NDAU CURRENCY SPECIFICATION

Version 1.2

July 22, 2019

ndau – A Buoyant Digital Currency

ndau is a digital currency uniquely designed to serve as a long-term store of value. In addition to the features available in traditional digital currencies, ndau supports sophisticated monetary policy and governance mechanisms. This specification describes the user-visible features of ndau and serves as an introduction to other materials. Extensive material about ndau can be found at the ndau Collective Knowledge Base: https://ndaucollective.org/knowledge-base

Account and Address Creation

Accounts

An account is a single repository of value on the ndau blockchain. An ndau holder may have many ndau accounts, managed together in an ndau wallet application.

An account has a single address that never changes. All ndau held in an account are indistinguishable: no transaction can specify which ndau in an account are to be affected by it, as there is no reason to do so. Unlike other digital currencies, ndau accounts have additional attributes other than their balances, so the words 'account' and 'address' are not synonyms but are sometimes used interchangeably. Every account has exactly one address, and every address is associated with exactly one account. An account's address never changes.

Account Creation

An account is created by the generation of a new ndau address and then by an ndau transaction that refers to that address. The address must first be used in a transaction that transfers ndau to it. Any number of transfers may be made into a newly-created account before any other action is taken on it.

Each account is governed by a set of **validation rules**. Validation rules provide sophisticated control over an account's transactions. They specify signature and other requirements that must be met if a transaction is to be valid. Before any transactions can be submitted from a newly-created account, its validation rules must be set.

An account's address is created from a public/private keypair known as the account's **ownership key**. That key is used to establish the account's initial validation rules.

Addresses

An ndau address is encoded as a 48-character string of letters and digits. It is a byte32 encoding, using a custom alphabet, of a portion of the SHA256 hash of the ownership public key, concatenated with additional marker and checksum information. ndau addresses are designed to be easily recognizable as ndau addresses and to be easily checked for valid format. To avoid confusion, ndau addresses use only lowercase letters, contain no accented characters, and do not contain the characters **O, o, 0, L, l,** or **1**. An ndau address always begins with the distinctive 2-letter prefix **nd** followed by one character that specifies the type of address. The address ends with a checksum so it can be trivially inspected for typos or transpositions.

Address Types

Each address type has different attributes and may be handled differently in some transactions. In most cases the designation is simply for ease of identification and has no semantic meaning. Account types with distinctive properties, such as exchange accounts, will have valid addresses whitelisted to prevent fraudulent use.

The ndau account types are:

User Address - type 'NDA'

This is an address for normal holding and transfer of ndau. It has no special attributes.

ndau Network Operations Address - type 'NDN'

These addresses identify accounts used by ndau engineering and operations. They behave the same as other user addresses but are distinguished for convenience.

ndau Endowment Address - type 'NDE'

Addresses used by the Axiom Foundation for the release of new ndau from the Endowment to be issued to an exchange or directly to a purchaser by a sale at the Target Price. A single canonical 'nde' address is used by the Endowment for releasing new ndau.

Exchange Address - type 'NDX'

'ndx' addresses are designated for use by cryptocurrency exchanges. Authorized exchanges will be whitelisted to indicate they're governed by the blockchain rules for exchanges.

Market Maker Address - type 'NDM'

Addresses used by the Market Maker to manage price discovery and liquidity.

Blockchain Policy Council Address – type 'NDB'

The Blockchain Policy Council (BPC) governs the ndau ecosystem. One aspect of that governance is the management of monetary policy through rate tables and other ndau system variables. This prefix identifies accounts controlled by the BPC.

Keypairs and Signatures

A ndau public/private keypair is used to generate signatures for transactions and other data. ndau uses ed25519 elliptic-curve cryptography (https://ed25519.cr.yp.to/ed25519-20110926.pdf) and secp256k1 HD wallet addresses (https://en.bitcoin.it/wiki/Secp256k1). ndau's BIP-44 registered coin type (at Satoshi Labs) is 20036 (0x80004e44) and ndau uses the ISO-compatible three-character code **XND**: https://github.com/satoshilabs/slips/blob/master/slip-0044.md

ndau Issuance, Target Price, and Floor Price

The ndau Endowment's role in monetary policy is to manage currency supply based on demand as indicated by the current Market Price. If the Market Price rises too high new ndau are issued from the Endowment, and if it falls too far the Endowment repurchases ndau and permanently removes them from circulation.

