

WhitePaper USD€

8495001XWFMRUTCAK575

DK 260210182959 en

E-money token issued by Eurodollar ApS, stabilised against USD and backed 1:1 with reserve assets.

Table of contents

- [Quick reference](#)
- [General information](#)
- [Summary - key information](#)
- [Parts A-G](#)
- [Part A - Information about the issuer of the e-money token](#)
- [Part B - Information about the e-money token](#)
- [Part C - Information about the offer to the public of the e-money token or its admission to trading](#)
- [Part D - Information on the rights and obligations attached to e-money tokens](#)
- [Part E - Information on the underlying technology](#)
- [Part F - Information on the risks](#)
- [Part G - Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts](#)

Quick reference

Key	Value
Token	USDE
Token name	USDY
Reference currency	USD
Issuer	Eurodollar ApS
Type of submission	Modify
Date of notification	11th Feb 2026
Blockchain network	Ethereum

General information

I.01 Date of notification

11th Feb 2026

I.02 Statement in accordance with Article 51(3) of Regulation (EU) 2023/1114

This crypto-asset white paper has not been approved by any competent authority in any Member State of the European Union. The issuer of the crypto-asset is solely responsible for the content of this crypto-asset white paper.

I.03 Compliance statement in accordance with Article 51(5) of Regulation (EU) 2023/1114

This crypto-asset white paper complies with Title IV of Regulation (EU) 2023/1114 of the European Parliament and of the Council and to the best of the knowledge of the management body, the information presented in this crypto-asset white paper is fair, clear and not misleading and the crypto-asset white paper makes no omission likely to affect its import.

I.04 Warning in accordance with Article 51(4), points (a) and (b), of Regulation (EU) 2023/1114

This e-money token is not covered by the investor compensation schemes under Directive 97/9/EC of the European Parliament and of the Council or the deposit guarantee schemes under Directive 2014/49/EU of the European Parliament and of the Council.

Summary - key information

I.05 Warning in accordance with Article 51(6), second subparagraph of Regulation (EU) 2023/1114

Warning

This summary should be read as an introduction to the crypto-asset white paper.

The prospective holder should base any decision to purchase this e-money token on the content of the crypto-asset white paper as a whole and not on the summary alone.

The offer to the public of this crypto-asset does not constitute an offer or solicitation to purchase financial instruments and that any such offer or solicitation can be made only by means of a prospectus or other offer documents pursuant to the applicable national law.

This crypto-asset white paper does not constitute a prospectus as referred to in Regulation (EU) 2017/1129 of the European Parliament and of the Council or any other offer document pursuant to Union or national law.

I.06 Characteristics of the crypto-asset

USD€ (also known as USDY) are crypto-assets which stabilise their value by reference to a single official currency, being USD. Each USD€ is backed by one (1) USD in value. USD€ holders have the right of redemption against the Issuer at any time and at par value at all times ranking pari passu and without any preference between themselves and, subject to the Danish Bankruptcy Act (in Danish: Konkursloven), ahead of all other creditors (secured or unsecured) of the Issuer.

USD€ are constituted through smart contracts deployed by Eurodollar on the Ethereum blockchain network.

I.07 Right of redemption

The Issuer will submit a redemption plan to the Authorities within 6 months of launching USD€ and update this section following filing of the redemption plan. The Issuer's redemption plan will explain how the Issuer intends to comply with its obligation to fulfil redemption requests to redeem USD€ for fiat or another EMT in the event it is not able to fulfil its obligations in the ordinary course of business. The redemption plan ensures that the Reserve Assets remain fully segregated from the Issuer's own assets and are applied to USD€ holders equitably. The Issuer will communicate with its Customers via their Accounts and, as appropriate, more broadly. It will provide notice of any mechanisms that have been adopted to ensure orderly implementation of distributing the Reserve Assets to all Customers and/or USD€ holders equitably. The Issuer may adjust the ordinary process to make Redemption Requests and implement another process notified to Customers and/or USD€ holders including key actions, information required and timeframes. Once the process timeframe has completed, the Issuer will apply the Reserve Assets equitably across all holders.

