Metl

Litepaper

V 2.0 | January 2023

API with ZK Service and MPC Network integrating banking rails to smart contracts

Written by: Anna Vladi | technology@metl.co

Contents

Summary

Overview

Just like TCP/IP transformed the web into a global, accessible network capable of information transfer, Web3 will do the same for the internet of value. Our mission is to become the intermediary between legacy financial systems and cryptosassets, and onboard the next billion users to Web3.

METL consists of price-stable ERC20s, banking APIs with ZK service and secure multi-party computation (MPC) to provide a native and secure highway to connect banking rails to smart contracts on any VM.

— USDr tokens are multichain USD-backed receipts.
— USDr tokens are exchanged for any ERC20 offered on AMMs.
— Banking APIs are used to produce zero knowledge (zk) proofs to verify transaction settlements on-chain and off-chain.
— MPC node operators use on-chain and off-chain proofs to mint and burn USDr tokens.

In summary - METL offers an autonomous, independently operated tech stack that seamlessly integrates banking rails to smart contracts.

Current banking API problems

— Banking APIs presently only offer end points from one centralized entity to another without native exposure to smart contracts
— There is no native interoperability from USD to a VM, chain or a smart contract
— APIs are generally closed sourced and operate by selective disclosure

Use Cases

— Non-intermediated access to crypto for individuals and businesses
— Non-custodial exchange of fiat/crypto for MSBs, broker dealers
— Non-custodial exchange of fiat/crypto for existing cryptocurrency exchanges.
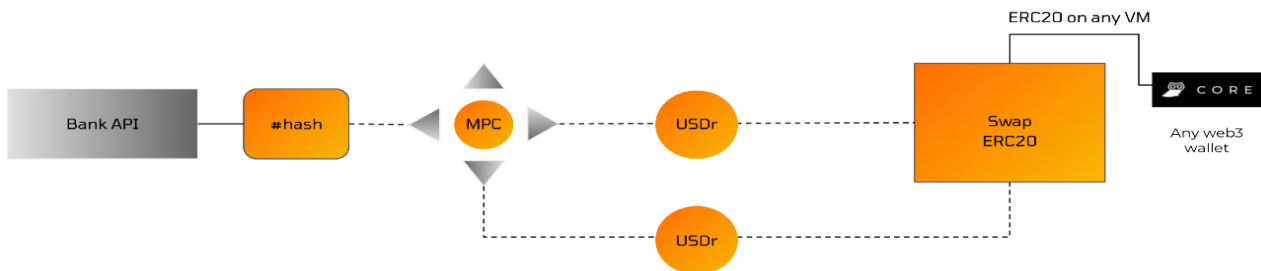— Direct staking into smart contracts from the user's bank account.

Technology

METL network consists of banking API, zk Service, AMM, MPC with node operators, a USD receipt token, and SDK.

# Architecture

Mint & Redeem

USDr

USDr is a smart contract that implements the ERC20 standard. It extends additional functionalities such as Access Control and zK proof verification - to allow authorized MPC node operators to mint and burn USDr tokens on behalf of users.

