The Gemini Dollar: A Regulated Stable Value Coin

Gemini Trust Company, LLC
dollar@gemini.com

Abstract. The Gemini dollar is a cryptographic token that is (i) issued by a New York trust company, (ii) strictly pegged 1:1 to the U.S. dollar, and (iii) built on the Ethereum network [1] according to the ERC20 standard for tokens. The Gemini dollar is a stable value coin that combines the creditworthiness and price stability of the U.S. dollar with the technological advantages of a cryptocurrency and the oversight of U.S. regulators. As an ERC20 compliant token, the Gemini dollar can be transferred on the Ethereum network. Gemini dollars are created at the time of withdrawal from the Gemini platform and redeemed or "destroyed" at the time of deposit into the Gemini platform.

1. Introduction

Cryptocurrencies have recently surged in popularity and investor interest. While they bear a promise perhaps as profound as the Internet itself, they suffer from substantial price volatility, thereby hindering their use as a medium of exchange and unit of account (two of the three functions of money). One proposed solution is the creation of a stable value coin (often called a "stablecoin"), whereby an issuer distributes a cryptographic token to customers in exchange for a specified fiat currency, like the U.S. dollar, at a fixed 1:1 exchange rate. Because the U.S. dollar is a highly desirable medium of exchange, as well as a globally accepted unit of account, it is a desirable peg for a stablecoin.

Several implementations of fiat-pegged stablecoins have been proposed, however, they all lack some combination of *supervision*, *transparency*, and *examination* [3]. As a result, doubts surrounding their solvency persist, as do concerns regarding the systemic risks they pose [4].

What is needed is a stablecoin that people can trust. In this paper, we propose the Gemini dollar, a *regulated* stablecoin that combines the creditworthiness and price stability of the U.S. dollar with the technological advantages of a cryptocurrency and the oversight of U.S. regulators.

2. Trust

Building a viable stablecoin is as much of a *trust* problem as it is a computer science one. While Bitcoin [4] created a system based on cryptographic proof instead of trust, a fiat-pegged stablecoin requires both due to its reliance on a centralized issuer.

Desirable outcomes in a system that relies (at least in part) on trust requires *oversight*. In the context of a stablecoin, we submit that the issuer must be licensed and subject to regulatory supervision. From this, transparency and examination become requirements of the system, ensuring its integrity and

engendering market confidence. We propose Gemini Trust Company, LLC (Gemini), a New York trust company, as the issuer of the Gemini dollar. Gemini operates under the direct supervision and regulatory authority of the New York State Department of Financial Services and is subject to the New York Banking Law and other applicable U.S. laws and regulations. Gemini maintains the necessary licenses and registrations to lawfully issue Gemini dollars.

3. Proof-of-Solvency

One desirable outcome of a stablecoin is convergence between the tokens issued and the U.S. dollars exchanged for their creation. The amount of tokens issued and in circulation can be observed on the blockchain, however, verifying the underlying U.S. dollar balance to demonstrate *proof-of-solvency* requires examination by a trusted party. For assurance, we propose that the audit committee of the board of directors of Gemini engage an independent registered public accounting firm to regularly examine and attest to the underlying U.S. dollar balance in accordance with the attestation standards established by the American Institute of Certified Public Accountants.

4. Creation, Redemption, and Transfer

A simple and elegant mechanism for creation and redemption is necessary to promote useability and encourage adoption. We achieve this by allowing Gemini customers to create and redeem Gemini dollars on the Gemini platform.

Gemini dollars are created at the time of withdrawal from the Gemini platform. Gemini customers may exchange U.S. dollars for Gemini dollars at a 1:1 exchange rate by initiating a withdrawal of Gemini dollars from their Gemini account to any Ethereum address they specify. The U.S. dollar amount of Gemini dollars is debited from a customer's Gemini account balance at the time of withdrawal.

Gemini dollars are redeemed or "destroyed" at the time of deposit into the Gemini platform. Gemini customers may exchange Gemini dollars for U.S. dollars at a 1:1 exchange rate by depositing Gemini dollars into their Gemini account. The U.S. dollar amount of Gemini dollars is credited to a customer's Gemini account balance at the time of deposit.

The Gemini dollar can be transferred on the Ethereum network.

