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

Dr. Luka Müller, Stephan D. Meyer, Christine Gschwend, Peter Henschel

Genesis Version

Executive Summary

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**.

Definitions

Blockchain Crypto Property ("BCP"): (1) Digital information containing all elements of a property right (*viz*. p. 1), (2) that is registered on a blockchain or in an alternative distributed ledger, (3) which can be transferred via a protocol, (4) and that may (or may not) carry out additional functions governed by an SCS, following coded and/or manual input. In the following we either use the term BCP or Token, which is the term widely used in the blockchain community.

Blockchain Technology: A blockchain is a type of distributed ledger in the form of a continuously growing list of records based on blocks, which are linked and secured using cryptographic signatures. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. Blockchains are inherently resistant to data modification. From a functional perspective, a blockchain can serve as an open, distributed ledger that can record transactions between two parties (accounts) efficiently and in a verifiable and permanent way.

Distributed Ledger Technology: Database of replicated, shared and synchronised information that is shared in a decentralized manner among network users.

Functions and Tokenizing: A BCP can include two sets of functions: (1) registration functions ("Terms"); and (2) input and output functions ("Conditions"). Tokenizing is the programming of all or part of these functions to a BCP. A Token will be issued and functional once released on a protocol.

Input and Output Functions (Conditions): These functions allow the BCP to interact with other BCPs or external data. The input and output functions are governed by an SCS, following coded or manual input by an agreed 3rd party (called an "Oracle").

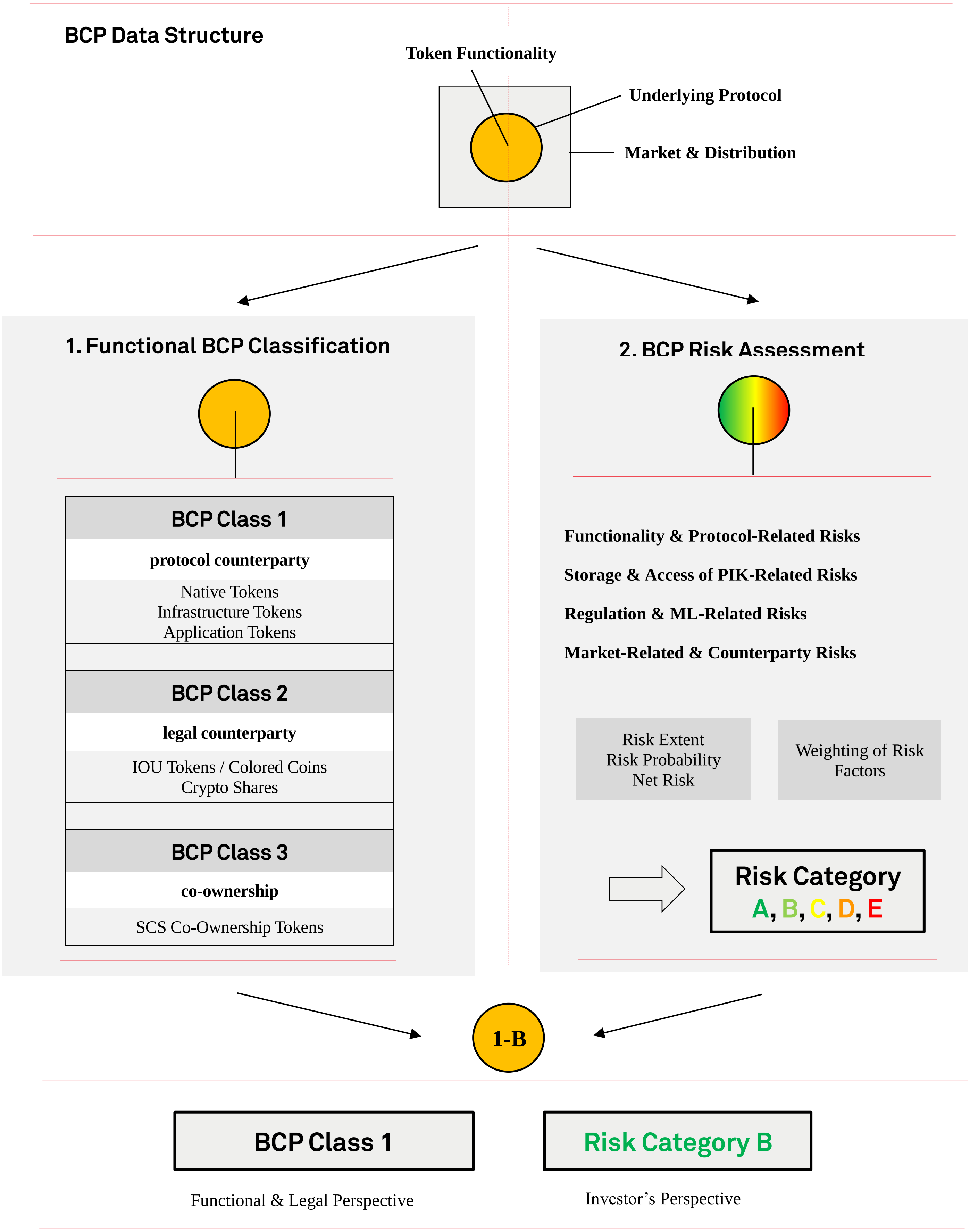
Access Concept and Intermediation: A user is the direct access to BCP, visible through the cryptographic address of the Public Key ("PUK") on the protocol. Intermediary functions are only possible through access, transfer of single-signature or use of multi-signature private keys ("PIK"). Co-ownership is made possible via code-defined SCS functions that cannot be changed or separated from the BCP once released to the protocol.