Parts A-G

✓ Part A – Information about the issuer of the e-money token

A.1 Statutory name

Eurodollar ApS

A.2 Trading name

Eurodollar ApS; Stablecoin Integration Services Danmark IVS; EUD ApS

A.3 Legal form

Private limited company (ApS)

A.4 Registered address

Registered address

Krudtløbsvej 12, 1439 København K

Country

Denmark

Sub-division

Hovedstaden

A.5 Head office

Head office

As registered address

Country

Denmark

Sub-division

As registered address

A.6 Registration date

2018-07-16

A.7 Legal entity identifier

8945001XWFMRUTCAK575

A.8 Another identifier required pursuant to applicable law

39729482

A.9 Contact telephone number

+45 6079 3777

A.10 E-mail address

info@eurodollar.fi

A.11 Response time (days)

3

A.12 Parent company

Rhinefield Holdings Ltd.

A.13 Members of the management body**Member #1**

1

Identity

Allan Pedersen

Business address

Krudtløbsvej 12, 1439 København K

Function

CEO & Executive Director

Member #2

2

Identity

Kam Dylan

Business address

Krudtløbsvej 12, 1439 København K

Function

Chief Legal Officer & Non-Executive Director

A.14 Business activity

The Issuer is an e-money institution and issues e-money tokens. It may also offer ancillary payment services, although its principal activity is serving as an EMT issuer.

A.15 Parent company business activity

The holding of shares in the issuer, and other affiliated and non-affiliated businesses.

A.16 Conflicts of interest

No conflicts of interest have been identified, and ongoing monitoring is in place.

A.17 Issuance of other crypto-assets

true

A.18 Activities related to other crypto-assets

false

E-money token issuer and DLT business association

A.19 Connection between the issuer and the entity running the DLT

false

A.20 Description of the connection between the issuer and the entity running the DLT

A.21 Newly established

false

A.22 Financial condition for the past three years

In accordance with the Danish Financial Statements Act (Lovbekendtgørelse 2022-11-14 nr. 1441 Årsregnskabsloven), the Issuer has prepared financial statements and appointed auditors. The annual financial statements of the Issuer have been prepared in accordance with the Danish Financial Statements Act for the fiscal years ended 2024, 2023 and 2022. There has been no material adverse change in the prospects of the Issuer since 9 October 2023 when the Parent Company acquired all the shares in the Issuer. The Issuer's statutory auditors are Martinsen Statsautoriseret Revisionspartnerselskab.

A.23 Financial condition since registration

A.24 Exemption from authorisation

false

A.25 E-money token authorisation

The Issuer is an authorised e-money institution and payment services provider in accordance with the Danish Payment Act (Lovbekendtgørelse 2023-01-18 nr. 53 om betalinger) and MiCAR. The Issuer is authorised and regulated by the DFSA.

A.26 Authorisation authority

Finanstilsynet

✓ Part B – Information about the e-money token

B.1 Name

EU Dollar

B.2 Abbreviation

USD€/USDY

B.3 Details of all natural or legal persons involved in design and development

Person #1

1

Type of person

Development team

Name of person

Eurodollar ApS

Business address of person

Krudtløbsvej 12, 1439 København K

Domicile of company

Denmark

Person #2

2

Type of person

Development team

Name of person

Rhinefield Technologies Limited

Business address of person

Athalassas, 176 3rd Fl., Office 301, 2025, Nicosia, Cyprus.

Domicile of company

Cyprus

A description of the characteristics of the e-money token, including the data necessary for classification of the crypto-asset white paper in the register referred to in Article 109, as specified in accordance with paragraph 8 of that Article

B.4 Type of white paper

E-money token white paper

B.5 Type of submission

Modify

B.6 Crypto-asset characteristics

USD€ are crypto-assets which stabilise their value by reference to a single official currency, being USD. Each USD€ is backed by one (1) USD in value. USD€ holders have the right of redemption against the Issuer at any time and at par value at all times ranking pari passu and without any preference between themselves and, subject to the Danish Bankruptcy Act (in Danish: Konkursloven), ahead of all other creditors (secured or unsecured) of the Issuer.

USD€ are constituted through smart contracts deployed by Eurodollar on the Ethereum blockchain network.

