MiCA White Paper

AmericanFortress Token (“$AF”)

Version 1.0
September 2025

White Paper in accordance with Markets in Crypto Assets Regulation (MiCAR)
for the European Union (EU) & European Economic Area (EEA).

Purpose: Public offer in Liechtenstein (Home
Member State) pursuant to Art. 3(1)(33)(c) MiCAR
and seeking admission to trading in EU/EEA.
Prepared and Filed by MatterFi Inc. Wyoming USA

NOTE: THIS CRYPTO-ASSET WHITE PAPER HAS NOT BEEN APPROVED BY ANY COMPETENT AUTHORITY IN ANY MEMBER STATE OF THE EUROPEAN UNION. THE OFFEROR AND PERSON SEEKING ADMISSION TO TRADING IS SOLELY RESPONSIBLE FOR THE CONTENT OF THIS CRYPTO-ASSET WHITE PAPER ACCORDING TO THE EUROPEAN UNION’S MARKETS IN CRYPTO-ASSET REGULATION (MICA).

TABLE OF CONTENTS

01 **DATE OF NOTIFICATION**

2025-09-16

COMPLIANCE STATEMENTS

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

Where relevant in accordance with Article 6(3), second subparagraph of Regulation (EU) 2023/1114, reference shall be made to ‘person seeking admission to trading’ or to ‘operator of the trading platform’ instead of ‘offeror’.

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

04 The crypto-asset referred to in this white paper may lose its value in part or in full, may not always be transferable and may not be liquid.

05 False (not applicable; COMMISSION IMPLEMENTING REGULATION (EU) 2024/2984)

06 The crypto-asset referred to in this white paper is not covered by the investor compensation schemes under Directive 97/9/EC of the European Parliament and of the Council. The crypto-asset referred to in this white paper is not covered by the deposit guarantee schemes under Directive 2014/49/EU of the European Parliament and of the Council.

SUMMARY

07 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 crypto-asset 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 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.

08 Characteristics of the crypto-asset

Under Regulation (EU) 2023/1114 (MiCA), the AmericanFortress ($AF) token is most appropriately treated as an “other crypto-asset” within Title II, since it neither maintains value by reference to an external asset nor promises redemption at par in legal tender; rather, it functions as a utility/access instrument that (i) enables reservation and locking of unique FortressNames for send-to-name transfers and (ii) fuels a privacy-preserving signaling layer used by wallets and infrastructure partners, with optional verifiable-credential features for KYC/AML-compatible interactions. In practical terms, $AF is consumed/locked to secure name reservations and to operate the signaling substrate, thereby creating endogenous demand that is tied to protocol use rather than to any promise of price stability or claims on issuer assets; unique counterparty-specific receive addresses, combined with multimodal signaling and optional credentials, deliver usability and confidentiality without altering on-chain settlement semantics.

Technically, $AF is minted on Ethereum mainnet at Token Generating Event (TGE), bridged 1-for-1 to Base via the official bridge, contract addresses are published in advance. Total supply is fixed at 10,000,000,000 $AF, with allocations and long-dated vesting.

The governance framework allows parameter adjustments—most notably the number of tokens locked per name—by ecosystem participants to maintain functional equilibrium as adoption scales; any buyback or additional locking language is rules-based and linked to protocol revenues (e.g., name sales), not to any commitment to maintain value.

Accordingly, issuers/offerors of $AF fall under Title II obligations: when $AF is offered to the public in the EEA or admitted to trading on an EEA platform, a crypto-asset white paper must be drawn up and notified to the competent authority of the Home Member State before publication; there is no prior approval requirement for such white papers, and standard exemptions (e.g., sub-€1m/12-month offers, free distributions, limited-network use) may apply subject to conditions. Marketing communications must be clearly identifiable and consistent with the white paper; additional CASP requirements apply where relevant.

09 Not applicable

10 Key information about the offer to the public or admission to trading

The AmericanFortress ($AF) token will be offered in the whole European Union and European Economic Area by MatterFi Inc., United States, with Liechtenstein designated as the Home Member State for MiCA purposes. In accordance with MiCA Title II, the crypto-asset white paper will be notified to the Financial Market Authority of Liechtenstein (FMA), Liechtenstein’s designated National Competent Authority—prior to publication; upon a completeness review, the FMA will transmit the white paper and associated data to ESMA and any relevant Host NCAs for entry in the EU-wide register and passporting mechanics.

The transaction structure consists of (i) a primary offer in Liechtenstein conducted by the issuer (no placement agent) subject to FMA-notified documentation and applicable exemptions, and (ii) admission to trading on Kraken’s EU venue operated from Ireland, a CASP authorised under MiCA by the Central

Bank of Ireland (CBI; the national competent authority of Ireland), enabling secondary market trading across the EEA under the platform's onboarding, AML/KYC and market-conduct rules. A separate US listing on Kraken or other trading venues may be contemplated but falls outside the scope of this EU white paper. Likewise, the $AF Token may be admitted to trading on other trading venues in the future. Secondary trading will be sought on Kraken (EU) operated by Payward Europe Solutions Limited ("PESL"), company no. 711781, registered address: 70 Sir John Rogerson's Quay, Dublin Docklands, Dublin 2, D02 R296, Ireland. PESL is authorised by the Central Bank of Ireland as a Crypto-Asset Service Provider (CASP) under Regulation (EU) 2023/1114 (MiCA) and European Union (Markets in Crypto-Assets) Regulations 2024 (S.I. No. 607/2024), CBI register no. C468360.

Offeror / Issuer	MatterFi Inc., 30 N Gould St, Ste 20466, Sheridan, WY 82801, USA; Home Member State: Liechtenstein (notification to the Financial Market Authority Liechtenstein before publication).
Total offer amount	$4,125,000 at TGE
Total number of tokens to be offered to the public	825,000,000
Subscription period	Oct 9th, 2025.
Minimum and maximum subscription amount	Not applicable
Issue price	$0.005
Subscription fees (if any)	None.
Target holders of tokens	Retail and professional investors in Liechtenstein for the primary offer; secondary market trading open to eligible EEA users on the authorized venue (post-admission), subject to onboarding and AML/KYC.
Description of offer phases	Admission to trading on Kraken (EU) operated by PESL; delivery as ERC-20 on Ethereum at TGE with 1:1 bridge to Base, contract addresses published ≥72h prior to TGE.
CASP responsible for placing the token (if any)	Not applicable (issuer conducts the offer directly; the venue is for secondary trading).
Form of placement	Direct subscription (issuer), with standard KYC/AML onboarding; tokens delivered on-chain to the subscriber's address.
Admission to trading	Payward Europe Solutions Limited ("PESL") trading as "Kraken", company no. 711781, 70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Ireland; authorised CASP by the Central Bank of Ireland (C468360) under MiCA and S.I. No. 607/2024 (as provided).
Total supply (info)	10,000,000,000 AF (fixed, non-inflationary).
Chain & custody (info)	Mint on Ethereum; bridge 1:1 to Base; contract addresses published ≥72h before Token Generating Event (TGE).
Allocation (info)	Community/User Incentives 3,000,000,000 (30%); Treasury 2,600,000,000 (26%); Engineering 1,200,000,000 (12%); Team & Advisors 1,000,000,000 (10%); Marketing 1,000,000,000 (10%); Liquidity/MM 400,000,000 (4%); MF Private Round 1 400,000,000 (4%); MF Private Round 2 400,000,000 (4%).