Platform(s): A platform allows interaction based on a protocol, on which BCP can be created and/or transferred. There are infrastructure platforms such as Ethereum ("Infrastructure Platforms") and specific user platforms built on an infrastructure platform ("Application Platforms"). Platform frequently include an inbuilt algorithm for burning, transacting and creating digital units.

Registration Functions (Terms): This function defines the legal nature of the BCP. There are basically three categories: (1) property right of an account entry (e.g. of a Bitcoin), (2) derivative of a property right leading to a legal right against a counterparty (share in a legal entity or fund, real estate, movable item, registered IP); and (3) a direct property (e.g. on IP).

Smart Contract System: The SCS is distributed-ledger-based computer protocol intended to define, verify, and enforce the functions of a BCP.

BCP Classification and Risk Assessment Method



BCP Data Structure

1. Functional BCP Classification

BCP Class 1

protocol counterparty

Native Tokens
Infrastructure Tokens
Application Tokens

BCP Class 2

legal counterparty

IOU Tokens / Colored Coins
Crypto Shares

BCP Class 3

co-ownership

SCS Co-Ownership Tokens

2. BCP Risk Assessment

Functionality & Protocol-Related Risks

Storage & Access of PIK-Related Risks

Regulation & ML-Related Risks

Market-Related & Counterparty Risks

Risk Extent
Risk Probability
Net Risk

Weighting of Risk Factors

Risk Category
A, B, C, D, E

BCP Class 1

Functional & Legal Perspective

Risk Category B

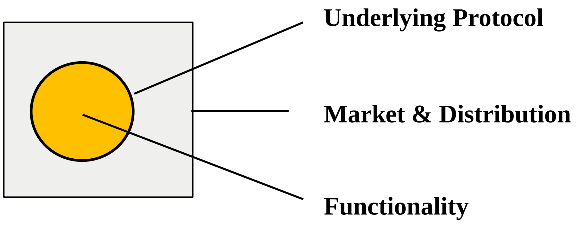
Investor’s Perspective

Genesis Version of 26.09.17

Introduction: Relevant Data

The BCP Classification and Risk Assessment is based on an analysis of the underlying protocol, market-related data and token functionality.

The data examined will represent the basis not only for the functional classification and risk assessment, but also for the resulting BCP rating.



Underlying Protocol Data

The first part, the evaluation of the underlying Token protocol, involves a broad range of different technical and conceptual aspects which may have an impact on the stability, security and/or proper functioning of the BCP. Such aspects are the:

- blockchain protocol used;
- launch date (history of stability);
- timestamping and consensus model (proof of work/stake/hybrid);
- governance model;
- hash algorithm (scrypt/SHA/others);
- number of full nodes;
- implementation of code-based multi-signature PIK;
- possibility of transaction analysis (transparency vs. pseudonymity vs. anonymity);
- implementation of a unit cap or another deflation model;
- past hard-fork history and future planned hard-forks;
- IP rights on underlying protocol.

Market & Distribution Data

The market evaluation focuses on the financial key figures as well as on the availability and tradability of the BCP. The financial data of BCP is analysed for a reference period of the last 30 and 180 days and is set in relation to Bitcoin (BTC) as the first BCP. Therefore, relevant factors are the:

- current Market Cap;
- exchange Listings (number of listings, importance of exchanges);
- price High/Low (30d & 180d & in relation to BTC);
- historical Volatility (30d & 180d & in relation to BTC);
- trading Volume High/Low (30d & 180d & in relation to BTC);
- market Cap High/Low (30d & 180d & in relation to BTC).

