed ledger technology, or more specifically blockchain technology, is increasingly providing solutions to this problem.

Blockchain technology can design digital information units that contain elements of a **property right** (according to civil law concepts) to which an owner has direct and exclusive access that can be defended against third parties (right in rem). It contains the tools to program a unique set of information that attributes a property right and enables a secure and registered public transfer of the new type of digitally-defined property: **Blockchain Crypto Property (“BCP”)**.

In addition, the introduction of Smart Contract Systems (“SCS”) at application levels of the blockchain have added immutable functions and property terms to BCPs, enabling not only the execution of bilateral and multilateral programs in accordance with contractual terms and conditions, but also the ability to create co-ownership-like organizations. A BCP is therefore defined as a digital property that can be registered on the blockchain and, in addition, may carry out coded functions governed by an SCS, following coded or manual input by an agreed party (called an “Oracle”).

In order to consistently assess the legal and tax implications, associated risks and investment suitability of BCPs in the tokenized ecosystem, a reliable classification model and risk assessment criteria are indispensable. By applying an assessment method based on functionality, rather than on a particular country’s legal concepts, the classification and risk assessments can be considered in all jurisdictions, regardless of national legal and regulatory frameworks. Though the BCP classification may ultimately lead to different assessments in each jurisdiction, it may facilitate the multijurisdictional understanding of existing and new applications in the tokenized ecosystem, as well as identify coins which may not have the essential characteristics of digital property (i.e. not a BCP). The objective of the risk assessment and resulting BCP rating is to increase awareness and serve as a basis for establishing governance and diligence standards for all different aspects of creating, offering, transferring and holding tokens.

With the above in mind, MME and its team of technology, banking, corporate law, tax and Anti-Money Laundering (“AML”) experts have developed a first draft proposal of a “Conceptual Framework for a Legal and Risk Assessment of Blockchain Crypto Property”.

This paper will:

- provide functional classification leading to three different **BCP Classes**; and
- provide a risk assessment model for BCP, resulting in **BCP Risk Categories**.

From Coins to Tokens – From Initial Coin Offerings (ICOs) to Token Generating Events (TGEs)

Initial Coin Offering (or “ICO”), is far more than a buzzword in the current crypto space. Many ambitious and potentially revolutionary projects raise funds using SCS and Tokens. In general, the term Coin is used for first generation (alt)coins; variations and evolutions of Bitcoin with the mere utility of a currency-like storage of value. Since the creation of Ethereum and Ether, the term Token has come to symbolize the beginning of a new area of Blockchain signature chains. In contrast to simple Coins, Tokens can now include complex and conditional layers of value and information. They can be related to any form of assets and equipped with features and conditions. Although the expression Token has established itself as the evolution of the classical Coin, the term ICO is still widespread in describing the Token distribution process of projects. ICOs neither represent the broad possibilities that a Token can offer, nor does it adequately represent the legal nature of most Token-generating projects.

What is the problem with ICO? Why should we also not simply use “Initial Token Offering” (ITO) as an alternative? First, the structure of the terms ICO and ITO obviously refers to the “Initial Public Offering (IPO)” – and therefore to a specific regulated activity. What may be considered as a catchy expression and analogy can involve an actual legal risk for a crypto project team. An IPO is an offering in which shares of a company are sold, usually to institutional investors. In general, with an IPO, securities are issued. Such securities usually are investment instruments denoting an ownership interest and providing evidence of a debt, a right to share in the earnings of the issuer or a right in the distribution of a property. In contrast, not all, but many Tokens do not represent such rights and should therefore not be classified as securities. Those Tokens simply provide ownership on the Token itself and specific forms of a consumptive use, for example as a right of use infrastructure (a platform) or intellectual property (software). There is neither a direct claim against the blockchain developing entity – often a foundation – nor any form of ownership of this legal entity. Of course, the applicability of regulations must be considered carefully and individually for every project, together with an experienced legal partner.

Secondly, the expression *offering* is suggesting that a blockchain developing entity is directly involved in the distribution process of the Tokens. In fact, Token buyers provide funds to a separate SCS which will behave as programmed (and allocate the funds to developers or escrows and the newly generated Tokens to the investors). From a legal perspective and in accordance with the relevant terms, there is often no direct claim against the blockchain developing entity.

