

WHITE PAPER

The Constant System

A more useful money

v1.0, Jan 1, 2019

written by Duy Huynh, Ning Tan, Daniel Nguyen, Gaël Vo, An Nguyen
on behalf of the entire Constant team

The latest version is available at <https://constant.money/whitepaper.pdf>

CONTENTS

Introduction	9
Stable unit of account	10
Reliable store of value	10
Efficient medium of exchange	10
Related work in economics	10
The freedom of money	10
The early years of central banking	11
A systematic and transparent monetary policy	11
A good normal anchor	12
Related work in cryptocurrency	12
Fiat collateralized	12
Crypto collateralized	13
Algorithmic	13
No silver bullet	14
Overview of the tokens	16
Utility Token: The Constant Stablecoin (CONST)	16
100% backed	16
1:1 pegged to the US dollar	16
Mining policy	17
Burning policy	17
Monetary supply policy	17
Units	17
Implementation	17
Governance Token: The Monetary Policy Token (MPT)	19
A Decentralized Autonomous Organization	20
MPT relationships	20
MPT holders	21
Responsibilities	21
Incentives	21
MPT governors	22
Responsibilities	22
Incentives	22
Mining policy	23
Burning policy	24
Monetary supply policy	24

Units	24
Implementation	24
Infrastructure Token: Ether (ETH)	27
Collateral Tokens: Trust Vault Assets	28
Overview of the Constant System	30
A hybrid approach	30
The Constant System: 3 key entities and 5 key functions	30
Business Model	31
Entity: The Constant Foundation	32
Purpose	32
Constant roadmap	32
2019 Application roadmap	32
2019 Market roadmap	33
Key members	34
Duy Huynh, Monetary Policy	34
Professor Thuc Nguyen, Applied Cryptography	35
Professor Dung Tran, Consensus & Scalability	35
Gaël Vo, Product Manager	36
Bao Le, Infrastructure	36
Bill Pelletier, E-Commerce	37
Ning Tan, Community, South East Asia	37
Justin Lucas, Community, South America	38
Key advisors	38
Entity: The Trust Vault	41
Purpose	41
Assets	41
Examination	41
Direct banking	41
Implementation	42
Entity: The Decentralized Payment Network	42
Purpose	42
Distributed ledger technology	43
Implementation	44
Function: Conducting monetary policy	44
1:1 pegged to the US dollar	44
Fees	44

Function: Managing the Trust Vault	47
Minting new Constant	48
Burning	49
Funds guarantee	49
Function: Handling payments and settlements safely and efficiently	49
Addresses and keys	50
Transactions	50
State transition system	51
Blocks	51
Function: Promoting adoption of Constant in everyday life	52
For personal	53
Fast international payments	53
Security and complete control over your money	53
Zero to low fees	53
Mobile payments made easy	54
Works everywhere, any time	54
For business	54
Protection against fraud	54
Fast international payments	54
Zero to low fees	54
Multi-signature	54
Online payments	55
Offline payments	55
For traders	55
Hedging	55
An alternative to traditional currency deposit	55
For developers	55
Be your own bank. Be your own payment gateway.	55
Simple yet powerful programming model	55
Integrate into your existing web sites or apps	56
Function: Create UI/UX guidelines for decentralized applications built with Constant	56
Vocabulary	56
Performance	56
Web	57
Mobile	59
Open source & code architecture	60

Conclusion	61
References	63

GLOSSARY

The Constant System

A new global financial infrastructure.

The Constant Foundation

The founding team of the Constant System.

Constant

A new international stable currency, 100% backed by the US dollar. Implemented as a burnable, mintable Ethereum ERC-20 token.

Trust Vault

A set of escrow accounts backing the issuance of Constant, routinely audited by a registered public accounting firm and managed by an independent trust company.

Ethereum

A decentralized application and smart contract platform.

ABSTRACT

The Constant System is a decentralized global financial infrastructure that enables a new set of financial applications for consumers and businesses. At the heart of the Constant System, there is a decentralized, borderless, stable currency, called Constant.

Constant is a cryptocurrency with 3 defining, differentiating characteristics that make it the ideal stablecoin. It is (1) a stable unit of account, (2) a secure store of value and (3) an efficient medium of exchange.

Constant is not minted out of thin air; it is always backed by valuable assets. The first release of Constant is backed by the US dollar only, combining the creditworthiness and price stability of the US Dollar with the technological advantages of decentralized ledger technology (blockchain technology). By maintaining a strict 1:1 peg, Constant is 100% backed by its equivalent in USD, held in a fully audited Trust Vault, managed by an independent Trust Company.

In subsequent releases, Constant will be backed by a broad variety of assets, including fiats like the US dollar and Euro, cryptocurrencies like Bitcoin and Ethereum, or tokenized assets like real estate and gold.

Different from other cryptocurrencies, Constant is designed for useability and real world practicality. Constant is an upgraded money, a practical alternative that bypasses the limitations of fiat currency, built to integrate seamlessly into daily use. In this white paper, we outline the Constant System and its monetary policy, and also describe the first of many practical use cases and applications of Constant.

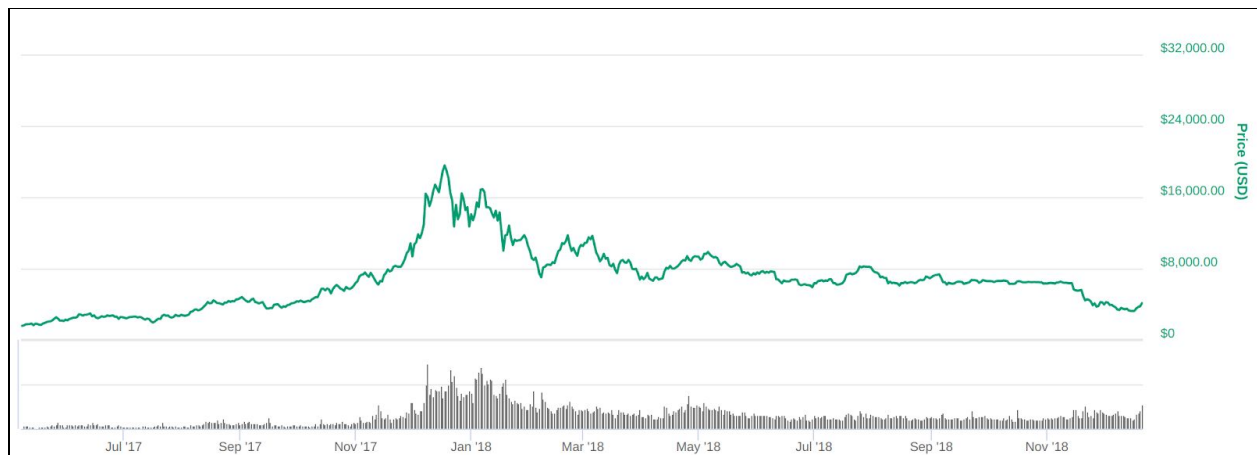
PART I

STABLECOIN OVERVIEW

1. Introduction

The total addressable market of money is about [90 trillion dollars](#). From its first use in the Tang Dynasty (A.D. 618-907), we've had more than a thousand years of practice holding and using paper currency. Its limitations are keenly felt, now more than ever. With the advent of cryptocurrency - borderless, frictionless, and decentralized - the world is beginning to think more broadly about how money should, and can, behave.

Bitcoin is a powerful cryptocurrency that fails to be the everyday money. Due to its volatility, you wouldn't use Bitcoin, or any coin, to buy a cup of coffee or shop online. No one would accept salaries or invoices in Bitcoin, so businesses don't. As for financial services - offering a loan or taking a deposit in an unstable coin is a gamble that few will take. As money, Bitcoin is unusable.



Bitcoin fluctuated between \$3,000 and \$20,000 from July 2017 to Nov 2018

The stability of Constant enables these use cases at scale. Like Bitcoin, it is a decentralized cryptocurrency; nobody owns or controls the Constant System. Unlike Bitcoin, however, Constant is stable, so you can spend it on everyday things. People all around the world continue to choose the US dollar for the benefits of price stability and creditworthiness, but especially in emerging markets, it nervously sits under mattresses or in precarious bank accounts. Constant is a digital upgrade of the US dollar that retains the benefits of the world reserve currency, in addition to total freedom.

Constant is a cryptocurrency that embodies the three integral characteristics of usable money: stable unit of account, efficient medium of exchange and secure store of value.

Stable unit of account

At its very core, Constant is built to maintain a 1:1 peg to the US dollar. The value of goods and services are easily measured in terms of Constant, which holds its value as the USD does, and is additionally designed to be easily converted at any time.

Reliable store of value

As far as savings go, Constant provides a viable refuge for multiple volatile economies. It affords the price stability of the USD with the accessibility of a borderless digital currency. Unlike many other digital currencies however, Constant straddles both worlds, and easily converts back to fiat. Each Constant is backed by 1 US dollar, held in a Trust Vault with a strict 100% collateralization.

Efficient medium of exchange

In addition to price stability and the practicalities that affords in any exchange of goods and services, Constant also reduces the friction, distance, expense and inefficiency of every transaction, made by anyone - to anyone - anywhere in the world.

2. Related work in economics

Constant is extensively influenced by both prior and current literature of monetary economics. There has been a lot of work discussing the practicalities of feasibility of a stable currency (Jevons 1875, Marshall 1877, Wicksell 1898, Fisher 1913, Hayek 1978, Bordo 1984, Black 1987, Cagan 1987, Dorn 1987, Patinkin 1993, Dorn 2017).

The freedom of money

The Constant System is designed to unshackle money. Constant currency holders control the System, independent of any governing body. The concept of monies free from governmental control was first proposed in “The Denationalization of Money” (Hayek 1976). Hayek proposed that market forces should dictate the issuance of money, not static government policy. At the time, it was an arresting but impractical idea. 42 years later however, technological leaps have given us the perfect infrastructure to bring Hayek’s idea to fruition - a government-independent blockchain, like Bitcoin and Constant, with its own native currency.

The early years of central banking

Constant offers efficiency gains, cost reductions and financial empowerment, simply by replacing middlemen banks with peer to peer technology. In the early years of central banking, individuals and businesses held accounts with the Bank of England and the Sveriges Riksbank. It was not practical during this era of paper bookkeeping to manually maintain a large number of private accounts. As the number grew, the system buckled and had to be discontinued. So people started to open accounts at separate commercial banks, which leads us to today: trillions of dollars trickle sluggishly within arbitrary geographical boundaries, waiting for multiple middlemen to take their cut before reaching their intended destination - sometimes more than a week later.

With distributed ledger technology, it is fairly simple for anyone to open an account on the blockchain and instantly send money across the world, bypassing commercial banks, antiquated payment structures, markups and inflated fees. The bookkeeping process has come a long way since paper, upgraded with military-grade cryptography and consensus algorithms. Transactions, balances and records are now transparent, verifiable and accessible from anywhere in the world. Money on the blockchain makes the world go round faster.