B.7 Website of the issuer

www.eurodollar.fi

B.8 Starting date of offer to the public or admission to trading

2026-02-11

B.9 Publication date

2026-02-10

B.10 Any other services provided by the issuer

issuer of e-money tokens; ancillary payment services

B.11 Language or languages of white paper

English

B.12 Digital token identifier code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available

USD€

B.13 Functionally fungible group digital token identifier, where available**B.14 Personal data flag**

true

B.15 LEI eligibility

true

B.16 Home member state

Denmark

B.17 Host member states

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czechia
- Denmark
- Estonia
- Finland

- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden

✓ Part C – Information about the offer to the public of the e-money token or its admission to trading

C.1 Public offering or trading

Offer to public

C.4 Trading platforms market identifier code (MIC)

C.5 Applicable law

Danish law

C.6 Competent court

Danish Institute of Arbitration

- ✓ Part D – Information on the rights and obligations attached to e-money tokens

D.1 Holder's rights and obligations

Holders can see their rights and obligations on the company's website at www.eurodollar.fi/legal

D.2 Conditions of modifications of rights and obligations

The rights and obligations attached to USD€ may be modified where the Issuer has given the Customer no less than two (2) months' notice. If the Customer wishes to not accept the changes, they will be able to close their Account. In certain, limited circumstances the Issuer could end the relationship with the Customer this includes where the Issuer believes that the Customer has participated in a Prohibited Activity.

D.3 Description of the rights of the holders

In the event that the Issuer can no longer fulfil its obligations, USD€ holders will benefit from certain rights under MiCAR and EMD2 this includes that the Reserve Assets will be treated as assets held for the benefit of the Customers. These assets will not be used to repay the Issuer's obligations. The distribution of assets in any insolvency situation will be subject to the Danish Bankruptcy Act (in Danish: Konkursloven).

D.4 Rights in implementation of recovery plan

The Issuer has submitted a recovery plan to the DFSA. The Issuer's recovery plan includes analysis of key scenarios including insolvency scenarios. It has identified key risk metrics and early warning indicators so that potential concerns can be addressed as soon as possible. In the event that the Issuer's recovery plan is triggered, the Issuer can implement various mechanisms to mitigate the impact on customers, safeguard the Reserve Assets and the integrity of the Eurodollar services. The mechanisms that the Issuer may implement and which affect the rights of Customers, including but not limited to: (i) daily monitoring of the percentage of liquid asset to total assets and, accordingly, implementing a cap on daily Redemption Requests; (ii) adjusting the Reserve Assets to more closely align with the flow of Redemption Requests; (iii) clear and consistent communication with its Customers via their Accounts and, as may be appropriate, more broadly; and (iv) temporary pause on fulfilling Redemption Requests.

D.5 Rights in implementation of redemption plan

The Issuer will submit a redemption plan to the Issuer within 6 months of launching USD€ and update this section following filing of the redemption plan. The Issuer's redemption plan will explain how the Issuer intends to comply with its obligation to fulfil redemption requests to redeem USD€ for fiat or another EMT in the event it is not able to fulfil its obligations in the ordinary course of business. The redemption plan ensures that the Reserve Assets remain fully segregated from the Issuer's own assets and are applied to USD€ holders equitably. The Issuer will communicate with its Customers via their Accounts and, as appropriate, more broadly. It will provide notice of any mechanisms that have been adopted to ensure orderly implementation of distributing the Reserve Assets to all Customers and/or USD€ holders equitably. The Issuer may adjust the ordinary process to make Redemption Requests and implement another process notified to Customers and/or USD€ holders including key actions, information required and timeframes. Once the process timeframe has completed, the Issuer will apply the Reserve Assets equitably across all holders.

D.6 Complaint submission contact

info@eurodollar.fi

D.7 Complaints handling procedures

The Issuer adopts a complaints handling procedure which seeks to address and solve Customer complaints promptly. Customers who wish to submit a complaint can contact Eurodollar at info@eurodollar.fi. Eurodollar will acknowledge customer complaints within [3] business days and solve the complaint to the customer's satisfaction as soon as reasonably practicable. Once Eurodollar receives the complaint, it will review the circumstances and seek to either resolve it based on the information already provided or request further information from the Customer. Having collected the information Eurodollar requires to propose a solution to the customer's satisfaction, Eurodollar will address the complaint more fully.

D.8 Dispute resolution mechanism

If the customer is not satisfied with the proposed solution, it can escalate the complaint to the next level of management. If the customer's complaint still remains unresolved the customer may close their account or reach out to the Danish Consumer Ombudsman at the following contact details:
Forbrugerombudsmanden Carl Jacobsens Vej 35 2500 Valby Telefon: 4171 5151

E-money token schemes details

D.9 Token value protection schemes

false

D.10 Token value protection schemes description

D.11 Compensation schemes

false

D.12 Compensation schemes description

D.13 Applicable law

Danish Law

D.14 Competent court

The Danish Institute of Arbitration

✓ Part E – Information on the underlying technology

E.1 Distributed ledger technology

The USD€ Tokens are issued and recorded on the Ethereum blockchain network, a public and permissionless distributed ledger.