Vesting (info)	Private R1 25% TGE, 75% linear over 8m; Private R2 10% TGE, 90% over 24m; Team 5% TGE, 95% over 24m; Eng 10% TGE, 3m cliff, then over 24m (TGE+27m); Mkt 4% TGE, 96% over 18m; Community 2.5% TGE, 97.5% over 96m; Treasury 0% TGE, 12m cliff, 100% over next 48m (TGE+60m).

A. PART A - INFORMATION ABOUT THE OFFEROR OR THE PERSON SEEKING ADMISSION TO TRADING

A.1 Name

MatterFi Inc. (offeror/issuer).

A.2 Legal Form

Corporation (Wyoming profit corporation, “Inc.”)

A.3 Registered Address

30 N Gould St, Ste 20466, Sheridan, WY 82801, USA.

A.4 Head Office

249 Bonneville Rd., Star Valley Ranch, WY 83127

A.5 Registration Date

6 November 2020 (initial filing, WY).

A.6 Legal Entity Identifier
254900SCRP0O8UPILI97

A.7 Another Identifier Required Pursuant to Applicable National Law

Wyoming company no. 2020-000956967; U.S. SEC CIK 0001855356; EIN 85-3798641.

A.8 Contact Telephone Number

+1 (617) 939-6295

A.9 E-mail Address

mehow@matterfi.com

A.10 Response Time (Days)

020

A.11 Parent Company

Not applicable

A.12 Members of the Management Body

Full Name	Business Address	Function
Michal “Mehow” Pospieszalski	30 N Gould St, Ste 20466, Sheridan, WY 82801, USA.	CEO
Jakub Żurawiński	same as above	VP Marketing & Sales.
Chris Odom	same as above	Technology Founder

A.13 Business Activity

MatterFi develops security and transaction infrastructure for digital assets (software/hardware wallet stack, privacy-preserving send-to-name addressing, decentralized KYC/AML and identity), and owns/operates the AmericanFortress brand, under which the AF utility token supports human-readable FortressNames and the protocol’s signaling/credential layer.

A.14 Parent Company Business Activity

Not applicable

A.15 Newly Established

false

A.16 Financial Condition for the past three Years

In 2023 and 2024, Matterfi Inc. strengthened its operational efficiency, expanded its business activities. Looking ahead to 2025, the company anticipates positive financial development, supported by market uptrends, an inflow of customer funds, and strong business performance. Increased adoption of digital assets and service expansion are expected to drive higher revenues and profitability, further reinforcing the company's financial position.

Unaudited interim balance sheet of MatterFi Inc as of Q2 2025.

Balance Sheet
MatterFi Inc
As of Q2, 2025

Distribution account	Total
Assets	
Cash and Cash Equivalents	504,280
Accounts Receivable	836,147
Other Assets	
Intellectual Property	45,000,000
Technical Acquisitions	185,000
Deployed Servers	45,000
Total for Assets	**46,570,427**
Long Term Liabilities	745,000
Equity	
Capital Equity	45,000,000
MatterFi Pre TGE Round	740,000
MatterFi Bridge Round	2,931,853
MatterFi Seed Round	1,536,577
Treasury Stock	25,000
Retained Loss	-4,408,002
Total for Liabilities and Equity	**46,570,427**

A.17 Financial Condition Since Registration

Matterfi Inc. has been continuously operating since its registration, supported by USD $6m in share capital and continuous business growth. Since its inception, the company has expanded its operations. The company has consistently reinvested in operations and technology ensuring long-term sustainability.

B. PART B - INFORMATION ABOUT THE ISSUER, IF DIFFERENT FROM THE OFFEROR OR PERSON SEEKING ADMISSION TO TRADING[1]

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

False

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

Not applicable

B.11 Business Activity

Not applicable

B.12 Parent Company Business Activity

Not applicable

C. 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.

C.2 Legal Form

Not applicable.

C.3 Registered Address

Not applicable.

C.4 Head Office

Not applicable.

C.5 Registration Date

Not applicable.

C.6 Legal Entity Identifier

Not applicable.

C.7 Another Identifier Required Pursuant to Applicable National Law

Not applicable.

C.8 Parent Company

Not applicable.

C.9 Reason for Crypto-Asset White Paper Preparation

Not applicable. PESL is not drawing up the $AF white paper; the document is prepared by the offeror/issuer MatterFi Inc. under Article 6(1), first subparagraph MiCAR (offer to the public/admission).

C.10 Members of the Management Body

Not applicable.

C.11 Operator Business Activity

Not applicable.

C.12 Parent Company Business Activity

Not applicable.

C.13 Other persons drawing up the white paper under Article 6 (1) second subparagraph MiCA

Not Applicable

C.14 Reason for drawing up the white paper under Article 6 (1) second subparagraph MiCA

Not Applicable

D. PART D - INFORMATION ABOUT THE CRYPTO-ASSET PROJECT

D.1 Crypto-Asset Project Name

AmericanFortress Protocol (“AF Protocol”)

D.2 Crypto-Assets Name

AmericanFortress Token

D.3 Abbreviation

$AF

D.4 Crypto-Asset Project Description

AmericanFortress is a privacy-preserving send-to-name transaction and identity layer that lets users pay to human-readable FortressNames™ instead of raw wallet addresses, while preventing third parties from mapping names to on-chain activity; the protocol uses public paycodes (hardened xpubs) plus a multimodal signaling scheme (combined off-chain, on-chain and in-line backup signaling with decoy “noise”) so that only counterparties can derive the unique per-counterparty receive address and recover their transaction history from encrypted signals, without operating a mixer and without disabling chain analytics.

The token $AF is the utility instrument within this system: it is locked to reserve a unique FortressName and to enable signaling/KYC-credential features, creating ongoing protocol-driven demand and reduced free float; governance contemplates dynamic parameter tuning (e.g., tokens-per-name) by ecosystem partners.

AmericanFortress™ is owned and operated by MatterFi, which also offers an SDK for wallets, fintechs and custodians to integrate send-to-name and compliance triggers.

D.5 Details of all persons involved in the implementation of the crypto-asset project

Full Name / Legal Person	Business Address	Function
MatterFi Inc.	*30 N Gould St, Ste 20466, Sheridan, WY 82801, USA.*	*Project developer; brand owner/operator of AmericanFortress.*
Michal “Mehow” Pospieszalski	*30 N Gould St, Ste 20466, Sheridan, WY 82801, USA.*	*Chief Executive Officer & Co-Founder (executive oversight, commercial integrations).*
Chris Odom	*30 N Gould St, Ste 20466, Sheridan, WY 82801, USA.*	*Technology Founder / Protocol architect (co-inventor).*
Community contributors / AF SDK partners	*Global (decentralized)*	*Open-source and integration contributors; wallet/custody implementers of AF SDK (ongoing).*

D.6 Utility Token Classification

false

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

Not applicable

D.8 Plans for the Token

Phase 1 - Protocol launch: core send-to-name, name reservations, initial partner onboarding. Phase 2 — Expanded blockchain compatibility and DeFi/wallet integrations. Phase 3 — Advanced privacy layers and governance tooling; ecosystem parameterization for sustainable tokenomics.