A systematic and transparent monetary policy

Monetary economists have reached a consensus that the conduct of monetary policy should be systematic and transparent.

“The Committee seeks to explain its monetary policy decisions to the public as clearly as possible. Such clarity facilitates well-informed decision-making by households and businesses, reduces economic and financial uncertainty, increases the effectiveness of monetary policy, and enhances transparency and accountability,”

The Federal Open Market Committee (2012)

The Constant System is systematic; everything runs exactly as programmed via smart contracts, without any possibility of downtime, censorship, fraud or third-party interference. The Constant System is transparent: it is open-source; its design is public, nobody owns or controls the Constant System and anyone can own part of it.

A good normal anchor

Almost all central banks have chosen **inflation targeting** as their nominal anchor. However, these inflation targets are not objectively or reliably fixed at specific values. The target can be warped by a whole host of external factors such as desired election outcomes, undermining the credibility of the central bank's nominal anchor.

Replacing inflation targeting with **price-level targeting** has been proposed by various economists. Price-level target is a specific numerical objective; that is, it is a natural focal point for household and business expectation, and serves as a credible nominal anchor.

By design, Constant is 100% backed. For the first release, Constant is backed by the US dollar, the world reserve currency. As the system develops over time, Constant will be backed by a broad variety of assets, including fiats like the US dollar and Euro, cryptocurrencies like Bitcoin and Ethereum, or tokenized assets like real estate and gold. The price-level target could be specified in terms of a **crypto asset index**, constructed from the publicly listed prices of crypto assets on various exchanges, fed by oracles. This method facilitates full transparency, and can be reproduced and verified by anyone, at any time.

3. Related work in cryptocurrency

There are 3 existing approaches to creating price stability for cryptocurrency: fiat collateralized, crypto collateralized, zero collateralized. The first release of Constant will be fiat collateralized, chosen for its unwavering stability.

Fiat collateralized

Fiat-collateralized stablecoins work like this: Alice sends 100 USD as collateral to Stablecoin Company and receives 100 stablecoin in return. This solution is simple for consumers to understand and easy for Stablecoin Company to build and execute. In terms of price stability, it's absolutely 100% stable.

Companies: [Tether](#) (USDT), [TrueUSD](#) (TUSD)

Crypto collateralized

A crypto-collateralized stablecoin works similarly to fiat-collateralized, but instead of using fiats, it uses other cryptocurrencies as collaterals. The problem is that cryptocurrencies are volatile. A crypto-collateralized stablecoin solves this by over-collateralizing.

For example: Alice sends 1 ETH (about \$100 value as of December 21, 2018) as collateral to Stablecoin Company and receives 50 stablecoins (about \$50 value) in return.

This comes with some limitations. First, it cannot be as stable as a fiat collateralized stable coin. Second, what if the value of the collateral, ETH, goes below \$50? Third, it's a very inefficient use of capital. Why would you want to lock up 1 ETH and only get out half of its value?

Companies: [MakerDAO](#) (DAI)

Algorithmic

This system was first proposed by Robert Sams as [Seigniorage Shares](#). The idea was to build an algorithmic central bank which issues and maintains the coin value at \$1. This would mimic and replace the real world central banks responsible for the monetary policies of a nation (e.g. Bank of England) or a group of nations (e.g. European Central Bank).

Assume the coin value is \$1.20 on the market due to fluctuating demand. The algorithm issues more coins until its value goes down to \$1.00, based on [Quantity Theory of Money](#). The newly minted coins are then auctioned on the open market, bringing in some extra profits, called **seigniorage profits**.

What if the coin value falls below \$1, say \$0.5? The algorithm cannot just recall the coins to reduce supply. A solution, as proposed by Robert Sams, is to issue **seigniorage shares** that people can buy. When new coins are minted, seigniorage profits will be split among the owners of the seigniorage shares. If the algorithm is a company, think of seigniorage shares as the ownership shares of that company, and owners of those shares as shareholders of the algorithm.

While this solution is elegant, a major drawback is that these seigniorage shares represent the future growth of the system. What if it never grows? Or keeps going downhill?

Companies: [Basis](#), [Carbon](#)

No silver bullet

Modern monetary policy is the result of thousands of years of economic evolution. When it comes to recreating monetary policy for cryptocurrency, there's no silver bullet or deus ex machina.

	Price Stability	Crash Proof	Collateral	Decentralized
Fiat collateral	Absolute	Yes	Yes, efficient	No
Crypto collateral	Somewhat today	No	Yes, inefficient	Yes
Algorithmic	Not yet	No	No	Yes

Constant is committed to developing a secure, stable system that integrates the strong points of all three models.

Initially, the Constant System will launch with a fiat-collateral solution. Meanwhile, the Constant R&D team continues to work on both crypto-collateral and algorithmic components for the long-term realization of the Constant System. Our hope is to incorporate these components into the future, optimal version of Constant.

PART II
THE TOKENS OF
THE CONSTANT SYSTEM

4. Overview of the tokens

The Constant System implements a multi-token approach. Each token is designed to serve one of the following purposes: utility, governance, infrastructure, and collaterals.

- The Constant Stablecoin (CONST): a **utility token** that is 1:1 pegged to the US dollar and designed to be used in everyday transactions.
- The Monetary Policy Token (MPT): a **governance token** that is required to conduct monetary policy of the Constant System.
- Ether (ETH): an **infrastructure token** that is used to pay for smart contract gas fees on the Ethereum network.
- The Trust Vault tokens: **collateral tokens** that are held in the Trust Vault in order to back the value of the Constant stablecoin.

5. Utility Token: The Constant Stablecoin (CONST)

The Constant Stablecoin (for short, just Constant) is the main utility token of the Constant System. It is designed to be a utility token for everyday transactions. Constant can be held and spent in the same the way we use the US dollar in everyday life, with a few new powerful features: borderless, frictionless, and decentralized.

100% backed

Every Constant is backed by 1 US dollar, held in a secure, audited escrow account managed by an independent trust company.

1:1 pegged to the US dollar

Constant is pegged 1:1 to the most stable, most usable currency in the world. One Constant always equals one US dollar, and is easily switched for USD at any time.

Mining policy

One new Constant is minted when there is one new US dollar deposited into the Trust Vault.

Burning policy

One existing Constant is burned when there is one existing US dollar withdrew from the Trust Vault.

Monetary supply policy

There is no limit in monetary supply for Constant.

Units

For simplicity, there are only two denominations in Constant.

Name	Value
Constant	≅ 1 US dollar
Nano	≅ 1 US cent or 1/100 Constant

Implementation

For practical purposes, Constant is implemented as an Ethereum ERC20 token, which has been widely adopted by millions of users around the world. The existing infrastructure, userbase and development community is strong and growing steadily; there are exchanges, wallets and software that support ERC20 compliant tokens.

The code is open-source at <https://github.com/constant-money/constant-mvp>

```
pragma solidity ^0.4.24;

import 'openzeppelin-solidity/contracts/token/ERC20/ERC20.sol';
import './Admin.sol';
import './IOracle.sol';
import './IMonetaryPolicy.sol';

contract Constant is ERC20, Admin {

    // token info
```

```

string public constant name = "Constant Stablecoin";
string public constant symbol = "CONST";
uint public constant decimals = 2;

// interface to external contracts
IMonetaryPolicy private monetary;
IOracle private oracle;

// events to track onchain-offchain relationships
event __transferByAdmin(bytes32 offchain);
event __purchase(bytes32 offchain);
event __redeem(bytes32 offchain);

constructor(address _monetary, address _oracle) public {
    monetary = IMonetaryPolicy(_monetary);
    oracle = IOracle(_oracle);
}

/**
 * @dev function to transfer CONST
 * @param from the address to transfer from
 * @param to the address to transfer to
 * @param value the amount to be transferred
 */
function transferByAdmin(
    address from,
    address to,
    uint value,
    bytes32 offchain
)
    public
    onlyAdmin
{
    _transfer(from, to, value);
    emit __transferByAdmin(offchain);
}

/**
 * @dev function to purchase new CONST
 * @param purchaser the address that will receive the newly minted CONST
 * @param value the amount of CONST to mint
 */
function purchase(

```

```

        address purchaser,
        uint value,
        bytes32 offchain
    )

    public
    onlyAdmin

{
    _mint(purchaser, value);
    emit __purchase(offchain);
}

/**
 * @dev function to burn CONST
 * @param redeemer the account whose CONST will be burnt
 * @param value the amount of CONST to be burnt
 */
function redeem(
    address redeemer,
    uint value,
    bytes32 offchain
)

    public
    onlyAdmin

{
    _burn(redeemer, value);
    emit __redeem(offchain);
}

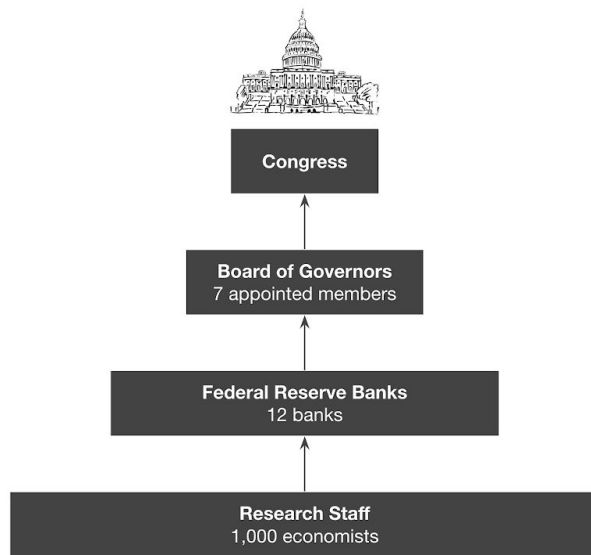
}

```

6. Governance Token: The Monetary Policy Token (MPT)

MPT holders basically form a committee that performs the function of the central bank of the Constant System. It conducts the Constant System monetary policy to achieve two objectives (1) stable prices and (2) maximum meaningful adoption of Constant in everyday life.

