

# **iXBRL XHTML White Paper**

**Human-Readable Rendering of MiCA XHTML Filing**

# Table of Contents

1. White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG VN4VFQXPX
2. Preamble
3. Part A – Information about the offeror or the person seeking admission to trading
4. Part B – Information about the issuer, if different from the offeror or person seeking admission to trading
5. Part C – Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114
6. Part D – Information about the crypto-asset project
7. Part E – Information about the offer to the public of crypto-assets or their admission to trading
8. Part F – Information about the crypto-assets
9. Part G – Information on the rights and obligations attached to the crypto-assets
10. Part H – information on the underlying technology
11. Part I – Information on risks
12. Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts



# White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG VN4VFQXPX

## Preamble

### ***00. Table of Contents***

- Preamble
- 01. Date of notification
- 02. Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114
- 03. Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114
- 04. Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114
- 05. Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114
- 06. Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114
- Summary
- 07. Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114
- 08. Characteristics of the crypto-asset
- 09. Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability
- 10. Key information about the offer to the public or admission to trading
- Part A – Information about the offeror or the person seeking admission to trading
- A.1 Name
- A.2 Legal form
- A.3 Registered address
- A.4 Head office
- A.5 Registration date
- A.6 Legal entity identifier
- A.7 Another identifier required pursuant to applicable national law
- A.8 Contact telephone number
- A.9 E-mail address
- A.10 Response time (Days)
- A.11 Parent company
- A.12 Members of the management body
- A.13 Business activity
- A.14 Parent company business activity
- A.15 Newly established
- A.16 Financial condition for the past three years
- A.17 Financial condition since registration

- Part B – Information about the issuer, if different from the offeror or person seeking admission to trading
  - B.1 Issuer different from offeror or person seeking admission to trading
  - B.2 Name
  - B.3 Legal form
  - B.4 Registered address
  - B.5 Head office
  - B.6 Registration date
  - B.7 Legal entity identifier
  - B.8 Another identifier required pursuant to applicable national law
  - B.9 Parent company
  - B.10 Members of the management body
  - B.11 Business activity
  - B.12 Parent company business activity
- Part C – Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114
  - C.1 Name
  - C.2 Legal form
  - C.3 Registered address
  - C.4 Head office
  - C.5 Registration date
  - C.6 Legal entity identifier
  - C.7 Another identifier required pursuant to applicable national law
  - C.8 Parent company
  - C.9 Reason for crypto-asset white paper preparation
  - C.10 Members of the management body
  - C.11 Operator business activity
  - C.12 Parent company business activity
  - C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114
  - C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114
- Part D – Information about the crypto-asset project
  - D.1 Crypto-asset project name
  - D.2 Crypto-assets name
  - D.3 Abbreviation
  - D.4 Crypto-asset project description
  - D.5 Details of all natural or legal persons involved in the implementation of the crypto-asset project
  - D.6 Utility Token Classification

- D.7 Key Features of Goods/Services for Utility Token Projects
- D.8 Plans for the token
- D.9 Resource allocation
- D.10 Planned use of collected funds or crypto-assets
- Part E – Information about the offer to the public of crypto-assets or their admission to trading
- E.1 Public offering or admission to trading
- E.2 Reasons for public offer or admission to trading
- E.3 Fundraising target
- E.4 Minimum subscription goals
- E.5 Maximum subscription goals
- E.6 Oversubscription acceptance
- E.7 Oversubscription allocation
- E.8 Issue price
- E.9 Official currency or any other crypto-assets determining the issue price
- E.10 Subscription fee
- E.11 Offer price determination method
- E.12 Total number of offered/traded crypto-assets
- E.13 Targeted holders
- E.14 Holder restrictions
- E.15 Reimbursement notice
- E.16 Refund mechanism
- E.17 Refund timeline
- E.18 Offer phases
- E.19 Early purchase discount
- E.20 Time-limited offer
- E.21 Subscription period beginning
- E.22 Subscription period end
- E.23 Safeguarding arrangements for offered funds/crypto-assets
- E.24 Payment methods for crypto-asset purchase
- E.25 Value transfer methods for reimbursement
- E.26 Right of withdrawal
- E.27 Transfer of purchased crypto-assets
- E.28 Transfer time schedule
- E.29 Purchaser's technical requirements
- E.30 Crypto-asset service provider (CASP) name
- E.31 CASP identifier
- E.32 Placement form
- E.33 Trading platforms name

- E.34 Trading platforms Market identifier code (MIC)
- E.35 Trading platforms access
- E.36 Involved costs
- E.37 Offer expenses
- E.38 Conflicts of interest
- E.39 Applicable law
- E.40 Competent court
- Part F – Information about the crypto-assets
- F.1 Crypto-asset type
- F.2 Crypto-asset functionality
- F.3 Planned application of functionalities
- A description of the characteristics of the crypto asset, including the data necessary for classification of the crypto-asset white paper in the register referred to in Article 109 of Regulation (EU) 2023/1114, as specified in accordance with paragraph 8 of that Article
- F.4 Type of crypto-asset white paper
- F.5 The type of submission
- F.6 Crypto-asset characteristics
- F.7 Commercial name or trading name
- F.8 Website of the issuer
- F.9 Starting date of offer to the public or admission to trading
- F.10 Publication date
- F.11 Any other services provided by the issuer
- F.12 Language or languages of the crypto-asset white paper
- F.13 Digital token identifier code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates
- F.14 Functionally fungible group digital token identifier
- F.15 Voluntary data flag
- F.16 Personal data flag
- F.17 LEI eligibility
- F.18 Home Member State
- F.19 Host Member States
- Part G – Information on the rights and obligations attached to the crypto-assets
- G.1 Purchaser rights and obligations
- G.2 Exercise of rights and obligations
- G.3 Conditions for modifications of rights and obligations
- G.4 Future public offers
- G.5 Issuer retained crypto-assets
- G.6 Utility token classification
- G.7 Key features of goods/services of utility tokens

- G.8 Utility tokens redemption
- G.9 Non-trading request
- G.10 Crypto-assets purchase or sale modalities
- G.11 Crypto-assets transfer restrictions
- G.12 Supply adjustment protocols
- G.13 Supply adjustment mechanisms
- G.14 Token value protection schemes
- G.15 Token value protection schemes description
- G.16 Compensation schemes
- G.17 Compensation schemes description
- G.18 Applicable law
- G.19 Competent court
- Part H – information on the underlying technology
- H.1 Distributed ledger technology (DTL)
- H.2 Protocols and technical standards
- H.3 Technology used
- H.4 Consensus mechanism
- H.5 Incentive mechanisms and applicable fees
- H.6 Use of distributed ledger technology
- H.7 DLT functionality description
- H.8 Audit
- H.9 Audit outcome
- Part I – Information on risks
- I.1 Offer-related risks
- I.2 Issuer-related risks
- I.3 Crypto-assets-related risks
- I.4 Project implementation-related risks
- I.5 Technology-related risks
- I.6 Mitigation measures
- Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts
- J.1 Adverse impacts on climate and other environment-related adverse impacts
- S.1 Name
- S.2 Relevant legal entity identifier
- S.3 Name of the crypto-asset
- S.4 Consensus Mechanism
- S.5 Incentive Mechanisms and Applicable Fees
- S.6 Beginning of the period to which the disclosure relates

- S.7 End of the period to which the disclosure relates
- S.8 Energy consumption
- S.9 Energy consumption sources and methodologies
- S.10 Renewable energy consumption
- S.11 Energy intensity
- S.12 Scope 1 DLT GHG emissions – Controlled
- S.13 Scope 2 DLT GHG emissions – Purchased
- S.14 GHG intensity
- S.15 Key energy sources and methodologies
- S.16 Key GHG sources and methodologies

**01. Date of notification**

**02. Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114**

**03. Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114**

**04. Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114**

**05. Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114**

**06. Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114**

**Summary**

**07. Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114**

**08. Characteristics of the crypto-asset**

The crypto-asset VFX referred to in this white paper is a crypto-asset other than EMTs and ARTs and is deployed natively on the VerifiedX network, according to the DTI FFG shown in section F.14, as of 2026-04-21. The maximum supply of the crypto-asset is 200,000,000 VFX tokens. The first activity of the VerifiedX network can be viewed on 2022-07-17 (source: <https://spyglass.verifiedx.io/block/1>).

