Polkadot Runtime

Protocol Specification

Web3 Foundation

Contents

Chapter 1

Extrinsics

1.1 Introduction

An extrinsic is a SCALE encoded array consisting of a version number, signature, and varying data types indicating the resulting Runtime function to be called, including the parameters required for that function to be executed.

1.2 Preliminaries

Definition 1 *An extrinsic , tx, is a tuple consisting of the extrinsic version, T_v (Definition 2), and the body of the extrinsic, T_b.*

$$tx := (T_v, T_b)$$

The value of T_b varies for each version. The current version 4 is described in section 1.3.1.

Definition 2 *T_v is a 8-bit bitfield and defines the extrinsic version. The required format of an extrinsic body, T_b, is dictated by the Runtime. Older or unsupported version are rejected.*

*The first bit of T_v indicates whether the transaction is **signed** (1) or **unsigned** (0). The remaining 7-bits represent the version number. As an example, for extrinsic format version 4, an signed extrinsic represents T_v as* `132` *while a unsigned extrinsic represents it as* `4`.

1.3 Extrinsics Body

1.3.1 Version 4

Version 4 of the Polkadot extrinsic format is defined as follows:

$$T_b := (A_i, Sig, E, M_i, F_i(m))$$

where each values represents:

- A_i: the 32-byte address of the sender (Definition 3).
- Sig: the signature of the sender (Definition 4).
- E: the extra data for the extrinsic (Definition 5).
- M_i: the indicator of the Polkadot module (Definition 7).
- $F_i(m)$: the indicator of the function of the Polkadot module (Definition 8).

Definition 3 *Account Id, A_i, is the 32-byte address of the sender of the extrinsic as described in the external SS58 address format.*

Definition 4 *The signature, Sig, is a varying data type indicating the used signature type, followed by the signature created by the extrinsic author. The following types are supported:*

$$Sig := \begin{cases} 0, & \textit{Ed25519, followed by: } (b_0, ..., b_{63}) \\ 1, & \textit{Sr25519, followed by: } (b_0, ..., b_{63}) \\ 2, & \textit{Ecdsa, followed by: } (b_0, ..., b_{64}) \end{cases}$$

Signature types vary in sizes, but each individual type is always fixed-size and therefore does not contain a length prefix. `Ed25519` *and* `Sr25519` *signatures are 512-bit while* `Ecdsa` *is 520-bit, where the last 8 bits are the recovery ID.*

The signature is created by signing payload P.

$$P := \begin{cases} Raw, & \textit{if } |Raw| \leq 256 \\ Blake2(Raw), & \textit{if } |Raw| > 256 \end{cases} \tag{1.1}$$
$$Raw := (M_i, F_i(m), E, R_v, F_v, H_h(G), H_h(B))$$

where each value represents:

- *M_i: the module indicator (Definition 7).*
- *$F_i(m)$: the function indicator of the module (Definition 8).*
- *E: the extra data (Definition 5).*
- *R_v: a UINT32 containing the specification version of* `14`.
- *F_v: a UINT32 containing the format version of* `2`.
- *$H_h(G)$: a 32-byte array containing the genesis hash.*

- $H_h(B)$: *a 32-byte array containing the hash of the block which starts the mortality period, as described in Definition 6.*

Definition 5 *Extra data, E, is a tuple containing additional meta data about the extrinsic and the system it is meant to be executed in.*

$$E := (T_{mor}, N, P_t)$$

where each value represents:

- T_{mor}: *contains the SCALE encoded mortality of the extrinsic (Definition 6).*
- N: *a compact integer containing the nonce of the sender. The nonce must be incremented by one for each extrinsic created, otherwise the Polkadot network will reject the extrinsic.*
- P_t: *a compact integer containing the transactor pay including tip.*

Definition 6 *Extrinsic **mortality** is a mechanism which ensures that an extrinsic is only valid within a certain period of the ongoing Polkadot lifetime. Extrinsics can also be immortal, as clarified in Section 6.*

The mortality mechanism works with two related values:

- M_{per}: *the period of validity in terms of block numbers from the block hash specified as $H_h(B)$ in the payload (Definition 4). The requirement is $M_{per} \geq 4$ and M_{per} must be the power of two, such as* `32`, `64`, `128`, *etc.*
- M_{pha}: *the phase in the period that this extrinsic's lifetime begins. This value is calculated with a formula and validators can use this value in order to determine which block hash is included in the payload. The requirement is $M_{pha} < M_{per}$.*

In order to tie a transaction's lifetime to a certain block ($H_i(B)$) after it was issued, without wasting precious space for block hashes, block numbers are divided into regular periods and the lifetime is instead expressed as a "phase" (M_{pha}) from these regular boundaries:

$$M_{pha} = H_i(B) \ mod \ M_{per}$$

M_{per} and M_{pha} are then included in the extrinsic, as clarified in Definition 5, in the SCALE encoded form of T_{mor} (Sect. 6). Polkadot validators can use M_{pha} to figure out the block hash included in the payload, which will therefore result in a valid signature if the extrinsic is within the specified period or an invalid signature if the extrinsic "died".