Target Price

The Endowment may issue up to 30,000,000 ndau in three phases of 10,000,000 ndau each. The Endowment always offers to issue new ndau at the published, algorithmically-defined Target Price based on the number of ndau already issued. The Target Price is denominated in USD and is initially USD $1. The Target Price increases every block of 1,000 ndau issued: each phase, therefore, consists of 10,000 blocks. During the first 10,000,000-ndau phase the Target Price doubles uniformly 14 times from USD $1 to USD $16,384 along an exponential curve. Numbering the first block of 1,000 ndau as Block Number 0, the Target Price for each Block Number in Phase 1 is:

$$\text{Phase 1 Target Price} = \$1 \times 2^{\frac{14 \times \text{Block Number}}{9{,}999}}$$

Floor Price

The Endowment will always repurchase ndau at a published Floor Price. The Floor Price is calculated as 50% of the Endowment's current value divided by the number of ndau currently in circulation. The Floor Price can always be determined by any ndau holder but it is constantly changing due to the changing values of the two factors that determine it.

$$\text{Floor Price} = \frac{\text{Endowment Value} \times 50\%}{\text{ndau In Circulation}}$$

ndau purchased by the Endowment at the Floor Price are permanently removed from circulation. They are not added back to the total 30,000,000 ndau the Endowment may issue.

Ecosystem Alignment Incentive and Locking

ndau accounts can, after meeting certain requirements, earn **Ecosystem Alignment Incentive (EAI)** payments. **EAI** payments are newly-created ndau not released from the Endowment.

EAI accrues over time based on the balance in an ndau account and the age of that balance. It is periodically credited to the account and is not available in that account's balance until it is credited. **EAI** always accrues at continuously-compounded rates based on the current **EAI** rate tables published by the **BPC**. These rates may change from time to time, and those **EAI** rate changes take effect immediately.

Since at any moment an account's current balance is the result of all the transactions that affected it since it was first created, its effective **EAI** rate is calculated based on its weighted average age. The weighted average age is the sum of each amount transferred into the account multiplied by the age of that transfer, divided by the total number of ndau in the account. Transfers of ndau out of the account do not affect it since they are assumed to be an average-aged sample of the account balance. **EAI** credits do not affect the weighted average age if they are credited to the account accruing them.

Locking

Accounts may be locked, and they earn an increased **EAI** rate for doing so based on bonus rate tables set by the **BPC**. No ndau may be transferred out of an account while it is locked, but transfers and other payments may be made into it and **EAI** credited to it. When an account is locked, a notice period is specified: that notice period and the locked **EAI** rate bonus for that period are recorded. The account then receives the then-current locking bonus rate: changes to those bonus rates affect all subsequent locked accounts but accounts already locked retain their original bonus rates.

An account owner gives notice when they want a locked account to be unlocked. A countdown period equal to the notice period specified when the account was locked then begins. **EAI** is still credited to the account during its countdown period, but no transfers may be made into (or out of) it.

While an account is locked, the length of the notice period is added to the account's weighted average age for the purpose of calculating its current effective unlocked **EAI** rate. If notice is given to unlock the account, then during the notice period the elapsed notice period time is subtracted from that total. The account's locked **EAI** rate bonus is then added to that unlocked **EAI** rate to determine the total **EAI** rate to be used.

A locked account may be re-locked at any time. The new lock period must either be longer than the current lock period or, if notice has been given to unlock the account, longer than the remaining notice period. The account is treated as if it had been immediately unlocked then locked with the new notice period.

Crediting EAI to Accounts

EAI is credited to accounts by active nodes in the ndau consensus network. An account must explicitly delegate this responsibility to a specific node, and accounts that have not been delegated to a node will not have **EAI** credited to them. The **Blockchain Policy Council (BPC)** may establish additional criteria an account must meet before its accrued **EAI** is credited.