VerifiedX is an open-source, decentralised Layer 1 blockchain designed to operate as a Bitcoin reliever chain, extending Bitcoin's utility through self-custodial, non-synthetic programmability. The network is intended to support the tokenisation, transfer, storage and exchange of digital and physical assets through on-chain functionality. It uses a consensus mechanism referred to as Proof of Assurance, under which validators are required to maintain an assured VFX balance in order to participate in block production. The network also includes a native smart contract framework based on self-executing smart contracts written in Trillium, under which contract instructions are processed directly by participating nodes rather than through a separate virtual machine. In addition, the network includes a mechanism for tokenised Bitcoin representation through vBTC and a beacon-based system for peer-to-peer transfer of media files, with locator data stored on-chain.

The crypto-asset VFX is used as the native crypto-asset of the VerifiedX network. It is used to pay transaction fees and network service fees, and those fees are burned when processed on-chain. VFX is required to participate as a validator through the assurance mechanism and may be used in connection with governance processes within the network. The crypto-asset is also used for minting supported token formats, including VFX10 NFTs and VFX20 fungible tokens, and for settlement of peer-to-peer transactions and other network activities. The network also supports vBTC as a tokenised representation of Bitcoin on a 1:1 basis, with minting and burning processes linked to verification of Bitcoin deposits and withdrawals by designated validator participants.

The crypto-asset does not grant any legally enforceable or contractual rights or obligations to its holders or purchasers. Any functionalities accessible through the underlying technology are purely technical or operational in nature and do not confer rights comparable to ownership, profit participation, governance, or similar entitlements known from traditional financial instruments.

### ***09. Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability***

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is “a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer”. This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or a service supplied solely by the issuer.

### ***10. Key information about the offer to the public or admission to trading***

VerifiedX LLC is seeking admission to trading on the Payward Global Solutions LTD (“Kraken”) platform in the European Union in accordance with Article 5 of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. The admission to trading is not accompanied by a public offer of the crypto-asset.

## **Part A – Information about the offeror or the person seeking admission to trading**

### ***A.1 Name***

VerifiedX LLC is the person seeking admission to trading.

### ***A.2 Legal form***

The legal form of VerifiedX LLC is NB58, which corresponds to "Limited Liability Company".

### ***A.3 Registered address***

The registered address of VerifiedX LLC is 5830 E 2nd St, Ste 7000, Casper, WY 82609, United States,

### ***A.4 Head office***

Not applicable.

### ***A.5 Registration date***

VerifiedX LLC was registered on 2023-10-17.

### ***A.6 Legal entity identifier***

The Legal Entity Identifier (LEI) of VerifiedX LLC is 254900AA88L2W6K01S70.

### ***A.7 Another identifier required pursuant to applicable national law***

### ***A.8 Contact telephone number***

### ***A.9 E-mail address***

### ***A.10 Response time (Days)***

VerifiedX LLC will respond to investor enquiries within 30 calendar days.

### ***A.11 Parent company***

VerifiedX LLC has no parent company.

### ***A.12 Members of the management body***

### ***A.13 Business activity***

The business activity of the legal entity consists of supporting and sponsoring the VerifiedX decentralised network and acting as the legal entity associated with the network for integrations, partnerships, and related administrative matters. The legal entity does not conduct any other business activity.

### ***A.14 Parent company business activity***

VerifiedX LLC does not have a parent company. Accordingly, no business activity of a parent company is to be reported in this section.

### ***A.15 Newly established***

VerifiedX LLC has been established since 2023-10-17 and is therefore newly established (i.e. less than three years).

### ***A.16 Financial condition for the past three years***

Not applicable. The company has been established for less than three years and its financial condition is provided in Part A.17 below.

### ***A.17 Financial condition since registration***

VerifiedX is a recently established legal entity with limited financial history and limited financial resources. Since its registration, the company has not generated material revenue and has not carried out for-profit commercial activities, service offerings, or other revenue-generating operations. It has not conducted or received financing rounds, external funding, public grants, or comparable third-party financing to date. No audited or unaudited financial statements covering a full financial year are available as of the date of this white paper.

## **Part B – Information about the issuer, if different from the offeror or person seeking admission to trading**

### ***B.1 Issuer different from offeror or person seeking admission to trading***

No

### ***B.2 Name***

Not applicable.

***B.3 Legal form***

Not applicable.

***B.4 Registered address***

Not applicable.

***B.5 Head office***

Not applicable.

***B.6 Registration date***

Not applicable.

***B.7 Legal entity identifier***

Not applicable.

***B.8 Another identifier required pursuant to applicable national law***

Not applicable.

***B.9 Parent company***

Not applicable.

***B.10 Members of the management body***

***B.11 Business activity***

Not applicable.

***B.12 Parent company business activity***

Not applicable.

**Part C – Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114**

***C.1 Name***

Not applicable since VerifiedX LLC is not a trading platform.

***C.2 Legal form***

Not applicable since VerifiedX LLC is not a trading platform.

***C.3 Registered address***

Not applicable since VerifiedX LLC is not a trading platform.

#### ***C.4 Head office***

Not applicable since VerifiedX LLC is not a trading platform.

#### ***C.5 Registration date***

Not applicable since VerifiedX LLC is not a trading platform.

#### ***C.6 Legal entity identifier***

Not applicable since VerifiedX LLC is not a trading platform.

#### ***C.7 Another identifier required pursuant to applicable national law***

Not applicable since VerifiedX LLC is not a trading platform.

#### ***C.8 Parent company***

Not applicable since VerifiedX LLC is not a trading platform.

#### ***C.9 Reason for crypto-asset white paper preparation***

Not applicable since VerifiedX LLC is not a trading platform.

#### ***C.10 Members of the management body***

#### ***C.11 Operator business activity***

Not applicable since VerifiedX LLC is not a trading platform.

#### ***C.12 Parent company business activity***

Not applicable since VerifiedX LLC is not a trading platform.

#### ***C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114***

Not applicable since VerifiedX LLC is not a trading platform.

#### ***C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114***

Not applicable since VerifiedX LLC is not a trading platform.

### **Part D – Information about the crypto-asset project**

#### ***D.1 Crypto-asset project name***

#### ***D.2 Crypto-assets name***

#### ***D.3 Abbreviation***

#### ***D.4 Crypto-asset project description***

VerifiedX (VFX) is an open-source, decentralised Layer 1 blockchain designed to support tokenised self-custody, on-chain storage, peer-to-peer commerce, and Bitcoin-related functionality within a broader distributed-ledger environment. VerifiedX operates as a Bitcoin relayer chain, providing infrastructure for the exchange and transfer of digital and physical assets, as well as for the deployment of smart-contract based applications and related on-chain services.