D.9 Resource Allocation

Fixed, non-inflationary total supply: 10,000,000,000 $AF; minted on Ethereum at TGE and bridged 1:1 to Base; combined cap across chains 10B.

Allocation (% of supply): Community/User Incentives 30%; Treasury 26%; Engineering 12%; Team & Advisors 10%; Marketing 10%; Liquidity/MM 4%; MF Private Round 1: 4%; MF Private Round 2: 4% (sum 100%). Vesting (illustrative): private rounds (25%/10% at TGE, remainder 8–24 months), team (5% at TGE, 24-month vest), engineering (3-month cliff + 24-month vest), marketing (18-month vest), community (97.5% over 96 months), treasury (12-month cliff + 48-month vest).

D.10 Planned Use of Collected Funds or Crypto-Assets

The offer proceeds (cash and/or crypto-assets) will be applied to the development, commercialization, and compliant operation of the AmericanFortress Protocol and its token economy, along the following non-exhaustive lines:

1. Core protocol & SDK engineering.
2. Enterprise licensing & integrations.
3. Institutional KYC/AML credentials.
4. Security, audits & operational safeguards.
5. Ecosystem growth & grants.
6. Regulatory, legal & compliance.
7. Liquidity & market access.
8. General corporate purposes.

E. 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

OTPC + ATTR

E.2 Reasons for Public Offer or Admission to Trading

To permit regulated EU access to $AF under MiCA by (i) notifying a white paper in Liechtenstein (Home Member State) and (ii) securing admission to trading on a CBI-authorised CASP (Kraken EU/PESL), thereby improving transparency, investor protection and secondary-market liquidity while ensuring marketing and disclosures are MiCA-consistent. (White papers for “other crypto-assets” are notified to the Home NCA and transmitted to ESMA for the EU register; they are not approved ex ante.) Public Offer and Admission to Trading is sought for overall project realization and to use funds according to Planned Use.

E.3 Fundraising Target

$4,125,000 at TGE available to the public.

E.4 Minimum Subscription Goals

Not applicable.

E.5 Maximum Subscription Goal

$4,125,000

E.6 Oversubscription Acceptance

Not applicable

E.7 Oversubscription Allocation

Not applicable

E.8 Issue Price

0.005 USD

E.9 Official Currency or Any Other Crypto-Assets Determining the Issue Price

Not applicable

E.10 Subscription Fee

Not applicable

E.11 Offer Price Determination Method

Set by MatterFi, Inc board based on market conditions and comparables.

E.12 Total Number of Offered/Traded Crypto-Asset

Fixed maximum supply 10,000,000,000 $AF, minted on Ethereum and bridged 1:1 to Base; combined cap across chains 10 B.

E.13 Targeted Holders

ALL

E.14 Holder Restrictions

None.

E.15 Reimbursement Notice

Not applicable

E.16 Refund Mechanism

Not applicable

E.17 Refund Timeline

Not applicable

E.18 Offer Phases

Not applicable

E.19 Early Purchase Discount

Not applicable

E.20 Time-Limited Offer

Not applicable

E.21 Subscription Period Beginning

Not applicable

E.22 Subscription Period End

Not applicable

E.23 Safeguarding Arrangements for Offered Funds/Crypto-Assets

Not applicable

E.24 Payment Methods for Crypto-Asset Purchase

Kraken accepts the following payment methods for buying listed tokens, depending on your region and account verification level:

- Credit/Debit Cards: Visa or Mastercard with 3D Secure (3DS) support, in the same legal name as your Kraken account. Available for users with Intermediate or Pro-level verified accounts in supported countries.
- Bank Transfers:
- SEPA: For users in the Single Euro Payments Area, including SEPA Instant for faster transfers.
- SWIFT: For international wire transfers in USD or EUR, suitable for corporate clients or worldwide deposits.
- Digital Wallets:
- Apple Pay/Google Pay: Supported in regions where these services are available, linked to a verified card or bank account.
- PayPal: Available for depositing funds (e.g., USD, EUR, GBP) in supported regions, which can then be used to buy tokens. Fees vary by region.
- Crypto Deposits: You can fund your account with supported cryptocurrencies (e.g., BTC, ETH, USDT) to buy other listed tokens using Kraken's Convert feature or trading pairs.
- Cash Balance: If you already have a fiat balance (e.g., USD, EUR) in your Kraken account, you can use it directly to purchase tokens.

E.25 Value Transfer Methods for Reimbursement

Not applicable.

E.26 Right of Withdrawal

For any retail (consumer) subscriber: 14-day withdrawal right under MiCA for "other crypto-assets" public offers.

E.27 Transfer of Purchased Crypto-Assets

On-chain delivery as ERC-20 on Ethereum to subscriber's address; optional user bridging to Base (1:1).

E.28 Transfer Time Schedule

Instantaneous upon purchase as purchases are via off chain exchange Kraken.

E.29 Purchaser's Technical Requirements

Self-custody or venue-compatible wallet capable of receiving ERC-20 tokens; ability to complete venue KYC/AML for secondary trading.

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

Payward Europe Solutions Limited ("PESL", trading as "Kraken").

E.31 CASP identifier

CBI register number C468360 (Ireland).

E.32 Placement Form

NTAV

E.33 Trading Platforms name

Kraken (EU) operated by PESL (company no. 711781; 70 Sir John Rogerson's Quay, Dublin 2, D02 R296).

E.34 Trading Platforms Market Identifier Code (MIC)

PGSL

E.35 Trading Platforms Access

Access for verified clients meeting PESL onboarding standards; CASPs operate under MiCA with AML/CFT obligations and NCA supervision (additional services may be provided under PESL's Irish EMI/payments framework where applicable).

E.36 Involved Costs

Not applicable

E.37 Offer Expenses

None.

E.38 Conflicts of Interest

Not applicable

E.39 Applicable Law

Liechtenstein Law, subject to any mandatory provisions of law to the contrary.

E.40 Competent Court

Courts of Liechtenstein, subject to any mandatory provisions of law to the contrary.

F. PART F - INFORMATION ABOUT THE CRYPTO-ASSETS

F.1 Crypto-Asset Type

Other Crypto-Asset

F.2 Crypto-Asset Functionality

$AF is the native utility token of the AmericanFortress Protocol, used to (i) lock and reserve unique FortressNames™ so users can transact “send-to-name” instead of handling raw addresses, and (ii) operate a privacy-preserving multimodal signaling layer that lets counterparties compute unique receive addresses and recover their transaction history while preventing third parties from correlating signals or inferring address mappings; the token’s core demand thus arises from locking for names and usage-based signaling, not from any peg, redemption right, or stability mechanism.