A Decentralized Autonomous Organization



Centralized Central Bank



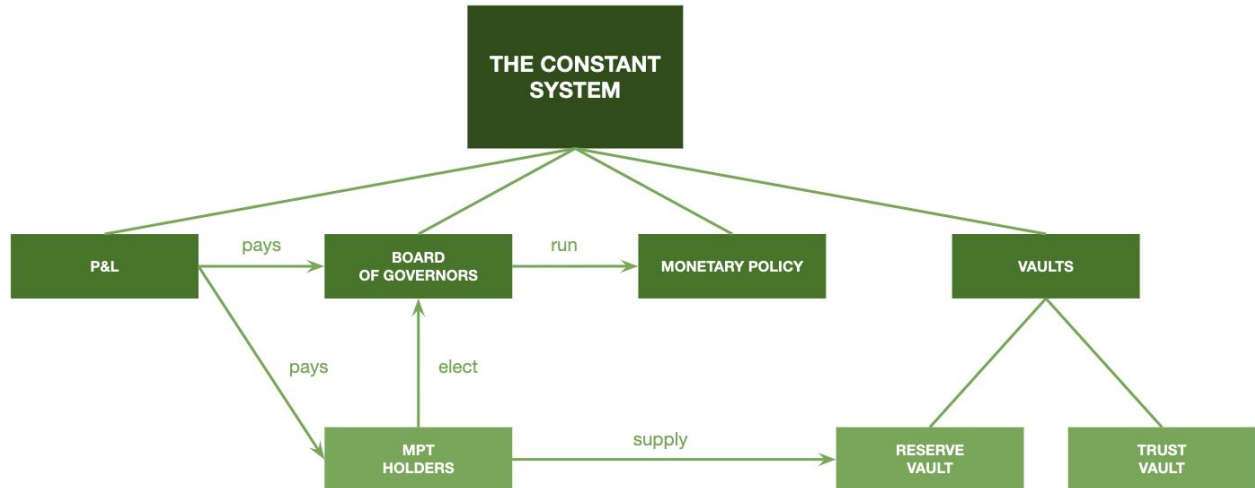
Decentralized Central Bank

The Constant System purposely rejected the concept of a centralized system such as a central bank. Instead, the Constant System is designed as a Decentralized Autonomous Organization (Jentzsch 2016) with three distinct features.

- a cryptonomic central bank governance token, called MPT
- a delegated Board of Governors, elected by MPT holders
- a decentralized decision making process, voted by MPT governors

We believe that having a dedicated Board of Governors, who is elected to conduct monetary policy, is a more optimal setup than waiting for every single user in the entire system to cast their vote on day-to-day proposal.

MPT relationships



MPT holders

Responsibilities

MPT holders elect the Board of Governors and delegate their voting power to the board. For example, Alice can delegate her voting power to Bob, a well-know monetary economist in the network.

Incentives

After accounting for all operational expenses (i.e. paying the Ethereum network for gas fees and paying the trust company for maintaining the Trust Vault), any amount of Constant left in the Constant System will be used to the benefit of the network. Some of the surplus will be used to payout dividends to MPT holders.

MPT holders will receive an amount of Constant proportional to MPT tokens they hold, relative to the total number of MPT tokens in the Constant System.

MPT_I	number of MPT tokens that a user I holds
MPT	the total number of MPT tokens in the entire system
P	the profit (net income) of the Constant System
R	allocation ratio of the Constant System profit to MPT holders initially: $R = 10\%$
P_I	dividend paid to user I

The dividend paid to user I is calculated as follows:

$$P_I = P \times R \times (MPT_I / MPT)$$

MPT governors

Responsibilities

MPT governors play an important role in the governance of the Constant System monetary policy. They submit new proposals to improve the monetary policy and vote on proposals proposed by other MPT governors.

For example, there is an outstanding proposal to increase the redeem fee from 0.5% to 0.7%. All MPT governors can cast their vote on the proposal. If the proposal meets the minimum quorum and passes majority margin, then the new redeem fee will be implemented.

The initial voting parameters are:

- **Purchase Fee:** The purchase fee is a fee paid by every purchase of Constant. The initial purchase fee is 0.0%.
- **Redeem Fee:** The redeem fee is a fee paid by every redemption of Constant. The initial redemption fee is 0.5%.
- **Transfer Fee:** The transfer fee is a fee paid by every transfer of Constant. The initial redemption fee is 0.0%.
- **Collateral Asset:** Constant will be backed by a broad variety of assets, including fiats like the US dollar and Euro, cryptocurrencies like Bitcoin and Ethereum, or tokenized assets like real estate and gold.

As the system evolves, new parameters will be added over time and some of the existing parameters may be removed as they become obsolete.

Incentives

After accounting for all operational expenses (i.e. paying the Ethereum network for gas fees and paying the trust company for maintaining the Trust Vault), any amount of Constant left in the Constant System will be used to the benefit of the network. Some of the surplus will be used to payout dividends to MPT governors.

MPT holders will receive an amount of Constant proportional to MPT tokens they hold, relative to the total number of MPT tokens in the Constant System.

$DMPT_I$	number of delegated MPT tokens that MPT governor I holds
$DMPT$	the total number of delegated MPT tokens in the entire system
P	the profit (net income) of the Constant System
DR	allocation ratio of the Constant System profit to MPT governors initially: $DR = 5\%$
DP_I	dividend paid to MPT governor I

The dividend paid to MPT governor I is calculated as follows:

$$DP_I = P \times DR \times (DMPT_I / DMPT)$$

Mining policy

Users of the system who want to contribute to monetary decisions can buy MPT with Constant and acquire the power to elect the Board of Governors. The Constant collected from the sale will be stored in the Reserve Vault.

The decision of issuing new MPT is proposed and voted by every member of the Board of Governors whenever they see the need of raising the Reserve Vault. Reserve Vault holds all the Constant raised from the sales of MPT. Unlike a physical central bank vault, which is usually 50 feet below the water and protected with an army, Reserve Vault is decentralized on various blockchains and protected by cryptographic algorithms.

Every proposal to issue new MPT contains:

M	the target amount of Constant to raise
D	the discount rate
E	the deadline of the sale
P_{MPT}	the market price of MPT (fed through Oracles)
$CONST_I$	the amount of Constant that user I pays with

If the proposal is approved by the Board of Governors, users have the chance to buy MPT directly from the Constant System at a discounted rate D compares to open market price. The sell is on the basis of first come, first served and ends either after the deadline or because M is reached.

The number of MPT user I received will be:

$$MPT_I = CONST_I / (P_{MPT} \times D)$$

Burning policy

MPT is not burnable.

Monetary supply policy

There is no limit in monetary supply for Constant.

Units

MPT is the single denomination of MPT.

Implementation

For practical purposes, MPT is also implemented as an Ethereum ERC20 token.

The code is open-source at <https://github.com/constant-money/constant-mvp>

```
pragma solidity ^0.4.24;

import 'openzeppelin-solidity/contracts/token/ERC20/ERC20.sol';
import './Admin.sol';

contract MonetaryPolicy is ERC20, Admin {

    // token info
    string public constant name = "Monetary Policy Token";
    string public constant symbol = "MPT";
    uint public constant decimals = 0;
    uint private supply;

    struct Proposal {
        bytes32 key;
        uint value;
        uint yes;
        uint no;
        uint deadline;

        // 0: empty, 1: proposed, 2: approved
        uint status;
    }

    // monetary policy parameters such as ratio, threshold
    mapping(bytes32 => uint) private params;

    // proposal
    Proposal[] private proposals;
```



```

// events for syncing onchain and offchain execution
event __transferByAdmin(bytes32 offchain);
event __mint(bytes32 offchain);
event __propose(uint pid, bytes32 offchain);
event __vote(bytes32 offchain);
event __setParam(bytes32 offchain);

/**
 * @dev constructor that populates a bunch of default params
 */
constructor() public {

    // secured loan
    params["ethRatio"] = 50; // 50%
    params["ethInterest"] = 300; // 3.00%
    params["ethThreshold"] = 80; // 3.00%

    // voting
    params["votingWindow"] = 7 * 1 days;
    params["quorum"] = 20; // 20%
    params["majorityMargin"] = 51; // 51%
}

/**
 * @dev function to transfer MPT
 * @param from the address to transfer from
 * @param to the address to transfer to
 * @param value the amount to be transferred
 */
function transferByAdmin(
    address from,
    address to,
    uint value,
    bytes32 offchain
)
    public
    onlyAdmin
{
    __transfer(from, to, value);
    emit __transferByAdmin(offchain);
}

/**
 * @dev function to mint new MPT

```

```

    * @param to the address that will receive the newly minted MPT
    * @param value the amount of MPT to mint
    */
function mint(
    address to,
    uint value,
    bytes32 offchain
)
    public
    onlyAdmin
{
    _mint(to, value);
    supply += value;
    emit __mint(offchain);
}

/**
 * @dev getter function to get a param value
 */
function param(bytes32 key) public view returns (uint){
    return params[key];
}

/**
 * @dev function to submit a new proposal
 */
function propose(bytes32 key, uint value, bytes32 offchain) public {
    Proposal memory p;
    p.key = key;
    p.value = value;
    p.deadline = now + params["votingWindow"];
    p.status = 1;

    proposals.push(p);

    emit __propose(proposals.length - 1, offchain);
}

/**
 * @dev function to vote on a proposal
 */
function vote(uint pid, bool yes, bytes32 offchain) public {
    Proposal storage p = proposals[pid];
    require(p.status == 1);
}

```

```

        require(now < p.deadline);

        if (yes)
            p.yes += balanceOf(msg.sender);
        else
            p.no += balanceOf(msg.sender);

        if ((p.yes + p.no) * 100 > params["quorum"] * supply) {
            if (p.yes * 100 > params["majorityMargin"] * (p.yes +
p.no)) {
                p.status = 2;
                params[p.key] = p.value;

                emit __setParam(offchain);
            }
        }

        emit __vote(offchain);
    }
}

```

7. Infrastructure Token: Ether (ETH)

For practical purposes, the initial release of the Constant System is implemented on top of the Ethereum network. Ethereum has been widely adopted by millions of users around the world. The existing infrastructure, userbase and development community is strong and growing steadily; there are exchanges, wallets and software that support ERC20 compliant tokens.

Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.

The Constant System is implemented as a set of Ethereum smart contracts. Everytime a smart contract executes one of its functions, there is a gas fee, required by the Ethereum network to be paid to its miners.

8. Collateral Tokens: Trust Vault Assets

By design, Constant is 100% backed. The first release of Constant, as outlined in this paper, is backed by the US dollar only. In subsequent releases, Constant will be backed by a broad variety of assets, including fiats like the US dollar and Euro, cryptocurrencies like Bitcoin and Ethereum, or tokenized assets like real estate and gold.

MPT holders can vote on adding, modifying, or removing an asset.