The VerifiedX network operates through a set of integrated technical components. These include vBTC, a Bitcoin-linked token representation that enables Bitcoin-related use cases within the network environment, including interaction with smart contracts. The project also includes Vault Accounts designed to support transaction recovery and asset-protection features, a Trillium smart-contract framework for self-executing smart contract logic, and a Beacon system intended to facilitate the transfer of larger media files without storing the full underlying content directly on-chain. More broadly, the network uses a custom validator model, on-chain governance processes, and a fixed-supply, deflationary fee design under which transaction and service fees are burned rather than redistributed through block rewards.

The project does not involve the granting of ownership, profit-participation rights, or legal claims against the project entity or its contributors. Instead, it centres on the creation of a technical environment in which the VFX crypto-asset may serve as a governance and functional input for certain protocol processes. The long-term evolution of the VerifiedX system, including the scope of available features, the decentralisation roadmap, validator-selection mechanisms, and the operational continuity of the infrastructure, may vary based on technical, economic, and regulatory considerations. All future developments remain subject to change.

### ***D.5 Details of all natural or legal persons involved in the implementation of the crypto-asset project***

Other person involved in implementation

United States

Other person involved in implementation

United States

Other person involved in implementation

United States

### ***D.6 Utility Token Classification***

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is “a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer”. This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or a service supplied solely by the issuer.

### ***D.7 Key Features of Goods/Services for Utility Token Projects***

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is “a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer”. This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or a service supplied solely by the issuer.

### ***D.8 Plans for the token***

This section provides an overview of the historical developments related to the VFX crypto-asset and a description of planned or anticipated project milestones as publicly communicated. All forward-looking elements are subject to significant uncertainty. They do not constitute commitments, assurances, or guarantees, and may be modified, delayed, or discontinued at any time. The implementation of past milestones cannot be assumed to continue in the future, and future changes may have adverse effects for token holders.

Past milestones:

- Roadmap Publication (December 2025): A roadmap was published describing planned protocol and product developments.
- Butterfly Application Launch (December 2025): The Butterfly peer-to-peer social payment and yield application was launched.
- Bug Bounty Program Release (December 2025): A bug bounty program was released to support the identification of vulnerabilities and technology issues.
- Token Unlocking Schedule (December 2025): A token unlocking schedule was published, relevant to the release profile of the crypto-asset.

Future milestones:

- Oracle Data / Validator Upgrade (Q1 2026, ongoing): An upgrade relating to oracle data and validator infrastructure is planned.
- P2P Smart Contract Release (Q1 2026, ongoing): Peer-to-peer smart contracts with automated execution based on minter parameters and inputs for decentralised and self-custodial borrowing and lending are planned for release.
- Privacy Layer (Q1 2026, ongoing): The introduction of an optional privacy layer is planned.
- Quantum Resistant Addresses (Q1 2026, ongoing): The introduction of quantum resistant addresses is planned.
- AI Smart Contract Writer (Q2 / Q3 2026): The release of an AI smart contract writer is planned.
- Smart Order Routing System Release (Q2 / Q3 2026): The release of a smart order routing system is planned.
- Butterfly Feature Upgrade (Q2 / Q3 2026): Further feature upgrades for the Butterfly application are planned.
- Mainnet Upgrade (Q2 / Q3 2026): A mainnet upgrade is planned.
- BTC / vBTC Validating Enablement (Q4 2026): Enablement of BTC / vBTC validating is planned.

Note: All future milestones are subject to significant uncertainty, including but not limited to technical feasibility, regulatory developments, market adoption, and community governance decisions. The project may modify, delay, or discontinue any of these initiatives at any time. Past implementation or performance outcomes do not constitute an indication of future results, and any such changes may materially affect the characteristics, availability, or perceived value of the VFX crypto-asset for its holders.

### ***D.9 Resource allocation***

VerifiedX has no ICO, disclosed venture, seed, or private funding rounds, and has not conducted any type of offering. Accordingly, no financial resources have been allocated to the project.

### ***D.10 Planned use of collected funds or crypto-assets***

Not applicable, as this white paper serves the purpose of admission to trading and is not associated with any fundraising activity for the crypto-asset project.

## **Part E – Information about the offer to the public of crypto-assets or their admission to trading**

### ***E.1 Public offering or admission to trading***

VerifiedX LLC is the person seeking admission to trading.

### ***E.2 Reasons for public offer or admission to trading***

The purpose of seeking admission to trading is to enable the crypto-asset to be listed on a regulated platform in accordance with the applicable provisions of Regulation (EU) 2023/1114 and Commission Implementing Regulation (EU) 2024/2984. The white paper has been drawn up to comply with the transparency requirements applicable to trading venues.

### ***E.3 Fundraising target***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.4 Minimum subscription goals***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.5 Maximum subscription goals***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.6 Oversubscription acceptance***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.7 Oversubscription allocation***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.8 Issue price***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.9 Official currency or any other crypto-assets determining the issue price***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.10 Subscription fee***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.11 Offer price determination method***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.12 Total number of offered/traded crypto-assets***

The maximum supply of the crypto-asset is 200,000,000 VFX. The effective circulating supply is approximately 137,700,000 VFX as of the date of this white paper.

### ***E.13 Targeted holders***

The admission of the crypto-asset to trading is open to all types of investors.

### ***E.14 Holder restrictions***

Holder restrictions are subject to the rules applicable to the crypto-asset service provider, as well as any additional restrictions that provider may impose.

#### ***E.15 Reimbursement notice***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

#### ***E.16 Refund mechanism***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

#### ***E.17 Refund timeline***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

#### ***E.18 Offer phases***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

#### ***E.19 Early purchase discount***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

#### ***E.20 Time-limited offer***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

#### ***E.21 Subscription period beginning***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

#### ***E.22 Subscription period end***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

#### ***E.23 Safeguarding arrangements for offered funds/crypto-assets***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

#### ***E.24 Payment methods for crypto-asset purchase***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

#### ***E.25 Value transfer methods for reimbursement***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

#### ***E.26 Right of withdrawal***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.27 Transfer of purchased crypto-assets***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.28 Transfer time schedule***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.29 Purchaser's technical requirements***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.30 Crypto-asset service provider (CASP) name***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.31 CASP identifier***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.32 Placement form***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.33 Trading platforms name***

The admission to trading is sought on Payward Global Solutions LTD ("Kraken").

### ***E.34 Trading platforms Market identifier code (MIC)***

The Market Identifier Code (MIC) of Payward Global Solutions LTD ("Kraken") is PGSL.

### ***E.35 Trading platforms access***

The token is intended to be listed on the trading platform operated by Payward Global Solutions LTD ("Kraken"). Access to this platform depends on regional availability and user eligibility under Kraken's terms and conditions. Investors should consult Kraken's official documentation to determine whether they meet the requirements for account creation and token trading.

### ***E.36 Involved costs***

The costs involved in accessing the trading platform depend on the specific fee structure and terms of the respective crypto-asset service provider. These may include trading fees, deposit or withdrawal charges, and network-related gas fees. Investors are advised to consult the applicable fee schedule of the chosen platform before engaging in trading activities.

### ***E.37 Offer expenses***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.38 Conflicts of interest***

MiCA-compliant crypto-asset service providers shall have strong measures in place in order to manage conflicts of interest. Due to the broad audience this white paper addresses, potential investors should always check the conflicts-of-interest policy of their respective counterparty.