Credential features allow users to attach blinded or unblinded KYC/AML proofs to a nym/name for compliant CeFi/DeFi interactions without public doxxing; chain analysis continues to function because the system is not a mixer, it merely ensures each counterparty interaction uses a deterministic derived, unique address.

F.3 Planned Application of Functionalities

Roll-out focuses on enterprise SDK integrations (wallets, custodians, processors), institutional KYC integrations, and staged roadmap phases: Phase 1 protocol launch with name reservations; Phase 2 expanded chain compatibility and DeFi/wallet partnerships; Phase 3 advanced privacy and governance tooling.

F.4 Type of white paper

OTHR

F.5 The type of submission

NEWT

F.6 Crypto-Asset Characteristics

ERC-20 token minted on Ethereum at TGE and bridged 1:1 to Base; combined supply cap fixed at 10 000 000 000 $AF; official Base bridge; contract addresses published ≥72 h pre-TGE on the project site and official channels; protocol is backwards-compatible with BIP-47/OBPP-5 public paycodes for interoperability. (Gas is paid in ETH when transacting on Ethereum.).
Its characteristics are defined by the Ethereum blockchain and the unique design of its smart contracts. $AF operates on the Ethereum network as an ERC-20 token, meaning all transactions are recorded on Ethereum’s distributed ledger. Ethereum is a mature, Turing-complete blockchain known for its smart contract functionality and widespread adoption. By leveraging Ethereum, $AF benefits from the platform’s security and interoperability: it can be stored in any Ethereum wallet and integrated into Ethereum’s vast DeFi ecosystem seamlessly.

Because it is an ERC-20 token, it inherits Ethereum’s consensus mechanism for transaction validation and network security. After Ethereum’s September 2022 upgrade (known as "The Merge"), Ethereum transitioned to a Proof-of-Stake (PoS) consensus algorithm. Consequently, transactions are confirmed by Ethereum’s validators who have staked ETH, providing rapid finality and high security. American Fortress token holders do not need to perform any mining; they rely on Ethereum’s consensus, paying gas fees in ETH for executing transfers or interacting with staking functions. This also ensures that $AF has a minimal carbon footprint compared to tokens previously dependent on Proof-of-Work mechanisms.

The American Fortress token smart contract implements standard ERC-20 functions (such as transfer, transferFrom, and approve) and includes unique logic for collateral partitions. This partition strategy allows designated contracts, known as collateral managers, to lock portions of an address’s $AF balance without transferring ownership, enabling verifiability on-chain. The contract also includes common security safeguards, such as the inability to mint new tokens, pause transactions, or blacklist addresses. The contract is immutable, meaning it cannot be altered after deployment, which

reinforces $AF's decentralized nature. Collateral manager contracts, such as Flexa's Capacity contract, act as programmable escrow agents capable of enforcing rules over staked $AF, such as unlocking it under certain conditions or after a specified time period.

F.7 Commercial name or trading name

$AF

F.8 Website of the issuer

https://www.matterfi.com
https://americanfortress.io/
https://americanfortress.io/whitepaper for general purpose token whitepaper and functionality
https://americanfortress.io/AF-mica-white-paper/ for this MiCA whitepaper

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

2025-10-15

F.10 Publication date

2025-10-15

F.11 Any other services provided by the issuer

Issuer develops wallet, custody, and security infrastructure and an enterprise SDK that integrates send-to-name, credentialed access, and compliance triggers.

F.12 Language or languages of the white paper

English

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, where available

DLMW9KPK3

F.14 Functionally Fungible Group Digital Token Identifier, where available

No FFG-DTI is currently assigned to $AF. This field will be updated upon issuance of a group identifier by the Digital Token Identifier Foundation or another competent authority, as per MiCA RTS Article 5.

F.15 Voluntary data flag

false

F.16 Personal data flag

false

F.17 LEI eligibility

true

F.18 Home Member State

Liechtenstein

F.19 Host Member States

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

G. PART G - INFORMATION ON THE RIGHTS AND OBLIGATIONS ATTACHED TO THE CRYPTO-ASSETS

G.1 Purchaser Rights and Obligations

Holders of $AF do not acquire claims on issuer assets, dividends, redemption rights, or a promise of value stability. $AF confers utility access to the AmericanFortress Protocol—principally (i) locking to reserve FortressNames™ and (ii) use of the privacy-preserving signaling/credential layer—subject to applicable law and any venue onboarding requirements; there are no equity, debt, or profit-share rights embedded in the token.

G.2 Exercise of Rights and Obligation

Use is on-chain, by sending $AF or locking $AF to reserve a name; wallets/SDKs invoke the multimodal signaling features, and users may attach blinded/unblinded KYC credentials to a name/nym for compliant interactions. There is no separate off-chain “exercise” of contractual rights.

G.3 Conditions for Modifications of Rights and Obligations

There are no tokenholder claims to modify financial rights because none are granted. The protocol may adjust operational parameters (e.g., tokens-per-name) through the governance framework and ecosystem-partner stewardship; such adjustments do not alter the fixed supply cap or create redemption/peg features. Technical remain as published.

G.4 Future Public Offers

Not currently contemplated; any future offer would be assessed under MiCA and notified as required.

G.5 Issuer Retained Crypto-Assets

As described in tokenomics, allocations under issuer/affiliates or subject to issuer stewardship/vesting include: Treasury 2,600,000,000 (26%), Liquidity/MM 400,000,000 (4%), Engineering 1,200,000,000 (12%), Team & Advisors 1,000,000,000 (10%) (vesting/cliffs per schedule). These do not grant purchasers any claim to issuer assets.

G.6 Utility Token Classification

No

G.7 Key Features of Goods/Services of Utility Tokens

Not applicable

G.8 Utility Tokens Redemption

Not applicable

G.9 Non-Trading Request

True

G.10 Crypto-Assets Purchase or Sale Modalities

See Part E (direct offer by MatterFi; admission to trading on Kraken EU/PESL).

G.11 Crypto-Assets Transfer Restrictions

$AF is freely transferable ERC-20, subject to applicable law/sanctions, venue terms, and smart-contract vesting applicable to certain allocations (e.g., team/treasury cliffs and linear vesting).

G.12 Supply Adjustment Protocols

Fixed, non-inflationary total supply of 10,000,000,000 $AF; no algorithmic rebase/peg, no protocol burn requirement. Any adoption-linked buybacks/locking are rules-based/discretionary and do not change total supply.

G.13 Supply Adjustment Mechanisms

Not applicable.

G.14 Token Value Protection Schemes

False

G.15 Token Value Protection Schemes Description

Not Applicable

G.16 Compensation Schemes

False

G.17 Compensation Schemes Description

Not Applicable

G.18 Applicable Law

Liechtenstein Law

G.19 Competent Court

Wyoming, USA.