PART III
THE CONSTANT SYSTEM:
THREE KEY ENTITIES AND
FIVE CORE FUNCTIONS

9. Overview of the Constant System

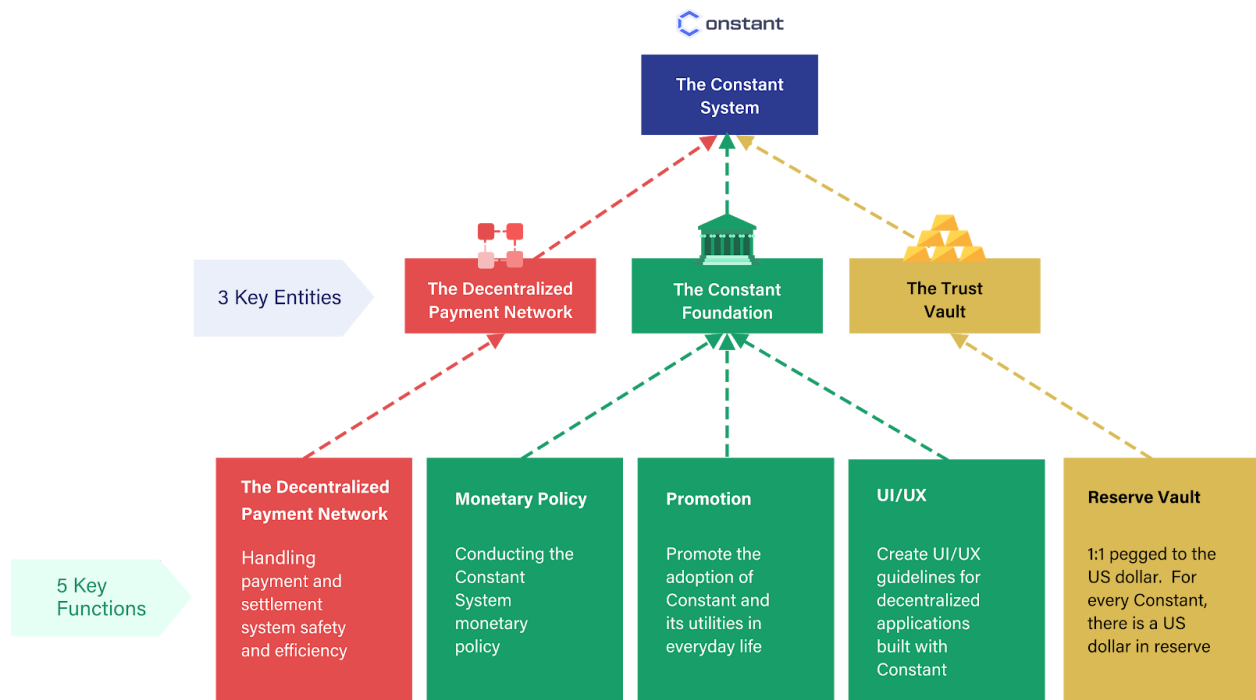
A hybrid approach

We, like the rest of the world, like the stability of the US dollar. The US dollar is backed by the battle-tested design of the Federal Reserve System, which was founded in 1913 as the central bank of the United States, and has established the US dollar as the most stable currency in the world.

We also like the innovation of decentralized ledger technologies (blockchain) from the field of computer science. Pioneered by Satoshi Nakamoto (Nakamoto 2009), blockchains are decentralized digital currency systems without central authorities such as banks. Transaction management and currency issuance are instead carried out collectively by the users of those networks. The Constant System runs on top of the Ethereum network (Vitalik 2013).

Constant is a hybrid. The first release of the Constant System combines the creditworthiness and price stability of the US Dollar with the technological advantages of Decentralized Ledger Technologies (blockchain). An audited, independent Trust Vault is integrated into the system to ensure security and stability, strictly maintaining a 1:1 peg between Constant and the US dollar.

The Constant System: 3 key entities and 5 key functions



The Constant System has 3 key entities:

- **The Decentralized Payment Network:** A peer-to-peer decentralized payment network that operates without central authority or banks. Processing and managing transactions are carried out collectively by the users of the network.
- **The Constant Foundation:** The founding team that makes initial decisions with regard to the building and running of the Constant System. This system is designed to become increasingly decentralized over time, so that decision-making powers will ultimately belong to the community at large.
- **The Trust Vault:** An escrow account that holds one US dollar for every Constant in circulation. The Trust Vault holding the USD is secured by an independent custodian, a chartered, regulated financial institution.

The Constant System performs 5 key functions in the user's interest to ensure the stability of the stablecoin, and work towards both growth and adoption.

- **Conducting** Constant's monetary policy to ensure stable prices in both global and local markets.
- **Handling** payments and settlements safely and efficiently through blockchain technologies, reducing expense and bypassing typical wait times and geographical borders.
- **Maintaining** an audited, 100%-backed reserve of USD for the equivalent amount of Constant in circulation.
- **Creating** UI/UX frameworks for decentralized applications built with Constant, focusing on the useable, simple and intuitive.
- **Promoting** meaningful adoption of Constant for use in everyday life.

Business Model

The Constant System is privately funded by the Constant Foundation. In the long run, the Constant System should be able to self-fund its operations by charging competitive fees on services such as transfers, purchases, and conversions.

Income derived from these fees will be directed towards covering the cost of those services, including gas payments to the Ethereum network and operation expenses for maintaining the Trust Vault.

Only after all expenses are paid for, will the net earnings of the Constant System be transferred to the Constant Foundation. The Constant Foundation will then distribute these earnings fairly among users of the system in accordance with a crypto-economics model.

10. Entity: The Constant Foundation

Purpose

The Constant Foundation is the founding team behind the Constant System. It is responsible for designing and implementing the Constant System and promoting the mass adoption of Constant in everyday life. Initially, the Constant Foundation makes decisions on building and running the Constant System. However, over time, decision-making powers will be decentralized and distributed to the community.

Constant roadmap

- Q1 Launch v1.0
 - Runs on Ethereum network
 -
- Q2 Launch Consumer Financial Services
 - Secured Loan
 - Savings
- Q3 Launch Constant Chain Testnet
- Q4 Launch Constant Chain Mainnet

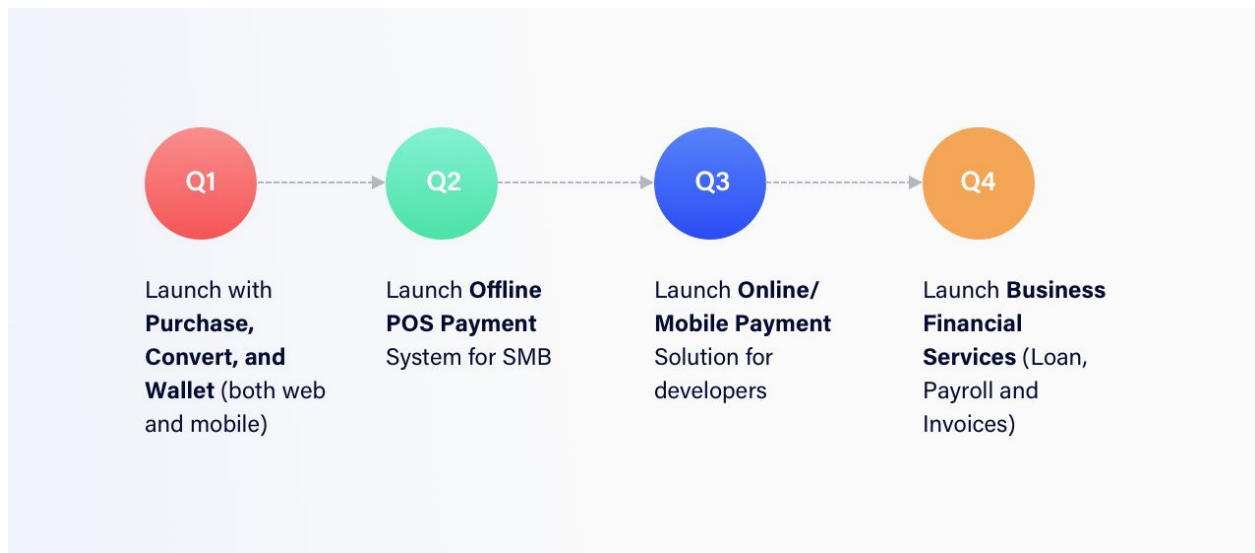
2019 Application roadmap

- Q1 Launch v1.0
 - Purchase
 - Redeem
- Q2 Launch Consumer Financial Services
 - Secured Loan
 - Savings
- Q3 Launch Constant API for developers

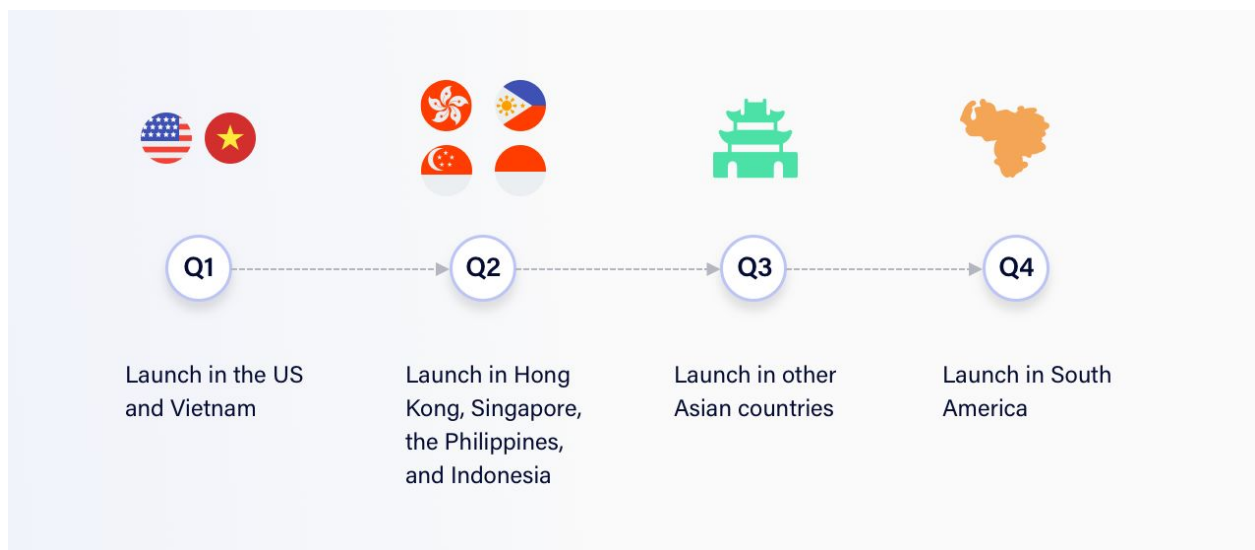
- Web integration
- Mobile integration

Q4 Launch Business Financial Services

- Loan
- Payroll
- Invoices
- Point of Sale



2019 Market roadmap



Key members

The Constant Foundation consists of 30 scientists, cryptographers, engineers, educators and business operators, on a mission to bring freedom to money. Many of us have worked together for years — either solving difficult scientific problems or engineering large-scale practical real world applications.



Duy Huynh, Monetary Policy

Duy works on the monetary policy of the Constant System. He spends most of his days studying the great economic thinkers of the last 100 years and turning their ideas into unstoppable lines of code. Prior to Constant, Duy founded Autonomous, a startup that combines AI & Robotics technologies to build smart office products. He grew the company to 100+ employees in 6 countries, with 300,000+ business customers in 60+ countries within the first 24 months.

