The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System

Download PDF English

Abstract

The Maker Protocol, also known as the Multi-Collateral Dai (MCD) system, allows users to generate Dai by leveraging collateral assets approved by "Maker Governance." Maker Governance is the community organized and operated process of managing the various aspects of the Maker Protocol. Dai is a decentralized, unbiased, collateral-backed cryptocurrency soft-pegged to the US Dollar. Resistant to hyperinflation due to its low volatility, Dai offers economic freedom and opportunity to anyone, anywhere.

This white paper is a reader-friendly description of the Protocol, which is built on the Ethereum blockchain. Technically savvy users might want to head directly to Introduction to the Maker Protocol in the Maker Documentation Portal for an in-depth explanation of the entire system.

About MakerDAO

MakerDAO is an open-source project on the Ethereum blockchain and a Decentralized Autonomous Organization[1] created in 2014. The project is managed by people around the world who hold its governance token, MKR. Through a system of scientific governance involving Executive Voting and Governance Polling, MKR holders manage the Maker Protocol and the financial risks of Dai to ensure its stability, transparency, and efficiency. MKR voting weight is proportional to the amount of MKR a voter stakes in the voting contract, DSChief. In other words, the more MKR tokens locked in the contract, the greater the voter's decision-making power.

About the Maker Protocol

The Maker Protocol, built on the Ethereum blockchain,[2] enables users to create currency. Current elements of the Maker Protocol are the Dai stablecoin, Maker Collateral Vaults, Oracles, and Voting. MakerDAO governs the Maker Protocol by deciding on key parameters (e.g., stability fees, collateral types/rates, etc.) through the voting power of MKR holders.

The Maker Protocol, one of the largest decentralized applications (dapps) on the Ethereum blockchain, was the first decentralized finance (DeFi) application to earn significant adoption.

About the Maker Foundation

The Maker Foundation, which is part of the global Maker community, built and launched the Maker Protocol in conjunction with a number of outside partners. It is currently working with the MakerDAO community to bootstrap decentralized governance of the project and drive it toward complete decentralization.

About the Dai Foundation

The Dai Foundation, based in Denmark, is self-governing and independent of the Maker Foundation. It was formed to house the Maker community's key intangible assets, such as trademarks and code copyrights, and it operates solely on the basis of objective and rigid statutes that define its mandate. Its purpose, as noted in the Dai Foundation Trust Deed, is to safeguard what cannot be technologically decentralized in the Maker Protocol.

Introduction

Beginning in 2015, the MakerDAO project operated with developers around the globe working together on the first iterations of code, architecture, and documentation. In December 2017, the first MakerDAO formal white paper was published, introducing the original Dai (now Sai) Stablecoin System.

The white paper described how anyone could generate Dai using that system by leveraging Ethereum (ETH) as collateral through unique smart contracts known as Collateralized Debt Positions (CDPs). Given that ETH was the only collateral asset accepted by the system, the Dai generated was called Single-Collateral Dai (SCD), or Sai. That white paper also included a plan to upgrade the system to support multiple collateral asset types in addition to ETH. What was then an intention, became a reality in November 2019.

The Dai Stablecoin System, today called the Maker Protocol, now accepts as collateral any Ethereum-based asset that has been approved by MKR holders, who also vote on corresponding Risk Parameters for each collateral asset. Voting is a critical component of the Maker decentralized governance process.

Welcome to **Multi-Collateral Dai** (**MCD**).

In MCD We Trust

Blockchain technology provides an unprecedented opportunity to ease the public's growing frustration with—and distrust of—dysfunctional centralized financial systems. By distributing data across a network of computers, the technology allows any group of individuals to embrace transparency rather than central-entity control. The result is an unbiased, transparent, and highly efficient permissionless system—one that can improve current global financial and monetary structures and better serve the public good.

Bitcoin was created with this goal in mind. But, while Bitcoin succeeds as a cryptocurrency on a number of levels, it is not ideal as a medium of exchange because its fixed supply and speculative nature results in volatility, which prevents it from proliferating as mainstream money.

The Dai stablecoin, on the other hand, succeeds where Bitcoin fails precisely because Dai is designed to *minimize price volatility.* A decentralized, unbiased, collateral-backed cryptocurrency that is soft-pegged to the US Dollar, Dai's value is in its stability.

Since the release of Single-Collateral Dai in 2017, user adoption of the stablecoin has risen dramatically, and it has become a building block for decentralized applications that help expand the DeFi (decentralized finance) movement. Dai's success is part of a wider industry movement for stablecoins, which are cryptocurrencies designed to maintain price value and function like money.