E.2 Protocols and technical standards

The distributed ledger technology is technology that allows the operation of a distributed ledger, i.e. a ledger that is not kept by a trusted intermediary but by a network of nodes. The distributed ledger technology, as implemented on the Ethereum blockchain is based on complex mathematical and cryptography concepts, which are described in this White Paper at a high level and in layman's terms.

The distributed ledger technology is based on asymmetric cryptography (also sometimes called public key cryptography) and makes use of the elliptic curve digital signature algorithm (or ECDSA). At a high level, asymmetric cryptography focuses on the interplay between a public key and a private key, which are two numbers that are mathematically related. The public key is – as its name indicates – public, while the private key must remain secret. The holder of the private key can generate signature messages that have certain mathematical properties. Using the signature message and the public key, it is possible to ascertain that the message was produced using the private key (and thus that the signature message is authentic). While it is possible to determine that the private key was used, current technology does not allow one to deduce the private key from signature messages. The features of asymmetric cryptography mean that, to validate the authenticity of a message, there is no need to know the secret private key of the message's sender. The sender therefore does not need to entrust anyone with a secret (the private key). In the distributed ledger technology, the sender broadcasts his message to certain participants of the distributed ledger networks. In a distributed ledger functioning as a blockchain, these participants validate transactions in blocks (which may be comprising hundreds of transactions or more). Each of these participants maintains its own record of the distributed ledger, and will update such record when a participant proposes to include a new "block" of transactions. A transaction is recorded after it has been added to a block of transactions that the participants have decided to include in their own record of the blockchain. In a distributed ledger context, the public key is often referred to as the "blockchain address" or "distributed ledger address".

E.3 Technology used

The Ethereum blockchain

The Ethereum blockchain is a distributed ledger that has essentially two categories of functions.

The first is related to Ether (or ETH). Ether is a crypto-asset that is recorded and traded on the Ethereum blockchain. Users of the Ethereum blockchain can trade Ethers on the Ethereum blockchain and use such Ethers as means of payment.

The second is the use of "smart contracts". The Ethereum blockchain allows for the creation of "smart contracts". Smart contracts are, in this context, distributed ledger addresses that are operated by computer code. Smart contracts can perform a large number of functions, including to create tokens. A token is not a computer program that can be separated from the smart contract or the distributed ledger on which it was created. Rather, a token is an entry in a register that is maintained using the smart contract. The proof that a particular distributed ledger address holds tokens is thus that the register is maintained through the smart contract which contains a corresponding entry.

E.4 Purchaser's technical requirements

Users can interact with the blockchain using minimal hardware requirements such as smartphones. Any modern computer with a good internet connection can become a network participant since it requires minimal software to send transactions.

To gain control over USD€ tokens, purchasers must fulfill several technical requirements. Firstly, they need a compatible digital wallet or similar technology that supports the blockchain standards on which USD€ operates, such as ERC-20 for Ethereum. Secondly, the purchaser must also have a secure means of generating and storing public and private keys. Thirdly, purchasers must ensure they have a sufficient amount of the respective blockchain's native crypto-asset (e.g., Ether (ETH) for Ethereum) to cover transaction fees.

Furthermore, purchasers may need to open an account with Eurodollar ApS or another entity that is authorised to offer USD€ Tokens, so that the prospective purchaser can acquire USD€. This process typically includes completing a Know-Your-Customer (KYC) procedure to comply with regulatory requirements. The KYC process involves providing personal identification information and verifying identity, which helps prevent fraud and ensure compliance with anti-money laundering (AML) regulations.

As USD€ is stored and transferred using public blockchains, purchasers may be able to acquire USD€ using some form of decentralized finance (DeFi) technologies. If USD€ is acquired from, or with the use of, DeFi, prospective purchasers should be aware that Eurodollar cannot guarantee the legitimacy of any such services.

E.5 Consensus mechanism

A global network of node operators collectively runs the Ethereum network. Consensus is achieved through a protocol called Proof of Stake. Specifically for Ethereum there exists multiple protocol implementations written in various programming languages and supported by different teams and companies, these implementations diversify the risk of software related bugs compromising the wider network.