Example

The extrinsic author choses $M_{per} = 256$ at block `10'000`*, resulting with $M_{pha} = 16$. The extrinsic is then valid for blocks ranging from* `10'000` *to* `10'256`.

Encoding

T_{mor} refers to the SCALE encoded form of type M_{per} and M_{pha}. T_{mor} is the size of two bytes if the extrinsic is considered mortal, or simply one bytes with the value equal to zero if the extrinsic is considered immortal.

$$T_{mor} := Enc_{SC}(M_{per}, M_{pha})$$

The SCALE encoded representation of mortality T_{mor} deviates from most other types, as it's specialized to be the smallest possible value, as described in Algorithm 1.1 and 1.2.

Algorithm 1.1 ENCODE MORTALITY

Input: M_{per}, M_{pha}

// If the extrinsic is immortal, specify
// a single byte with the value equal to zero.

1: **return** $\begin{cases} 0 & if\ extrinsic\ is\ immortal \end{cases}$

2: **Init** $factor = \text{LIMIT}(M_{per} >> 12,\ 1,\ \phi)$
3: **Init** $left = \text{LIMIT}(\text{TZ}(M_{per}) - 1,\ 1,\ 15)$
4: **Init** $right = \frac{M_{pha}}{factor} << 4$

// Returns a two byte value
5: **return** $left|right$

Algorithm 1.2 DECODE MORTALITY

Input: T_{mor}

1: **return** $\begin{cases} Immortal & if\ T_{mor}^{b0} = 0 \end{cases}$

2: **Init** $enc = T_{mor}^{b0} + (T_{mor}^{b1} << 8)$
3: **Init** $M_{per} = 2 << (enc\ mod\ (1 << 4))$
4: **Init** $factor = \text{LIMIT}(M_{per} >> 12,\ 1,\ \phi)$
5: **Init** $M_{pha} = (enc >> 4) * factor$
6: **return** (M_{per}, M_{pha})

- *T_{mor}^{b0}: the first byte of T_{mor}.*
- *T_{mor}^{b1}: the second byte of T_{mor}.*
- LIMIT(num, min, max): *Ensures that num is between min and max. If min or max is defined as ϕ, then there is no requirement for the specified minimum/maximum.*

- TZ(num): *returns the number of trailing zeros in the binary representation of* num. *For example, the binary representation of* `40` *is* `0010 1000`, *which has three trailing zeros.*
- $>>$: *performs a binary right shift operation.*
- $<<$: *performs a binary left shift operation.*
- $|$: *performs a bitwise OR operation.*

Definition 7 *M_i is an indicator for the Runtime to which Polkadot module, m, the extrinsic should be forwarded to.*

M_i is a varying data type pointing to every module exposed to the network.

$$M_i := \begin{cases} 0, & System \\ 1, & Utility \\ ... & \\ 7, & Balances \\ ... & \end{cases}$$

Definition 8 *$F_i(m)$ is a tuple which contains an indicator, m_i, for the Runtime to which function within the Polkadot module, m, the extrinsic should be forwarded to. This indicator is followed by the concatenated and SCALE encoded parameters of the corresponding function, $params$.*

$$F_i(m) := (m_i, params)$$

The value of m_i varies for each Polkadot module, since every module offers different functions. As an example, the `Balances` *module has the following functions:*

$$Balances_i := \begin{cases} 0, & transfer \\ 1, & set\_balance \\ 2 & force\_transfer \\ 3 & transfer\_keep\_alive \end{cases}$$

Chapter 2

Weights

2.1 Motivation

The Polkadot network, like any other permissionless system, needs to implement a mechanism to measure and to limit the usage in order to establish an economic incentive structure, to prevent the network overload, and to mitigate DoS vulnerabilities. In particular, Polkadot enforces a limited time-window for block producers to create a block, including limitations on block size, which can make the selection and execution of certain extrinsics too expensive and decelerate the network.

In contrast to some other systems such as Ethereum which implement fine measurement for each executed low-level operation by smart contracts, known as gas metering, Polkadot takes a more relaxed approach by implementing a measuring system where the cost of the transactions (referred to as 'extrinsics') are determined before execution and are known as the weight system.