### ***E.39 Applicable law***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

### ***E.40 Competent court***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

## **Part F – Information about the crypto-assets**

### ***F.1 Crypto-asset type***

#### ***F.2 Crypto-asset functionality***

VerifiedX (VFX) is the native crypto-asset of the VerifiedX blockchain and functions as the principal on-chain technical component within the VerifiedX protocol environment. VFX is used within the network for the payment of transaction fees and service fees, including fees associated with transfers, network services, Vault accounts, DNS-related functions, and peer-to-peer auction activity. VFX is also used in connection with the minting of tokenised assets on the network, including VFX10 and VFX20 token standards, and supports additional on-chain activities such as transfers, peer-to-peer exchange, lending, swaps, and other interactions made available within the VerifiedX ecosystem.

VFX is further integrated into the operation of the VerifiedX blockchain through its Proof of Assurance consensus model. Participants seeking to join the validator pool are required to assure a specified balance of VFX in order to participate in block creation and validator activity. VFX also functions as a governance-related input within the network, as validator participation is linked to voting on network proposals, protocol changes, upgrades, and other enhancements within the VerifiedX environment. In addition, VFX is used in connection with specialised blockchain features such as State Accounts, Vault Accounts, and the minting and use of Bitcoin-linked, self-custodial, non-synthetic representations such as vBTC within the VerifiedX ecosystem.

The VFX crypto-asset does not confer ownership, profit participation, governance rights over the issuer or any related entity, or any form of economic entitlement. All functionalities are technical in nature and relate exclusively to interactions within the VerifiedX protocol environment. The usability of VFX depends on factors such as the continued operation of the relevant protocol infrastructure, the performance and security of the VerifiedX blockchain, the correct functioning of consensus and smart-contract related systems, and future development decisions associated with the VerifiedX project.

#### ***F.3 Planned application of functionalities***

Future milestones:

- Oracle Data / Validator Upgrade (Q1 2026, ongoing): An upgrade relating to oracle data and validator infrastructure is planned.
- P2P Smart Contract Release (Q1 2026, ongoing): Peer-to-peer smart contracts with automated execution based on minter parameters and inputs for decentralised and self-custodial borrowing and lending are planned for release.
- Privacy Layer (Q1 2026, ongoing): The introduction of an optional privacy layer is planned.

- Quantum Resistant Addresses (Q1 2026, ongoing): The introduction of quantum resistant addresses is planned.
- AI Smart Contract Writer (Q2 / Q3 2026): The release of an AI smart contract writer is planned.
- Smart Order Routing System Release (Q2 / Q3 2026): The release of a smart order routing system is planned.
- Butterfly Feature Upgrade (Q2 / Q3 2026): Further feature upgrades for the Butterfly application are planned.
- Mainnet Upgrade (Q2 / Q3 2026): A mainnet upgrade is planned.
- BTC / vBTC Validating Enablement (Q4 2026): Enablement of BTC / vBTC validating is planned.

Note: All future milestones are subject to significant uncertainty, including but not limited to technical feasibility, regulatory developments, market adoption, and community governance decisions. The project may modify, delay, or discontinue any of these initiatives at any time. Past implementation or performance outcomes do not constitute an indication of future results, and any such changes may materially affect the characteristics, availability, or perceived value of the VFX crypto-asset for its holders.

***A description of the characteristics of the crypto asset, including the data necessary for classification of the crypto-asset white paper in the register referred to in Article 109 of Regulation (EU) 2023/1114, as specified in accordance with paragraph 8 of that Article***

***F.4 Type of crypto-asset white paper***

The white paper type is "Other crypto-assets" (i.e. OTHR).

***F.5 The type of submission***

The type of submission is NEWT, which stands for "New".

***F.6 Crypto-asset characteristics***

The crypto-asset referred to herein is a crypto-asset other than EMTs and ARTs, and is available on the VerifiedX network. The crypto-asset is fungible up to 8 digits after the decimal point. The crypto-asset constitutes a digital representation recorded on distributed-ledger technology and does not confer ownership, governance, profit participation, or any other legally enforceable rights. Any functionalities associated with the token are limited to potential technical features within the relevant platform environment. These functionalities do not represent contractual entitlements and may depend on future development decisions, technical design choices, and operational conditions. The crypto-asset does not embody intrinsic economic value; instead, its value, if any, is determined exclusively by market dynamics such as supply, demand, and liquidity in secondary markets.

***F.7 Commercial name or trading name***

***F.8 Website of the issuer***

***F.9 Starting date of offer to the public or admission to trading***

***F.10 Publication date***

***F.11 Any other services provided by the issuer***

No further services are currently planned.

### ***F.12 Language or languages of the crypto-asset white paper***

***F.13 Digital token identifier code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates***

***F.14 Functionally fungible group digital token identifier***

### ***F.15 Voluntary data flag***

This white paper has been submitted on a mandatory basis under Regulation (EU) 2023/1114.

### ***F.16 Personal data flag***

Yes, this white paper contains personal data as defined in Regulation (EU) 2016/679 (the GDPR).

### ***F.17 LEI eligibility***

The issuer is eligible for a Legal Entity Identifier (LEI).

### ***F.18 Home Member State***

Ireland

### ***F.19 Host Member States***

Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Iceland, Liechtenstein, Norway

## **Part G – Information on the rights and obligations attached to the crypto-assets**

### ***G.1 Purchaser rights and obligations***

The crypto-asset does not grant any legally enforceable or contractual rights or obligations to its holders or purchasers. Any functionalities accessible through the underlying technology are of a purely technical or operational nature and do not constitute rights comparable to ownership, profit participation, governance, or similar entitlements known from traditional financial instruments. Accordingly, holders do not acquire any legally enforceable claim against the issuer of the crypto-asset or any third party.

### ***G.2 Exercise of rights and obligations***

As the crypto-asset does not confer any legally enforceable rights or obligations, there are no applicable procedures or conditions for their exercise. Any interaction or functionality that may be available within the project's technical infrastructure – such as participation mechanisms or protocol-level features – serves operational purposes only and does not create, evidence, or constitute any contractual or statutory entitlement.

### ***G.3 Conditions for modifications of rights and obligations***

As the crypto-asset does not confer any legally enforceable rights or obligations, there are no conditions or mechanisms for modifying such rights or obligations. Adjustments to the technical protocol, smart contract logic, or related systems may occur in the ordinary course of development or maintenance. Such changes do not alter the legal position of holders, as no contractual rights exist and no rights arise under applicable law or regulation. Holders should not interpret technical updates or governance-related changes as amendments to legally binding entitlements.

#### ***G.4 Future public offers***

No future public offers of crypto-assets are currently planned by the issuer at the time of writing this white paper.

#### ***G.5 Issuer retained crypto-assets***

The current amount retained by VerifiedX LLC is approximately 32.3 million VFX, which are reserved for partnerships, bug bounties, integrations, and liquidity purposes.

#### ***G.6 Utility token classification***

No – the crypto-asset project does not concern utility tokens as defined in Article 3(9) of Regulation (EU) 2023/1114.

#### ***G.7 Key features of goods/services of utility tokens***

Not applicable, as the crypto-asset described herein is not a utility token.

#### ***G.8 Utility tokens redemption***

Not applicable, as the crypto-asset described herein is not a utility token.

#### ***G.9 Non-trading request***

The admission to trading is sought.