When **EAI** is credited to an account, fees are deducted from it to support ndau ecosystem services. These fees are set by the **BPC**, but currently total 15% of **EAI**: 1% for Market Maker operations, 4% for software development, and 10% for network operations and node rewards. Additional fees (up to 5%) may be imposed by the **BPC** and exchanged for tokens belonging to the same account but on other blockchains devoted to non-currency services. No such fees are currently in effect.

An account may be redelegated to a different node at any time. Nodes are required to credit **EAI** at intervals no shorter than a length specified by the **BPC** (currently one day). The **BPC** also specifies a maximum interval (currently 30 days) over which **EAI** may accrue before being credited. If a node fails to credit an account's accrued **EAI** over a longer period, the next time it is credited (by either the same node or a redelegated node) the accrued **EAI** will be calculated as if it were last credited at the maximum interval before the present.

Destination Account

An account's accrued **EAI** is normally credited to it but it may be directed to a different destination account. **EAI** credits directed to a different account *do* affect that account's weighted average age in the same manner as transfers into that account. That destination account may be unlocked or locked, but if it is locked it may not currently be in its countdown period. The destination account may not itself be directing its **EAI** to a different account, nor can an account direct its **EAI** to a different account if it is itself already the destination of another account's **EAI**. Directing **EAI** to an account imposes no additional constraints on it: if the destination account is unlocked it may be locked at any time.

Transferring ndau

Transfers

ndau can be transferred from one account to another subject to certain fees and restrictions. Transfers specify a source account, a destination account, and the quantity of ndau to be transferred. The source account may not be locked: the destination account may be unlocked or locked, but if it is locked it may not be in its unlock countdown period.

Account Balances, EAI, and Recourse Periods

Any time an unlocked account has an available balance of ndau that available balance can be transferred to another account.

Transfers of ndau are subject to the source account's recourse period, during which the amount of the transfer is not included in the destination account's available balance. All newly-created ndau accounts are assigned a default recourse period established by the **BPC** (currently one hour). An account owner can change the length of that period, including setting it to zero, at any time. The new recourse period will not become effective until after the length of the current recourse period has elapsed. Transfers to authorized exchange accounts are not subject to the sending account's recourse period.

ndau transferred into an account is immediately included in that account's balance (and deducted from the source account's balance) at the time of the transfer for the purpose of calculating the account's weighted average age and EAI accrual rate. As each transfer reaches the end of its recourse period it is added to the destination account's available balance. ndau in pending transfers cannot be transferred or used to pay fees.

Stabilization Incentive Burn

The **Stabilization Incentive Burn** (SIB) is a mechanism to stabilize and support the market price of ndau. When in effect it is imposed as an additional fee when ndau are transferred from one account to another. Based on observed transactions, a current Market Price is regularly published to the ndau network. If the Market Price of ndau drops below 95% of the current Target Price, the SIB fee is imposed on all transfers. If the Market Price is 95% of the Target Price, the SIB fee is 0%. It increases linearly until it reaches 50% if the Market Price equals the Floor Price. To reduce the supply of ndau and support the Market Price, ndau paid as SIB fees are removed permanently from circulation ("burned").

$$\text{SIB} \;=\; 50\% \times \frac{(\text{Target Price} \times 95\%) - \text{Market Price}}{(\text{Target Price} \times 95\%) - \text{Floor Price}}$$

Transaction Fees

All transactions require transaction fees based on the transaction type, the size of the transaction in bytes, and the number of ndau involved. A table of transaction fees is published by the BPC specifying each of these parameters for each transaction type. The source account for a transfer must have an available balance greater than or equal to the sum of the amount to be transferred, the transaction fee, and the SIB fee if it is in effect.

$$\text{Total Cost} = \text{Transfer Amount} + \text{Transaction Fee} + \text{SIB Fee}$$

Transaction Validation Rules

Validation Rules

ndau accounts are protected by security mechanisms more powerful and more flexible than those offered by other digital currencies. Transactions may be required to meet multiple criteria before being accepted as valid, such as having multiple signatures, minimum or maximum amounts, and there may be different signature rules for different transaction types.