H. PART H – INFORMATION ON THE UNDERLYING TECHNOLOGY

H.1 Distributed ledger technology

$AF is an ERC-20 crypto-asset issued on Ethereum mainnet; at TGE it is bridged 1:1 to Base (an Ethereum L2; the combined supply across chains is capped at 10 billion $AF. In addition to L1/L2 settlement, the AmericanFortress Protocol (AFP) layers “send-to-name” addressing, privacy-preserving signaling, and public-paycode infrastructure to compute per-counterparty receive addresses and to signal transactions through redundant on-chain and off-chain paths

Key characteristics of Ethereum as the DLT for $AF include:

Network Decentralization: Ethereum is maintained by a large network of independent validator nodes spread across the globe. As of 2025, there are over half a million active validators securing Ethereum’s PoS network, distributed across many countries and operators (ranging from individual stakers to staking pools and institutional node providers). No single entity controls Ethereum; consensus is achieved collectively through the protocol rules. This means $AF transactions, recorded on Ethereum, benefit from a very high degree of censorship-resistance and uptime. There is no central authority that can arbitrarily alter $AF balances or block $AF transfers – any such attempt would require compromising Ethereum’s core (which would require control of >2/3 of staked ETH, an extremely high economic barrier). Thus, Ethereum provides $AF with a neutral and resilient ledger.

Ledger Structure: Ethereum’s ledger uses an account-based model (each address has a balance). American Fortress tokens are recorded as balances in the $AF smart contract, which itself is an entry in Ethereum’s global state. When $AF is transferred, the ledger updates the balances in the contract for the sender and recipient addresses. All such state changes are grouped into blocks (one block roughly every 12 seconds). Ethereum’s ledger is linear (one canonical chain of blocks, ignoring temporary forks) and each block references the previous one, forming a tamper-evident chain. The state (including $AF balances) is fully replicated on every node; any node can independently verify all $AF transactions by executing the contract code from genesis to current block. This ensures transparency – anyone can use a block explorer to see $AF’s total supply, any address’s $AF balance, and all $AF transfers or staking events historically.

Smart Contract Execution: Ethereum’s distributed ledger isn’t just a simple transaction record; it runs the EVM (Ethereum Virtual Machine) which executes smart contract code. The American Fortress token contract and its associated collateral manager contracts are deployed code on Ethereum. Every Ethereum node executes these contracts’ code as part of processing blocks, ensuring uniform outcomes. This means the ledger not only stores balances but also enforces $AF’s rules (like partitions and transfer logic) in a decentralized way. The Ethereum ledger’s consensus rules ensure that if, say, an $AF collateral manager contract says “don’t release this $AF until time X or condition Y,” then no transaction can bypass that without fulfilling conditions – because all nodes will reject invalid state changes. In essence, Ethereum provides a global computer where $AF’s business logic runs, with full consistency and auditability.

Public Accessibility: Ethereum is a public blockchain, so anyone with an internet connection can run a node or query the network. $AF’s ledger data is available via many public block explorers (like Etherscan) and API services. The open nature means stakeholders – including regulators or auditors – can verify $AF’s on-chain data independently. For example, one can confirm the foundation’s wallet balances, or track the movement of $AF into and out of staking contracts. This transparency is a core attribute of the underlying DLT, contributing to trust in $AF’s circulating supply and usage.

Security and Finality: With Ethereum’s Proof-of-Stake, once an Ethereum block is finalized (which happens through checkpointing every ~32 blocks in an epoch, when >2/3 validators attest), the transactions in it (including $AF transactions) are extremely unlikely to ever revert. Finality on Ethereum is often achieved within 6–12 minutes (1–2 epochs). Additionally, Ethereum’s design post-Merge includes slashing for malicious validators and economic guarantees that make reverting finalized blocks practically infeasible without an attacker burning billions in value. For $AF users, this means after a short wait, their transactions (transfers or stake changes) are permanent and reliable on the ledger. Ethereum’s ledger, being one of the most valuable and secure, has proven robust

against attacks. Since the Merge, it has had no major security incidents and continues to be actively fortified by its community (e.g., discussing inclusion lists to resist censorship, etc.). This underpins $AF's reliability: the ledger itself is highly secure.

$AF Whitepaper: https://americanfortress.io/whitepaper

Public block explorer: https://etherscan.io/

$AF Main repository: Proprietary software.

H.2 Protocols and Technical Standards

Core token standard: ERC-20 on Ethereum. Public-key curve compatibility for address derivations/signaling spans both secp256k1 and Ed25519, enabling cross-ecosystem wallet computation of per-peer receive addresses. AFP remains backward-compatible with BIP-47 / OBPP-5 public paycodes, facilitating interoperability with legacy paycode schemes; privacy signaling employs the Noise Protocol to inject decoy signals and resist trivial metadata linkage.

H.3 Technology Used

AFP introduces FortressNames (human-readable identifiers), cryptographic public paycodes, and multimodal signaling (simultaneous off-chain and on-chain pathways) for resilient delivery and recovery of transaction history on wallet restore. Credentialed access permits optional, privacy-preserving KYC/AML proofs (blinded or unblinded) without centralized storage; proofs can be presented to authorized counterparties while keeping personal data off-chain and unlinkable to rotating receive addresses.

H.4 Consensus Mechanism

$AF relies on the consensus of its settlement layers: Ethereum mainnet (post-Merge Proof-of-Stake) for canonical issuance and Base (settling to Ethereum) for bridged balances. $AF does not operate an independent consensus layer; transaction finality and safety inherit from Ethereum/L2.

1. **Validator Staking and Block Proposal:** Ethereum's PoS relies on validators who have staked 32 ETH each to participate. At any given time, one validator is pseudo-randomly chosen as the **block proposer** for a 12-second slot. That validator proposes a block containing new transactions (including any $AF transactions pending in the mempool). Because Ethereum blocks often include many token transfers and contract calls, an $AF transfer or contract call is just one of many transactions that could be in the block. The proposer includes it and broadcasts the block.

2. **Attestation (Voting):** After a block is proposed, a committee of validators (randomly selected subset of all validators for that slot) **attests** (votes) on the block's validity and on the chain head they see (this vote also helps finalize the epoch checkpoints). These attestation votes are basically saying "we consider this block and all before it legitimate." If the $AF transaction is in this block, validators in effect are validating that transaction along with the rest. If something were invalid (like a double-spend attempt or contract rule violation), honest validators would refuse to attest and the block would be rejected. However, since $AF's rules are enforced by Ethereum's EVM, an invalid $AF transaction (say transferring more tokens than available) would never even be considered valid – it would fail EVM execution. Thus, by the time validators attest, they're mainly checking the block's signature and that they received the same block. Attestations are gathered and once a supermajority endorses the block, it becomes part of the chain.

3. **Epochs and Finality:** Ethereum groups 32 slots into an epoch (~6.4 minutes). At epoch boundaries, the protocol uses Casper FFG to finalize checkpoints. If >2/3 of validators (by stake weight) attested to the sequence of blocks up to a checkpoint, that checkpoint is **finalized**. Once finalized, it's immutable barring an exceptional attack. For $AF transactions, this means after an epoch or two, the transaction can be considered irreversible. In practice, $AF transfers are usually considered confirmed after one block for everyday use (which is probabilistic finality), but for absolute certainty

(like large value), one might wait ~12 minutes for finality. This is still vastly faster than Proof-of-Work confirmations for equivalent certainty.