To sum up, what sometimes is called an Initial Coin Offering does neither relate to a coin nor does it include an offering in a legal sense. And it has nothing to do with the legal term and regulated activity of an Initial Public Offering. MME consequently supports using the expression “**Token Generating Event**” (TGE) for current and future projects.

Classification of Tokens

To legally analyse crypto Tokens issued at a TGE or sold on an exchange platform, a classification framework for blockchain crypto Tokens is indispensable. As described above, there are lots of possibilities to design Tokens from a technical, conceptual or legal point of view.

Therefore, the first relevant aspect is what should be an adequate connecting factor for such a classification. Tokens may be distinguished based on several criteria, i.e. technical aspects regarding the underlying blockchain (permissioned/non-permissioned, open/public, proof of work/hybrid/proof of stake). For a legal functional qualification, it is useful to focus on the counterparty.

Therefore, as a working model, we distinguish between the following three major classes of BCPs and Tokens.

BCP Class 1: Native Tokens / Cryptocurrencies (No Counterparty)

BCP Class 1 describes a BCP which can be transferred on a decentralized public ledger protocol which allows an immutable transaction from user 1 to user 2. The BCP has only a registration function to register a property right of an account entry (“native BCP”). Mining of the BCP is usually based on a proof of work concept or proof of stake once established. The issue amount is limited and/or a transparent deflation structure exists.

Therefore, the BCP Class 1 refers to Tokens without any underlying asset. The owner of a Native Token does not have any relative or absolute right, except for the right relating to the Token itself (specifically: on the “chain of digital signatures” or the register entry). The fact that a Token might be used on a specific blockchain system, for example as “gas”, does not undermine it from being assigned to the BCP Class 1. The relevant criteria for this category is the lack of a relative right against a counterparty as the Token generator or a third party, and the lack of any code-based revenue functions. BCP Class 1 Tokens can be sub-divided into the following 3 classes:

(1) Native Currency Tokens

Native Currency Tokens are simple mediums of exchange, units of account and stores of value. **Examples** of Native Currency Tokens are **Bitcoin, Bitcoin Cash, Litecoin, Monero, ZCash**.

(2) Infrastructure Tokens

In addition to acting as mediums of exchange, units of account and stores of value, Infrastructure Tokens provide the possibility to use a specific blockchain infrastructure or technology that does not directly refer to payments. **Examples** of Infrastructure Tokens are **Ether, Ether Classic, IOTA, Ripple, Tezos**.

(3) Application Tokens

Application Tokens can be used as a means of payment for a specific non-infrastructure application or a specific business model. Usually, the application tokens are not based on an independent blockchain but use existing infrastructure (e.g. Ethereum). **Examples** of Application Tokens are **Golem, Gnosis, Wings**.

+ Swiss Law:

There is **no written form requirement** in Swiss Law for the transfer of BCP Class 1. Furthermore, the exchange of Bitcoin to FIAT is **exempted from the Value Added Tax (VAT)**. From our point of view, all different kind of native, currency-like Tokens fulfil the requirement of exclusion from VAT in regard to exchanges either from FIAT to BCP Class 1 or BCP Class 1 to other BCP Class 1 Tokens (i.e. Bitcoin to Ether). It is not a security.

BCP Class 2: Counterparty Tokens

The second category, BCP Class 2, refers to Tokens, which include any form of a relative right either against the Token generator or a third-party. The relative right might be a (legal) right to use the Token generator’s services, a right to receive a financial payment, a right to receive an asset or a bundle of shareholder’s right.

Based on the different characteristics of these relative rights, we distinguish between the following sub-classes in our BCP Class 2: (1) IOU Tokens / Colored Coins and (2) C-Shares.

(1) IOU Tokens / Colored Coins

IOU Tokens represent any forms of an IOU or claim against the token holder or a third party. Examples of such an underlying claim can be the:

- payment of a specific amount;
- participation on future income;
- delivery of a material or immaterial asset.

Typically, the details of the IOU are part of a separate contract between the Token buyer and the Token generator. **Examples** are Tokens on the **Lykke Marketplace**.

(2) C-Shares

The shareholders' rights are also qualified as relative rights. Because of the specific characteristics of Token-based shares, they form a separate sub-category in our classification – C-Shares. In Switzerland, MME together with Swisscom and Blockhaus Investments are currently developing the legal, technical and operational possibilities to trade shares on blockchains¹.