For example, in February 2019, JPMorgan became the first bank in the United States to create and test a digital coin that represents 1 USD.[3] As the cryptocurrency industry grows, other banks, financial services companies, and even governments will create stable digital currencies (e.g., Central Bank Digital Currencies), as will large organizations outside of the finance sector. Facebook, for example, announced its plans for Libra, "a stable digital cryptocurrency that will be fully backed by a reserve of real assets,"[4] in June 2019. However, such proposals forfeit the core value proposition of blockchain technology: global adoption of a common infrastructure without a central authority or administrator that may abuse its influence.

An Overview of the Maker Protocol and Its Features

The Maker Protocol

The Maker Protocol is one of the largest dapps on the Ethereum blockchain. Designed by a disparate group of contributors, including developers within the Maker Foundation, its outside partners, and other persons and entities, it is the first decentralized finance (DeFi) application to see significant adoption.

The Maker Protocol is managed by people around the world who hold its governance token, MKR. Through a system of scientific governance involving Executive Voting and Governance Polling, MKR holders govern the Protocol and the financial risks of Dai to ensure its stability, transparency, and efficiency. One MKR token locked in a voting contract equals one vote.

The Dai Stablecoin

The Dai stablecoin is a decentralized, unbiased, collateral-backed cryptocurrency soft-pegged to the US Dollar. Dai is held in cryptocurrency wallets or within platforms, and is supported on Ethereum and other popular blockchains.

Dai is easy to generate, access, and use. Users generate Dai by depositing collateral assets into Maker Vaults within the Maker Protocol. This is how Dai is entered into circulation and how users gain access to liquidity. Others obtain Dai by buying it from brokers or exchanges, or simply by receiving it as a means of payment.

Once generated, bought, or received, Dai can be used in the same manner as any other cryptocurrency: it can be sent to others, used as payments for goods and services, and even held as savings through a feature of the Maker Protocol called the Dai Savings Rate (DSR).

Every Dai in circulation is directly backed by excess collateral, meaning that the value of the collateral is higher than the value of the Dai debt, and all Dai transactions are publicly viewable on the Ethereum blockchain.

What Properties of Dai Function Similarly to Money?

Generally, money has four functions:

1. A store of value
2. A medium of exchange
3. A unit of account
4. A standard of deferred payment

Dai has properties and use cases designed to serve these functions.

Dai as a Store of Value

A store of value is an asset that keeps its value without significant depreciation over time. Because Dai is a stablecoin, it is designed to function as a store of value even in a volatile market.

Dai as a Medium of Exchange

A medium of exchange is anything that represents a standard of value and is used to facilitate the sale, purchase, or exchange (trade) of goods or services. The Dai stablecoin is used around the world for all types of transactional purposes.

Dai as a Unit of Account

A unit of account is a standardized measurement of value used to price goods and services (e.g., USD, EUR, YEN). Currently, Dai has a target price of 1USD (1 Dai = 1 USD). While Dai is not used as a standard measurement of value in the off-chain world, it functions as a unit of account within the Maker Protocol and some blockchain dapps, whereby Maker Protocol accounting or pricing of dapp services is in Dai rather than a fiat currency like USD.

Dai as a Standard of Deferred Payment

Dai is used to settle debts within the Maker Protocol (e.g., users use Dai to pay the stability fee and close their Vaults). This benefit separates Dai from other stablecoins.

Collateral Assets

Dai is generated, backed, and kept stable through collateral assets that are deposited into Maker Vaults on the Maker Protocol. A collateral asset is a digital asset that MKR holders have voted to accept into the Protocol.

To generate Dai, the Maker Protocol accepts as collateral any Ethereum-based asset that has been approved by MKR holders. MKR holders must also approve specific, corresponding Risk Parameters for each accepted collateral (e.g., more stable assets might get more lenient Risk Parameters, while more risky assets could get stricter Risk Parameters). Detailed information on Risk Parameters is below. These and other decisions of MKR holders are made through the Maker decentralized governance process.

Maker Vaults

All accepted collateral assets can be leveraged to generate Dai in the Maker Protocol through smart contracts called Maker Vaults. Users can access the Maker Protocol and create Vaults through a number of different user interfaces (i.e., network access portals), including Oasis Borrow and various interfaces built by the community. Creating a Vault is not complicated, but generating Dai does create an obligation to repay the Dai, along with a Stability Fee, in order to withdraw the collateral leveraged and locked inside a Vault.

Vaults are inherently non-custodial: Users interact with Vaults and the Maker Protocol directly, and each user has complete and independent control over their deposited collateral as long the value of that collateral doesn't fall below the required minimum level (the Liquidation Ratio, discussed in detail below).