The distribution data relates to aspects of pre-functional/functional as well as the contribution structure (public and /or private sales). They further include information regarding the method of contribution, cross-border aspects as well as issuing structure and governance. Relevant points are the:

- pre-sale, pre-allocation, community allocation;
- price finding mechanism, contribution cap;
- issuing legal structure;
- AML, contributor suitability compliance;
- cross-border offering;
- distribution control;
- SCS/code audit;
- after TGE governance.

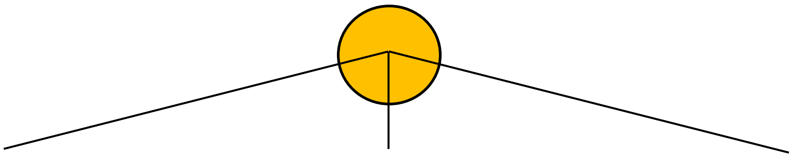
Functional Data

The functional & conceptual evaluation of the BCP is of high importance for the classification of the BCP. Relevant functional aspects are the:

- use of the registration function;
- existence of underlying assets (IOU, share or others)
- target use of the BCP (medium of exchange, unit of account and store of value/access right to infrastructure/access right to application/ownership definer)

1. Functional BCP Classification

BCP classes can be distinguished for a risk assessment based on the technical aspects of the underlying protocol (permissioned/non-permissioned, open/public, proof of work/hybrid/proof of stake). However, from a legal and regulatory perspective, it must be focussed on the underlying or inherent function of the Token. The most relevant element of the function is the existence and the quality of a counterparty. For example, if the Token includes some form of asset and a counterparty, it will have significant legal and regulatory differences compared to a native "currency" Token. Following the above, our BCP distinguish between three major classes of BCPs and Tokens:



protocol counterparty	legal counterparty	co-ownership
BCP Class 1	**BCP Class 2**	**BCP Class 3**
Native Tokens Infrastructure Tokens Application Tokens	IOU Tokens / Colored Coins Crypto Shares	SCS Co-Ownership Tokens

BCP Class 1: 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 specifc 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-infrastructural 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**.

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 blockchains[1].

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).

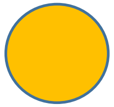
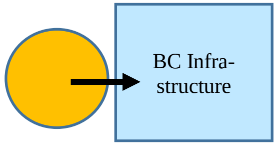
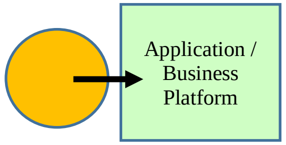
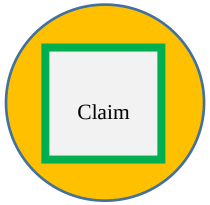
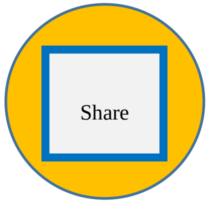
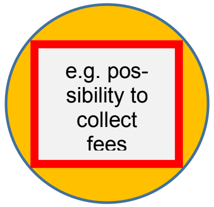
In contrast to the BCP Class 1 Application Tokens, BCP Class 3 tokens have, as mentioned above, additional input and output functions besides the registration function, i.e. the possibility to co-own a SCS platform (IP) and receive financial returns for the use of the ownership.

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.

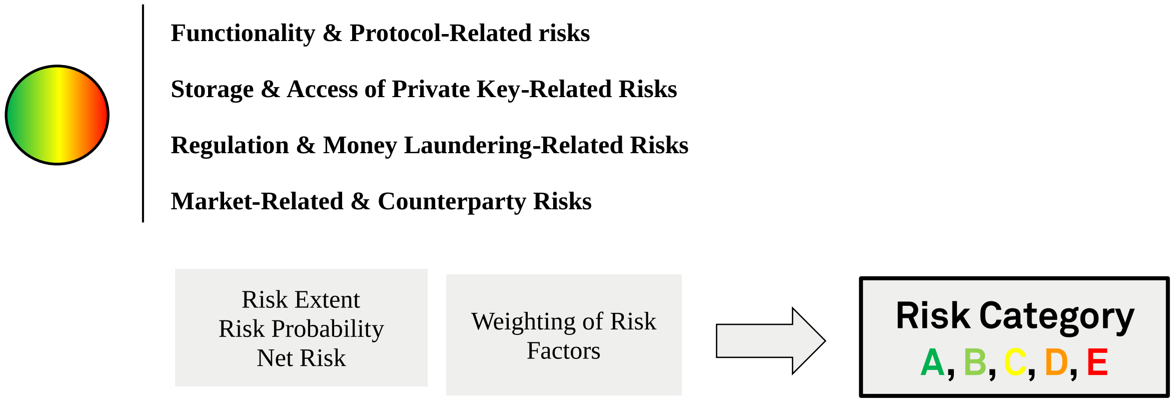
An **example** of BCP Class 3 are the **Singular DTV SNGLS**, where the platform includes an inbuilt transfer of digital units to the SCS.