E.6 Incentive mechanisms and applicable fees

Ethereum node operators stake capital, either pooled from a larger group or individually, and in exchange of honest network participation receives ETH rewards. The probability of validating a new block is determined by how large of a stake a person holds. Validators do not receive block rewards, instead they collect network fees as their reward.

E.7 Use of distributed ledger technology

false

E-money token's audit details

E.9 Audit

true

E.10 Audit outcome

The first version of the USD€ smart contracts were audited on 08/12/2023 by Fixed Point Solutions LLC. The scope of the audit was the following: ● Ensure malicious actors cannot call functions that are only meant to be called by the Eurodollar team and automated software. This involves any function with a specific role. ● Ensure the protocol implements corresponding standards ERC20, ERC4626. ● Ensure the protocol implements upgradeability patterns correctly. ● Ensure the system is safe from front running attacks, e.g. when updating the price oracle. ● Ensure the system is safe from precision loss exploits.

Issues identified during the audit were reviewed, validated, assessed and remediated prior to launch.

Eurodollar conducted a further audit of the updated USD€ smart contracts by way of a public bug bounty. The public bounty programme ran from 04.11.2024 to 18.11.2024 on Hats.Finance. The programme enabled independent security researchers to test the smart contracts for any security vulnerabilities. Any issues identified during the programme were reviewed, validated, assessed and remediated prior to launch.

Eurodollar endeavours to carry out future audits for each major upgrade to the Eurodollar protocol.

∨ Part F – Information on the risks

F.1 Issuer-related risks

a. Failure to maintain an e-money licence in Denmark There exists a regulatory risk associated with the Issuer maintaining the necessary e-money licence with the DFSA. Failure to maintain this licence would have significant negative implications for the Issuer's operations and the overall success of USD€ and the business of the Issuer. In particular, it would mean that it would not be able to issue EMTs such as USD€. The regulatory landscape surrounding EMIs is subject to stringent requirements and oversight. The process of maintaining an e-money licence involves continuously demonstrating compliance with various regulatory frameworks, including anti-money laundering (AML) and know-your-customer (KYC) regulations, as well as meeting specific capital adequacy and operational standards. Potential mitigating factors include proactive engagement with regulatory authorities, meticulous adherence to regulatory requirements, and ongoing monitoring of changes in the regulatory landscape.

b. Insolvency risk The Issuer is mandated by the Danish Payment Act (Betalingsloven) section 35 to hold all customer funds backed on a 1:1 basis with the corresponding USD paid at issuance of USD€ in segregated accounts. This is a requirement designed to safeguard these funds by keeping them distinct from the Issuer's own assets. In the event of insolvency, the assets are distributed according to Danish bankruptcy order as set out in the Danish Bankruptcy Act (Konkursloven) section 92-98. It is essential to note that customer funds and assets held in segregated accounts are addressed before this bankruptcy order, cf. section 82, ensuring protective measures for customers and USD€ holders. Initially, debt incurred by the bankruptcy estate, such as the administrator's fees and necessary purchases for estate management, is addressed. This is followed by costs related to any prior liquidation or reconstruction of the Issuer. Then come claims for wages, pensions, and holiday pay. After these, ordinary claims, which comprise the majority of creditors' claims, are settled. Lastly, subordinated claims are addressed, which include interest accrued after the commencement of the bankruptcy and certain fines and promises.

c. Operational Risk There are a number of risks related to external and internal circumstances or events which may harm the operating business of the Issuer. These are related to losses due to incorrect or insufficient controls, errors caused by humans or systems; and/or legal risks, among others. In particular, the Issuer depends on reputable and reliable ledger systems on which the smart contracts in the blockchain will be conducted. Should their service or operation among others be constrained or a disruption occurs, the Issuer may be unable to, temporarily or permanently, issue additional, or redeem existing, USD€. Any of these risks may be detrimental and can adversely impact the Issuer's ability

to perform its obligations under USD€. The mitigant adopted in this regard is that the Issuer implements an IT security policy which means that copies of transactional information are held in more than one location. The Issuer would expect to be able to retrieve this information and fulfil Redemption Requests from the Reserve Assets accordingly.