+ Swiss Law:

If the specific right of use is qualified as a relative right, there currently is a **written form requirement** in Swiss Law for the transfer of such relative rights. If the Token were considered as a (physical) bearer instrument (e.g. vouchers), the transfer of the Token would also lead to the transfer of the relative right. Otherwise, but far more complex, the Tokens could be issued as an intermediated security by a regulated intermediary. In this case the written form requirement would also not apply. The qualification as a security are to be made on a case by case basis.

The applicability of the **VAT** depends on the specific underlying value. The transfer of rights and shares is exempted from VAT acc. to MWSTG 21 II 19. e. ("securities, rights [or] derivatives"). If the underlying value is a service or usage right chargeable to VAT, the following situations must be distinguished: (1) Where the Tokens is qualified as a "means of payment" for an unspecified use, there will be no VAT charge at the time of a TGE. (2) At the time of using the service, if the Token is for a specific service only, the TGE may be considered as prepayment according to MWSTG 40 I c, which would lead to a VAT charge at the time of the TGE.

BCP Class 3: SCS Co-Ownership Tokens

The third category, BCP Class 3, includes the more complex cases in which the Token provides technical, SCS-based co-ownership rights. These tokens, respectively the SCS, may further collect and transmit values or contain other functions (e.g. voting).

In contrast to the BCP Class 1 Application Tokens, BCP Class 3 tokens have, as mentioned above, additional input and output functions besides the registration function, i.e. the possibility to co-own a SCS platform (IP) and receive financial returns for the use of the ownership.

In contrast to BCP Class 2, a BCP Class 3 token holder does not have a direct claim or other relative rights against the token generator or a third party. Any cash-flow is based on absolute rights, usually copyrights, on the IP, either on the SCS itself or other intellectual works. The IP is co-owned by all Token holders as programmed in the SCS. Moreover, BCP Class 3 Token holders do not have any interest in a company or any other legal person, nor are the value or cash-flow of the Token derived from the profit of any legal person.

An **example** of BCP Class 3 are the **Singular DTV SNGLS**, where the platform includes an inbuilt transfer of digital units to the SCS.

¹ See C-Share introduction video on: <https://www.youtube.com/watch?v=OVNW0cvTNtQ>

+ Swiss Law:

Regarding the transfer of an absolute right on IP, it must be distinguished between copyrights on the one hand and design, patent and trademark rights on the other. For the first one, there is no **written form requirement**, in contrast to the other IP rights.

The applicability of the VAT depends on the underlying asset and the parties. Any assessment of a Token's qualification as a security must be made on a case by case basis.

BCP Risk Assessment



The categorization of BCP in risk classes depends on the technical, legal and market risks associated with the specific BCP.

Protocol-Related Risks (Underlying Technology)

Risk of Security Weaknesses of the Underlying Technology: The BCP relies on open-source software with the inherent risk that a developer or other third parties may insert weaknesses or bugs into the underlying technology, causing the system to lose BCP that is registered in the public ledger.

Risk of Weaknesses or Exploitable Breakthroughs in the Field of Cryptography: The development of cryptography is continuing. Code cracking, or technical advances such as the development of quantum computers, could present risks to cryptocurrencies and the BCP, which may result in the theft or loss of BCP.

Risk of Underlying Technology Attacks: The underlying technology used for the BCP may be susceptible to various and different network attacks, including but not limited to denial of service attacks and race condition attacks. Any successful attacks present a risk for BCP transactions, i.e. the proper execution and sequencing.

Risk of Blockchain Consensus Attacks: The user must understand and accept that, as with other public blockchain-based systems that rely on independent validators, the underlying technology may be susceptible to consensus attacks, including but not limited to, double-spending, majority voting power and censorship attacks. Any successful attack presents a risk to the BCP, expected proper execution and sequencing of BCP transactions.

Storage, Access of Private Key (PIK)-Related Risks

Wallet System Risk: The BCP may be accessed by a wallet provider with one or several private keys (PIK) stored in its storage system. Certain PIK may also be stored by accredited service providers (e.g. a bank) to facilitate transfers. Users in such cases will not be granted any access to the PIK. Moreover, the user must be aware that the value represented by the BCP is stored in a public ledger, which is neither the property nor under the control of a specific legal person or user of the wallet.