#### ***G.10 Crypto-assets purchase or sale modalities***

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

#### ***G.11 Crypto-assets transfer restrictions***

The crypto-assets themselves are not subject to any technical or contractual transfer restrictions and are generally freely transferable. However, crypto-asset service providers may impose restrictions on buyers or sellers in accordance with applicable laws, internal policies or contractual terms agreed with their clients.

#### ***G.12 Supply adjustment protocols***

No - there are no fixed protocols that increase the supply of the crypto-asset in response to changes in demand as of 2026-04-21.

However, the protocol includes a built-in fee-burning mechanism under which all transaction fees and network service fees are permanently burned at the time of processing, reducing the circulating supply over time. In addition, it is possible to decrease the circulating supply by transferring crypto-assets to so-called “burn addresses”. These are addresses from which the tokens are no longer intended to be transferred or accessed, effectively removing them from circulation.

#### ***G.13 Supply adjustment mechanisms***

For the crypto-asset in scope, the supply is limited to 200,000,000 tokens. Investors should note that changes in the supply of the crypto-asset can have a negative impact.

#### ***G.14 Token value protection schemes***

No – the crypto-asset does not have any mechanisms or schemes in place that aim to stabilise or protect its market value. Its value is determined solely by market supply and demand, and may be subject to significant volatility.

### ***G.15 Token value protection schemes description***

Not applicable, as the crypto-asset in scope does not have any value protection scheme in place.

### ***G.16 Compensation schemes***

No – the crypto-asset does not have any compensation scheme.

### ***G.17 Compensation schemes description***

Not applicable, as the crypto-asset in scope does not have any compensation scheme in place.

### ***G.18 Applicable law***

Applicable law likely depends on the location of any particular transaction with the token.

### ***G.19 Competent court***

Competent court likely depends on the location of any particular transaction with the token.

## **Part H – information on the underlying technology**

### ***H.1 Distributed ledger technology (DTL)***

The crypto-asset in scope is implemented on the VerifiedX network following the standards described below.

### ***H.2 Protocols and technical standards***

The crypto-asset in scope is implemented on the VerifiedX network following the standards described below.

The following applies to VerifiedX:

The crypto-asset operates on a defined set of protocols and technical standards intended to support the operation, security, and functionality of the VerifiedX blockchain network. Below are some of the key ones:

#### 1. Network protocols

- The crypto-asset operates on a decentralised Layer 1 blockchain network with peer-to-peer communication between nodes.
- Peer communication and message propagation are handled through a P2P layer using SignalR and websockets to maintain open connections between nodes.
- Nodes query peers for the latest block and broadcast newly generated blocks to the network to remain synchronised.

#### 2. Consensus and validation standards

- The crypto-asset uses a custom consensus mechanism referred to as Proof-of-Assurance (PoA).
- Validators are required to maintain 5,000 VFX in their wallet to participate in block crafting and governance.
- Block production is assigned through rotating randomised casters. Casters generate cryptographic proofs using SHA256-based hashing, and the network deterministically selects a winner from the available proofs.
- Other validators then lock the selected winner and vote to confirm block production. If the selected caster fails to produce the block, backup winners may be selected from the available proofs.

#### 3. Cryptographic and data integrity standards

- The crypto-asset uses SHA-256, frequently in double SHA-256 form, for transaction hashes, Merkle roots, and validator proofs.
- ECDSA is used for private keys, transaction signing, and verification of block origin.
- Transactions within a block are organised into Merkle trees formed from double SHA-256 hashes for integrity verification.
- Addresses are encoded using Base58.
- Timestamps follow the UNIX epoch standard.

#### 4. Wallet and address standards

- The network follows BIP-32 and BIP-39 standards for hierarchical deterministic wallets and mnemonic recovery phrases.

#### 5. Protocol improvement standards

- The network uses an on-chain voting process for protocol changes and network improvements.
- Validators participate in voting on proposals, enhancements, and changes to network parameters.
- Significant protocol changes require an 80% approval vote from the validator pool before implementation.

### ***H.3 Technology used***

The crypto-asset in scope is implemented on the VerifiedX network following the standards described below.

The following applies to VerifiedX:

1. Decentralised ledger: The VerifiedX blockchain operates as a decentralised account-based ledger that records transfers, balances, and related state changes in a manner intended to preserve an ordered and verifiable record of transactions.
2. Private key management: To safeguard their VFX holdings, users must securely store their wallet private keys and recovery phrases.
3. Cryptographic integrity: The network uses ECDSA for key generation and transaction signing, and SHA-256, including double SHA-256 in certain cases, for hashing functions such as transaction identification and Merkle-tree construction.

### ***H.4 Consensus mechanism***

The crypto-asset in scope is implemented on the VerifiedX network following the standards described below.

The following applies to VerifiedX:

The crypto-asset's consensus mechanism is Proof of Assurance (PoA), which is intended to support network security and decentralisation through validator participation based on wallet-held VFX balances. To participate in validation, a validator must maintain 5,000 VFX in its wallet. Block production is assigned through rotating randomised casters. Participating casters generate cryptographic proofs using SHA256-based hashing and broadcast them to the network. Other validators then deterministically lock a winner based on the outcome of those proofs and vote to confirm that caster as the block producer. The selected caster is then expected to submit the queued block to the chain. If the selected caster fails to do so, backup winners may be selected from the available proofs.

The network maintains a target block time of approximately 12 seconds. Once a block is confirmed by the validator pool and added to the chain, the model is described as deterministic under normal operating conditions. The network also includes a fallback approach for hostile scenarios in which honest validators reject an invalid chain and continue operating separately. The protocol distinguishes between ordinary validator inactivity and malicious conduct. Where a validator is

determined by peer vote to have acted maliciously, the assured coins may be permanently locked and sacrificed by the network.

### ***H.5 Incentive mechanisms and applicable fees***

The crypto-asset in scope is implemented on the VerifiedX network following the standards described below.

The following applies to VerifiedX:

The crypto-asset's incentive mechanism does not rely on protocol-level block rewards or inflation. Instead, the VerifiedX network operates with a fixed lifetime supply of 200,000,000 VFX and a deflationary design. Following a protocol upgrade, block rewards were reduced to zero. The current protocol does not issue new VFX as rewards for block production. Validators do not receive automated protocol-level compensation in the form of newly minted tokens or redistributed transaction fees. Rather, validator participation is linked primarily to governance rights within the network, including participation in the approval of network proposals and changes.

Transaction fees apply to network use and are paid by the sender of a transaction. These fees are kept at near-zero levels by protocol design. Transaction and network service fees are not redistributed to validators, miners, or a treasury. Instead, such fees are permanently burned at the time of the transaction. Additional network service fees may also apply in connection with services such as Vault accounts, DNS, and peer-to-peer auctions, and these fees are likewise burned.

The protocol also includes a penalty mechanism for malicious validator behaviour. Where a validator is determined by the validator pool to have acted maliciously, the assured coins required for validator participation may be permanently locked and rendered unspendable.

### ***H.6 Use of distributed ledger technology***

No – the DLT is not operated by the issuer, the offeror, the person seeking admission to trading, or any third party acting on their behalf.

### ***H.7 DLT functionality description***

Not applicable, as the DLT is not operated by the issuer, the offeror, the person seeking admission to trading, or any third party acting on their behalf.

### ***H.8 Audit***

An audit of the technology used was conducted.