At age 18, Duy moved from Vietnam to the US to study at the University of Wisconsin, where he completed a 4-year college degree in 3 semesters. At age 19, Duy was a PhD researcher at the University of Maryland in the High Dependability Computing Program, funded by NASA, the Semantic Web and Fujitsu. Duy later dropped out to pursue his interest in building real world applications and became a software architect at IBM.

In another past life, Duy was a competitive programmer. He was an ACM ICPC World Finalist, USA Computing Olympiad winner, and Vietnam Computing Olympiad winner.



Professor Thuc Nguyen, Applied Cryptography

Thuc is a leading expert in the field of applied cryptography, and will work on privacy, post-quantum cryptography, randomness, and all things cryptography at Constant. His current focus is on preserving the anonymity and confidentiality of Constant transactions through zero-knowledge proofs.

Thuc is a professor of applied cryptography at the National University of Vietnam, where he co-founded the Department of Applied Cryptography and Computer Security. Thuc also co-leads the Decentralized Cryptography Research Group, designing innovative cryptographic tools and developing privacy-preserving cryptosystems that simultaneously achieve post-quantum security and practicality. He also leads key projects on security and cryptography for the Vietnamese government.



Professor Dung Tran, Consensus & Scalability

Dung works on the consensus & scalability algorithms at Constant. His current focus is on increasing transaction throughput while preserving consensus properties. Dung has extensive research and practical experience in distributed systems, computer networks, and game

theory, making him the perfect candidate for designing and implementing consensus and scalability mechanisms at Constant.

Dung also lectures at the National University of Vietnam. As well as teaching courses on distributed systems, Dung has published several papers on bandwidth measurement and estimation, and is the author of two textbooks, *Operation Systems* and *Computer Networks*. He holds a PhD in computer science from the University of Texas.



Gaël Vo, Product Manager

Gaël designs, develops, and manages new innovative financial products at Constant, including remittance, loans, salary, invoicing, and many others. Prior to Constant, he worked as a financial engineer at BNP Paribas where he created a new framework to replace and centralize complex applications, enabling users and other developers to control the system independently.

Gaël holds a dual master's degree in computer science and telecommunications from Institut National des Sciences Appliquées de Lyon, and an MBA in finance from Simon Business School in New York. As an MBA intern at Five Star Bank, Gaël developed an automation layer within loan management that cut processing time by 83%. Gaël hopes to create the future of banking in emerging economies.



Bao Le, Infrastructure

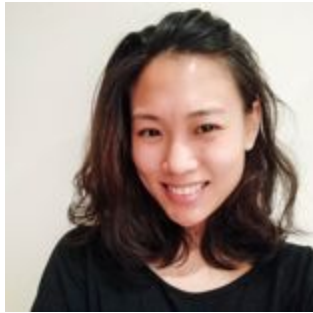
Bao works on the infrastructure layer of Constant, integrating both on-chain and off-chain components such as the consensus protocol, privacy-preserving zero-knowledge proofs, and monetary policy algorithms. Prior to Constant, Bao built highly scalable systems for emerging markets, including Viettel Group, Vietnam's largest mobile network operator, where he scaled their products for 63M subscribers, and Central Group, Thailand's number 1 retail and service group business.

Bao leverages his deep knowledge of peer-to-peer applications, cryptography, game theory, and network applications to build highly scalable systems that quantify performance, availability, and extensibility in each line of code. Bao continues to acquire new cryptography techniques, knowledge of computer networks, and regularly researches existing networks to improve, find, and integrate new protocols and solutions.



Bill Pelletier, E-Commerce

Bill works on integrating Constant as a payment method for major e-commerce retailers. Prior to Constant, Bill worked closely with some of the world's biggest e-commerce retailers, including Amazon, Overstock, Target, Wayfair and Home Depot. Before that, he developed the investment portfolio of a major bank as a private banker, and has also advised multiple high profile clients on mergers & acquisition, trust & estates, and provided litigation support.



Ning Tan, Community, South East Asia

Ning works on getting Constant into the hands of 700 million people in South East Asia. She specializes in creating and clarifying concepts, distilling meaning and building useful things. Prior to Constant, Ning was the Director of Communications at Autonomous, where she loved helping people in over 60 countries find ways to work smarter.

She has also created voices for a variety of IoT products, eager robots, decentralized applications, and a very clever brain from the US military. Working closely with teams and communities from the USA, Europe, Hong Kong, Philippines, Vietnam, Singapore and Indonesia, she has spent years easing the integration of disruptive tech and considers herself lucky to have been exposed to multiple diverse perspectives.

While conducting postgraduate research at the University of Oxford, she mapped patterns in human thinking, piecing together the refrain of questions that drive the birth of revolutions. Ning also leads a double life as an amateur ceramicist.



Justin Lucas, Community, Latin America

Justin works on getting Constant to people in Mexico, Venezuela, Bolivia, Argentina, and soon, to other countries in Latin America. Prior to Constant, Justin was the General Manager of Autonomous North America, where he launched and scaled Autonomous in the US and Canada. Throughout his time living and working in the UK, Hawaii, Japan, Vietnam and the US, he understands the need of a borderless currency.

Key advisors



Ha Tran, Vice President, Goldman Sachs

Mr. Ha Tran, CFA, has been in the forefront of Technology and Finance over the last 15 years, holding positions in electronic trading and risk management at Goldman Sachs. He led several innovative efforts to overhaul old ways of doing finance, including Automation, Simulation and Machine Learning. Mr. Tran is currently at working on a project to bring structured and complex financial products a step closer to the general public.



Tien Nguyen, Engineering Manager, Essential

Tien has built some of this decade's most important products. He built mobile payments for emerging markets at Google and payment hardware and software solutions for SMB businesses at Square. Tien also built the Android app at Uber. He is currently leading app development at Essential.



Minh Doan, Co-founder, Harmony

Minh Doan worked on Google's Assistant, Play and Plus for 5 years and holds the patent for "Publisher Click-Ring Fraud Detector" at Google. He was a former champion at USA Computing Olympiad Open and many other Informatics Olympiads. Minh was a doctoral candidate in algorithms and distributed systems at the University of California, Irvine. He has a master's degree in computer science and applied mathematics from Moscow State University. His research paper, "An effective ant-based algorithm for the degree-constrained minimum spanning tree problem", was published at IEEE Congress on Evolutionary Computation.

11. Entity: The Trust Vault

Purpose

Constant cannot be minted from thin air. Every Constant that circulates on the market must be backed by a tangible asset, held in an audited Trust Vault, managed by an independent Trust Company.

Assets

Initially, the Trust Vault will accept a single asset type - the US dollar, because of its creditworthiness, price stability, and especially its liquidity.

Gradually, multiple asset types will be enabled and introduced to the Trust Vault. Potential assets fall broadly among these types:

- Cryptocurrencies (BTC, ETH)
- Tokenized commodities such as gold ([DGX](#), CryptoBullion, AUcoin)
- Tokenized real estate and rental properties ([Harbor](#), REX, Real, SmartRE, REIDAO, Estate Coin, RealCoin)

- Tokenized stock, bonds, and other financial instruments
- Tokenized fine art (Maecenas)
- Tokenized company shares (Polymath)

Examination

The US dollar escrow balance in the Trust Vault is examined monthly by a registered public accounting firm, in order to verify the 1:1 peg and provide frequent, transparent reports to all users of the system.

Direct banking

While the Constant System builds and provides all utilities, users only ever transact directly with the bank of the independent trust company. The Constant Foundation never touches their funds.

Implementation

The Constant System designates Prime Trust, an independent technology-driven trust company, to manage the Reserve Vault. As a chartered, regulated financial institution, Prime Trust is overseen by the banking commissioner's office at the [Financial Institutions Division](#). As a trust company, Prime Trust holds cash and non-cash assets such as stocks, bonds, Bitcoin and other cryptocurrencies, tokens, real estate, and private business ownership interests. The Prime Trust team has deep experience in all facets of trust operations, banking, securities regulations, and governmental affairs.

12. Entity: The Decentralized Payment Network

Purpose

The Decentralized Payment Network is responsible for handling all payments in the Constant System. It uses distributed ledger technology (blockchain), a digital innovation that reinvents payments, clearing, and settlement processes - reducing operational and financial inefficiencies of payment systems. The blockchain, collectively maintained and secured by users of the system, presents a safer, more efficient, and more decentralized alternative to the classic double-entry book keeping maintained by a central authority.



Distributed ledger technology

Distributed ledger technology is a remarkable alternative to the existing financial infrastructure. In terms of efficiency, it eliminates intermediaries and their ridiculous markups, and allows peer-to-peer direct transactions. In terms of finality, it provides an immutable record that cannot be altered retrospectively. In terms of speed, settlement can be near real time. In terms of safety, it uses cryptographic proofs without a central authority or trusted third party.

The Decentralized Payment Network provides:

- **Ubiquity:** universal access for everyone (personal, business, non-profit, the unbanked) for multiple use cases, with cross-border functionality.
- **Safety:** a secure system that holds immutable records with cryptographic integrity without a central authority or a trusted third party.
- **Speed:** near real-time clearance and settlement of transactions.
- **Low cost:** elimination of intermediaries and centralized monolithic infrastructure costs.
- **Convenience:** easy access with just an internet connection.

- **Finality:** irreversible peer-to-peer settlements of transactions, immutably recorded on a ledger that cannot be altered retrospectively.

Implementation

The decentralized payment network is built on top of Ethereum, a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference. This framework supports various programs (or smart contracts) that enable minting Constant, burning Constant, transferring Constant among the users of the system, and maintaining the Trust Vault.

13. Function: Conducting monetary policy

Initially, the Constant Foundation sets and runs the Constant System monetary policy. Over time, decision-making power will be decentralized and distributed to Constant holders.

Constant monetary policy is conducted with two goals in mind:

1. to achieve stable prices.
2. to maximize meaningful adoption of Constant in everyday life.

In order to achieve these two goals, the Constant System implements a dual-token model. The Constant stablecoin is the main utility token of the system, and the Growth Token is linked to the future growth of the Constant System, a reward to users for their contribution to the system.

1:1 pegged to the US dollar

Constant is pegged 1:1 to the most stable, most usable currency in the world. One Constant always equals one US dollar, and is easily switched for USD at any time.

Fees

The Constant System charges fees on transfer, purchase and conversion services. This income is used to cover the cost of those services, including gas payments to the Ethereum network, legal fees, and operation expenses for maintaining the Trust Vault.

The first release of Constant will be launched in the US and Vietnam with extremely competitive fees. The operations team is working towards similarly friendly fees for the rest of the world.

It's easy and affordable to get and redeem Constant.