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

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 oftechnical 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 (Standards)	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

2. BCP Risk Assessment



Functionality & Protocol-Related risks

Storage & Access of Private Key-Related Risks

Regulation & Money Laundering-Related Risks

Market-Related & Counterparty Risks

Risk Extent
Risk Probability
Net Risk

Weighting of Risk Factors

Risk Category
A, B, C, D, E

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 pass-word (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

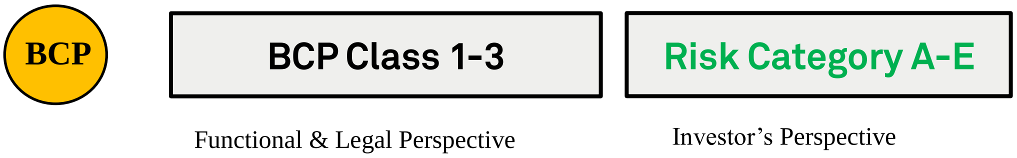
General Market Risks: Several market-related risks must be evaluated when issuing blockchain-based products. Besides the market liquidity, market size/cap and listings on crypto exchanges, the potential collusion of operators ("Operators"), market manipulation and challenges regarding market surveillance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

3. Summarized Assessment Result



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.

Annex: BCP Classification & Assessment of Bitcoin (BTC)

BCP Evaluation	**Token**			
	₿	**Bitcoin (BTC)**		**Measures necessary**
	Underlying BCP Protocol			
	Protocol Name	**Bitcoin Blockchain**		

	Direct / Multilayer Token	**Direct**	Direct = independent BC
			Multilayer = based on diff. BC	

	Launch	**January 2009**		
	BC Characteristics	**public & permissionless**	public & permissionless	
	Timestamping	**Proof of Work (fixed, halving)**	Proof of work / stake / hybrid	
	Hash Algorithm	**SHA256d**	scrypt / SHA / others	
	Avg. Amount of (full) Nodes	**9243**	min. 500	
	Multisig Wallets	**yes**		
	Possibility of Tx Analysis	**yes**		
	Unit Cap	**21M**		
	Hard Fork History	**Hard forked in July 2017 (BTC – BCH), SegWit Activation in August 2017**		
	IP rights	**Open Source**		
	Market Capitalisation & Distribution			
	Market Cap	**$ 75,858,208,934 (06.09.17)**	min. USD 100 Mio.	
	Exchange Listings	**most major (10+)**	min. 1 major	
	Price High/Low (180d)	**$ 4734 (31.08.17) / $ 940 (25.03.17)**		
	In relation to BTC	**1**		
	Historical Volatility (180d)	**37.74%**		
	In relation to BTC	**1**		
	Price High/Low (30d)	**$ 4734 (31.08.17) / $ 2720 (02.08.17)**		
	In relation to BTC	**1**		

Historical Volatility (30d)	**31.28%**	
In relation to BTC	**1**	
Trading Volume High/Low (180d)	**$ 4.26B (22.08.17) / $ 146M (06.03.17)**	
In relation to BTC	**1**	
Trading Volume High/Low (30d)	**$ 4.26B (22.08.17) / $ 1.03B (07.08.17)**	
In relation to BTC	**1**	
Market Cap High/Low (180d)	**$ 81.2B (31.08.17) / $ 15.2B (25.03.17)**	
In relation to BTC	**1**	
Market Cap High/Low (30d)	**$ 81.2B (31.08.17) / $ 44.4B (02.08.17)**	
In relation to BTC	**1**	
pre-sale, pre-allocation, community allocation	**Decentralised non-TGE-distribution**	
price finding mechanism, contribution cap	**Decentralised non-TGE-distribution**	
issuing legal structure	**Decentralised non-TGE-distribution**	
AML, contributor suitability compliance	**Decentralised non-TGE-distribution**	
cross-border offering	**Decentralised non-TGE-distribution**	
after TGE governance	**Decentralised non-TGE-distribution**	
distribution control	**Decentralised non-TGE-distribution**	
SCS/code audit	**Decentralised**	
Registration Function & Underlying Assets		
Registration Function	**BCP account entry**	
Underlying Assets (“Colored Coin”)	**None**	
Target Use	**Medium of exchange, unit of account and store of value**	
	Means of payment (transaction fees) on Bitcoin blockchain	
BCP Classification		
BCP Class	**1**	
Sub-Class	**Native Currency Token**	

