permalink: / layout: page

title: Dai Stablecoin System Simplified, v0.8

The Dai Stablecoin System

https://makerdao.com/

Rune Christensen, Nikolai Mushegian, Daniel Brockman, Kenny Rowe, Andy Milenius, Ryan Zurrer

This is a condensed overview of the Dai Stablecoin System as defined in the "Purple Paper": https://makerdao.com/purple. The Purple Paper is a formal specification and reference implementation that is modified by an RFC process.

Abstract

We propose a new cryptocurrency called Dai that is backed by escrowed collateral and has its price stabilized against major world currencies. Dai is generated by users through the Maker platform, a decentralized application that runs on the Ethereum blockchain. The Maker platform guarantees that Dai can only be generated when a user posts an excess of Ethereum-based digital assets as collateral. After being generated, the dai can be sold off and enter circulation. An autonomous feedback mechanism continuously modifies the incentives for generating and holding Dai, matching supply with demand to stabilize the market price of Dai against shocks. The systemic risk of the aggregate collateral portfolio is managed by holders of a separate digital asset called MKR, which governs the Maker platform by direct vote. MKR also acts as an access token to the Maker system: Fees accrued by generating Dai can only be paid in MKR. If the system becomes insolvent due to crash in the value of some of its collateral, new MKR is automatically minted and sold off to cover the shortfall. This gives MKR holders a strong incentive to govern the system well.

Introduction

The blockchain revolution has long been touted as the key to many seemingly intractable global problems, from mundane topics like international remittances to lofty ambitions like global financial inclusion. However, the process of mainstream adoption has been slow due to one harsh reality: price volatility of decentralized digital assets.

A cryptocurrency with price stability is a crucial component of the blockchain economy, as the majority of interesting Decentralized Applications require a stable medium of exchange to be usable. Popular digital assets such as Bitcoin (BTC) and Ether (ETH) are too volatile to allow individuals and businesses plan long term activities. Therefore, it will be necessary to have cryptocurrencies with price stability before widespread adoption of blockchain technology can

occur.

While there are a range of projects in the blockchain space aiming to create a cryptocurrency with price stability, the majority use a centralized custodian of the funds. This erases many of the benefits offered by the decentralized platforms on which they are used, limiting their ability to interconnect and synergize in a permissionless manner. For a cryptocurrency with price stability to fit coherently into the decentralized ecosystem, it must adhere to the principles of decentralization.

Hayek postulates that the most successful form of money in an economy of competing private currencies would be the one with the most stable value, i.e. the one that has least volatility against a consumer price index. For this reason, it is important that a cryptocurrency with price stability is optimized for price stability and economic efficiency above all else. It is this principle that has guided the design of the Dai Stablecoin System.

Basic Mechanics

Dai is a cryptocurrency backed by other digital assets as collateral. Regular users of Dai can use it as money without having to interact with the advanced mechanics of the Dai Stablecoin System. From their point of view, Dai will just be another cryptocurrency obtained from a cryptocurrency exchange or broker, but with the unique feature of having price stability.

Any user that has collateral assets can generate Dai. The collateral assets are then cryptographically locked inside the Dai Stablecoin System. The collateral and Dai-denominated debt becomes locked in a smart contract called a Collateralized Debt Position (CDP); the collateral can only be retrieved if the CDP user pays down the debt of the CDP, by burning an equivalent amount of Dai. CDPs are owned by Ethereum accounts, and can be freely transferred to other users like any digital asset. However, CDPs are not fungible with each other.

Immediately after generating Dai through a CDP, the CDP user will sell it on the market to regular stability-seeking users who demand Dai for use as money. Hence, CDP users are not themselves interested in price stability. On the contrary, they are seeking leveraged exposure to the assets used as collateral in their CDP (see Example 2 below for an explanation on how leverage is achieved with CDPs).

The solvency of the Dai Stablecoin System is protected by a set of Risk Parameters, which are directly controlled by holders of the MKR digital asset through voting - one MKR gives one vote.