4. **Liveness and Security:** Ethereum's PoS is designed to be secure as long as at least 2/3 of the stake is honest. In the event of an attempt to violate consensus rules (e.g., a malicious fork), the **slashing mechanism** punishes misbehaving validators by destroying some of their staked ETH. This deters attacks. For an $AF user, this means the consensus mechanism has strong economic incentives to continue processing transactions correctly and not revert them. The chance of a fork that changes $AF transactions after finality is astronomically low (would require >1/3 validators colluding and willing to lose billions in stake). This secure finality is a huge boon for $AF's use-case, because $AF often underpins value transfers – knowing the collateral is locked and won't be unwound is crucial for trust.

5. **No Mining, Energy Efficiency:** Under PoS, Ethereum has no mining. $AF transactions are confirmed without energy-intensive computations. Validators only perform relatively light cryptographic operations (signing messages, etc.), so the consensus is extremely energy-efficient (over 99.95% less energy than previous PoW). This means $AF usage doesn't carry the high environmental cost that earlier blockchain transactions did. There's no advantage in computing power; consensus weight comes from staked ETH. For $AF holders, this doesn't directly change how they use $AF, but it has peripheral benefits: lower network fees generally (because PoS allows Ethereum to target scalability upgrades), and more predictability (since block production is smoother without the randomness of PoW). It also aligns $AF with sustainability goals, which might improve acceptance among environmentally conscious enterprises and regulators.

6. **Consensus Governance:** Ethereum's consensus parameters (like block size, validators count, etc.) are determined by the Ethereum protocol and can be changed via network upgrades (with social consensus and offline coordination). $AF holders do not have a direct role in Ethereum's consensus (unless they themselves stake ETH or participate in Ethereum governance as community members). However, any major changes in Ethereum consensus (like sharding introduction or changes to validator rewards) are widely communicated and subject to community agreement. $AF, being simply an ERC-20, will continue to work seamlessly through such changes as long as Ethereum exists and supports smart contracts. For instance, when Ethereum transitions to **sharding**, $AF transactions might get processed in a shard and then finalized in the beacon chain, but that complexity is abstracted away – from $AF's perspective, it will still see a robust ledger.

Ethereum's **Proof-of-Stake (Casper/Gasper) consensus** ensures $AF transactions are securely ordered and finalized by a decentralized network of validators. Blocks with $AF transfers are produced (~ every 12s), and finality is reached typically within a few minutes. The consensus is **Byzantine Fault Tolerant** (can tolerate up to ~33% dishonest stake) and uses economic penalties (slashing) to discourage There is no mining competition; instead, consensus is achieved through weighted voting by stakers, making it efficient and stable. This mechanism underpins $AF's reliability
– $AF inherits Ethereum's very high uptime (Ethereum has historically extremely few outages) and irreversibility. In essence, $AF's trust model is the same as Ethereum's: trust in the protocol and economic incentives of validators.

(Technical reference: See Ethereum's official documentation on Proof-of-Stake finality, EIP-3675 for the Merge specs, and academic papers on Casper FFG and Gasper for detailed analysis of probabilities of finality and security margins. Those confirm the swift finality and security assumptions described.)

H.5 Incentive Mechanisms and Applicable Fees

At the protocol (utility) layer, $AF is consumed for reserving unique FortressNames and for incentivizing participants who operate off-chain signaling and data-availability infrastructure; tokenomics earmark a community/user-incentive allocation, with the model emphasizing genuine utility-driven locking over buybacks/burns. Users pay the native network gas fees of the settlement chain (e.g., ETH on Ethereum/Base) when transacting.

H.6 Use of Distributed Ledger Technology

False — $AF is issued and transferred on public blockchains (Ethereum / Base) not operated by the issuer or a third party on its behalf.

H.7 DLT Functionality Description

Not applicable

H.8 Audit

True

H.9 Audit Outcome

All Team Finance contracts are audited. Audit reports available at https://www.team.finance.

I. PART I – INFORMATION ON RISKS

I.1 Offer-Related Risks

I.1 Offer-Related Risks:

- Regulatory pathway risk (notification, not approval). White papers for “other crypto-assets” are notified to the Home NCA without ex-ante approval; if the notification pack is considered incomplete or marketing materials are inconsistent, publication/admission can be delayed or refused, which may affect timing and liquidity expectations (and would require supplementary disclosures once remedied).

- Admission and venue risk. Admission to trading on a CASP venue is subject to venue rules; there is no assurance of listing, continued listing, or of specific trading pairs or market-making depth; venue decisions (e.g., suspensions/delistings, maintenance, geographic restrictions) can materially affect price discovery, liquidity and secondary-market access.

- Distribution and onboarding risk. Subscription (primary) and trading (secondary) are conditioned on KYC/AML onboarding; jurisdictional/sanctions filters or failure to pass KYC can bar participation; retail 14-day withdrawal mechanics (where applicable) may alter settlement profiles and short-term float.

- Supply overhang and vesting risk. Post-TGE cliffs and linear unlocks for team/treasury/rounds can increase circulating supply and weigh on price if demand ramps more slowly than the unlocking schedule; even with rules-based programmatic behaviour, allocation releases remain a market-structure risk (see schedules).

- Tax and accounting uncertainty. Tax treatment of token subscriptions and subsequent disposals varies by jurisdiction and can change; adverse interpretations (e.g., VAT on certain services, withholding, or characterisation of token uses) may impact net proceeds and user behaviour.

- Marketing/communications risk. Any inconsistency between marketing, social media, or community communications and the notified white paper can trigger corrective actions or sanctions, including forced amendments and temporary halts.

I.2 Issuer-Related Risks

- Early-stage company risk and going-concern dependency. Execution relies on MatterFi’s ability to recruit, finance, and retain key personnel; macro or sector funding cycles may constrain delivery timeframes.

- Key-person and partner concentration. A limited management/engineering core and reliance on specific enterprise partners/exchanges increase operational concentration risk.

- Regulatory perimeter and multi-jurisdiction exposure. Operating an identity-enabled protocol and enterprise SDK invites heightened scrutiny across AML/KYC, privacy, and consumer-protection regimes; divergent interpretations across Member States and third-countries can raise compliance and cost burdens.

- IP and brand risk. Challenges to trademarks, patents, or open-source/licensing positions around send-to-name, public paycodes, and SDK components could delay integrations or require refactoring.

- Information-security and incident response. A material breach of infrastructure or compromise of credentials (including partner-hosted components) could impair availability and reputation.

I.3 Crypto-Assets-Related Risks

- **Lack of Intrinsic Value / Absence of Backing:** $AF is not backed by any tangible asset or legal obligation; its value is purely determined by supply and demand in the market. Unlike, say, an asset-referenced token which has reserves, or a share which has claim on company assets, $AF's worth comes from the expectation that others will use it as collateral or want it.

- **Self-Custody Risk:** If holders keep $AF in their own wallets, they face the risk of losing access (through lost private keys, mishandled seed phrases, etc.).This isn't unique to $AF but is a crypto-asset risk: losing one's private key means losing the $AF irreversibly. There's no recovery mechanism due to the decentralized nature.