Interacting with a Maker Vault

- **Step 1: Create and Collateralize a Vault**
  A user creates a Vault via the Oasis Borrow portal or a community-created interface, such as Instadapp, Zerion, or MyEtherWallet, by funding it with a specific type and amount of collateral that will be used to generate Dai. Once funded, a Vault is considered collateralized.
- **Step 2: Generate Dai from the Collateralized Vault**
  The Vault owner initiates a transaction, and then confirms it in her unhosted cryptocurrency wallet in order to generate a specific amount of Dai in exchange for keeping her collateral locked in the Vault.
- **Step 3: Pay Down the Debt and the Stability Fee**
  To retrieve a portion or all of the collateral, a Vault owner must pay down or completely pay back the Dai she generated, plus the Stability Fee that continuously accrues on the Dai outstanding. The Stability Fee can only be paid in Dai.
- **Step 4: Withdraw Collateral**
  With the Dai returned and the Stability Fee paid, the Vault owner can withdraw all or some of her collateral back to her wallet. Once all Dai is completely returned and all collateral is retrieved, the Vault remains empty until the owner chooses to make another deposit.

Importantly, each collateral asset deposited requires its own Vault. So, some users will own multiple Vaults with different types of collateral and levels of collateralization.

Liquidation of Risky Maker Vaults

To ensure there is always enough collateral in the Maker Protocol to cover the value of all outstanding debt (the amount of Dai outstanding valued at the Target Price), any Maker Vault deemed too risky (according to parameters established by Maker Governance) is liquidated through automated Maker Protocol auctions. The Protocol makes the determination after comparing the Liquidation Ratio to the current collateral-to-debt ratio of a Vault. Each Vault type has its own Liquidation Ratio, and each ratio is determined by MKR voters based on the risk profile of the particular collateral asset type.

Maker Protocol Auctions

The auction mechanisms of the Maker Protocol enable the system to liquidate Vaults even when price information for the collateral is unavailable. At the point of liquidation, the Maker Protocol takes the liquidated Vault collateral and subsequently sells it using an internal market-based auction mechanism. This is a Collateral Auction.

The Dai received from the Collateral Auction is used to cover the Vault's outstanding obligations, including payment of the Liquidation Penalty fee set by MKR voters for that specific Vault collateral type.

If enough Dai is bid in the Collateral Auction to fully cover the Vault obligations plus the Liquidation Penalty, that auction converts to a Reverse Collateral Auction in an attempt to sell as little collateral as possible. Any leftover collateral is returned to the original Vault owner.

If the Collateral Auction does not raise enough Dai to cover the Vault's outstanding obligation, the deficit is converted into Protocol debt. Protocol debt is covered by the Dai in the Maker Buffer. If there is not enough Dai in the Buffer, the Protocol triggers a Debt Auction. During a Debt Auction, MKR is minted by the system (increasing the amount of MKR in circulation), and then sold to bidders for Dai.

Dai proceeds from the Collateral Auction go into the Maker Buffer, which serves as a buffer against an increase of MKR overall supply that could result from future uncovered Collateral Auctions and the accrual of the Dai Savings Rate (discussed in detail below).

If Dai proceeds from auctions and Stability Fee payments exceed the Maker Buffer limit (a number set by Maker Governance), they are sold through a Surplus Auction. During a Surplus Auction, bidders compete by bidding increasing amounts of MKR to receive a fixed amount of Dai. Once the Surplus Auction has ended, the Maker Protocol autonomously destroys the MKR collected, thereby reducing the total MKR supply.

Example (Collateral Auction Process):

A large Vault becomes undercollateralized due to market conditions. An Auction Keeper then detects the undercollateralized Vault opportunity and initiates liquidation of the Vault, which kicks off a Collateral Auction for, say, 50 ETH.

Each Auction Keeper has a bidding model to assist in winning auctions. A bidding model includes a price at which to bid for the collateral (ETH, in this example). The Auction Keeper uses the token price from its bidding model as the basis for its bids in the first phase of a Collateral Auction, where increasing Dai bids are placed for the set amount of collateral. This amount represents the price of the total Dai wanted from the collateral auction.

Now, let's say the Auction Keeper bids 5,000 Dai for the 50 ETH to meet this amount. The Dai bid is transferred from the Vault Engine to the Collateral Auction contract. With enough Dai in the Collateral Auction contract to cover the system's debt plus the Liquidation Penalty, the first phase of the Collateral Auction is over.

In order to reach the price defined in its bidding model, the Auction Keeper submits a bid in the second phase of the Collateral Auction. In this phase, the objective is to return as much of the collateral to the Vault owner as the market will allow. The bids that the Auction Keepers place are for fixed Dai amounts and decreasing amounts of ETH. For instance, the bidding model of the Keeper in this example seeks a bid price of 125 Dai per ETH, so it offers 5000 Dai for 40 ETH. Additional Dai for this bid is transferred from the Vault Engine to the Collateral Auction contract. After the bid duration limit is reached and the bid expires, the Auction Keeper claims the winning bid and settles the completed Collateral Auction by collecting the won collateral.

Key External Actors

In addition to its smart contract infrastructure, the Maker Protocol involves groups of external actors to maintain operations: Keepers, Oracles, and Global Settlers (Emergency Oracles), and Maker community members. Keepers take advantage of the economic incentives presented by the Protocol; Oracles and Global Settlers are external actors with special permissions in the system assigned to them by MKR voters; and Maker community members are individuals and organizations that provide services.