d. Changes in the Regulatory Environment The Issuer issues USD€ which, as an EMT, is subject to a regulatory environment that is evolving. Regulatory changes are to be expected at a national and international level. This may have a material adverse effect on the Issuer's cost of operations, net assets and overall financial position, and thus negatively affect its ability to fulfil claims arising from USD€. Therefore, it cannot be ruled out that negative effects of a change in the regulatory environment may result in the Issuer no longer being able to operate economically and having to discontinue their business partially or as whole. The implementation of MiCAR serves as a mitigating factor in this regard as it offers some regulatory certainty. The Issuer endeavours to monitor regulatory developments and participate in consultations as reasonably practicable and possible. It seeks to maintain an open and ongoing relationship with the DFSA.

e. Reliance on key personnel The Issuer's operational success will depend on the continuing efforts of its directors. The loss of the service of one or more directors may have an adverse effect on the Issuer's operations and its ability to perform its obligations in respect of USD€.

f. Cybersecurity related risks The Issuer is susceptible to operational, information security and related "cyber" risks. In general, cyber incidents can result from deliberate attacks or unintentional events. Cyber incidents include, but are not limited to, gaining unauthorized access to digital systems (e.g., through "hacking" or malicious software coding) for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyberattacks may also be carried out in a manner that does not require gaining unauthorized access, such as causing denial-of-service attacks on websites (i.e., efforts to make network services unavailable to intended users). Cybersecurity failures by, or breaches of, the systems have the ability to cause disruptions and impact business operations of the Issuer, potentially resulting in: financial losses, interference with the business activity of the Issuer, disclosure of confidential information, impediments to transfers, submission of erroneous transfers or erroneous creation or redemption requests, the inability of the Issuer or its service providers to transact business, breaches of applicable privacy and other laws, regulatory fines, penalties, reputational damage, reimbursement or other compensation costs, or additional compliance costs. All of this could negatively impact the financial position of the Issuer and could result in it failing to

fulfil Redemption Requests. g. Risk of Data Breach The Issuer maintains significant amounts of data surrounding transactions, transaction executions, as well as customer data. A significant data breach may have wide reaching adverse effects, including trading losses and loss of reputation, which may negatively impact the Issuer's business and financial performance. The Issuer has implemented internal IT security policies and procedures to prevent data breaches. h. Reputational Risk There is a potential for negative public perception or loss of trust in the Issuer or USD€ itself. The Issuer's reputation may deteriorate due to cases in which stakeholders' perception of the Issuer or USD€ differs negatively from the Issuer's actual conduct, performance or business practice. Realisation of reputational risks could have material adverse effects on the Issuer's business, results of operations and USD€. i. The Issuer has a limited business history The Issuer was acquired by the Eurodollar group on 30 April 2024 so it does not have significant "track-record" of issuing EMTs or other related activity. This is due to the fact that there was no regulatory framework governing the issuance of EMTs until the recent implementation of MiCAR. Prior to its acquisition, the Issuer was a software services company specialising in the digital, crypto-assets sector. j. Risks relating to third parties The Issuer is able to deliver USD€ by working with one or more third parties. This is the risk that if those third parties cannot, for any reason, deliver their services, the Issuer's ability to deliver the Services, in particular, fulfil Redemption Requests could be affected too. The Issuer seeks to use third parties of good standing conducting due diligence on the third parties it engages although it cannot and does not endorse any particular third party. Additionally, the Issuer enters into agreements which contain provisions to protect delivery of the services including an ability to terminate services in the event of material disruption or delays. k. Market risks This risk is that if there is unexpected market activity, the Issuer may not be able to fulfil Redemption Requests within the expected timeframe. For example, it may not be able to

F.2 Token-related risks

a. Under-collateralization risk There is a risk that due to mismanagement or fraud relating to the Reserve Assets, USD€ may end up with reserves which are not equivalent to the total number of USD€ in circulation. The Reserve Assets would be lower than required to meet all Redemption Requests and therefore this could compromise the Issuer's ability to fulfil Redemption Requests at par in a timely manner. If this risk materialise, the Issuer would implement its recovery or redemption plans to ensure that the Reserve Assets are duly rebalanced.

b. Liquidity risks This is the risk that the Reserve Assets may not all be readily liquidated, therefore, if there is a particularly high demand for Redemption Requests, the Issuer may not be able to fulfil all requests in a timely manner. The Issuer would manage high demand by implementing certain mechanisms provided for in its redemption plan including pausing Mint Requests and/or Redemption Requests.

c. Limited secondary market liquidity of USD€ Although USD€ is freely transferable, there can be no assurance that a secondary market for USD€ will develop, or, if a secondary market does develop, that it will provide the holders of USD€ with liquidity or that it will continue for the life of USD€. This risk is mitigated by USD€ Holders being able to make Redemption Requests which means that, in the ordinary course, USD€ Holders could expect to redeem their USD€ for fiat or another EMT from the Issuer.