- **Technical Bugs and Smart Contract Risk:** While $AF's contracts were audited, the possibility of an undiscovered vulnerability can't be zero. A bug in $AF's token contract seems very unlikely at this point (given its simplicity and time in market). However, a bug in collateral manager contracts or future upgrades could cause issues (e.g., someone exploiting the contract to withdraw more $AF than they should).

- **Taxation Risk:** Using or trading $AF can trigger taxable events under various jurisdictions' laws. For instance, in many countries, spending $AF (using it to pay for something or converting to fiat) may be a taxable disposal subject to capital gains tax on any appreciation. Receiving $AF as a reward for staking might be considered income and taxed accordingly at the time of receipt (and then again capital gains when sold, in some systems). VAT may apply.

- **Network Security Risks (Ethereum's security):** $AF relies on Ethereum's security assumptions. If Ethereum were compromised (via a 51% attack or critical consensus bug), $AF transactions and balances could be falsified or reverted. This is extremely unlikely given Ethereum's size and audits, but not impossible. The theoretical risk of a successful coordinated attack on Ethereum (maybe by a state actor or major exchange collusion) would have devastating effects: transactions could be censored or re-written, potentially causing double-spends or theft of $AF if the ledger is manipulated. However, practically finality and slashing make sustained attacks expensive.

- No redemption/peg or profit-share; market volatility. $AF confers utility only (locking for FortressNames and use of the signaling/credential layer) and offers no redemption right at par, no claim on reserves, no dividends; token prices can be highly volatile and may go to zero.

- Functional-demand dependency. Endogenous demand depends on locking for names and signaling usage; if user adoption or enterprise integrations lag, demand for $AF may be insufficient to absorb unlocks and circulating supply.

- Discretionary buyback/locking. Any buyback/locking is adoption-linked and rules-based, funded from protocol revenues (primarily name sales), and may not occur or may be paused/modified, providing no value-stabilisation.

- Concentration and liquidity. Holdings by treasury, team, or early rounds, even if vested/locked, can create perceived or real supply concentration; secondary-market liquidity may be thin around listing and during market stress.

  Many of these risks are inherent to all cryptocurrencies, not just $AF. $AF holders should fully understand the nature of the asset: it's a volatile, unbacked token in a nascent technology and regulatory space. They should evaluate their risk tolerance accordingly and possibly seek professional advice (technical or financial) if they are unsure about aspects like security or tax.

I.4 Project Implementation-Related Risks

- **Scalability and Throughput Limits**
  $AF relies on Ethereum, which could become a bottleneck during high transaction volumes, raising gas fees or slowing processing. This threatens the "instant" nature of payments. If collateral actions like staking/unstaking become too costly, user experience may degrade. The team is exploring off-chain solutions and L2s to handle scale, but seamless rollout remains challenging.

- **Competitive Innovation Risk**
  Crypto moves quickly, and $AF must adapt to evolving standards and innovations (e.g., cross-chain collateral or L2s). Falling behind in infrastructure choices or misjudging the market (e.g., shifting too early to a custom chain) could waste resources or limit adoption. Strategic missteps could prevent $AF from keeping pace with more agile or better-funded rivals.

- **Security Threats and Hacks:** Beyond smart contract bugs, risks include app-layer hacks or economic attacks (e.g., price manipulation on lending platforms). As integrations grow, the attack surface expands. A breach in bridging infrastructure or collateral systems could have serious consequences. Ongoing audits and conservative risk management are essential to prevent such threats.

- Partner and ecosystem adoption. The model presumes wallet/custodian/processors integrate the enterprise SDK; failure to convert pipeline partners, or partner off-boarding, delays network effects.

- Off/On-chain coordination and signaling. AF relies on multimodal signaling (off-chain, on-chain, in-line backup) and decoy noise; outages, spam/DoS on signaling endpoints, or UX regressions could degrade privacy/usability, slowing uptake.

- Credential provider dependencies. Optional blinded/unblinded KYC proofs require reputable attestations; changes in provider policies, false-positive rates, or regulatory demands may fragment experiences or raise costs.

- Competitive pressure. Alternative naming/identity and privacy approaches (including L1/L2 native schemes) may out-compete AF on distribution or wallet defaults, constraining protocol adoption.

I.5 Technology-Related Risks

- **Network Security and 51% Attack Risk (Ethereum):**Ethereum's proof-of-stake consensus is robust given an honest supermajority, but it's not invulnerable to theoretical attacks. For example, a well-funded adversary could attempt to accumulate a very large amount of ETH to influence or disrupt consensus (the worst-case scenario would be >66% stake to violate finality, or even >33% to stall finality). The cost would be extremely high (tens of billions of USD for 33%, much more for 66%), making it unlikely except for perhaps a state-level actor with a motive to sabotage Ethereum. If such an attack happened, $AF transactions could be censored or the ledger forked. While attackers get slashed if caught, a short-term attack might still cause chaos before being addressed. Another vector is a Sybil attack on consensus: Ethereum mitigates Sybil by requiring stake, but if someone got hold of, say, a large exchange's keys or multiple large validators, they could try to manipulate a fork. This is far-fetched but within "tail risk".

- **Software Bugs and Exploits:** Both Ethereum's protocol implementation and $AF's smart contracts could in theory harbor undiscovered bugs. Ethereum has multiple clients (e.g., Geth, Nethermind, Prysm, etc.), and while extensively tested, there have been occasional bugs.

- **Validator Centralization & Cloud Dependence:** A significant number of Ethereum validators and infrastructure providers run on cloud services (AWS, Google Cloud, etc.). If, hypothetically, one major cloud provider (like AWS) had an outage that affected a large portion of Ethereum nodes, the network could lose performance or blocks. This happened on smaller scales (some Infura outages, etc.).

- **RPC/Front-end Ecosystem Risks:** Many users interact with $AF through third-party services (wallets, block explorers). If those services (like Infura for wallets, or Etherscan for checking balances) have issues, users might incorrectly perceive $AF's network is down even if core consensus is fine. For instance, if Etherscan were to show erroneous data due to an API issue, some might panic. Or if a popular wallet had a bug showing a wrong balance, it could cause confusion.

- **Reputation and Ecosystem Risk:** This is intangible but important: if any technical mishap or association tarnishes $AF's reputation (like a hack, or being used in a notable fraud), it could reduce willingness of merchants or users to touch it. Even if fixed later, reputation damage can have lasting impact (some projects never fully recover community trust after big hacks).

- Base-layer and bridge risks. $AF is minted on Ethereum and bridged 1:1 to Base via the official bridge; Ethereum/L2 outages, consensus bugs, or bridge custody failures could cause loss, desynchronisation, or protracted withdrawal delays.

- Smart-contract and integration risk. Errors in token, registry, or SDK contracts—or unsafe third-party integrations—can enable theft, lockouts, or malfunction; while contracts are to be published ≥72 h pre-TGE, undiscovered defects may persist.

- Cryptography and privacy-model assumptions. AF's public paycode design (a hardened xpub), counterparty-unique addresses, and encrypted signaling seek to thwart address-graph linkage; nevertheless, implementation mistakes, key-material exposure, side-channel leaks, or novel analytics could reduce privacy in practice.