Mint

1. Users transfer funds to Metl using any supported banking network (eg. RTP, ACH).
2. Upon settlement, Metl's MPC system mints and swaps USDr tokens in exchange for an ERC20 of choice.
3. The exchanged tokens are then transferred to an EOA[4] and EVM, provided by the user.
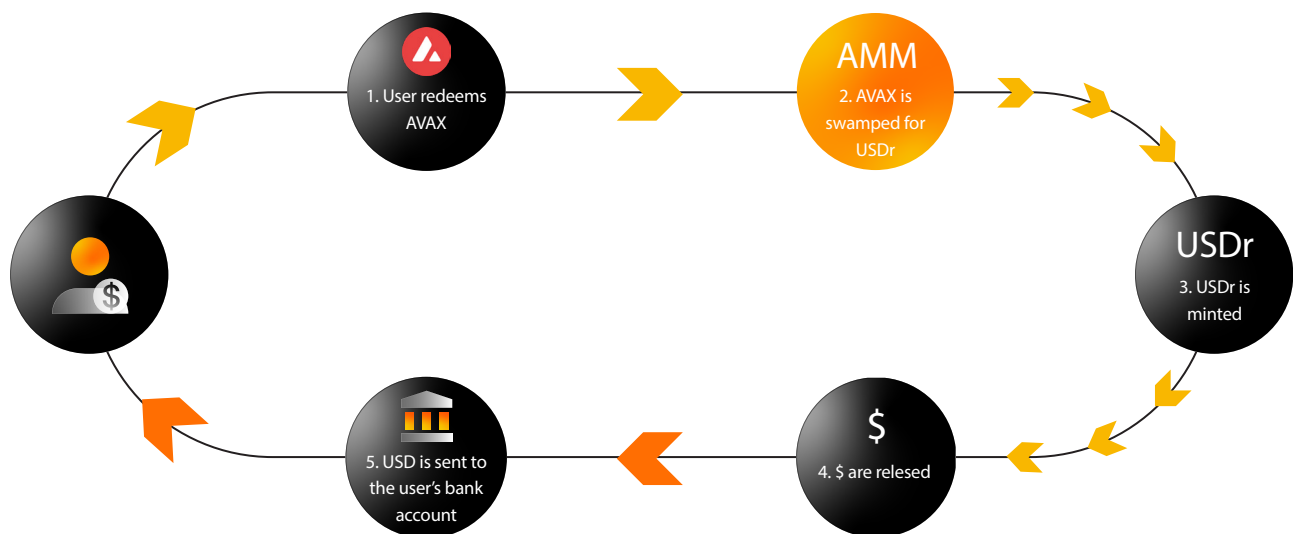
Lock & Mint
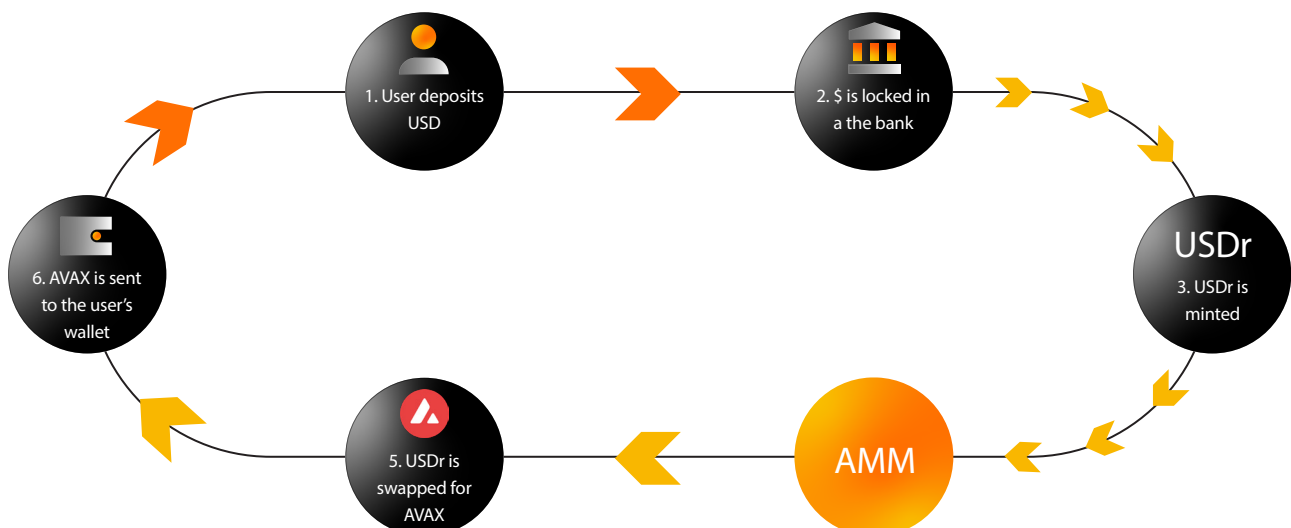
Burn

1. Users convert their ERC20 tokens to fiat by notifying the MPC system, providing a wallet, chainId and amount of the tokens to be redeemed.
2. MPC node operators freeze and independently verify the request.
3. If authorized, a given node operator will initiate a request to the banking API to transfer USD to the user's bank account.
4. USDr token is burned once ACH settles into user's originating bank account

Release & Burn

1. User redeems AVAX

AMM
2. AVAX is swamped for USDr

USDr
3. USDr is minted

$
4. $ are relesed

5. USD is sent to the user's bank account

Access Control

The USDr token contract implements a variation of Open Zeppelin's 'Access Control' - providing roles and rules to access permissioned functions in the USDr contract.[5]

AMM

Automated market makers (AMMs) allow ERC20 tokens to be traded in an autonomous and permissionless manner.[6] AMMs use pre-programmed mathematical equations to adjust prices based on supply in order to make sure the ratio of assets in any liquidity pool remains balanced.

METL may leverage externally operated AMMs such as Trader Joe in the case of Avalanche, and Aave in the case of ZKSync to swap USDr tokens in exchange for the ERC20 asset requested by the user (onramp) and vice versa, to swap a given ERC20 for USDr tokens (offramp).