Keepers

A Keeper is an independent (usually automated) actor that is incentivized by arbitrage opportunities to provide liquidity in various aspects of a decentralized system. In the Maker Protocol, Keepers are market participants that help Dai maintain its Target Price ($1): they sell Dai when the market price is above the Target Price, and buy Dai when the market price is below the Target Price. Keepers participate in Surplus Auctions, Debt Auctions, and Collateral Auctions when Maker Vaults are liquidated.

Price Oracles

The Maker Protocol requires real-time information about the market price of the collateral assets in Maker Vaults in order to know when to trigger Liquidations.

The Protocol derives its internal collateral prices from a decentralized Oracle infrastructure that consists of a broad set of individual nodes called Oracle Feeds. MKR voters choose a set of trusted Feeds to deliver price information to the system through Ethereum transactions. They also control how many Feeds are in the set.

To protect the system from an attacker attempting to gain control of a majority of the Oracles, the Maker Protocol receives price inputs through the Oracle Security Module (OSM), not from the Oracles directly. The OSM, which is a layer of defense between the Oracles and the Protocol, delays a price for one hour, allowing Emergency Oracles or a Maker Governance vote to freeze an Oracle if it is compromised. Decisions regarding Emergency Oracles and the price delay duration are made by MKR holders.

Emergency Oracles

Emergency Oracles are selected by MKR voters and act as a last line of defense against an attack on the governance process or on other Oracles. Emergency Oracles are able to freeze individual Oracles (e.g., ETH and BAT Oracles) to mitigate the risk of a large number of users trying to withdraw their assets from the Maker Protocol in a short period of time, as they have the authority to unilaterally trigger an Emergency Shutdown.

DAO Teams

DAO teams consist of individuals and service providers, who may be contracted through Maker Governance to provide specific services to MakerDAO. Members of DAO teams are independent market actors and are not employed by the Maker Foundation.

The flexibility of Maker Governance allows the Maker community to adapt the DAO team framework to suit the services needed by the ecosystem based on real-world performance and emerging challenges.

Examples of DAO team member roles are the Governance Facilitator, who supports the communication infrastructure and processes of governance, and Risk Team members, who support Maker Governance with financial risk research and draft proposals for onboarding new collateral and regulating existing collateral.

While the Maker Foundation has bootstrapped Maker Governance to date, it is anticipated that the DAO will take full control, conduct MKR votes, and fill these varied DAO team roles in the near future.

The Dai Savings Rate

The Dai Savings Rate (DSR) allows any Dai holder to earn savings automatically and natively by locking their Dai into the DSR contract in the Maker Protocol. It can be accessed via the Oasis Save portal or through various gateways into the Maker Protocol. Users aren't required to deposit a minimum amount to earn the DSR, and they can withdraw any or all of their Dai from the DSR contract at any time.

The DSR is a global system parameter that determines the amount Dai holders earn on their savings over time. When the market price of Dai deviates from the Target Price due to changing market dynamics, MKR holders can mitigate the price instability by voting to modify the DSR accordingly:

- If the market price of Dai is above 1 USD, MKR holders can choose to gradually decrease the DSR, which will reduce demand and should reduce the market price of Dai toward the 1 USD Target Price.
- If the market price of Dai is below 1 USD, MKR holders can choose to gradually increase the DSR, which will stimulate demand and should increase the market price of Dai toward the 1 USD Target Price.

Initially, adjustment of the DSR will depend on a weekly process, whereby MKR holders first evaluate and discuss public market data and proprietary data provided by market participants, and then vote on whether an adjustment is necessary or not. The long-term plan includes implementation of the DSR Adjustment Module, an Instant Access Module that directly controls both the DSR and the Base Rate. This module allows for easy adjustment of the DSR (within strict size and frequency boundaries set by MKR holders) by an MKR holder on behalf of the larger group of MKR holders. The motivation behind this plan is to enable nimble responses to rapidly changing market conditions, and to avoid overuse of the standard governance process of Executive Voting and Governance Polling.

Governance of the Maker Protocol

Use of the MKR Token in Maker Governance

The MKR token—the governance token of the Maker Protocol—allows those who hold it to *vote* on changes to the Maker Protocol. Note that anyone, not only MKR holders, can *submit* proposals for an MKR vote.

Any voter-approved modifications to the governance variables of the Protocol will likely not take effect immediately in the future; rather, they could be delayed by as much as 24 hours if voters choose to activate the Governance Security Module (GSM). The delay would give MKR holders the opportunity to protect the system, if necessary, against a malicious governance proposal (e.g., a proposal that alters collateral parameters contrary to established monetary policies or that allows for security mechanisms to be disabled) by triggering a Shutdown.