- Recovery and data-loss risk. Although the scheme supports history recovery on wallet restore, loss of user keys, corrupted backups, or signaling unavailability could impair reconstruction of past addresses and confuse counterparties.

- Parameter-governance risk. Adjustments to operational parameters (e.g., tokens-per-name) intended to keep the system in equilibrium can have unintended side-effects (e.g., pricing out segments, creating churn in reservations) if calibrated poorly.

I.6 Mitigation Measures

- Conservative issuance and custody posture. Ethereum mint, Base official bridge, and ≥72 h pre-TGE contract publication to permit community scrutiny and third-party audits; staged rollouts and change-controls around bridge/treasury keys.

- Privacy by design, not mixing. Counterparty-unique receive addresses derived from public paycodes plus encrypted, multimodal signaling with decoy noise provide privacy without operating a mixer, maintaining compatibility with chain analytics and reducing regulatory friction.

- Credentialed compliance. Optional blinded/unblinded KYC proofs integrated at the nym/name level enable compliant flows without public doxxing, avoiding centralised KYC stores and limiting breach blast-radius.

- Ecosystem governance and parameter tuning. Governance allows tokens-per-name and similar parameters to be tuned with partner input to preserve functional equilibrium as adoption scales (subject to transparent disclosures and change notices).

- Supply discipline and demand focus. Fixed, non-inflationary 10,000,000,000 supply, avoidance of cosmetic burns, and a rules-based, adoption-linked buyback/locking posture tie any treasury actions to real usage (primarily name-sale revenues), which reduces incentives for destabilising supply tinkering.

J. PART J - INFORMATION ON THE SUSTAINABILITY INDICATORS IN RELATION TO ADVERSE IMPACT ON THE CLIMATE AND OTHER ENVIRONMENT-RELATED ADVERSE IMPACTS

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

J.1 Mandatory information on principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism

$AF settles on Ethereum proof-of-stake (PoS) (and is bridgeable 1:1 to Base, which ultimately settles to Ethereum). Post-Merge, Ethereum's network power demand fell by ~99.9–99.99%, with annual electricity consumption in the single-digit GWh range rather than TWh; consequently, the consensus-layer carbon footprint is orders of magnitude lower than under proof-of-work. Estimates from the Cambridge Blockchain Network Sustainability Index (CBNSI) place Ethereum's annual electricity around ~6.5 GWh/year (point-in-time), and its annualized GHG emissions around ~2.8 ktCO_2e, with an energy mix that is ~32% renewables (and ~16% nuclear, i.e., ~48% "sustainable" incl. nuclear). These figures are network-level (not $AF-specific) because, under PoS, validator electricity is the dominant driver and is largely throughput-agnostic; per-transaction intensities are therefore derived metrics and should be interpreted with care.

Because $AF rides on Ethereum PoS, the principal environmental externalities are those of Ethereum's consensus layer (with any L2 overhead de-minimis relative to L1 settlement). Public references from Cambridge CCAF indicate single-digit GWh/year electricity and low single-kilotonne CO_2e emissions annually; the renewable share of validator energy is estimated around one-third, with a further ~one-sixth nuclear. Per-transaction intensities presented here are allocation metrics and not direct measurements of incremental energy, as PoS validator power draw is broadly independent of throughput.

General information	
S.1 Name *Name reported in field A.1*	MatterFi Inc.
S.2 Relevant legal entity identifier Identifier referred to in field A.2	**254900SCRP0O8UPILI97**
S.3 Name of the crypto-asset Name of the crypto-asset, as reported in field D.2	$AF
S.4 Consensus Mechanism The consensus mechanism, as reported in field H.4	Ethereum Proof-of-Stake (PoS) (canonical ledger); Base L2 used operationally but settles to Ethereum. PoS security is provided by validators that stake 32 ETH, propose/attest blocks, and are rewarded/penalized via protocol incentives (incl. EIP-1559 fee burn + tips; inactivity/slashing penalties).
S.5 Incentive Mechanisms and Applicable Fees Incentive mechanisms to secure transactions and any fees applicable, as reported in field H.5	Ethereum validators earn issuance + priority fees (tips); the base fee is burned under EIP-1559. Misbehavior or prolonged downtime can be slashed/penalized. Users pay gas in ETH; L2 usage (e.g., Base) ultimately incurs L1 data availability costs

S.6 Beginning of the period to which the disclosure relates	2024-01-01
S.7 End of the period to which the disclosure relates	2024-12-31
Mandatory key indicator on energy consumption	
S.8 Energy consumption Total amount of energy used for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions, expressed per calendar year	Total annual electricity used for validation and ledger integrity ~6,490,000 kWh per annum (≈ 6.49 GWh/a) — Ethereum network total (point-in-time annualization; CBNSI).
Sources and methodologies	
S.9 Energy consumption sources and Methodologies Sources and methodologies used in relation to the information reported in field S.8	Estimates based on Cambridge CBNSI: bottom-up node/validator telemetry, client requirements and measured hardware profiles, with continuous monitoring and annualization of observed power demand; methodology and daily updates documented by CCAF.

J.2 Supplementary information on principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism

Supplementary key indicators on energy and GHG emissions	
S.10 Renewable energy consumption Share of energy used generated from renewable sources, expressed as a percentage of the total amount of energy used per calendar year, for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions.	~32% (renewables share of Ethereum validator energy mix; ~48% sustainable incl. ~16% nuclear).
S.11 Energy intensity Average amount of energy used per validated transaction	~0.0105 kWh/tx (derived: 6.49 GWh/year ÷ ~1.7M tx/day ≈ 620M tx/year). Caveat: PoS energy is largely load-invariant; per-tx metrics are allocation artefacts.
S.12 Scope 1 DLT GHG emissions – Controlled Scope 1 GHG emissions per calendar year for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions	0.00 tCO_2e/a (no issuer-owned/controlled consensus facilities).
S.13 Scope 2 DLT GHG emissions – Purchased Scope 2 GHG emissions, expressed in tCO2e per calendar year for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions	~2,800 tCO_2e/a (network-level annualised emissions, CBNSI).
S.14 GHG intensity Average GHG emissions (scope 1 and scope 2) per validated transaction	~0.0045 $kgCO_2e/tx$ (≈ 4.5 g/tx) (derived: 2,800,000 kg ÷ ~620,000,000 tx).
Sources and methodologies	
S.15 Key energy sources and methodologies Sources and methodologies used in relation to the information reported in fields S.10 and S.11	Validator geographies and client/hardware assumptions from CBNSI; renewable share from CCAF's energy-mix estimate (renewables ~32%, nuclear ~16%); transaction counts from chain analytics (rolling average ~1.6–1.8M tx/day in 2025).
S.16 Key GHG sources and methodologies Sources and methodologies used in relation to the information reported in fields S.12, S.13 and S.14	CBNSI Ethereum GHG model: converts estimated validator electricity demand by geography and grid mix into annualised $ktCO_2e$; methodology published by CCAF (post-Merge PoS focus).