The price of Dai in the open market is kept stable around a variable Target Price, denominated in SDR. At launch the Target Price is initially set to be equal to approximately 1 USD (~0.75 SDR).

The stability of the Dai around the Target Price is maintained by a fully automatic subsystem, known as the Target Rate Feedback Mechanism, which continuously modifies the incentives for generating and holding Dai. This feedback mechanism dampens the volatility of Dai and enables it to maintain liquidity even during demand shocks.

As such, Dai is not a pegged currency: it does not maintain a constant peg to an existing fiat

currency. Rather, it is a free-floating currency that experiences low volatility against other currencies, comparable to the volatility of major currency pairs such as USD vs EUR (although Dai will likely be more volatile during its early stages).

Liquidation and Shoring-up Liquidity

To ensure there is always enough collateral in the system to cover the value of all outstanding Dai (according to the Target Price), a CDP can be liquidated if it is deemed too risky. The Dai Stablecoin System decides when to liquidate a CDP by comparing a Risk Parameter called the Liquidation Ratio with the actual collateral-to-debt ratio of the CDP.

Each type of collateral asset has its own unique Liquidation Ratio controlled by MKR voters and decided based on the risk profile of that particular asset. The Dai Stablecoin System uses Oracles to measure the market price of collateral held in CDPs. Oracles are trusted external actors tasked with providing continuous price data.

Liquidation means that the Dai Stablecoin System automatically buys the collateral of the CDP and subsequently sells it off in an automatic auction. The auction mechanism enables the system to settle CDPs even when price information is unavailable.

In order for the system to take over the collateral of the CDP so it can be sold off, it first needs to raise enough Dai to cover the CDP debt. This is called a Debt Auction, and works by diluting the supply of the MKR digital asset and selling it to the bidders of the Debt Auction. In this auction, the system is trying to dilute MKR as little as possible while still covering the debt.

In parallel, the collateral of the CDP is sold off in a Collateral Auction where all proceeds (also denominated in Dai) up to the CDP debt amount plus a Liquidation Penalty (another Risk Parameter determined by MKR voting) is used to buy up MKR and burn it (directly counteracting the MKR dilution that happened during the Debt Auction). If enough Dai is bid to fully cover the CDP debt plus the Liquidation Penalty, the Collateral Auction switches to a reverse bid mechanism and tries to sell as little collateral as possible; any leftover collateral is returned to the original owner of the CDP.

CDPs continually accumulate a Stability Fee which is calculated from their current debt at a rate determined by the Stability Fee risk parameter for that particular CDP type. The Stability Fee has to paid when the CDP user wants to close the CDP and retrieve their collateral. The Stability Fee is accounted for in Dai, and is paid by burning an amount of MKR with equivalent value according to a price feed. There is no other way to pay the fee than with MKR, and this functionality is what gives MKR value, since it means that MKR is required to utilize the advanced features of the Dai Stablecoin System.

Liquidations aren't guaranteed to be profitable even if triggered when the collateral-to-debt ratio of the CDP is positive. Slippage during a market crash could cause the Collateral Auction to burn less MKR than what was diluted from the Debt Auction, resulting in net loss for MKR holders due to a net increase of the MKR supply.

Target Price, Target Rate, and the Sensitivity Parameter

The Dai Target Price is used to determine the collateral-to-debt ratio of a CDP, and thus the Target Price represents the price at which Dai is backed by collateral in the long term. The Target Price is continuously adjusted according to the current Target Rate. Automatic Target Rate adjustments ensure that the Dai market price remains stabilized around the Target Price in the short term.

When the market price of Dai is below the Target Price, the Target Rate increases. This causes the Target Price to increase at a higher rate, causing generation of Dai to become more expensive. This leads to CDP users covering their CDPs and leaving the ecosystem, causing the outstanding supply of Dai to decrease. At the same time, the increased Target Rate causes the capital gains from holding Dai to increase, leading to a corresponding increase in Dai demand. This combination of reduced supply and increased demand causes the Dai market price to increase, pushing it up towards the Target Price.