Polling and Executive Voting

In practice, the Maker Governance process includes proposal polling and Executive Voting. Proposal polling is conducted to establish a rough consensus of community sentiment before any Executive Votes are cast. This helps to ensure that governance decisions are considered throughtfully and reached by consensus prior to the voting process itself. Executive Voting is held to approve (or not) changes to the state of the system. An example of an Executive Vote could be a vote to ratify Risk Parameters for a newly accepted collateral type.

At a technical level, smart contracts manage each type of vote. A Proposal Contract is a smart contract with one or more valid governance actions programmed into it. It can only be executed once. When executed, it immediately applies its changes to the internal governance variables of the Maker Protocol. After execution, the Proposal Contract cannot be reused.

Any Ethereum Address can deploy valid Proposal Contracts. MKR token holders can then cast approval votes for the proposal that they want to elect as the Active Proposal. The Ethereum address that has the highest number of approval votes is elected as the Active Proposal. The Active Proposal is empowered to gain administrative access to the internal governance variables of the Maker Protocol, and then modify them.

The MKR Token's Role in Recapitalization

In addition to its role in Maker Governance, the MKR token has a complementary role as the recapitalization resource of the Maker Protocol. If the system debt exceeds the surplus, the MKR token supply may increase through a Debt Auction (see above) to recapitalize the system. This risk inclines MKR holders to align and responsibly govern the Maker ecosystem to avoid excessive risk-taking.

MKR Holder Responsibilities

MKR holders can vote to do the following:

- Add a new collateral asset type with a unique set of Risk Parameters.
- Change the Risk Parameters of one or more existing collateral asset types, or add new Risk Parameters to one or more existing collateral asset types.
- Modify the Dai Savings Rate.
- Choose the set of Oracle Feeds.
- Choose the set of Emergency Oracles.
- Trigger Emergency Shutdown.
- Upgrade the system.

MKR holders can also allocate funds from the Maker Buffer to pay for various infrastructure needs and services, including Oracle infrastructure and collateral risk management research. The funds in the Maker Buffer are revenues from Stability Fees, Liquidation Fees, and other income streams.

The governance mechanism of the Maker Protocol is designed to be as flexible as possible, and upgradeable. Should the system mature under the guidance of the community, more advanced forms of Proposal Contracts could, in theory, be used, including Proposal Contracts that are bundled. For example, one proposal contract may contain both an adjustment of a Stability Fee and an adjustment of the DSR. Nonetheless, those revisions will remain for MKR holders to decide.

Risk Parameters Controlled by Maker Governance

Each Maker Vault type (e.g., ETH Vault and BAT Vault) has its own unique set of Risk Parameters that enforce usage. The parameters are determined based on the risk profile of the collateral, and are directly controlled by MKR holders through voting.

The Key Risk Parameters for Maker Vaults are:

- **Debt Ceiling**: A Debt Ceiling is the maximum amount of debt that can be created by a single collateral type. Maker Governance assigns every collateral type a Debt Ceiling, which is used to ensure sufficient diversification of the Maker Protocol collateral portfolio. Once a collateral type has reached its Debt Ceiling, it becomes impossible to create more debt unless some existing users pay back all or a portion of their Vault debt.

- **Stability Fee**: The Stability Fee is an annual percentage yield calculated on top of how much Dai has been generated against a Vault's collateral. The fee is paid in Dai only, and then sent into the Maker Buffer.
- **Liquidation Ratio**: A low Liquidation Ratio means Maker Governance expects low price volatility of the collateral; a high Liquidation Ratio means high volatility is expected.
- **Liquidation Penalty**: The Liquidation Penalty is a fee added to a Vault's total outstanding generated Dai when a Liquidation occurs. The Liquidation Penalty is used to encourage Vault owners to keep appropriate collateral levels.
- **Collateral Auction Duration**: The maximum duration of Collateral auctions is specific to Maker Vaults. Debt and Surplus auction durations are global system parameters.
- **Auction Bid Duration**: Amount of time before an individual bid expires and closes the auction.
- **Auction Step Size**: This Risk Parameter exists to incentivize early bidders in auctions, and prevent abuse by bidding a tiny amount above an existing bid.

Risk and Mitigation Responsibilities of Governance

The successful operation of the Maker Protocol depends on Maker Governance taking necessary steps to mitigate risks. Some of those risks are identified below, each followed by a mitigation plan.

A malicious attack on the smart contract infrastructure by a bad actor.

One of the greatest risks to the Maker Protocol is a malicious actor—a programmer, for example, who discovers a vulnerability in the deployed smart contracts, and then uses it to break the Protocol or steal from it.

In the worst-case scenario, all decentralized digital assets held as collateral in the Protocol are stolen, and recovery is impossible.

Mitigation: The Maker Foundation's highest priority is the security of the Maker Protocol, and the strongest defense of the Protocol is Formal Verification. The Dai codebase was the first codebase of a decentralized application to be formally verified.