Cyber Security Risk: Cyber security risk is defined as the risk of financial loss, disruption of business activities or reputation damage resulting from absent or insufficient protection safeguarding information technology systems (e.g. hacker attack, virus transmission, and network downtime), poor change management practices or leakage of information. Investors and users are the most exposed to risks of losing funds by investing, storing, managing or transferring cryptographic tokens. Organizations must ensure they provide investors and users with the best tools and security protocols to protect them from theft, malfunctions, and technical incompetence.

Risk of Insufficient User Wallet Encryption: User wallets should be encrypted with a strong password (min 12 characters, alphanumeric, containing special characters such as uppercase letters, spaces or symbols). A standard and well-tested encryption algorithm should be used.

Risk of Insufficient User Wallet Backups: Users should be able to download an encrypted backup of their keys.

Risk of Insufficient Contingency Tools: User should not lose access to funds due to software malfunctioning. User software should contemplate potential network congestion.

Regulation and Money Laundering-Related Risks

Regulatory Risks: Blockchain technologies have been the subject of regulatory scrutiny by various regulatory bodies around the globe. Regulatory risks vary depending on the Token generating structure, mechanisms and classification. The generating and holding of BCP may impact regulatory inquiries or regulatory action, which could impede or limit the ability to hold BCP and/or to generate BCP.

Money Laundering Risks: Where a Token Generating Event accepts and generates assets within the same infrastructure (e.g. ETH – ETH), the buyer's PUK can easily be traced and screened. Conversely, money laundering risks are more likely to be present where Fiat currency is accepted in the initial Token generation without an AML/KYC pre-screening of the buyer, or when a Token is exchanged for another from a different infrastructure in the issuing processes, reducing the visibility of the original PUK.

Following the initial Token offer, funds raised by a corporation may be misappropriated by individuals or groups where there are insufficient controls. Alternative business models that provide strong governance, such as that of a Foundation, significantly reduce the risk of ML by ensuring independent audits and disclosure to authorities of fund management.

Finally, in daily trading, while the anonymity of the BCP sender's true identity carries inherent risks for ML abuse (the individual may be black-listed), the transaction history visible in a pseudonymous system, such as Bitcoin or Ethereum, allows the recipient to complete a KYC/AML screening of the entire history of the asset's transfers.

Market-Related and Counterparty-Related Risks

General Market Risks: Several market-related risks must be evaluated when issuing blockchain-based products. Besides the market liquidity, market size/cap and listings on crypto exchanges, the potential collusion of operators ("Operators"), market manipulation and challenges regarding market surveillance must also be addressed.

Risk of Value Decrease of BCP: Market conversion rate of BCP may change significantly between the time of user's instruction and the time of conversion. Hence, there is a risk of not timely execution.

Operator Counterparty Risk: As all functions of the Operators are not yet regulated, no self-regulating schemes exist and market prices remain volatile (see above), there is an increased operator (counterparty) risk. In particular, an operator would not be in the position to execute a transaction due to organizational, financial and/or regulatory restraints.

Risk of Alternative (Hard-Forked) Underlying Technologies: Alternative underlying technology could be established, which uses the same open source code and open source protocol as the BCP. The official Underlying Technology may compete with these alternative networks, which could potentially negatively impact the value of the BCP.

Summarized Assessment Result



BCP Class 1-3

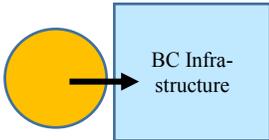
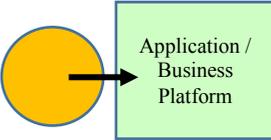
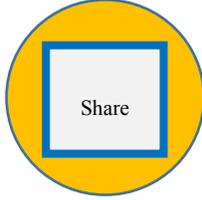
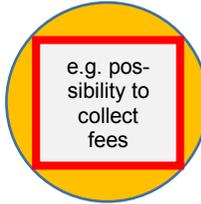
Functional & Legal Perspective

Risk Category A-E

Investor's Perspective

The final stage of a BCP assessment combines the BCP Class, which considers technical aspects, value and the presence of counterparties, together with the BCP Risk Category, based on security, legal and market considerations. The resulting BCP Rating is therefore derived from a standard and holistic assessment of the BCP that aims to provide visibility to regulators and protection to investors, ultimately leading to higher trust and adoption of blockchain technologies.