5. Contract Specification

The specifications of the Gemini dollar require a network that allows for the development of decentralized applications (including smart contracts) that may be used to store and transfer value according to certain conditions set by the developer. The Ethereum network fulfills this criteria and has a technical standard for tokens, the 'ERC20' standard [4], which has experienced widespread, global adoption. As a result, there already exists a plethora of software and services that support ERC20 compliant tokens and provide access to and usability for end users (cf., Tether as originally built on Omni Layer, a protocol built on top of the Bitcoin blockchain [5]). Alternatively, if the Gemini dollar were built as the native token of its own blockchain, it would take time for a similarly vibrant ecosystem of third-party developers and software to emerge. As a result, we have built the Gemini dollar as an ERC20 compliant token on the Ethereum

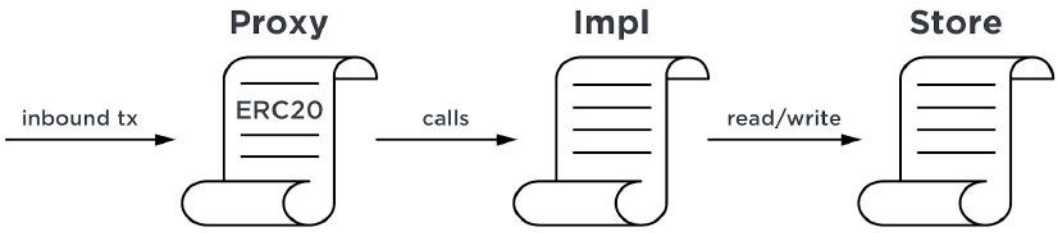
network. Consequently, the Gemini dollar can be transferred on the Ethereum network and stored in any Ethereum address.

6. Contract Separation

As a regulated issuer, we need a technical design and implementation that gives us the ability to upgrade the Gemini dollar token so we can:

1) Resolve vulnerabilities;
2) Extend the system with new features;
3) Improve the system and optimize its operational efficiency; and
4) Pause, block, or reverse token transfers in response to a security incident (i.e., catastrophic event) or if legally obligated or compelled to do so by a court of law or other governmental body.

We enable upgrades (the mechanism for which we describe in more detail below) by building a system of smart contracts that cooperate with each other. The core components of the Gemini dollar system are three smart contracts that we refer to as *'Proxy,' 'Impl,'* and *'Store.'* The smart contract known as 'Proxy' is the public face of the Gemini dollar — it is the Gemini dollar's permanent address on the Ethereum blockchain. There is, and will only ever be, one instance of 'Proxy.' It provides the interface with which token holders can interact and perform operations such as transferring tokens and viewing token balances; however, 'Proxy' contains neither the code nor the data that comprises the behavior and state of the Gemini dollar. Instead, 'Proxy' delegates the right to execute the logic that governs token transfers, issuance, and other core features to the smart contract known as 'Impl.' In turn, 'Impl' does not directly control the data that constitutes the ledger of the Gemini dollar (i.e., the mapping of token holders to their balances); instead, it delegates ownership of the ledger to the smart contract known as 'Store' — the external and eternal Gemini dollar ledger.