In addition to formal system verification, contracted security audits by the best security organizations in the blockchain industry, third-party (independent) audits, and bug bounties are part of the Foundation's security roadmap. To review the formal verification report and various Maker Protocol audits, visit Maker's Multi-Collateral Dai Security Github repository.

These security measures provide a strong defense system; however, they are not infallible. Even with formal verification, the mathematical modeling of intended behaviors may be incorrect, or the assumptions behind the intended behavior itself may be incorrect.

A black swan event

A black swan event is a rare and critical surprise attack on a system. For the Maker Protocol, examples of a black swan event include:

- An attack on the collateral types that back Dai.
- A large, unexpected price decrease of one or more collateral types.
- A highly coordinated Oracle attack.
- A malicious Maker Governance proposal.

Please note that this list of potential "black swans" is not exhaustive and not intended to capture the extent of such possibilities.

Mitigation: While no one solution is failsafe, the careful design of the Maker Protocol (the Liquidation Ratio, Debt Ceilings, the Governance Security Module, the Oracle Security Module, Emergency Shutdown, etc.) in conjunction with good governance (e.g., swift reaction in a crisis, thoughtful risk parameters, etc.) help to prevent or mitigate potentially severe consequences of an attack.

Unforeseen pricing errors and market irrationality

Oracle price feed problems or irrational market dynamics that cause variations in the price of Dai for an extended period of time can occur. If confidence in the system is lost, rate adjustments or even MKR dilution could reach extreme levels and still not bring enough liquidity and stability to the market.

Mitigation: Maker Governance incentivizes a sufficiently large capital pool to act as Keepers of the market in order to maximize rationality and market efficiency, and allow the Dai supply to grow at a steady pace without major market shocks. As a last resort, Emergency Shutdown can be triggered to release collateral to Dai holders, with their Dai claims valued at the Target Price.

User Abandonment for Less Complicated Solutions

The Maker Protocol is a complex decentralized system. As a result of its complexity, there is a risk that inexperienced cryptocurrency users will abandon the Protocol in favor of systems that may be easier to use and understand.

Mitigation: While Dai is easy to generate and use for most crypto enthusiasts and the Keepers that use it for margin trading, newcomers might find the Protocol difficult to understand and navigate. Although Dai is designed in such a way that users need not comprehend the underlying mechanics of the Maker Protocol in order to benefit from it, the documentation and numerous resources consistently provided by the Maker community and the Maker Foundation help to ensure onboarding is as uncomplicated as possible.

Dissolution of The Maker Foundation

The Maker Foundation currently plays a role, along with independent actors, in maintaining the Maker Protocol and expanding its usage worldwide, while facilitating Governance. However, the Maker Foundation plans to dissolve once MakerDAO can manage Governance completely on its own. Should MakerDAO fail to sufficiently take the reins upon the Maker Foundation's dissolution, the future health of the Maker Protocol could be at risk.

Mitigation: MKR holders are incentivized to prepare for the Foundation's dissolution after it completes "gradual decentralization" of the project. Moreover, successful management of the system should result in sufficient funds for governance to allocate to the continued maintenance and improvement of the Maker Protocol.

General Issues with Experimental Technology

Users of the Maker Protocol (including but not limited to Dai and MKR holders) understand and accept that the software, technology, and technical concepts and theories applicable to the Maker Protocol are still unproven and there is no warranty that the technology will be uninterrupted or error-free. There is an inherent risk that the technology could contain weaknesses, vulnerabilities, or bugs causing, among other things, the complete failure of the Maker Protocol and/or its component parts.

Mitigation: See "A malicious attack on the smart contract infrastructure by a bad actor" above. The Mitigation section there explains the technical auditing in place to ensure the Maker Protocol functions as intended.

Price Stability Mechanisms

The Dai Target Price

The Dai Target Price is used to determine the value of collateral assets Dai holders receive in the case of an Emergency Shutdown. The Target Price for Dai is 1 USD, translating to a 1:1 USD soft peg.

Emergency Shutdown

Emergency Shutdown (or, simply, Shutdown) serves two main purposes. First, it is used during emergencies as a last-resort mechanism to protect the Maker Protocol against attacks on its infrastructure and directly enforce the Dai Target Price. Emergencies could include malicious governance actions, hacking, security breaches, and long-term market irrationality. Second, Shutdown is used to facilitate a Maker Protocol system upgrade. The Shutdown process can only be controlled by Maker Governance.

MKR voters are also able to instantly trigger an Emergency Shutdown by depositing MKR into the Emergency Shutdown Module (ESM), if enough MKR voters believe it is necessary. This prevents the Governance Security Module (if active) from delaying Shutdown proposals before they are executed. With Emergency Shutdown, the moment a quorum is reached, the Shutdown takes effect with no delay.