The same mechanism works in reverse if the Dai market price is higher than the Target Price: the Target Rate decreases, leading to an increased demand for generating Dai and a decreased demand for holding it. This causes the Dai market price to decrease, pushing it down towards the Target Price.

This mechanism is a negative feedback loop: Deviation away from the Target Price in one direction increases the force in the opposite direction. The magnitude of the Target Rate adjustments depends on how long the market price remains on the same side of the Target Price. Longer deviations result in aggressive adjustments, while shorter deviations result in small adjustments.

The Target Price and the Target Rate are entirely determined by market dynamics, and thus not directly controlled by MKR voters. Voters can only set the feedback mechanism's Sensitivity Parameter. This is a global parameter that determines the magnitude of target rate change in response to Dai target/market price deviation, which allows tuning the rate of feedback to the scale of the system. The Sensitivity Parameter is not considered a Risk Parameter because it does not impact Dai solvency.

Risk Management of The Dai Stablecoin System

The MKR asset allows holders to vote to perform the following Risk Management actions:

- Add new CDP type: Creates a new CDP type with a unique set of Risk Parameters.
- Modify existing CDP types: Change the Risk Parameters of one or more Existing CDP types that were already added.
- Modify the Sensitivity Parameter.
- Choose the set of trusted oracles. The Dai Stablecoin System derives its internal prices for collateral, the market price of Dai, and the market price of MKR based on the median of the values given by the set of trusted oracles. This ensures consistent operation of the system even in the event that up to half of the oracles suffer a technical failure.

Risk Parameters

Collateralized Debt Positions of The Dai Stablecoin System have multiple Risk Parameters. Each CDP Type has its own unique set of Risk Parameters, and these parameters are determined based on the risk profile of the collateral used by the CDP Type. The parameters are directly controlled by MKR holders through voting, with one MKR giving its holder one vote.

Debt Ceiling

Debt ceiling is the maximum amount of debt that can be created by a single type of CDP. Once enough debt has been created by CDPs of a given type, it becomes impossible to create more unless existing CDPs are closed. The debt ceiling is used to ensure sufficient diversification of the collateral portfolio.

Liquidation Ratio

Liquidation ratio is the collateral-to-debt ratio at which a CDP becomes vulnerable to Liquidation. A low Liquidation Ratio means MKR voters expect low price volatility of the collateral, while a high Liquidation Ratio means high volatility is expected.

Stability Fee

The Stability Fee is a fee paid by every CDP. It is defined as a yearly percentage that is calculated on top of the existing debt of the CDP, accounted for in Dai. When the CDP user closes their CDP they have to pay the stability fee by burning an amount of MKR that has equivalent value to the fee, calculated according to a price feed.

Penalty Ratio

The penalty ratio is used to determined the maximum amount of Dai raised from a Collateral Auction that is used to buy and burn MKR, in order to counteract the MKR dilution caused by the Debt Auction. Any leftover collateral is left in the CDP. The penalty ratio is used to cover the inefficiency of the liquidation mechanism.

Limbo Duration

A CDP enters limbo in the unlikely event that price information for collateral is not available (such as if all the oracles simultaneously suffer a technical failure). The limbo duration determines how long before all CDPs of that type can be liquidated.

Examples

The Dai Stablecoin System can be used by anyone with collateral without any further restrictions or sign-up process.

Example 1: Bob wants to generate 100 Dai. He locks an amount of ETH worth significantly more than 100 Dai into a CDP and uses it to generate 100 Dai. The 100 Dai is instantly sent directly to his

Ethereum account. Assuming that the Stability Fee is 1% per year, Bob will need to pay 100 Dai to cover the CDP, and pay 1 Dai worth of MKR, if he decides to retrieve his ETH after one year.

One of the primary use cases of CDPs is margin trading by CDP users.