Validation rules specify one or more validation keys and an optional validation script. Those keys and validation script are used to validate any transactions submitted for that account. Validation scripts have access to the current transaction, account state, and system variables but may not modify them. They may not generate new transactions or trigger external events of any sort: they perform no function other than to determine the validity of a transaction submitted for an account. Since all system variables and properties of the account and transaction are available to the validation script, it may establish validation rules for specific transaction types or rules based on specific values in the transaction or account.

When an account is established the initial set of validation rules is specified. After these rules are set the account always has one or more validation keys assigned to it. It may or may not have a validation script. All subsequent transactions must be signed with one or more of the validation keys currently assigned to the account. They must also be authorized as valid by the current validation script if one is present. If there is no validation script assigned, then the transaction's signature alone is sufficient to validate it. If a validation script is present, the transaction signature only indicates that the transaction was properly formatted and was submitted by at least one valid signer. The validation script will then be executed to determine the validity of the transaction. Transactions may have up to 16 signatures, but all signatures must appear in that account's current list of validation keys. A validation script may later be removed from an account's validation rules, but there must always be at least one validation key present.

Changing Validation Rules and Keys

An account's validation keys or validation script, or both, may be changed at any time. Just as with any other transaction, an attempt to change an account's validation rules is also validated by the account's current rules. An account holder can, therefore, establish validation rules that prevent any further changes to those rules.

There are restrictions on these changes to prevent inappropriate uses, such as changing keys to effect a transfer of a locked account. An account **change of control** is the changing of more than 50% of an account's validation keys within a specified period of time (a BPC-set system variable). If a change to an account's validation rules and keys results in a change of control, that change is treated as if it were an attempt to transfer the entire balance of the account to itself.

- If the account is unlocked the key change is permitted. The account's weighted average age (for EAI calculations) is set to 0, and a SIB fee (if one is in effect) is charged based on the entire balance of the account.
- If the account is locked the key change is not permitted.

Validation scripts are written in ndau's unique stack-based scripting language, **Chaincode**. Details are available in the **Chaincode Technical Reference**.

Staking

Staking is the act of putting some quantity of ndau at risk to ensure good faith actions on the part of the staker. It is somewhat similar to a performance bond: if the staker fails to take some particular action, or acts contrary to their stated intent, the staked ndau may be forfeited ("slashed"). Unlike a bond, however, the staked ndau are never transferred to another account as a remedy for the staker's behavior.

Staking is always associated with a particular purpose. Stake is required to run an active ndau network node and receive node rewards. It is required to serve as an elected BPC member, raise a dispute over an ndau transaction, or for other purposes.

Staked ndau may not be transferred, since they must remain available to be slashed. Each staking action may require a minimum amount of stake and a minimum lock period.

When an account submits a transaction requiring stake, the staking rules are checked to determine whether stake has been properly created for that purpose. In order for the transaction to be valid, the account must already be staked with the minimum balance required. An account may be staked for more than one purpose at a time, and multiple amounts from one account may be staked for the same purpose. The total amount staked from an account, however, may not exceed its available balance.

Each transaction requiring stake has a corresponding transaction that releases it, allowing it to be unstaked. The `RegisterNode` transaction registers an active ndau network node: the account submitting it must already have staked sufficient ndau to the node registration staking rules. When an `UnregisterNode` transaction is submitted to remove that node from active status, all staked amounts are released to be unstaked. The node registration's staking rules, however, may impose additional criteria (usually a delay period) before any staked amounts may be unstaked. This delay allows stake to be slashed for actions taken while the node is registered but discovered shortly after it has been unregistered.

Other ndau accounts may contribute to an account's stake. The new account is staked for the same purpose and under the same criteria, and it is also subject to slashing. This additional staking provides benefit to the original account and the new account can expect to receive some share in that benefit or other reward as a result. Since total stake is a major factor in determining the amount of node rewards an active node may receive, additional stakers will increase a node's ability to receive those rewards. In exchange, that node may be expected to share a portion of those rewards with those stakers.