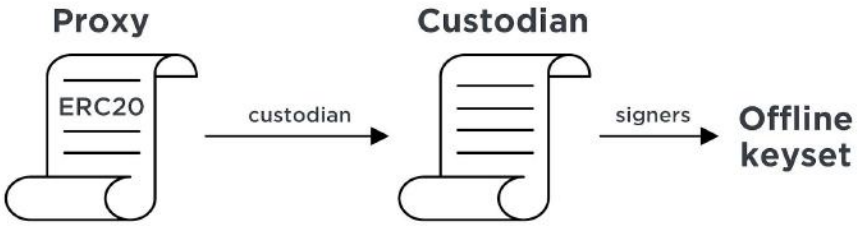


7. Contract Custodianship

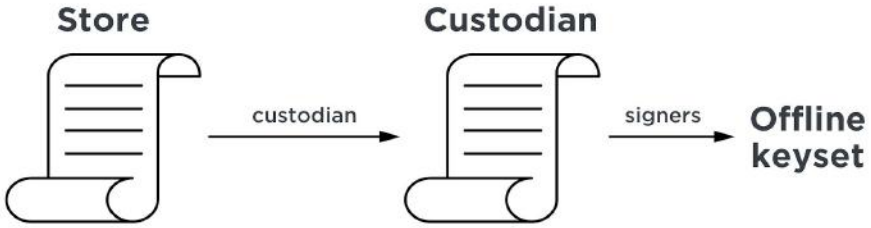
For certain high-risk actions in the Gemini dollar system, we need an offline approval mechanism. We, therefore, require each smart contract in the Gemini dollar system to look to a custodian for approval. A custodian may be another smart contract or a keyset (online or offline). A custodian may look to another custodian, which may look to another custodian, and so forth, thereby creating a chain of custody or "custodianship." For instance, a smart contract may look to another smart contract, which ultimately looks

to a keyset for approval. If a smart contract's custodianship terminates to an offline keyset, an offline approval mechanism for its actions has been created.

For example, 'Proxy' looks to a smart contract called *'Custodian,'* which ultimately looks to an offline keyset for approval.

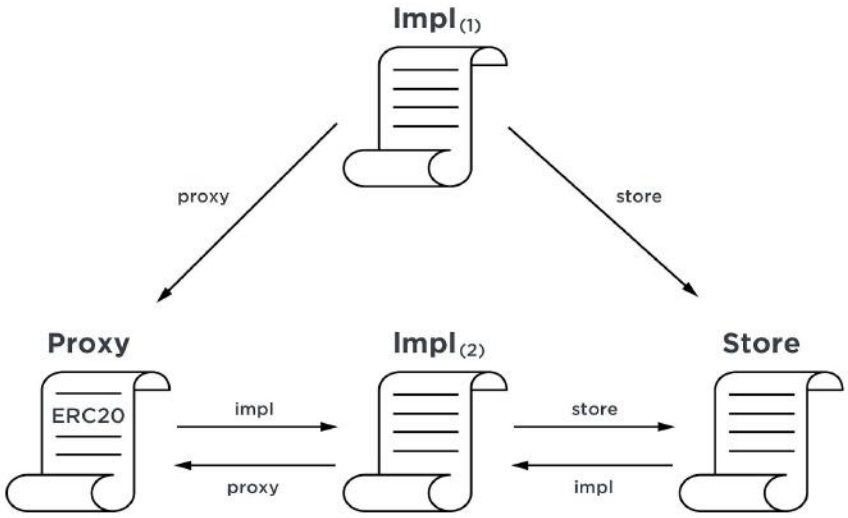


Likewise, 'Store' looks to 'Custodian,' which ultimately looks to an offline keyset for approval.



8. Contract Upgrades

Upgrading the Gemini dollar token is a high-risk action that utilizes the Gemini dollar system's offline approval mechanism. To do this, we replace the current instance of 'Impl' by instructing 'Proxy' (via 'Custodian') to delegate active token implementation to a new instance of 'Impl,' and instructing 'Store' (via 'Custodian') to treat this new instance of 'Impl' as its single trusted source when accepting updates to the Gemini dollar ledger.

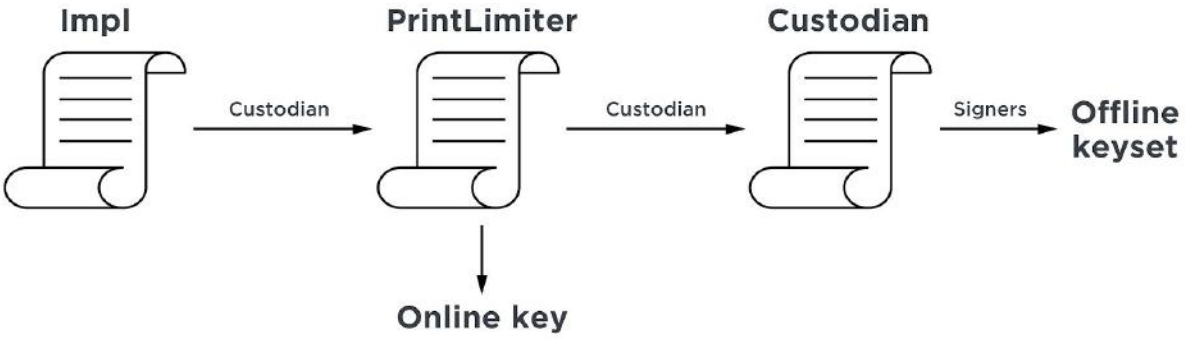


The above diagram reflects a post-upgrade state of the world, whereby the previous instance of ‘Impl’(1) has been replaced by a new instance of ‘Impl’(2). The instance of ‘Proxy’ now delegates to ‘Impl’(2). Similarly, the instance of ‘Store’ now only accepts calls from ‘Impl’(2). The previous instance of ‘Impl’ remains, but has become inert because it is now unlinked from the system.