There are three phases of Emergency Shutdown:

1. **The Maker Protocol shuts down**; **Vault owners withdraw assets.**
   When initiated, Shutdown prevents further Vault creation and manipulation of existing Vaults, and freezes the Price Feeds. The frozen feeds ensure that all users are able to withdraw the net value of assets to which they are entitled. Effectively, it allows Maker Vault owners to immediately withdraw the collateral in their Vault that is not actively backing debt.
2. **Post-Emergency Shutdown auction processing**
   After Shutdown is triggered, Collateral Auctions begin and must be completed within a specific amount of time. That time period is determined by Maker Governance to be slightly longer than the duration of the longest Collateral Auction. This guarantees that no auctions are outstanding at the end of the auction processing period.
3. **Dai holders claim their remaining collateral**
   At the end of the auction processing period, Dai holders use their Dai to claim collateral directly at a fixed rate that corresponds to the calculated value of their assets based on the Dai Target Price. For example, if the ETH/USD Price Ratio is 200, and a user holds 1000 Dai at the Target Price of 1 USD when Emergency Shutdown is activated, The user will be able to claim exactly 5 ETH from the Maker Protocol after the auction processing period. There is no time limit for when a final claim can be made. Dai holders will get a proportional claim to each collateral type that exists in the collateral portfolio. Note that Dai holders could be at risk of a haircut, whereby they do not receive the full value of their Dai holdings at the Target Price of 1 USD per Dai. This is due to risks related to declines in collateral value and to Vault owners having the right to retrieve their excess collateral before Dai holders may claim the remaining collateral. For more detailed information on Emergency Shutdown, including the claim priorities that would occur as a result, see the published community documentation.

The Future of the Maker Protocol: Increased Adoption and Full Decentralization

Addressable Market

A cryptocurrency with price stability serves as an important medium of exchange for many decentralized applications. As such, the potential market for Dai is at least as large as the entire decentralized blockchain industry. But the promise of Dai extends well beyond that into other industries.

The following is a non-exhaustive list of current and immediate markets for the Dai stablecoin:

- **Working capital, hedging, and collateralized leverage**. Maker Vaults allow for permissionless trading by users, who can use the Dai generated against Vault collateral for working capital. To date, there have been numerous instances where Vault owners use their Dai to buy additional ETH (same asset as their collateral), thereby creating a leveraged but fully collateralized position.
- **Merchant receipts, cross-border transactions, and remittances**. Foreign exchange volatility mitigation and a lack of intermediaries mean the transaction costs of international trade are significantly reduced when using Dai.

- **Charities and NGOs** when using transparent distributed ledger technology.
- **Gaming**. For blockchain game developers, Dai is the currency of choice. With Dai, game developers integrate not only a currency, but also an entire economy. The composability of Dai allows games to create new player behavior schemes based around decentralized finance.
- **Prediction markets**. Using a volatile cryptocurrency when making an unrelated prediction only increases one's risk when placing the bet. Long-term bets become especially infeasible if the bettor must also gamble on the future price of the volatile asset used to place the bet. That said, the Dai stablecoin would be a natural choice for use in prediction markets.

Asset Expansion

Should MKR holders approve new assets as collateral, those assets will be subject to the same risk requirements, parameters, and safety measures as Dai (e.g., Liquidation Ratios, Stability Fees, Savings Rates, Debt Ceilings, etc.).

Evolving Oracles

MakerDAO was the first project to run reliable Oracles on the Ethereum blockchain. As a result, many decentralized applications use MakerDAO Oracles to ensure the security of their systems and to provide up-to-date price data in a robust manner. This confidence in MakerDAO and the Maker Protocol means that Maker Governance can expand the core Oracle infrastructure service to better suit the needs of decentralized applications.

Conclusion

The Maker Protocol allows users to generate Dai, a stable store of value that lives entirely on the blockchain. Dai is a decentralized stablecoin that is not issued or administered by any centralized actor or trusted intermediary or counterparty. It is unbiased and borderless — available to anyone, anywhere.

All Dai is backed by a surplus of collateral that has been individually escrowed into audited and publicly viewable Ethereum smart contracts. Anyone with an internet connection can monitor the health of the system anytime at daistats.com.

With hundreds of partnerships and one of the strongest developer communities in the cryptocurrency space, MakerDAO has become the engine of the decentralized finance (DeFi) movement. Maker is unlocking the power of the blockchain to deliver on the promise of economic empowerment today.

For more information, visit the MakerDAO website.

APPENDIX

Dai Use-Case Benefits and Examples

The Maker Protocol can be used by anyone, anywhere, without any restrictions or personal-information requirements. Below are a few examples of how Dai is used around the world:

Dai Offers Financial Independence to All

According to the World Bank's Global Findex Database 2017, about 1.7 billion adults around the world are unbanked.[5] In the US alone, according to a 2017 survey by the FDIC, around 32 million American households are either unbanked or underbanked,[6] meaning that they either have no bank account at all or they regularly use alternatives to traditional banking (e.g., payday or pawn shop loans) to manage their finances. Dai can empower every one of those people; all they need is access to the internet.