Example 2: Bob wishes to go margin long on the ETH/Dai pair, so he generates 100 SDR worth of Dai by posting 150 SDR worth of ETH to a CDP. He then buys another 100 SDR worth of ETH with his newly generated Dai putting him at a net 1.66x ETH/SDR exposure. He's free to do whatever he wants with the 100 SDR worth of ETH he obtained by selling the Dai, while the original ETH collateral (150 SDR worth) remains locked in the CDP until the debt plus the Stability Fee is covered.

Although CDPs are not fungible with each other, the ownership of a CDP is transferable. This allows CDPs to be used in smart contracts that perform more complex methods of Dai generation (for example, involving more than one actor).

Example 3: Alice and Bob collaborate using an Ethereum OTC contract to issue 100 SDR worth of Dai backed by ETH. Alice contributes 50 SDR worth of ETH, while Bob contributes 100 SDR worth. The OTC contract takes the funds and creates a CDP, thus generating 100 SDR worth of Dai. The newly generated Dai are automatically sent to Bob. From Bob's point of view, he is buying 100 SDR worth of Dai by paying the equivalent value in ETH. The contract also transfers ownership of the CDP to Alice. She ends up with 100 SDR worth of debt (denominated in Dai) and 150 SDR worth of ETH (locked in the CDP). Since she started with only 50 SDR worth of ETH, she is now 3x long ETH/SDR.

Liquidations ensure that in the event of a price crash in the collateral that backs a CDP type, the system will automatically be able to close CDPs that become too risky as result, ensuring that the outstanding Dai supply remain fully collateralized and solvent.

Example 4: Let's assume that we have an Ether CDP type with a liquidation ratio of 145%, a penalty ratio of 105%, and our Ether CDP is outstanding with a collateral to debt ratio of 150% . Then, the Ether price crashes 10% against the Target Price. This causes the collateral to debt ratio of the CDP to fall to ~135%. As it falls below its liquidation ratio, traders can trigger its liquidation and begin bidding with Dai for buying MKR in the debt auction. Traders can also begin bidding with Dai for buying the ~135 Dai worth of collateral in the collateral auction. Once there is at least 105 Dai being bid on the Ether collateral, traders reverse bid to take the least amount of collateral for 105 Dai and the remainder is returned to owner of the CDP prior to its liquidation.

Keepers and Oracles: The external actors that support the Dai Stablecoin System.

A keeper is an independent (usually automated) actor that is incentivized by profit opportunities to contribute to decentralized systems. In the context of The Dai Stablecoin System, keepers trigger CDP liquidations, and participate in the Debt Auctions and Collateral Auctions that happen during the liquidations.

Keepers also trade Dai around the Target Price. Keepers will want to sell Dai when the market price is higher than the Target Price. Similarly, keepers buy Dai when the market price is below the Target Price. This is in order to profit from the expected long-term convergence towards the Target Price.

Price feed oracles are another crucial group of external actors that the Dai Stablecoin System requires to function. Oracles are independent external actors or decentralized applications that provide a data feed onto the blockchain for smart contracts to consume. The Dai Stablecoin System needs information about the market price of the Dai and its deviation from the Target Price in order to adjust the target rate. It also needs information about the market price of the assets used as collateral in CDPs, in order to know when liquidations should be triggered.

Addressable Market

As mentioned above, a cryptocurrency with price stability is a basic requirement for the majority of decentralized applications, and as such the potential market for Dai is at least as large as the entire blockchain industry. The following is a short non-exhaustive list of some of the immediate markets (both blockchain industry and wider industry) for the Dai Stablecoin System, in its capacity as a cryptocurrency with price stability and its use case as a decentralized margin trading platform:

Prediction Markets & Gambling Applications: It is logical to not want to increase one's risk by placing a bet with a volatile cryptocurrency. Long term bets become especially infeasible if the user also has to also gamble on the future price of the volatile asset used to place the bet. Instead, a cryptocurrency with price stability like Dai will be the natural choice for prediction market and gambling users.

Financial Markets: Hedging, Derivatives, Leverage etc: CDPs will allow for easier leveraged trading. Dai will also be useful as stable and reliable collateral in custom derivative smart contracts, such as options or CFD's.