### ***H.9 Audit outcome***

The core technology of the VerifiedX network has undergone full-stack security audits by Halborn, covering the core protocol, validator service, peer-to-peer system and vBTC (sources: <https://www.halborn.com/audits/verifiedx/verifiedx-core-c81f69>, <https://www.halborn.com/audits/verifiedx/verifiedx-core-1e750c>, accessed 2026-04-21). All findings identified in the audits were remediated by the developers and reviewed and approved by Halborn.

In addition, the project has integrated blockchain tracing and compliance monitoring tools provided by Merkle Science for VFX and vBTC-related transactions.

## **Part I – Information on risks**

### ***I.1 Offer-related risks***

#### **1. Regulatory and Compliance**

Regulatory frameworks applicable to crypto-asset services in the European Union and in third countries are evolving. Supervisory authorities may introduce, interpret, or enforce rules that affect

(i) the eligibility of this crypto-asset for admission to trading, (ii) the conditions under which a crypto-asset service provider may offer trading, custody, or transfer services for it, or (iii) the persons or jurisdictions to which such services may be provided. As a result, the crypto-asset service provider admitting this crypto-asset to trading may be required to suspend, restrict, or terminate trading or withdrawals for regulatory reasons, even if the crypto-asset itself continues to function on its underlying network.

## 2. Trading venue and connection risk

Trading in the crypto-asset depends on the uninterrupted operation of the trading venues on which it is listed and, where applicable, on its technical connections to external liquidity sources or venues. Interruptions such as system downtime, maintenance, faulty integrations, API changes, or failures at an external venue can temporarily prevent order placement, execution, deposits, or withdrawals, even when the underlying blockchain is functioning. In addition, trading platforms in emerging markets may operate under differing governance, compliance, and oversight standards, which can increase the risk of operational failures or disorderly market conditions.

## 3. Market formation and liquidity conditions

The price and tradability of the crypto-asset depend on actual trading activity on the venues to which the service provider is connected, whether centralised exchanges (CEXs) or decentralised exchanges (DEXs). Trading volumes may at times be low, order books thin, or liquidity concentrated on a single venue. In such conditions, buy or sell orders may not be executed in full or may be executed only at a less favourable price, resulting in slippage.

**Volatility:** The market price of the crypto-asset may fluctuate significantly over short periods, including for reasons that are not linked to changes in the underlying project or protocol. Periods of limited liquidity, shifts in overall market sentiment, or trading on only a small number of CEXs or DEXs can amplify these movements and lead to higher slippage when orders are executed. As a result, investors may be unable to sell the crypto-asset at or close to a previously observed price, even where no negative project-specific event has occurred.

## 4. Counterparty and service provider dependence

The admission of the crypto-asset to trading may rely on several external parties, such as connected centralised or decentralised trading venues, liquidity providers, brokers, custodians, or technical integrators. If any of these counterparties fail to perform, suspend their services, or apply internal restrictions, the trading, deposit, or withdrawal of the crypto-asset on the listing crypto-asset service provider can be interrupted or halted.

**Quality of counterparties:** Trading venues and service providers in certain jurisdictions may operate under regulatory or supervisory standards that are lower or differently enforced than those applicable in the European Union. In such environments, deficiencies in governance, risk management, or compliance may remain undetected, which increases the probability of abrupt service interruptions, investigations, or forced wind-downs.

**Delisting and service suspension:** The crypto-asset's availability may depend on the internal listing decisions of these counterparties. A delisting or suspension on a key connected venue can materially reduce liquidity or make trading temporarily impossible on the admitting service provider, even if the underlying crypto-asset continues to function.

**Insolvency of counterparties:** If a counterparty involved in holding, routing, or settling the crypto-asset becomes insolvent, enters restructuring, or is otherwise subject to resolution measures, assets held or processed by that counterparty may be frozen, become temporarily unavailable, or be recoverable only in part or not at all, which can result in losses for clients whose positions were maintained through that counterparty. This risk applies in particular where client assets are held on an omnibus basis or where segregation is not fully recognised in the counterparty's jurisdiction.

## 5. Operational and information risks

Due to the irrevocability of blockchain transactions, incorrect transaction approvals or the use of wrong networks or addresses will typically make the transferred funds irrecoverable. Because

trading may also rely on technical connections to other venues or service providers, downtime or faulty code in these connections can temporarily block trading, deposits, or withdrawals even when the underlying blockchain is functioning. In addition, different groups of market participants may have unequal access to technical, governance, or project-related information, which can lead to information asymmetry and place less informed investors at a disadvantage when making trading decisions.

#### 6. Market access and liquidity concentration risk

If the crypto-asset is only available on a limited number of trading platforms or through a single market-making entity, this may result in reduced liquidity, greater price volatility, or periods of inaccessibility for retail holders.

### ***1.2 Issuer-related risks***

#### 1. Insolvency of the issuer

As with any commercial entity, the issuer may face insolvency risks. These may result from insufficient funding, low market interest, mismanagement, or external shocks (e.g. pandemics, armed conflicts). In such a case, ongoing development, support, and governance of the project may cease, potentially affecting the viability and tradability of the crypto-asset.

#### 2. Legal and regulatory risks

The issuer operates in a dynamic and evolving regulatory environment. Failure to comply with applicable laws or regulations in relevant jurisdictions may result in enforcement actions, penalties, or restrictions on the project's operations. These may negatively impact the crypto-asset's availability, market acceptance, or legal status.

#### 3. Operational risks

The issuer may fail to implement adequate internal controls, risk management, or governance processes. This can result in operational disruptions, financial losses, delays in updating the white paper, or reputational damage.

#### 4. Governance and decision-making

The issuer's management body is responsible for key strategic, operational, and disclosure decisions. Ineffective governance, delays in decision-making, or lack of resources may compromise the stability of the project and its compliance with MiCA requirements. High concentration of decision-making authority or changes in ownership/control can amplify these risks.

#### 5. Reputational risks

The issuer's reputation may be harmed by internal failures, external accusations, or association with illicit activity. Negative publicity can reduce trust in the issuer and impact the perceived legitimacy or value of the crypto-asset.

#### 6. Counterparty dependence

The issuer may depend on third-party providers for certain core functions, such as technology development, marketing, legal advice, or infrastructure. If these partners discontinue their services, change ownership, or underperform, the issuer's ability to operate the project or maintain investor communication may be impaired. This could disrupt project continuity or undermine market confidence, ultimately affecting the crypto-asset's value.

### ***1.3 Crypto-assets-related risks***

#### 1. Valuation risk

The crypto-asset does not represent a claim, nor is it backed by physical assets or legal entitlements. Its market value is driven solely by supply and demand dynamics and may fluctuate significantly. In the absence of fundamental value anchors, such assets can lose their entire market value within a very short time. Historical market behaviour has shown that some types of

crypto-assets have become worthless. Investors should be aware that this crypto-asset may lose all of its value.

## 2. Market volatility risk

Crypto-asset prices can fluctuate sharply due to changes in market sentiment, macroeconomic conditions, regulatory developments, or technology trends. Such volatility may result in rapid and significant losses. Holders should be prepared for the possibility of losing the full amount invested.

## 3. Liquidity and price-determination risk

Low trading volumes, fragmented trading across venues, or the absence of active market makers can restrict the ability to buy or sell the crypto-asset. In such situations, it is not guaranteed that an observable market price will exist at all times. Spreads may widen materially, and orders may only be executable under unfavourable conditions, which can make liquidation costly or temporarily impossible.

