

取扱暗号資産の概要説明書（カルダノ）

一般社団法人日本暗号資産取引業協会（JVCEA）が公表する「取扱暗号資産の概要説明書」を基に作成しています。
情報の正確性、信頼性、完全性を保証するものではありません。

概要書更新年月日	2023年12月8日
暗号資産の名称	カルダノ/エイダ
ティッカーコード（シンボル）	ADA
一般的な性格	分散型の価値保有・価値移転の台帳データ維持のための、価値記録を行う記録者への対価・代償として発行される暗号資産
保有・移転記録の秘匿性	アドレスを生成するアルゴリズムは、EdDSA（エドワーズ曲線デジタル署名アルゴリズム）が採用されている。公開鍵からアドレスを生成するためにHMAC-SHA512ハッシュ関数を使用している。
価値移転記録の信頼性確保の仕組み	Proof of Stake コンセンサス・アルゴリズム（分散台帳内の不正取引を排除するために、記録者全員が合意する必要があるが、その合意形成方式）の一つであり、保有している基軸暗号資産の量が多いほどブロック生成（承認）の成功確率が上昇する承認方式。
保有・移転記録の最低単位	1lovelace = 0.000001ADA
発行者	あり
発行主体概要	Cardano Foundationがエコシステムの監督者、IOHKが研究・技術開発担当、EMURGO Pte. Ltd.がブロックチェーンソリューションサービスの開発と提供を担っている。
発行方法	初期発行と、分散型の価値保有・価値移転の台帳データ維持のための、価値記録を行う記録者への対価・代償としてプログラムにより自動発行される。
発行可能数	45,000,000,000 ADA
価値移転認証の仕組み	台帳形式 価値移転認証を求める暗号データを記録者が解読し、利用者および移転内容の真正性を確認して価値移転記録台帳の記録を確定する。
価値移転ネットワークの信頼性に関する説明	独自のPoSコンセンサスアルゴリズム（ウロポロス）で、完全にランダムに選ばれた記録者達によってブロックが承認される仕組みである。保有量が多いほど記録者に選ばれる確率が上昇するため、記録者による悪意のある行動を抑制し信頼性を保つことができる。
記録者の信用力に関する説明	完全にランダムに選出された記録者がブロックの承認を行う。記録者による多数の合意がなければ不正が成立せず、記録者が十分に多数であることによって、個々の記録者の信用力に頼らず、記録保持の仕組みそのものを信用の基礎としている。
その他事項	現状なし。 暗号資産に関する法律が整備されていなかった2015年から2016年にかけてエイダは主に日本でプレセールが行われ、マルチ商法と思われる代理店方式で販売されていた経緯があり、その価値や取引所上場に関して、利用者とのトラブルが発生していたが、ICO後は、このような形式での販売は行われていない。 また、エイダはその初期段階でカジノプラットフォームを一つの用途として宣伝されていたが、現在ではそのような宣伝はされていない。