d. Secondary market price There is a risk that the price of USD€ in the secondary market becomes unstable from time to time compared to USD. The price of USD€ in the secondary market could be affected by several factors including but not limited to the perception of the Reserve Assets, including but not limited to their value or safety, or market movements relating to the Reserve Assets.

e. Limited recovery risk In the event of the Issuer's insolvency or liquidation, claims of USD€ holders will rank *pari passu*, meaning they will be treated equally to each other and USD€ holders will share in any distributions from the remaining assets of the Issuer on a proportional basis and so may not recover an amount equal to the USD€ they bought. As a mitigating factor, Customer funds and assets held in segregated accounts are addressed before the bankruptcy order, ensuring protective measures for USD€ holders (see section F.1(b) (Insolvency Risk) for more details).

f. Payments in a currency other than USD Where payments in respect of USD€ are made in a currency other than USD, such payments will be made on the basis that one USD€ is worth exactly one USD. The risk is that the customer could receive a different amount of USD€ than expected if they have paid in a currency other than USD due to the conversion rate that may be applied by their or the Issuer's bank, for example. Customers could mitigate this risk by enquiring about currency conversion rates and options that may be available from

different service providers. g. Taxation risks Depending on the laws and regulations applicable to the USD€ Holder, purchases and sales of USD€ could be subject to taxes. The Issuer cannot guarantee what tax treatment the USD€ Holders transfers or Redemption Requests will attract and the tax treatment may differ from country to another.

F.3 Technology-related risks

a. Risk relating to blockchain technology The Issuer is reliant on blockchain technology for the performance of certain critical functions in respect of USD€, including (without limitation) the issuance, transfer and redemption of USD€. Blockchain technology is relatively new and untested, and subject to known and unknown risks, including the risks set out below:

- i. The blockchain source code could be updated, amended, altered or modified from time to time by the developers and/or the community of users. There can be no guarantee that such update, amendment, alteration or modification will not adversely affect the functionality of USD€.
- ii. Changes to the protocol that govern the blockchain may result in the development of parallel chains of blocks (so-called "hard forks") when some of the blockchain's nodes are validating transactions on the basis of the old version of the protocol, while other nodes are validating transactions on the basis of the new protocol. The smart contract governing USD€ makes it possible for the Issuer to "freeze" USD€ (i.e. to prevent execution of transactions on the blockchain) until the Issuer has made a decision as to which version of the protocol it will support. In the event of such a freeze, holders of frozen USD€ will not be in a position to transfer or redeem such USD€. Such a freeze may however occur after the hard fork has started to take effect. This could lead to significant uncertainties as to the ownership of the underlying assets which have been transferred (by way of USD€) immediately before the freeze has been implemented.
- iii. Blockchain technology functions based on concepts belonging to asymmetric cryptography, or public key cryptography. Scientific research regarding blockchain technology is still at an early stage. Code cracking or technical advances such as the development of quantum computers, could present a risk for all blockchain technology. This could result in the theft, loss, disappearance, destruction or devaluation of USD€.
- iv. Hackers or other groups or organisations may attempt to interfere with digital wallets maintained by Tokenholders in any number of ways, including without limitation denial of service attacks, Sybil attacks, spoofing, smurfing, malware attacks or consensus based attacks.
- v. Blockchain settlement issues can be caused by delayed or failed transactions and network problems. This could result in the delay or failure of certain critical functions in respect of USD€, including (without limitation) the issuance, transfer and redemption of USD€ and the ability for Tokenholders to vote on certain matters relating to them.

b. Smart contracts The USD€ Tokens are created and managed under the terms of a so-called "smart contract", i.e. computer code that defines the manner in which digital tokens can be created, transferred and cancelled. Smart contracts are non-trivial pieces of computer code and their interactions with the blockchain for which they

have been created are complex. It cannot be excluded that the code for the smart contract used by the Issuer contains flaws, errors, defects and bugs, which may disable some functionality of the USD€ Tokens, expose Tokenholders' information or otherwise be harmful to the Tokenholders or the Issuer. E.g., should the smart contract based on which the USD€ Tokens are operated cease to function for any reason, certain critical functions in respect of the USD€ Tokens, including (without limitation) the issuance, transfer and redemption of USD€ Tokens will be impaired.