## 4. Crypto-asset security risk

Loss or theft of private keys, unauthorised access to wallets, or failures of custodial or exchange service providers can result in the irreversible loss of assets. Because blockchain transactions are final, recovery of funds after a compromise is generally impossible.

## 5. Fraud and scam risk

The pseudonymous and irreversible nature of blockchain transactions can attract fraudulent schemes. Typical forms include fake or unauthorised crypto-assets imitating established ones, phishing attempts, deceptive airdrops, or social-engineering attacks. Investors should exercise caution and verify the authenticity of counterparties and information sources.

## 6. Legal and regulatory reclassification risk

Legislative or regulatory changes in the European Union or in the Member State where the crypto-asset is admitted to trading may alter its legal classification, permitted uses, or tradability. In third countries, the crypto-asset may be treated as a financial instrument or security, which can restrict its offering, trading, or custody.

## 7. Absence of investor protection

The crypto-asset is not covered by investor-compensation or deposit-guarantee schemes. In the event of loss, fraud, or insolvency of a service provider, holders may have no access to recourse mechanisms typically available in regulated financial markets.

## 8. Counterparty risk

Reliance on third-party exchanges, custodians, or intermediaries exposes holders to operational failures, insolvency, or fraud of these parties. Investors should conduct due diligence on service providers, as their failure may lead to the partial or total loss of held assets.

## 9. Reputational risk

Negative publicity related to security incidents, misuse of blockchain technology, or associations with illicit activity can damage public confidence and reduce the crypto-asset's market value.

## 10. Community and sentiment risk

Because the crypto-asset's perceived relevance and expected future use depend largely on community engagement and the prevailing sentiment, a loss of public interest, negative coverage or reduced activity of key contributors can materially reduce market demand.

## 11. Macroeconomic and interest-rate risk

Fluctuations in interest rates, exchange rates, general market conditions, or overall market volatility can influence investor sentiment towards digital assets and affect the crypto-asset's market value.

## 12. Taxation risk

Tax treatment varies across jurisdictions. Holders are individually responsible for complying with all applicable tax laws, including the reporting and payment of taxes arising from the acquisition, holding, or disposal of the crypto-asset.

#### 13. Anti-money-laundering and counter-terrorist financing risk

Wallet addresses or transactions connected to the crypto-asset may be linked to sanctioned or illicit activity. Regulatory responses to such findings may include transfer restrictions, reporting obligations, or the freezing of assets on certain venues.

#### 14. Market-abuse risk

Due to limited oversight and transparency, crypto-assets may be vulnerable to market-abuse practices such as spoofing, pump-and-dump schemes, or insider trading. Such activities can distort prices and expose holders to sudden losses.

#### 15. Legal ownership and jurisdictional risk

Depending on the applicable law, holders of the crypto-asset may not have enforceable ownership rights or effective legal remedies in cases of disputes, fraud, or service failure. In certain jurisdictions, access to exchanges or interfaces may be restricted by regulatory measures, even if on-chain transfer remains technically possible.

#### 16. Concentration risk

A large proportion of the total supply may be held by a small number of holders. This can enable market manipulation, governance dominance, or sudden large-scale liquidations that adversely affect market stability, price levels, and investor confidence.

### ***1.4 Project implementation-related risks***

As this white paper relates to admission to trading of the crypto-asset, the risk description below reflects general implementation risks typically associated with crypto-asset projects and relevant for the crypto-asset service provider.

Delays, failures, or changes in the implementation of the project as outlined in its public roadmap or technical documentation may negatively impact the perceived credibility or usability of the crypto-asset. This includes risks related to project governance, resource allocation, technical delivery, and team continuity.

Key-person risk: The project may rely on a limited number of individuals for development, maintenance, or strategic direction. The departure, incapacity, or misalignment of these individuals may delay or derail the implementation.

Timeline and milestone risk: Project milestones may not be met as announced. Delays in feature releases, protocol upgrades, or external integrations can undermine market confidence and affect the adoption, use, or value of the crypto-asset.

Delivery risk: Even if implemented on time, certain functionalities or integrations may not perform as intended or may be scaled back during execution, limiting the crypto-asset's practical utility.

### ***1.5 Technology-related risks***

As this white paper relates to admission to trading of the crypto-asset, the following risks concern the underlying distributed ledger technology (DLT), its supporting infrastructure, and related technical dependencies. Failures or vulnerabilities in these systems may affect the availability, integrity, or transferability of the crypto-asset.

#### 1. Blockchain dependency risk

The functionality of the crypto-asset depends on the continuous and stable operation of the blockchain(s) on which it is issued. Network congestion, outages, or protocol errors may temporarily or permanently disrupt on-chain transactions. Extended downtime or degradation in network performance can affect trading, settlement, or the usability of the crypto-asset.

## 2. Smart contract vulnerability risk

The smart contract that defines the crypto-asset's parameters or governs its transfers may contain coding errors or security vulnerabilities. Exploitation of such weaknesses can result in unintended token minting, permanent loss of funds, or disruption of token functionality. Even after external audits, undetected vulnerabilities may persist due to the immutable nature of deployed code.

## 3. Wallet and key-management risk

The custody of crypto-assets relies on secure private key management. Loss, theft, or compromise of private keys results in irreversible loss of access. Custodians, trading venues, or wallet providers may be targeted by cyberattacks. Compatibility issues between wallet software and changes to the blockchain protocol (e.g. network upgrades) can further limit user access or the ability to transfer the crypto-asset.

Outdated or vulnerable wallet software:

Users relying on outdated, unaudited, or unsupported wallet software may face compatibility issues, security vulnerabilities, or failures when interacting with the blockchain. Failure to update wallet software in line with protocol developments can result in transaction errors, loss of access, or exposure to known exploits.

## 4. Network security risks

Attack risks: Blockchains may be subject to denial-of-service (DoS) attacks, 51% attacks, or other exploits targeting the consensus mechanism. These can delay transactions, compromise finality, or disrupt the accurate recording of transfers.

Centralisation concerns: Despite claims of decentralisation, a relatively small number of validators or a high concentration of stake may increase the risk of collusion, censorship, or coordinated network downtime, which can affect the resilience and operational reliability of the crypto-asset.

## 5. Bridge and interoperability risk

Where tokens can be bridged or wrapped across multiple blockchains, vulnerabilities in bridge protocols, validator sets, or locking mechanisms may result in loss, duplication, or misrepresentation of assets. Exploits or technical failures in these systems can instantly impact circulating supply, ownership claims, or token fungibility across chains.

## 6. Forking and protocol-upgrade risk

Network upgrades or disagreements among node operators or validators can result in blockchain "forks", where the blockchain splits into two or more incompatible versions that continue separately from a shared past. This may lead to duplicate token representations or incompatibilities between exchanges and wallets. Until consensus stabilises, trading or transfers may be disrupted or misaligned. Such situations may be difficult for retail holders to navigate, particularly when trading platforms or wallets display inconsistent token information.

## 7. Economic-layer and abstraction risk

Mechanisms such as gas relayers, wrapped tokens, or synthetic representations may alter the transaction economics of the underlying token. Changes in transaction costs, token demand, or utility may reduce its usage and weaken both its economic function and perceived value within its ecosystem.

## 8. Spam and network-efficiency risk

High volumes of low-value ("dust") or automated transactions may congest the network, slow validation times, inflate ledger size, and raise transaction costs. This can impair performance, reduce throughput, and expose address patterns to analysis, thereby reducing network efficiency and privacy.