USA - For Popular

USA - For Student

Vietnam

Other countries

PURCHASE

Change your money to Constant with Prime Trust, an accredited US financial institution.

FREE
on all purchases

min \$1,000 tx size

TRANSFER

Move your money across the world. You can send it to anyone, anywhere in the world.

FREE
for all transfer

REDEEM

Get USD for Constant, anytime. Anyone who holds Constant can get 1 USD for 1 Constant.

0.5%
per redemption


Special price for Student. Limited offer.



 USA - For Popular

 USA - For Student

 Vietnam

 Other countries

PURCHASE

Change your money to Constant with Prime Trust, an accredited US financial institution.

FREE

on all purchases

min \$1,000 tx size

TRANSFER

Move your money across the world. You can send it to anyone, anywhere in the world.

FREE

for all transfer

REDEEM

Get USD for Constant, anytime. Anyone who holds Constant can get 1 USD for 1 Constant.

0.25% ~~0.5%~~

per redemption

It's easy and affordable to get and redeem Constant.

 USA - For Popular

 USA - For Student

 Vietnam

 Other countries

PURCHASE

Change your money to Constant with Prime Trust, an accredited US financial institution.

FREE

on all purchases

min \$1,000
purchase amount

TRANSFER

Move your money across the world. You can send it to anyone, anywhere in the world.

FREE

for all transfer

REDEEM

Get USD for Constant, anytime. Anyone who holds Constant can get 1 USD for 1 Constant.

0.5%

per redemption

min \$35 fee

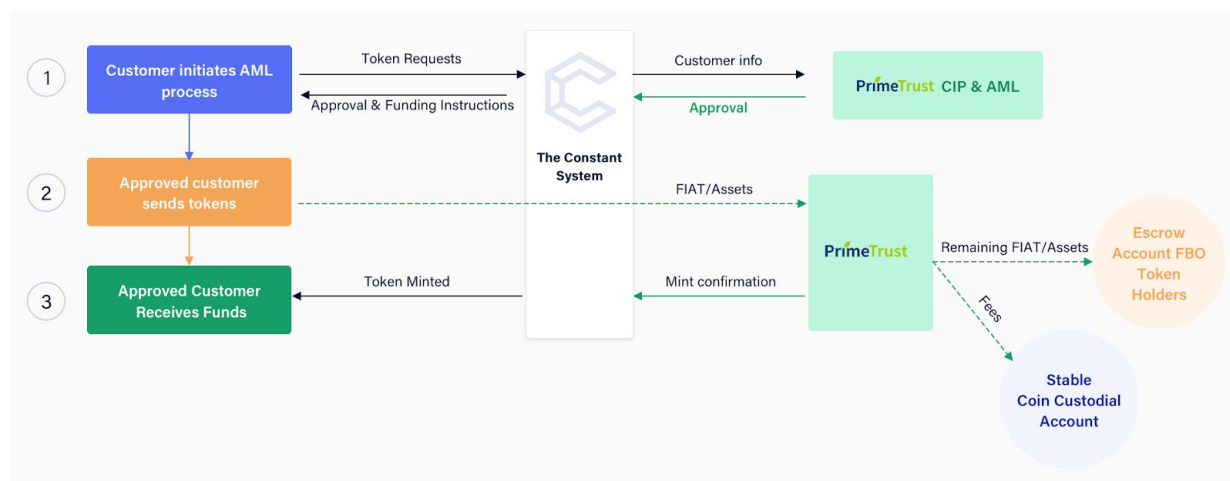
14. Function: Managing the Trust Vault

The Trust Vault comprises of a set of fully audited, independent escrow accounts. One of the most widely used legal vehicles for third party funds management, escrow accounts enable regular attestations and strong legal protection for Constant holders.

Our legal framework enables users to exchange USD directly with Constant escrow accounts. The Constant System cannot touch the funds. When purchasing Constant or converting to USD, users send or receive USD straight from Constant escrow accounts, managed by independent Trust Company partners.

Constant designates licensed trust companies to securely hold the funds backing Constant. For increased security and to avoid any potential conflicts of interest, Constant does not and will not have access or control over any escrowed funds.

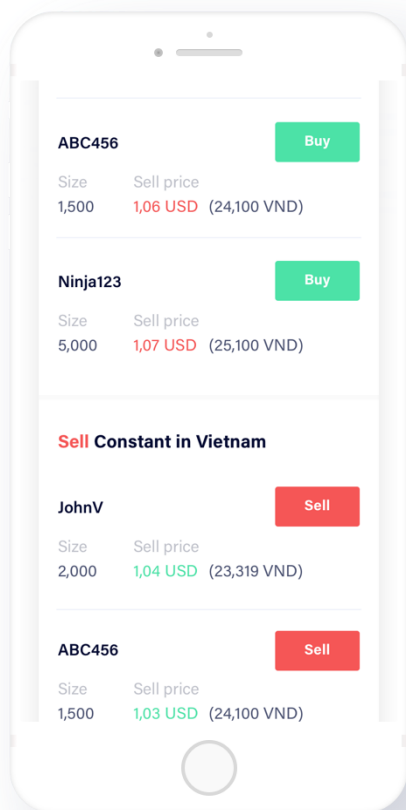
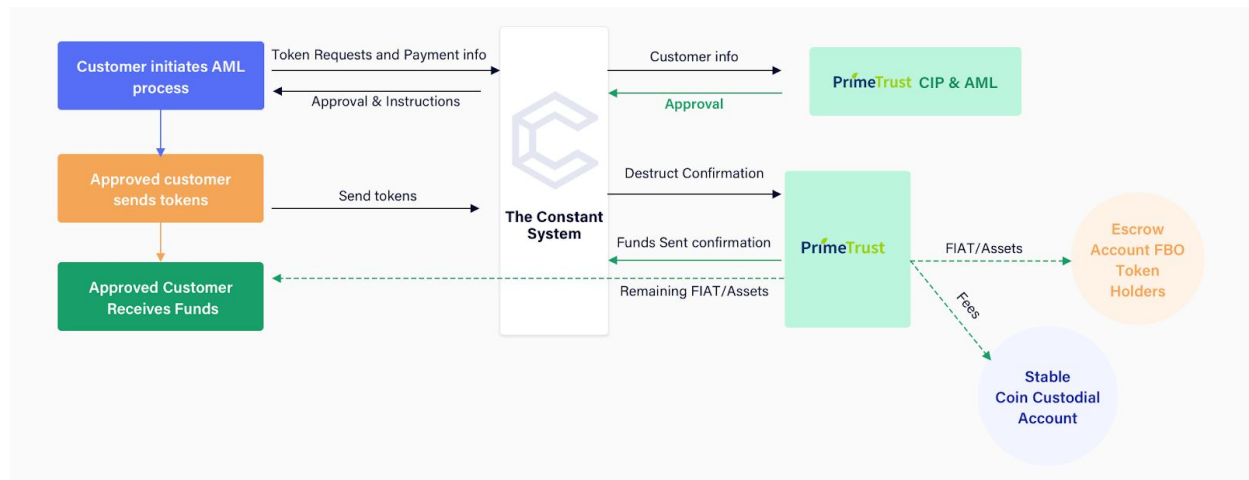
Minting new Constant



If Constant is to become a legitimate alternative to fiat, it must similarly stay in keeping with world regulations. To purchase Constant, users must first pass a KYC/AML check. Once complete, they are able to deposit their USD directly into the escrowed Trust Vault of an accredited trust company that operates independently from Constant. Once funds reach the Trust Vault, the custodian's API instructs the System's smart contract to mint the equivalent in Constant, which is then sent straight to the user's public Ethereum address.

This separation of entities is integral to ensuring the long-term stability of the system. As an additional security feature, users' funds will continue to be held safely in this independent escrow account, inaccessible by both the Constant System and the impartial third party.

Burning



To switch Constant to USD, users must also have completed KYC/AML verification. Constant tokens can then be sent to the Constant smart contract, which (1) burns those tokens, removing them from circulation, and (2) automates the return of the equivalent USD from the escrowed Trust Vault.

In this way, the Constant System has no access to any user funds, and the independent financial institution can only enable the movement of Constant and USD through trustless escrow accounts.

Funds guarantee

These escrow accounts are security guaranteed and covered up to \$5,000,000 USD. All funds in your account are 100% FDIC insured.

15. Function: Handling payments and settlements safely and efficiently

The most important function of the Constant System is to manage the payment system. The Constant System uses distributed ledger technology (blockchain) as its payment system, reducing expense and bypassing typical wait times and geographical borders. Details of every transaction are recorded on this public ledger.

Using either a searchable transaction ID (TxHash) or the Ethereum wallet addresses of either sender or recipient, anyone is able to quickly pull up the value of the relevant transaction, the time in which it occurred, and any fees paid to the Ethereum miners for processing the transaction and securing the network (Gas).

Transaction Information

TxHash:	0x759c93d4b9849dba3287772d90b2e3f8356f86f4bddb0883f64148e7a3fefabf
TxReceipt Status:	Success
From (sender's wallet address)	0xf111bfc69f3ad5c2103ea54b1d1d48f6e3724610
To (recipient's wallet address)	0x689c56aef474df92d44a1b70850f808488f9769c
Value (transaction value in ETH)	0.4299262415 Ether
Gas Limit:	21000
Gas Used By Transaction:	21000 (100%)
Gas Price:	0.000000006 Ether (6 Gwei)
Actual Tx Cost/Fee:	0.000126 Ether (\$0.02)

Addresses and keys

Each Constant user has one or more Constant address(es). A Constant address is a 20-byte address of digits and characters, generated from a public key. An address can be used to receive funds or send out funds.

An address could be controlled by either a **single signature** or **k-out-of-n multiple signatures**.