Taken together, the custodianship of ‘Proxy’ and ‘Store’ makes Gemini dollar system upgrades possible. In addition, custodianship itself can be upgraded. For example, if we need to change our offline keyset, we can instruct ‘Custodian’ to instruct ‘Proxy’ to look to a new instance of ‘Custodian’ that looks to a new offline keyset.

9. Printing Tokens

Printing tokens is a high-risk action — the amount of Gemini dollars issued and in circulation must never exceed the underlying U.S. dollar balance. We need a solution that provides the security of an offline approval mechanism yet the flexibility of an online approval mechanism. We propose a hybrid solution whereby the custodianship of ‘Impl,’ the smart contract that controls increases to supply of Gemini dollar tokens, involves both an online and offline approval mechanism. To implement this unique approach, we insert a smart contract called *‘PrintLimiter’* into the ‘Impl’ chain of custody.



With the approval of an *online* key, 'Impl' may print Gemini dollars up to an amount or "limit" as specified by 'PrintLimiter.' This limit may be increased with approval of an *offline* keyset (or decreased with approval of an *online* key). This solution gives the Gemini dollar system the desired level of security and flexibility with respect to token issuance.

10. Contract Security

The Gemini dollar system implements the following security features:

1) Offline Keys: Keys that approve high-risk actions are stored offline in Gemini's proprietary Cold Storage System.
2) Key Generation: Keys are generated, stored, and managed onboard hardware security modules (HSMs). We only use HSMs, each a "signer," that have achieved a rating of FIPS PUB 140-2 Level 3 or higher [7].
3) Dual Control (Multisignature): High-risk actions require approval (i.e., digital signatures) from at least two signers. We utilize an *M* of *N* signing design, whereby *M=2.* This provides both security and fault tolerance.
4) Time Lock: Even after approval, high-risk actions are locked for a minimum period of time before being executed. This provides a grace period to detect — and preemptively respond to — potential security incidents.
5) Revocation: Pending actions can be revoked, allowing for the nullification of erroneous or malicious actions before being executed.

11. Conclusion

We have proposed a solution for a stablecoin that establishes trust through cryptographic proof and regulatory oversight. Our technical design is implemented on the Ethereum network. It includes an upgrade feature, an offline approval mechanism for high-risk actions, and a hybrid online-offline approval mechanism for token issuance that provides the desired level of security and flexibility. Our trust implementation involves linking licensed financial institutions and examiners to form a network of trust. Together, these implementations form the Gemini dollar, a regulated stablecoin that can serve as a viable medium of exchange and unit of account for centralized and decentralized applications.

References

[1] V. Buterin et al., "A next-generation smart contract and decentralized application platform," https://github.com/ethereum/wiki/wiki/White-Paper, 2014.

[2] M. Hochstein, "Tether Confirms Its Relationship With Auditor Has 'Dissolved'," In *CoinDesk*, www.coindesk.com/tether-confirms-relationship-auditor-dissolved/, January 2018.

[3] N. Popper, “Warning signs about another giant bitcoin exchange,” In *New York Times*, https://www.nytimes.com/2017/11/21/technology/bitcoin-bitfinex-tether.html, November 2017.

[4] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” https://bitcoin.org/bitcoin.pdf, 2008.

[5] Ethereum Wiki, “ERC20 Token Standard,” https://theethereum.wiki/w/index.php/ERC20_Token_Standard.

[6] Tether. Tether: Fiat currencies on the Bitcoin blockchain. https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf.

[7] National Institute for Standards and Technology, “Digital Signature Standard (DSS),” In *Federal Information Processing Standards Publication 186-4*, https://csrc.nist.gov/publications/detail/fips/186/4/final, July 2013.