## 9. Front-end and access-interface risk

If users rely on centralised web interfaces or hosted wallets to interact with the blockchain, service outages, malicious compromises, or domain expiries affecting these interfaces may block access to

the crypto-asset, even while the blockchain itself remains fully functional. Dependence on single web portals introduces a critical point of failure outside the DLT layer.

#### 10. Decentralisation claim risk

While the technical infrastructure may appear distributed, the actual governance or economic control of the project may lie with a small set of actors. This disconnect between marketing claims and structural reality can lead to regulatory scrutiny, reputational damage, or legal uncertainty – especially if the project is presented as ‘community-governed’ without substantiation.

### ***1.6 Mitigation measures***

The following measures are in place or have been adopted to mitigate the risks described in this white paper:

- Security auditing: The VerifiedX network has been audited by Halborn, a tier 1 blockchain security firm, to identify and address potential vulnerabilities in the protocol and its supporting infrastructure.
- Compliance monitoring: The project has integrated with Merkle Science for blockchain tracing and compliance monitoring, covering both VFX and vBTC transactions, to support the detection and prevention of illicit activity.
- Open-source codebase: The VerifiedX project is fully open-source, with all source code publicly available on GitHub, enabling independent review, verification, and contribution by any party.
- On-chain governance: Significant protocol changes require an 80% approval vote from the validator pool before implementation, providing a decentralised decision-making mechanism for network upgrades and parameter changes.
- Malicious validator penalties: The protocol includes a penalty mechanism under which validators determined by peer vote to have acted maliciously may have their assured coins permanently locked and rendered unspendable, discouraging adversarial behaviour.
- Bug bounty program: A bug bounty program has been established to support the identification of vulnerabilities and technology issues through coordinated external reporting.

## **Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts**

### ***J.1 Adverse impacts on climate and other environment-related adverse impacts***

#### ***S.1 Name***

#### ***S.2 Relevant legal entity identifier***

#### ***S.3 Name of the crypto-asset***

#### ***S.4 Consensus Mechanism***

The crypto-asset in scope is implemented on the VerifiedX network following the standards described below.

The following applies to VerifiedX:

The crypto-asset’s consensus mechanism is Proof of Assurance (PoA), which is intended to support network security and decentralisation through validator participation based on wallet-held VFX balances. To participate in validation, a validator must maintain 5,000 VFX in its wallet. Block production is assigned through rotating randomised casters. Participating casters generate

cryptographic proofs using SHA256-based hashing and broadcast them to the network. Other validators then deterministically lock a winner based on the outcome of those proofs and vote to confirm that caster as the block producer. The selected caster is then expected to submit the queued block to the chain. If the selected caster fails to do so, backup winners may be selected from the available proofs.

The network maintains a target block time of approximately 12 seconds. Once a block is confirmed by the validator pool and added to the chain, the model is described as deterministic under normal operating conditions. The network also includes a fallback approach for hostile scenarios in which honest validators reject an invalid chain and continue operating separately. The protocol distinguishes between ordinary validator inactivity and malicious conduct. Where a validator is determined by peer vote to have acted maliciously, the assured coins may be permanently locked and sacrificed by the network.

### ***S.5 Incentive Mechanisms and Applicable Fees***

The crypto-asset in scope is implemented on the VerifiedX network following the standards described below.

The following applies to VerifiedX:

The crypto-asset's incentive mechanism does not rely on protocol-level block rewards or inflation. Instead, the VerifiedX network operates with a fixed lifetime supply of 200,000,000 VFX and a deflationary design. Following a protocol upgrade, block rewards were reduced to zero. The current protocol does not issue new VFX as rewards for block production. Validators do not receive automated protocol-level compensation in the form of newly minted tokens or redistributed transaction fees. Rather, validator participation is linked primarily to governance rights within the network, including participation in the approval of network proposals and changes.

Transaction fees apply to network use and are paid by the sender of a transaction. These fees are kept at near-zero levels by protocol design. Transaction and network service fees are not redistributed to validators, miners, or a treasury. Instead, such fees are permanently burned at the time of the transaction. Additional network service fees may also apply in connection with services such as Vault accounts, DNS, and peer-to-peer auctions, and these fees are likewise burned.

The protocol also includes a penalty mechanism for malicious validator behaviour. Where a validator is determined by the validator pool to have acted maliciously, the assured coins required for validator participation may be permanently locked and rendered unspendable.

### ***S.6 Beginning of the period to which the disclosure relates***

### ***S.7 End of the period to which the disclosure relates***

### ***S.8 Energy consumption***

40602.60000 kWh/a

### ***S.9 Energy consumption sources and methodologies***

For the calculation of energy consumption, the so-called "bottom-up" approach is used. Nodes are considered the central factor for the energy consumption of the underlying network. The relevant assumptions are based on empirical findings obtained through public information sites, open-source crawlers, and crawlers developed in-house. The main determinants for estimating the hardware used within the network are the requirements for operating the relevant client software. The energy consumption of the relevant hardware devices was measured in certified test laboratories. Where available, the Functionally Fungible Group Digital Token Identifier (FFG DTI) is used to determine all technically equivalent implementations of the crypto-asset in scope, and the relevant mappings are updated regularly based on data from the Digital Token Identifier Foundation.

Information regarding the hardware used and the number of participants in the network is based on assumptions that are verified on a best-effort basis using empirical data. In general, participants are assumed to act largely economically rationally. In line with the precautionary principle, conservative assumptions are made where uncertainty exists, meaning that estimates tend towards the higher end of the reasonably plausible adverse impacts.

### ***S.10 Renewable energy consumption***

31.4129168171 %

### ***S.11 Energy intensity***

0.00011 kWh

### ***S.12 Scope 1 DLT GHG emissions – Controlled***

0.00000 tCO<sub>2e</sub>/a

### ***S.13 Scope 2 DLT GHG emissions – Purchased***

13.51308 tCO<sub>2e</sub>/a

### ***S.14 GHG intensity***

0.00002 kgCO<sub>2e</sub>

### ***S.15 Key energy sources and methodologies***

To determine the proportion of renewable energy usage, the locations of the nodes are determined using public information sites, open-source and in-house-developed crawlers. Where no information is available on the geographic distribution of nodes, comparable reference networks are used, taking into account similarities in incentivisation structure and consensus mechanism. This geographic information is then combined with publicly available data from Our World in Data. The resulting intensity is calculated as the marginal energy consumption with respect to one additional transaction.

Ember (2025); Energy Institute, Statistical Review of World Energy (2024), with major processing by Our World in Data. "Share of electricity generated by renewables - Ember and Energy Institute" [dataset]. Underlying sources: Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy". Retrieved from: <https://ourworldindata.org/grapher/share-electricity-renewables>

### ***S.16 Key GHG sources and methodologies***

To determine the GHG emissions, the locations of the nodes are to be determined using public information sites, open-source and in-house-developed crawlers. Where no information is available on the geographic distribution of nodes, comparable reference networks are used, taking into account similarities in incentivisation structure and consensus mechanism. This geographic information is then combined with publicly available data from Our World in Data. The resulting intensity is calculated as the marginal emission intensity with respect to one additional transaction.

Ember (2025); Energy Institute, Statistical Review of World Energy (2024), with major processing by Our World in Data. "Carbon intensity of electricity generation - Ember and Energy Institute" [dataset]. Underlying sources: Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy". Retrieved from: <https://ourworldindata.org/grapher/carbon-intensity-electricity>. Licensed under CC BY 4.0.