BCP Risk Assessment	**Risk Assessment**		**Measures required**
	Full Source Code Screening Required?		
	No	**Sufficient Market Experience with Token**	
	General BCP 1 Risk*	**Specific Risks (Deviation from General Risks)**	
	*Risk Definitions based on the separate “BCP Risk Assessment (BCP RA)” **Risk Categories: 1 (very low risk) - 5 (very high risk)**		
	Functionality & Protocol-Related Risks (“Underlying Technology”)		
	Risk of security weaknesses of the Underlying Technology:	**Long history of stability and functionality**	
		Risk Extent	**3**
		Risk Probability	**1**
		Net Risk	**2**
	Risk of weaknesses of the used cryptography:	**SHA256 expected to remain secure** **ECDSA may be vulnerable to quantum computing attacks**	
		Risk Extent	**3**
		Risk Probability	**2**
		Net Risk	**2.5**
	Risk of Underlying Technology attacks:	**Long history of stability and functionality**	
		Risk Extent	**3**
		Risk Probability	**1**
		Net Risk	**2**
	Risk of blockchain consensus attacks	**very stable PoW consensus mechanism** **regional centralisation of mining in certain countries**	
		Risk Extent	**3**
		Risk Probability	**1**
		Net Risk	**2**
	Storage & Access of Private Key (“PIK”)-Related risks		
	Wallet System Risk:	**no deviation from general BCP 1 risk**	
		Risk Extent	**3**
		Risk Probability	**2**
		Net Risk	**2.5**
	Cyber Security Risk	**no deviation from general BCP 1 risk**	
		Risk Extent	**3**
		Risk Probability	**2**
		Net Risk	**2.5**

	Risk of insufficient User wallet encryption:	no deviation from general BCP 1 risk		
		Risk Extent	3	
		Risk Probability	2	
		Net Risk	2.5	
	Risk of insufficient User wallet backups	no deviation from general BCP 1 risk		
		Risk Extent	3	
		Risk Probability	2	
		Net Risk	2.5	
	Risk of insufficient contingency tools	no deviation from general BCP 1 risk		
		Risk Extent	2	
		Risk Probability	2	
		Net Risk	2	
	Regulation-Related Risks			
	Regulation-Related Risks	no deviation from general BCP 1 risk		
		Risk Extent	2	
		Risk Probability	2	
		Net Risk	2	
	Market-Related and Counterparty-Related Risks			
	General Market Risks	no deviation from general BCP 1 risk		
		Risk Extent	2	
		Risk Probability	2	
		Net Risk	2	
	Risk of Value Decrease of BCP	no deviation from general BCP 1 risk		
		Risk Extent	2	
		Risk Probability	2	
		Net Risk	2	
	Operator Counterparty Risk	no deviation from general BCP 1 risk		
		Risk Extent	2	
		Risk Probability	2	
		Net Risk	2	
	Risk of alternative (hard-forked) Underlying Technologies	hard forked in July 2017, SegWit2x fork planned		
		Risk Extent	2	
		Risk Probability	3	
		Net Risk	2.5	

BCP General Risk Score			
Risk:	**Net Risk**	**Weighting (1 - 3)**	**W Risk**
Functionality & Protocol related risks (“Underlying Technology”)	**2.125**	**3**	**6.375**
Storage & Access of Private Key (“PIK”) related risks	**2.4**	**2**	**4.8**
Regulation related risks and Money Laundering (ML) related risks	**2**	**1**	**2**
Market related risks and counterparty related risks	**2.125**	**2**	**4.25**
			17.425

Risk Score A: <18.5	Risk Score B: 18.5<=X< 20.5	Risk Score C: 20.5<= X<22	Risk Score D: >= 22
Risk Category:	**A**		

Bitcoin	**BTC**	**BCP Class**	**1**
		Sub-Class	**Native Currency Token**
		Risk Category	**A**
MME BCP Rating:		**BCP 1 A**	

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
Zollstrasse 62 | 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