Merchant receipts, Cross-border transactions and remittances: Foreign exchange volatility mitigation and lack of middlemen means the transaction costs of international trade can be significantly reduced by using Dai.

Primary Risks and their Mitigation

There are many potential risks facing the successful development, deployment, and operation of the Dai Stablecoin System. It is vital that both the Maker community and the Dai Foundation take all necessary steps to mitigate these risks as much as possible. The following is a list of the primary risks identified and the accompanying plan for risk mitigation:

Malicious hacking attack against the smart contract infrastructure

The greatest risk to the system during its early stages is the risk of a malicious programmer finding an exploit in the deployed smart contracts, and using it to break or steal from the system before the vulnerability can be fixed. In a worst case scenario, all decentralized digital assets that are held

as collateral in The Dai Stablecoin System, such as Ether or Augur Reputation, could be stolen without any chance of recovery. The part of the collateral portfolio that is not decentralized, such as Digix Gold IOU's, would not be stolen in such an event as they can be frozen and controlled through a centralized backdoor.

Mitigation: The Dai Stablecoin System will have emergency security features that allows oracles to enact global settlement of the system if they detect a security breach. Global settlement means that Dai regular functionality stops, and Dai holders are instead able to claim digital assets directly from the CDPs with a value equal to the Target Price of the Dai they were holding (with the leftover collateral going to CDP users, as if their CDP had been liquidated). This feature will allow the system to deflect attacks that enable the attacker to slowly drain assets out of the smart contracts, but does not defend against attacks that enable the attacker to instantly drain all the collateral at once.

The more general and long term mitigation strategy is to invest heavily in an in-house team of world class programmers who specialize in developing secure smart contracts while also continuously performing independent security audits in parallel. Contract security and best practices have been the highest priority of the Dai development effort since its inception. The codebase has already undergone two independent security audits by arguably some of the best security researchers in the blockchain industry.

In the very long term, the risk of getting hacked can theoretically be completely mitigated through formal verification of the code, which means using functional programming to mathematically prove that the codebase does not contain any exploits. While complete formal verification is a very long term goal, significant work towards it has already been completed, including creating a full implementation of The Dai Stablecoin System in the functional programming language Haskell.

Black Swan Event in one or more Collateral assets

The highest impact risk is a potential Black Swan event on collateral used for the Dai. This could either happen in the early stages of Dai Stablecoin System, before MKR is robust enough to support inflation moments, or after the Dai Stablecoin System supports a diverse portfolio of collateral.

Mitigation: CDP collateral will be limited to ETH in the early stages with the debt ceiling limited initially, growing gradually over time. In addition, one of our experimental projects called Sai will provide pertinent lessons learned, potentially including new Stability Levers.

Competition & the Importance of Ease-of-Use

As mentioned previously, there is a large amount of money and brainpower working on cryptocurrency with price stability. By virtue of having "true decentralization", The Dai Stablecoin System is by far the most complex model being contemplated in the blockchain industry. A perceived risk is a movement among cryptocurrency users where the ideals of decentralization are exchanged for the simplicity and marketing of centralized digital assets.

Mitigation: We expect that Dai will be very easy to use for a regular crypto-user. Dai will be a standard Ethereum token adhering to the ERC20 standard and easily available with high liquidity

across the ecosystem. Dai has been designed in such a way that the average user need not understand the underlying mechanics of the system in order to use it.

The complexities of the Dai Stablecoin System will need to be understood primarily by Keepers and capital investment companies that use the Dai Stablecoin System for margin trading, and these types of users have enough resources to onboard themselves as long as there is abundant and clear documentation of every aspect of the system's mechanics, which the Maker community and Dai Foundation will ensure is the case.

The Dai Foundation will also invest heavily in core branding and international educational material during the initial launch of Dai. If resources permit, the Dai Foundation will use the surplus of its MKR holdings on charity projects, which if done correctly and on a large enough scale, will guarantee positively biased exposure in mainstream media and growth of the Dai brand.