c. Loss or theft of USD€ Control over USD€ tokens requires a so-called "private key", i.e. a code that is paired with the blockchain address on which USD€ has been recorded. Loss or theft of the private key associated with a particular blockchain address may make it difficult or impossible for a Tokenholder to identify itself as the legitimate owner of USD€ recorded on the relevant blockchain address. The terms of the USD€ Tokens specify the procedure to be followed if a Tokenholder loses access to its USD€, e.g. because the corresponding private key has been lost or stolen. The applicable procedure involves the Tokenholder being in a position to demonstrate in a manner satisfactory to the Issuer that (i) the relevant USD€ has been lost or stolen and (ii) it is the rightful owner of the lost or stolen USD€. Such demonstration may be difficult to bring, particularly if the Tokenholder has not previously identified itself to the Issuer as the owner of the blockchain address with which the lost or stolen private key is associated.

d. Lack of anonymity Any trades of USD€ are public shortly after such trades are entered into. Although the data made available on the public version of a blockchain is anonymous, it will include the blockchain address of each Tokenholder transacting in USD€, and the entire trading history of each blockchain address (including the number of USD€ traded, the price of each trade and the balance of USD€ held in each digital wallet). As a result, the trading history of each blockchain address is available to the general public and it may be possible for members of the public to determine the identity of the holders of certain blockchain addresses based on publicly available information.

e. Additional fees payable USD€ are only transferable in the form of digital tokens recorded on the blockchain. On the Ethereum blockchain, every operation of the smart contract is subject to a fee (so-called "gas"), which must be paid in a cryptocurrency, called "Ether", in order for an operation to be executed. Gas fees are not only due in the event of a transfer of USD€ from one blockchain address to another, but also for other operations, such as the deployment of the smart contract on the blockchain or communications between Tokenholders and the Issuer (provided that such communications take place through the blockchain by means of the smart contract). Gas fees are generally payable by the party that

initiates the operation. Tokenholders may therefore be required to pay gas fees in order to conduct certain critical operations in respect of their USD€. Gas fees are outside the control of the Issuer; they vary from time to time and are determined by supply and demand. It is therefore possible that the gas fee in respect of a transaction in USD€ may amount to more than the value of such USD€, thereby making the transaction economically unviable.

F.4 Mitigation measures

Mitigation measures are included in-line, in the above statement of associated risks.

- ✓ Part G – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts

G.1 Adverse impacts on climate and other environment-related adverse impacts

Eurodollar deploys smart contracts on the Ethereum blockchain using proof of stake mechanism (PoS) rather than proof of work (PoW). PoS is widely considered materially more environmentally friendly than PoW and research suggests that PoS is as much as 99.95% more energy efficient than PoW. However, despite these improvements, Ethereum's PoS still consumes energy for its operation. The estimated annual energy consumption of the Ethereum network post-Merge is approximately 0.026 TWh per year, with a carbon footprint of 870 tonnes CO₂ equivalent/ per year (<https://ethereum.org/en/energy-consumption/>). Eurodollar is committed to providing clear and detailed information on the environmental impacts of its operations, however, as the Eurodollar protocol has not been launched and USD€ has not been issued, the Issuer currently does not have calculations about the energy consumption or other environmental factors affecting USD€. The environmental impact of the Eurodollar protocol will be reviewed on an ongoing basis, this section will be updated as more information becomes available following issuance of USD€.

General information about adverse impacts

S.1 Name

Eurodollar ApS

S.2 Relevant legal entity identifier

8945001XWFMRUTCAK575

S.3 Name of the crypto-asset

EU Dollar

S.4 Consensus mechanism

A global network of node operators collectively runs the Ethereum network. Consensus is achieved through a protocol called Proof of Stake. Specifically for Ethereum there exists multiple protocol implementations written in various programming languages and supported by different teams and companies, these implementations diversify the risk of software related bugs compromising the wider network.

S.5 Incentive mechanisms and applicable fees

Ethereum node operators stake capital, either pooled from a larger group or individually, and in exchange of honest network participation receives ETH rewards. The probability of validating a new block is determined by how large of a stake a person holds. Validators do not receive block rewards, instead they collect network fees as their reward.

S.6 Beginning of period to which disclosed information relates

2026-02-10

S.7 End of period to which disclosed information relates

9999-12-31

Sources and methodologies

S.9 Energy consumption sources and methodologies

<https://ethereum.org/en/energy-consumption/>