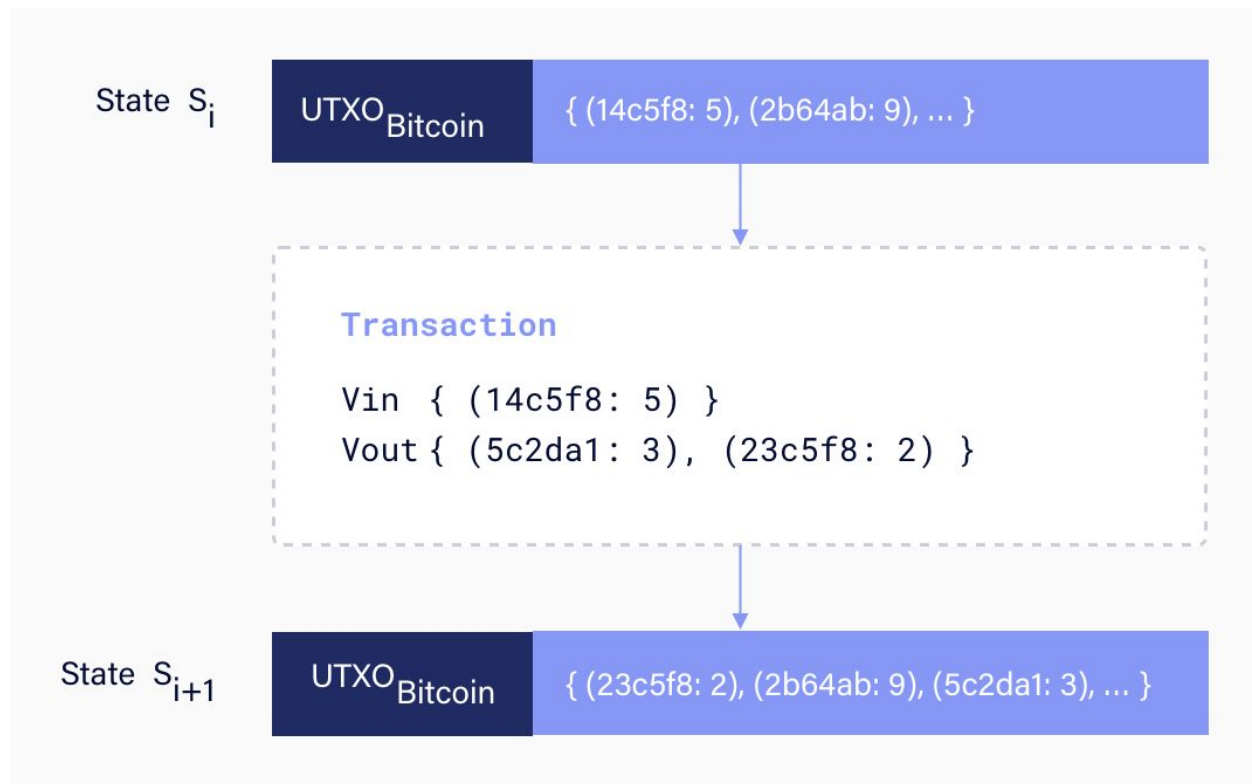
Transactions

Enabling and securing transactions are foundational to the Constant System. The System is primarily designed to ensure that transactions can be created, propagated on the network, validated, and finally added to the ledger.

Transactions are data packages that encode the transfer of value or information between users in the Constant network. In the System, different transactions perform different tasks. Some transaction types simply transfer value between users; others transfer information, such as voting or multisig, with or without value, between them.

State transition system

Blockchains like Bitcoin or Ethereum are essentially transaction-based state transition systems. For example, a transfer transaction of 3 bitcoins moves the Bitcoin network from state S_i to S_{i+1} .



Constant can also be thought of as a transaction-based state transition system. It begins with the genesis state and incrementally executes transactions to arrive at the next state.

Note that, while the state is a crucial component of the network, it is not stored on the blockchain. Only transactions are stored on the blockchain. The state is often stored in memory or in a fast key-value database such as [LevelDB](#).

Blocks

Multiple transactions are packaged into a block and multiple blocks are cryptographically chained together. This is what constitutes the blockchain.

Each block is written into the blockchain as an immutable record, based upon the consensus of the users in the network. Transactions that are packaged into a block are final and irreversible.



16. Function: Promoting adoption of Constant in everyday life

Constant moves faster and more freely than fiat. It is designed for security and transparency, and built for flexibility, practicality and cost-efficiency. This upgraded money is both currency and infrastructure, easily integrated into both life and code. Addressed to users below is a broad outline of realistic use cases of Constant, as well as the role the Constant Foundation will play in facilitating those use cases.

The Constant Foundation is responsible for:

- Easing meaningful adoption of the Constant stablecoin for use in personal or business capacities.
- Building tools to enable developers to design new online and offline payment services. Supporting them in creating solutions that previously could not exist, due to the limitations of existing financial structures.
- Developing the first group of applications to help users get more out of Constant, and as blueprints for other developers to begin building their own decentralized applications with Constant.

For personal

Fast international payments

Sending Constant across the world is easier than walking your cash across the street, and much faster than relying on the traditional banking system. Constant doesn't make you wait 3 business days, charge extra fees for making an international transfer, and doesn't dictate minimum or maximum amounts you can send.

Security and complete control over your money

Constant transactions are secured by military-grade cryptography, so nobody can take your money or make a payment on your behalf. The blockchain is immutable, so no one can alter a previous transaction or dispute an occurrence. Constant is designed for freedom, peace of mind and autonomy.

Zero to low fees

Banks typically charge between \$15 to \$35 to receive international transfers. There are zero fees involved when receiving Constant, no matter how far it has travelled. When it comes to sending Constant, fees are low and fixed, regardless of amount. This means that there are no transaction limits, and that sending 1,000,000 Constant costs the same as sending 1.

Mobile payments made easy

The Constant payment system is available via mobile web, so there is no need to download an app. Simply scan to pay, or display the QR code representing your account address to the other party, so they can scan it and complete the transaction.

Works everywhere, any time

Like email, it's a protocol. The Constant System never sleeps, or takes weekends off - and the tens of thousands of miners that sustain the system don't take bank holidays. To make any payment or transaction, all that is needed is the account address of the receiver. Any ERC20 compatible software, wallet, or exchange can receive it.

For business

Protection against fraud

Credit cards, Paypal, or even ACH encounter problems with chargebacks and reversed payments. Constant payments are irreversible and secure, meaning that the cost of fraud is minimized for businesses.

Fast international payments

Paying a supplier in China, a freelancer in a London, or a local vendor in New York costs the same low fee, and takes the same amount of time - mere minutes - no matter the amount or destination. Constant enables unlimited transfers of unlimited amounts, to anywhere in the world, so you and your business can move quicker.

Zero to low fees

It costs you nothing to receive Constant, compared to the \$15 - \$35 international transfer fee that banks typically charge. As for outward payments, Constant replaces the standard \$45 international wiring fee with a low, fixed fee. So that no matter the size or location of your business or finances, you remain as time and cost efficient as possible.

Multi-signature

Constant also offers more complex solutions for larger organizations. A multi-signature scheme allows Constant to be spent only if a denoted subset of people collectively authorize the transaction. Businesses can also lock requirements in place and automate payments when those requirements are fulfilled, eliminating anxiety and needless back and forth. For example, a large transaction of over 100,000 Constant can be executed only after both CEO and CFO have digitally signed off on it.

Online payments

Adding Constant as an additional payment option on your ecommerce site is straightforward. There are many 3rd party payment processing services that support ERC20 and provide stable APIs.

Offline payments

Accepting offline payments is as simple as scanning a QR code. You can use any digital wallet to scan the QR code from any wallet your customer happens to have, as long as they both support the common ERC20 standard.

For traders

Hedging

Constant prices are immune to pump and dumps, and remain stable no matter how volatile the cryptocurrency market is. By converting your other cryptocurrencies like BTC and ETH into Constant when the market is downwards trending, you can hedge against uncertainty and volatility and protect the value of your assets.

An alternative to traditional currency deposit

Use Constant as an alternative to traditional fiat deposit and withdrawal methods for lower fees and faster transaction processing times. Convert your fiats into Constant without exposure to the volatility of BTC or ETH.

For developers

Be your own bank. Be your own payment gateway.

You don't need approval from a bank or payment processor. You can just boot up a node and become your own. The flexibility of Constant allows you to build products, systems and your best ideas - in any way you like, for any customer or client.

Simple yet powerful programming model

The blockchain programming model ensures that you no longer have to store customer information on your server and be responsible for protecting it. The chain itself is the most secure database, immutable and protected from any single point of failure. All private keys are stored and managed by users on the client side. Taking payments is as simple as a few API calls to the blockchain via the [web3.js library](#).

Integrate into your existing web sites or apps

Since Constant is an ERC20 token, you can seamlessly integrate Constant into your existing web and mobile apps via commonly used tools like [Metamask](#). Easily tap into the active user base of the dynamic Ethereum ecosystem.

17. Function: Create UI/UX guidelines for decentralized applications built with Constant

Constant is designed for useability and real world practicality. We hope that one day Constant will be integrated seamlessly into daily use. We describe the first of many practical use cases and applications of Constant in the preceding sections, but for these use cases to work at scale, we need to establish an empathetic design system that never alienates.

The product design team at the Constant Foundation is working on adapting familiar frameworks, words and behaviors to better communicate new ideas and welcome new interactions.

Vocabulary

Don't	Do
Cryptocurrency	Digital money
Blockchain	Public record
20-byte address	Email address

Performance





At some point in the future, we believe that the Constant System will be 100% decentralized. We are not there yet. Asking a user to wait 10 minutes for a transaction confirmation is 10 minutes too long. The reality in January 2019 is that if we make it the user's responsibility to understand gas fees and navigate multiple disparate platforms to buy the 10 cents worth of Ether needed to place a simple vote, no one will. And so the decentralized democracy grinds to a halt.

The Constant Foundation is committed to finding the ideal balance of decentralization, that optimizes the user experience while still preserving the transparency, security and stability that will remain at the very core of the System.

Web

Here are some screenshots of the initial release of the Constant System on the web.

Constant is a more useful money.

- 
1 Constant = 1 USD.
 Constant is pegged to the most stable, most usable currency in the world.
- 
Fully backed.
 Switch Constant for USD anytime. Every Constant is backed by 1 USD, held in an unhackable trust.
- 
Borderless.
 Constant moves instantly from your account to anyone, anywhere in the world.
- 
Low fees.
 It costs nothing to send or receive Constant. Unlimited transfers of any amount.

[Watch how it works](#) 

DIRECT
1.00 USD

LOCAL
23,500 VND

TRANSFER
Free

BUY CONSTANT FOR USD

[Buy 1,000 Const](#)

SELL CONSTANT USD

[Sell instantly](#)


Make instant international transfers

Send money to anyone, anywhere in the world, and they'll receive it within minutes.



Trade crypto more safely

Constant makes it easier and safer to buy or sell Bitcoin. No matter how low Bitcoin goes, Constant never loses value.



Build new financial solutions

Automate and secure payments, salaries and even loans, with advanced smart contract technology.



Save time and money

Make online and mobile purchases faster, and receive your items faster. Oh, and zero fees.