Pricing Errors, Irrationality & Unforeseen Events

A number of unforeseen events could potentially occur, such as a problem with the price feed from the Oracles or other unexpected events such as irrational market dynamics that cause variation in the value of Dai for an extended period. If confidence is lost in the system, the target rate adjustment or even MKR dilution could hit extreme levels and still not bring liquidity and stability to the market.

Mitigation: The Maker community will need to incentivize a sufficiently large capital pool to act as Keepers of the market in order to maximize rationality and market efficiency as well as grow the Dai Stablecoin System gradually at a steady pace. The Dai Foundation will also deploy its large capital reserves to act as a keeper, ensuring that even in the complete absence of any other well capitalized early-stage keepers, the Dai Foundation alone will be able to keep the system rational.

Failure of centralized infrastructure

The Dai Foundation will play a major role in the development and governance of the Dai Stablecoin System in its early days - budgeting for expenses, hiring new developers, seeking partnerships and institutional users, and interfacing with regulators and other key external stakeholders. Should the Dai Foundation fail in some capacity, for legal reasons or due to internal problems with management, the future of the Dai Stablecoin System could be at risk without a proper backup plan.

Mitigation: The Maker community exists partly to act as the decentralized counterparty to the Dai Foundation. It is a loose collective of independent actors who are all aligned by holding the MKR digital asset, giving them a strong incentive to see the Dai Stablecoin System succeed. During the early phases of MKR distribution, great care was taken to ensure that the most important core developers received a significant MKR stake. In the event the Dai Foundation is no longer able to be at the forefront of continued development of the Dai Stablecoin System, large individual MKR holders will be incentivized to fund developers, or develop themselves, in an effort to protect the value of their token.

Glossary of Terms

Collateralized Debt Position (CDP): A smart contract whose users receive an asset (Dai), which effectively operates as a debt instrument with an interest rate. The CDP user has posted collateral in excess of the value of the loan in order to guarantee their debt position.

Dai: The cryptocurrency with price stability that is the asset of exchange in the Dai Stablecoin System. It is a standard Ethereum token adhering to the ERC20 standard.

Debt Auction: The reverse-auction selling MKR for Dai to cover Emergency Debt when a CDP becomes undercollateralized.

Collateral Auction: The auction selling collateral in a liquidated CDP. It is designed to prioritize covering the debt owed by the CDP, then to give the owner the best price possible for their collateral refund.

The Dai Foundation: A non-profit foundation based in Zug, Switzerland, which exists to support the development of The Dai Stablecoin System software infrastructure.

Keepers: Independent economic actors that trade Dai, CDPs and/or MKR, create Dai or close CDPs and seek arbitrage on The Dai Stablecoin System and as a result help maintain Dai market rationality and price stability.

MKR: The ERC20 token that pays Stability Fees in the system, is used for voting on governance decisions as well as used as a liquidity backstop in the case of insolvent CDPs.

MKR Voters: MKR holders who actively manage the risk of The Dai Stablecoin System by voting on Risk Parameters.

Oracles: Ethereum accounts (contracts or users) selected to provide price feeds into various components of The Dai Stablecoin System.

Risk Parameters: The variables that determine when the Dai Stablecoin System automatically judges a CDP to be Risky, allowing Keepers to liquidate it.

Sensitivity Parameter: The variable that determines how aggressively the Dai Stablecoin System automatically changes the Target Rate in response to Dai market price deviations.

Target Rate Feedback Mechanism: The way the Dai Stablecoin System adjusts the Target Rate to cause market forces to maintain stability around the Target Rate.

SDR: The Special Drawing Rights, a basket of national currencies maintained by the International Monetary Fund. Widely seen in finance as the most stable reference point for real world values.

Links

Chat - Primary platform of community interaction

Forum - For debate and proposals

Subreddit - Best place to get latest news and links

Wiki - Learn about the Dai Stablecoin System in greater detail

GitHub - Repository of the public Dai Stablecoin System code

TeamSpeak - For governance meeting conference calls

SoundCloud - Governance meeting recordings

Oasis - MKR and Dai decentralized exchange