[5] https://github.com/OpenZeppelin/openzeppelin-contracts-upgradeable/blob/master/contracts/access/AccessControlEnumerableUpgradeable.sol
[6] https://uniswap.org/whitepaper-v3.pdf

Banking APIs

Banking APIs provide status of the banking transactions on the banking ledger. Settled banking transactions provide inputs into zk proof:

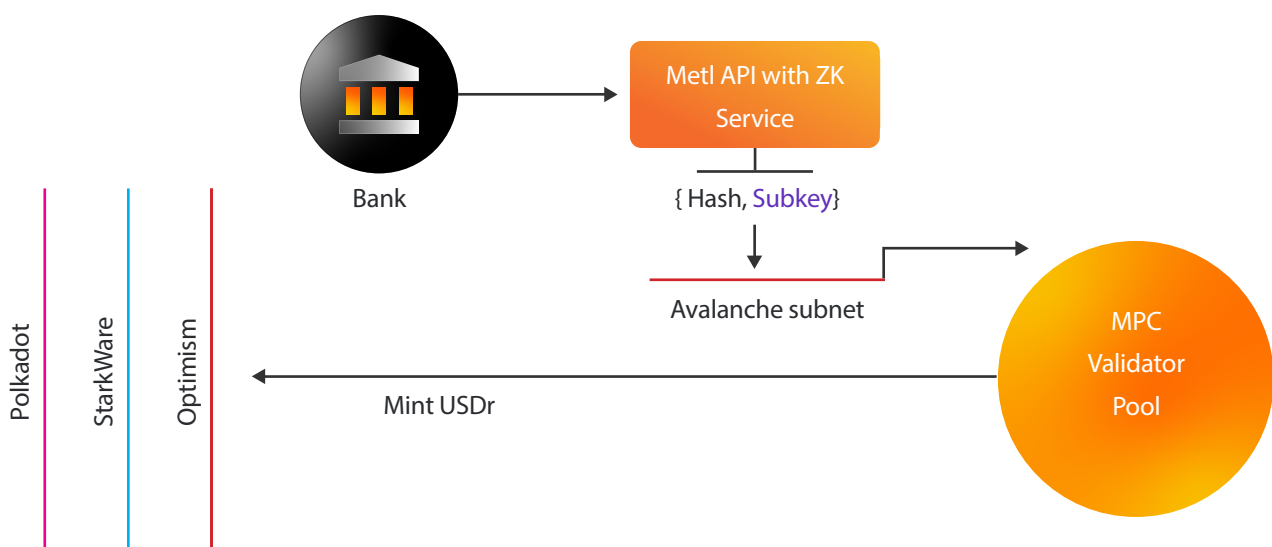RequestDate | MintRequest | Bank_id | User_name | Account_id | Routing_id | Amount | Currency

zK Service

Poseidon[7] hash function is planned to be used for encrypting banking data on chain. It is designed to minimize prover and verifier time on proof generation and size of the proof when zero-knowledge proofs are generated and validated. For privacy and security reasons as well as computational intensity, this data maybe be stored using outsourced verifiable computation such as oracles or on a private side chain such as Avalanche's subnet[8].

MPC

The tokenized representation model[9] is used by METL to provide universal interoperability. An all-encompassing level of interoperability between banking systems and EVMs is made possible by METL's MPC network. METL is able to instantiate a decentralized, permission-less, and trust-less custodian capable of locking assets on banking networks and processing one-to-one pegged representations of them on other VMs by combining consensus with secure multi-party computation (MPC) methods. Users can interact with numerous programs, assets, and chains in this fashion using just one transaction.

zkMPC Construct

[7] https://eprint.iacr.org/2019/458.pdf

[8] https://docs.avax.network/subnets

[9] https://cointelegraph.com/nonfungible-tokens-for-beginners/asset-tokenization-a-beginners-guide-to-converting-real-assets-into-digital-assets

Economics

Metl's MPC network is underpinned by a staking implementation, to incentivize and sustain reliable service provision of the METL network, including the regular distribution of a subsidy to active MPC service-providers.

This subsidy is generated through the scheduled expansion of the native token's circulating supply, following a 'two-phase' model where subsidies are ultimately supported by protocol fees only. The "two-phase" approach has been designed to maximize operational efficiency at the start (cold start problem) and to secure long-term network decentralization.

Details pertaining rules for stake management, including locking, splitting, extending, and withdrawing stakes will be provided in a separate 'Economics Paper', where the impact of individual staking configurations on global supply dynamics is analyzed.

At the time of writing, our team is considering the use of a separate staking model to provide protocol performance exposure to non-node operators. Specifically the use of a voting escrow (ve) contract, where stakes are used to allocate protocol emissions and fees.

Legal & Licenses

Given the state of our regulatory framework, Metl's banking partners have provided approval that we can operate in all US states except NY.

Patent for the tech stack was issued by USPTO in August 2021. We are currently filing a continuation application to allow the pursuit of additional claims.

Glossary

chainID- ID as it relates to each EVM chain where USDr is deployed.

MPC- multi-party computation is a subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private.

Zero-knowledge - is a concept from cryptography, an interactive method for one party to prove to another that a (usually mathematical) statement is true without revealing anything other than the veracity of the statement.

AMM- Automated Market Maker platform to swap ERC20 tokens.

USDr- USD receipt token that is an ERC20 standard with a short life span that can exist on any EVM, can be swampt for any ERC20 in an AMM and be managed by MPC.