As the world's first unbiased stablecoin, Dai allows anyone to achieve financial independence, regardless of their location or circumstances. For example, in Latin America, Dai has provided an opportunity for individuals and families to hedge against the devaluation of the Argentine peso[7] and the Venezuelan bolívar. On the islands of Vanuatu in the South Pacific, where residents pay very high money transfer fees, Oxfam International, a U.K.-based non-profit; Australian startup, Sempo; and Ethereum startup ConsenSys have successfully piloted a cash-assistance program through which 200 residents on the island of Efate were each given 50 Dai to pay a local network of vendors.[8]

Self-Sovereign Money Generation

Oasis Borrow allows users to access the Maker Protocol and generate Dai by locking their collateral in a Maker Vault. Notably, users do not need to access any third-party intermediary to generate Dai. Vaults offer individuals and businesses opportunities to create liquidity on their assets simply, quickly, and at relatively low cost.

Savings Earned Automatically

Dai holders everywhere can better power their journeys to financial inclusion by taking advantage of the Dai Savings Rate, which, as detailed earlier, builds on the value of Dai by allowing users to earn on the Dai they hold and protect their savings from inflation.

For example, if Bob has 100,000 Dai locked in the DSR contract, and the DSR set by Maker Governance is 6% per year, Bob will earn savings of 6,000 Dai over 12 months. Additionally, because exchanges and blockchain projects can integrate the DSR into their own platforms, it presents new opportunities for cryptocurrency traders, entrepreneurs, and established businesses to increase their Dai savings and Dai operating capital. Due to this attractive mechanism, Market Makers, for example, may choose to hold their idle inventory in Dai and lock it in the DSR.

Fast, Low-cost Remittances

Cross-border remittances, whether for the purchase of goods or services or to simply send money to family and friends, can mean high service and transfer fees, long delivery timelines, and frustrating exchange issues due to inflation. The Dai stablecoin is used around the world as a medium of exchange because people have confidence in its value and efficiency.

Remittance users benefit from Dai in the following ways:

- **Low-cost domestic and international transfers.** Dai provides immediate cost savings, as low gas fees replace high bank and wire service fees. Low cost allows for more frequent transactions.
- **Anytime service.** Dai doesn't rely on bank-like hours of operation. The Maker Protocol can be accessed 24/7/365.
- **Convenient on/off ramps.** Users can take advantage of the many fiat on and off ramps that exchange fiat currencies to Dai. These options allow users to bridge the gap between the fiat and cryptocurrency world, and easily cash out Dai holdings in their local currencies.
- **Increased security and confidence.** The blockchain offers high levels of security and consumer trust.

Stability in Volatile Markets

As noted above, Dai is both a readily accessible store of value and a powerful medium of exchange. As such, it can help protect traders from volatility. For example, it provides traders with a simple way to maneuver between positions smoothly and remain active in the market without having to cash out and repeat an on-ramp/off-ramp cycle.

Dai as an Ecosystem Driver and DeFi Builder

As more and more users become aware of Dai's value as a stablecoin, more developers are integrating it into the dapps they build on the Ethereum blockchain. As such, Dai is helping to power a more robust ecosystem. In short, Dai allows dapp developers to offer a stable method of exchange to their users who would rather not buy and sell goods and services using speculative assets.

Additionally, because Dai can be used to pay for gas in the Ethereum ecosystem, by creating DeFi dapps that accept Dai instead of ETH, developers offer users a smoother onboarding experience and a better overall experience.

Glossaries

- MakerDAO Glossary of Terms
- Maker Protocol Glossary (terms, variables, functions, and more)

System and Community Resources

- MakerDAO on GitHub
- MakerDAO Documentation
- MakerDAO.com
- The MakerDAO Blog
- The MakerDAO Forum
- The MakerDAO Chat
- MakerDAO on Reddit
- MakerDAO on Twitter

Notes

1. Note that Decentralized Autonomous Organizations, or DAOs, are understood in the Ethereum community as largely social and technical communities centered around a particular mission or project, and does not necessarily imply the existence of traditional corporate forms. ↩
2. https://ethereum.org/ ↩
3. https://www.jpmorgan.com/global/news/digital-coin-payments ↩
4. https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper*en*US.pdf ↩
5. https://globalfindex.worldbank.org/ ↩
6. https://www.fdic.gov/householdsurvey/ ↩
7. https://slideslive.com/38920018/living-on-defi-how-i-survive-argentinas-50-inflation ↩
8. https://www.coindesk.com/oxfam-trials-delivery-of-disaster-relief-using-ethereum-stablecoin-dai ↩