Special price for US Student

[See more](#)

Earn your first Constant

We provide an affordable transfer money service



Sign up an account

Completed



Purchase Constant

5 CONSTANT
for first order



Invite some friends to join Constant
Sign up required

5 CONSTANT
for first successful transaction order

Email addresses, separate by commas

Send invites

Or

Share your link

<http://constant.com/join/1358bf92>

Copy link

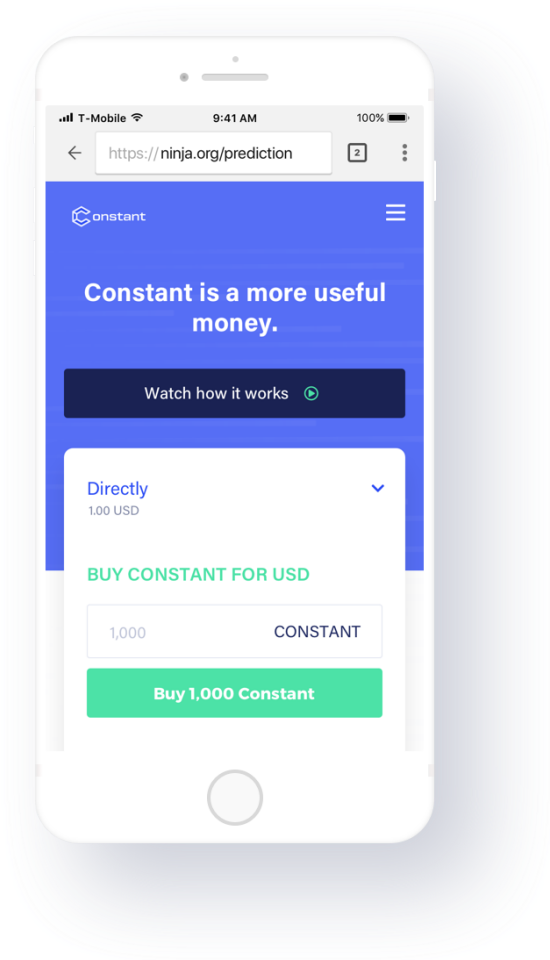
Twitter

Messenger

Facebook

Mobile

Here are some screenshots of the initial release of the Constant System on mobile.



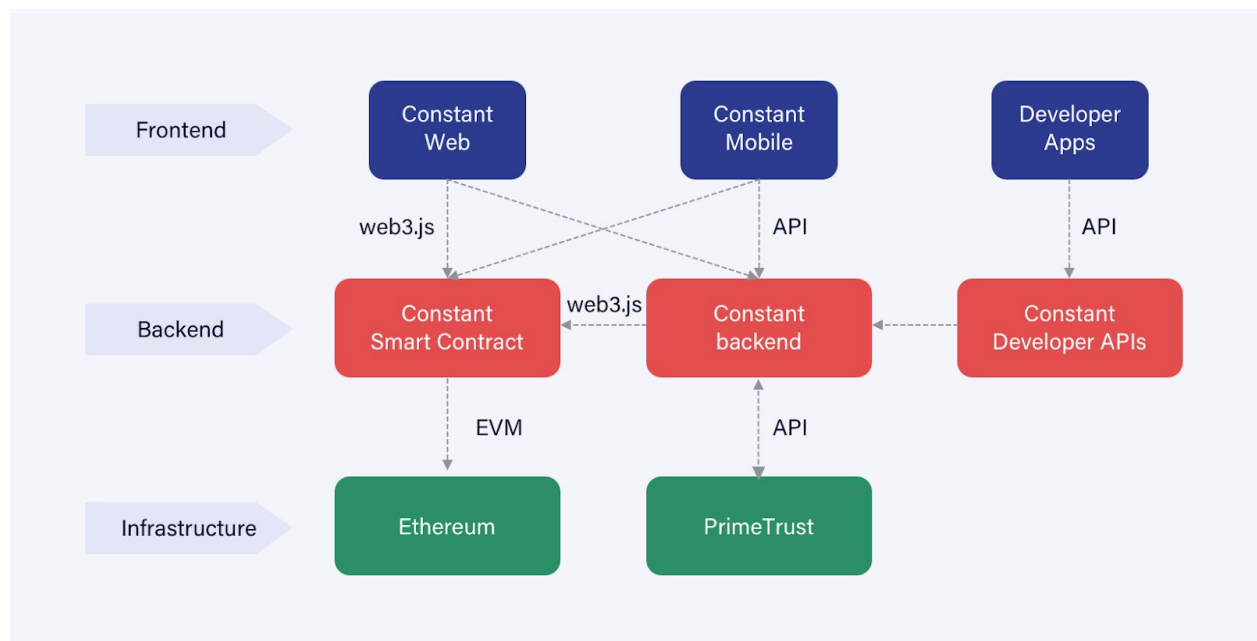
18. Open source & code architecture

Constant is open source at <https://github.com/constant-money>. Its design is public; the Constant System is built to evolve with the community.

At the infrastructure layer, Constant is built on top of the Ethereum network to enable payments, and Prime Trust API, for escrow.

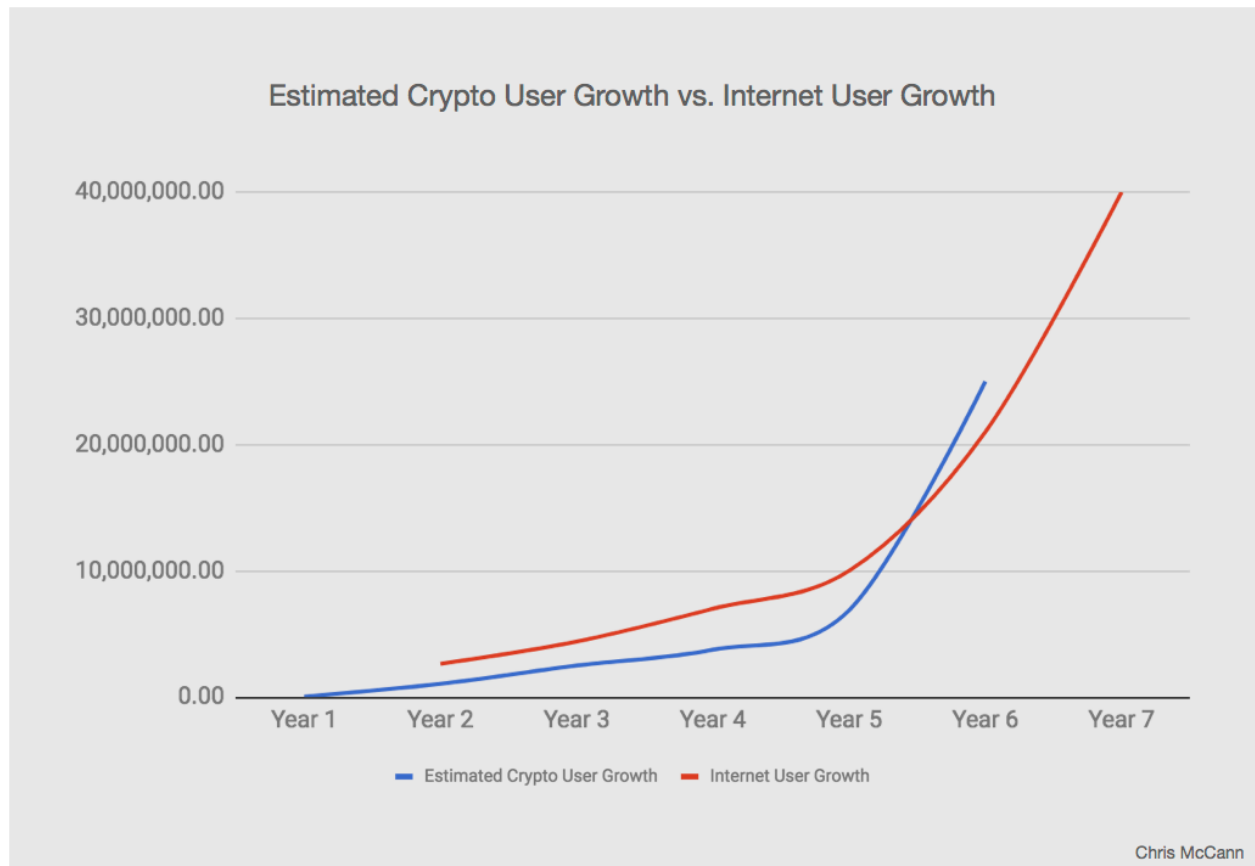
On the backend, Constant includes a number of smart contracts for minting and burning Constant. It also includes off-chain components to provide better UX. Finally, it includes a set of developer APIs to enable developers to integrate Constant into their products.

On the frontend, Constant provides both web and mobile interfaces. We hope that over time, more web and mobile apps will be built with Constant.



19. Conclusion

The Internet in 1994 looked nothing like what we have today. Blockchain's 1994 is happening right now. The volatility of currencies like Bitcoin and Ether have attracted attention to the rapidly developing, increasingly divisive crypto sphere - populating it with bright-eyed developers and early adopters, alongside a majority of speculators and traders.



There is a great deal of evolution to come before crypto proves to be ultimately useful. The volatility that characterizes the current landscape has also made the prevalent narrative of financial revolution unconvincing at best. For crypto to be the new money, we should feel secure spending it, saving it, and getting paid in it. It needs to hold its value.

The Constant System is designed to meet these essential conditions, open up bigger possibilities, and bring the world closer together. By pioneering a stable global zone in the crypto wild west, Constant hopes to lead the shift towards real world applicability. By building a freer and more useful money for anyone, anywhere, Constant hopes to help make the world go round better.

References

Andalfatto, D. 2015. *Fedcoin: On the Desirability of a Government Cryptocurrency*. Blog post.

Barrdear, J. 2016. *The Macroeconomics of Central Bank Issued Digital Currencies*. Bank of England Staff Working Paper 605.

Buterin, V. 2014. *A Next Generation Smart Contract & Decentralized Application Platform*.
<https://github.com/ethereum/wiki/wiki/White-Paper>

Dowd, K. 1992. *The Experience of Free Banking*. New York: Routledge.

Dowd, K. 2014. *New Private Monies*. The Institute of Economic Affairs.

Fisher, I. 1913. *A Compensated Dollar*. Quarterly Journal of Economics 27: 213-235.

Fisher, I. 1920. *Stabilizing the Dollar*. New York: Macmillan.

Friedman, M. 1951. *Commodity-reserve Currency*. Journal of Political Economy 59: 203-232.

Friedman, M. 1960. *A Program for Monetary Stability*. Bronx: Fordham University Press.

Hayek, F. A. 1977. *A Free-Market Monetary System*. Journal of Libertarian Studies, Volume 3, Number 1. . <https://mises.org/daily/3204>

Hayek, F. A. 1977. *Denationalisation of Money*. The Institute of Economic Affairs.
<https://mises.org/books/denationalisation.pdf>

Jentzsch, C. 2016. *Decentralized Autonomous Organization*.
<https://download.slock.it/public/DAO/WhitePaper.pdf>

Merkle, R.C. 1980. *Protocols for public key cryptosystems*. In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133.

Nakamoto, S. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*.
www.bitcoin.org/bitcoin.pdf

Rogoff, K. 2014. *Costs and benefits to phasing out paper currency*. Presented at NBER Macroeconomics Annual Conference.

Sams, R. 2014. *A Note on Cryptocurrency Stabilisation: Seigniorage Shares*.
<https://github.com/rmsams/stablecoins/blob/master/paper.pdf>