Functional BCP Classification Overview

BCP Class	BCP Class 1			BCP Class 2		BCP Class 3
	protocol counterparty / no legal counterparty			natural/legal person as counterparty		co-ownership
Sub-Class	Native Currency Tokens	Infrastructure Tokens	Application Tokens	IOU Tokens / Colored Coins	C-Shares	SCS Co-Ownership Tokens
						
Usage	Simple medium of exchange, unit of account and store of value	In addition: access rights to technology / infrastructure	In addition: access rights to application / business platform	In addition: tokenization of relative rights / claims	In addition: tokenization of shareholder rights	In addition: participation on and co-ownership of technical platform/IP
Underlying Value	No underlying relative or absolute right (other than the one on the Token itself)	No underlying relative or absolute right (other than the one on the Token itself)	No underlying relative or absolute right (other than the one on the Token itself)	Relative right (claim) against the Token issuer or a third party	Relative right (share) against the Token issuer or a third party	Technical, code-based co-ownership rights, e.g. on IP
Examples	Bitcoin, Bitcoin Cash, Litecoin, Monero, ZCash.	Ether, Ether Classic, IOTA, Ripple, Tezos	Golem, Gnosis, Wings	Lykke "IOU" Coins, Tether	MME C-Shares	SNGLS
Transfer	Transfer of Token leads to a transfer of an absolute right on the Token (in specific: on the "chain of digital signatures") itself	Transfer of Token leads to a transfer of an absolute right on the Token (in specific: on the "chain of digital signatures") itself	Transfer of Token leads to a transfer of an absolute right on the Token (in specific: on the "chain of digital signatures") itself	Transfer of Token leads to a transfer of a relative right (claim)	Transfer of Token leads to a transfer of relative (shareholders') rights	Transfer of Token leads to a transfer of an absolute right on the Token (in specific: on the "chain of digital signatures") itself
Legal/Regulatory/Tax Qualification	subject to relevant jurisdiction	subject to relevant jurisdiction	subject to relevant jurisdiction	subject to relevant jurisdiction	subject to relevant jurisdiction	subject to relevant jurisdiction
Investor suitability/governance/AML	based on the relevant legal/regulatory/tax qualification	based on the relevant legal/regulatory/tax qualification	based on the relevant legal/regulatory/tax qualification	based on the relevant legal/regulatory/tax qualification	based on the relevant legal/regulatory/tax qualification	based on the relevant legal/regulatory/tax qualification

MME Integrated Approach

MME has set up a team of technology, banking, corporate law, distribution, tax and AML experts jointly providing solutions and expertise for crypto, blockchain and fintech projects. Whether you are developing, procuring, or investing in these areas, we understand the opportunities and challenges your business can face. We have been supporting clients from across the full spectrum. New technologies, such as distributed ledger technologies (blockchain), are part of our daily business. This assures that our legal expertise is combined with a thorough technical understanding of the technology underlying our client's business models.

Your Contact Persons



Dr. Luka Müller-Studer
Legal Partner

+41 44 254 99 66
luka.mueller@mme.ch



Stephan D. Meyer
Research Associate | Crypto

+41 41 726 99 66
stephan.meyer@mme.ch



Peter Henschel
Managing Director Compliance

+41 44 254 99 66
peter.henschel@mme.ch



Chris Gschwend
Senior Compliance Advisor

+41 41 726 99 66
christine.gschwend@mme.ch

MME is an innovative, cutting edge consulting firm for all of your legal, tax, and compliance needs. Our crypto, blockchain and fintech clients range from established international institutions to some of the world's most innovative startups with the potential to become market disrupters. MME is a member of World IT Lawyers (www.worlditlawyers.com) and founding member of the Digital Finance Compliance Association (<http://en.dfca.ch/>) as well as the Crypto Valley Association (<https://cryptovalley.swiss/>).

Office Zurich

Kreuzstrasse 42 | P.O. Box 1412 | CH-8032 Zurich
T +41 44 254 99 66 | F +41 44 254 99 60

Office Zug

Gubelstrasse 11 | P.O. Box 613 | CH-6301 Zug
T +41 41 726 99 66 | F +41 41 726 99 60

www.mme.ch
office@mme.ch