The Polkadot weight system introduces a mechanism for block producers to measure the cost of running the extrinsics and determine how "heavy" it is in terms of execution time. Within this mechanism, block producers can select a set of extrinsics and saturate the block to its fullest potential without exceeding any limitations (as described in section 2.2.1). Moreover, the weight system can be used to calculate a fee for executing each extrinsics according to its weight (as described in section 2.6.1).

Additionally, Polkadot introduces a specified block ratio (as defined in section 2.2.1), ensuring that only a certain portion of the total block size gets used for regular extrinsics. The remaining space is reserved for critical, operational extrinsics required for the functionality by Polkadot itself.

To begin, we introduce in Section 2.2 the assumption upon which the Polkadot transaction weight system is designed. In Section 2.2.1, we discuss the limitation Polkadot needs to enforce on the block size. In Section 2.3, we describe in detail the procedure upon

which the weight of any transaction should be calculated. In Section 2.5, we present how we apply this procedure to compute the weight of particular runtime functions.

2.2 Assumptions

In this section, we define the concept of weight and we discuss the considerations that need to be accounted for when assigning weight to transactions. These considerations are essential in order for the weight system to deliver its fundamental mission, i.e. the fair distribution of network resources and preventing a network overload. In this regard, weights serve as an indicator on whether a block is considered full and how much space is left for remaining, pending extrinsics. Extrinsics which require too many resources are discarded. More formally, the weight system should:

- prevent the block from being filled with too many extrinsics
- avoid extrinsics where its execution takes too long, by assigning a transaction fee to each extrinsic proportional to their resource consumption.

These concepts are formalized in Definitions 9 and 12:

Definition 9 *For a block B with $Head(B)$ and $Body(B)$ the block length of B, $Len(B)$, is defined as the amount of raw bytes of B.*

Definition 10 *Targeted time per block denoted by $T(B)$ implies the amount of seconds that a new block should be produced by a validator. The transaction weights must consider $T(B)$ in order to set restrictions on time intensive transactions in order to saturate the block to its fullest potential until $T(B)$ is reached.*

Definition 11 *Available block ration reserved for normal, noted by $R(B)$, is defined as the maximum weight of none-operational transactions in the Body of B divided by $Len(B)$.*

Definition 12 *Polkadot block limits as defined here should be respected by each block producer for the produced block B to be deemed valid:*

1. $Len(B) \leq 5 \times 1'024 \times 1'024 = 5'242'880$ *Bytes*
2. $T(B) = 6$ *seconds*
3. $R(B) \leq 0.75$

Definition 13 *The Polkadot transaction weight function denoted by $\mathcal{W}$ as follows:*

$$\mathcal{W} : \mathcal{E} \to \mathbb{N}$$
$$\mathcal{W} : E \mapsto w$$

where w is a non-negative integer representing the weight of the extrinsic E. We define the weight of all inherent extrinsics as defined in the Polkadot Host Specification to be equal to 0. We extend the definition of $\mathcal{W}$ function to compute the weight of the block as sum of weight of all extrinsics it includes:

$$\mathcal{W} : \mathcal{B} \to \mathbb{N}$$
$$\mathcal{W} : B \mapsto \sum_{E \in B} (W(E))$$

In the remainder of this section, we discuss the requirements to which the weight function needs to comply to.

- Computations of function $\mathcal{W}(E)$ must be determined before execution of that E.
- Due to the limited time window, computations of $\mathcal{W}$ must be done quickly and consume few resources themselves.
- $\mathcal{W}$ must be self contained and must not require I/O on the chain state. $\mathcal{W}(E)$ must depend solely on the Runtime function representing E and its parameters.

Heuristically, "heaviness" corresponds to the execution time of an extrinsic. In that way, the $\mathcal{W}$ value for various extrinsics should be proportional to their execution time. For example, if Extrinsic A takes three times longer to execute than Extrinsic B, then Extrinsic A should roughly weighs 3 times of Extrinsic B. Or:

$$\mathcal{W}(A)\ 3 \times \mathcal{W}(B)$$

Nonetheless, $\mathcal{W}(E)$ can be manipulated depending on the priority of E the chain is supposed to endorse.

2.2.1 Limitations

In this section we discuss how applying the limitation defined in Definition 12 can be translated to limitation $\mathcal{W}$. In order to be able to translate those into concrete numbers, we need to identify an arbitrary maximum weight to which we scale all other computations. For that we first define the block weight and then assume a maximum on it block length in Definition 14:

Definition 14 *We define the block weight of block B, formally denoted as $\mathcal{W}(B)$, to be:*

$$\mathcal{W}(B) = \sum_{n=0}^{|\mathcal{E}|} (W(E_n))$$

We require that:

$$\mathcal{W}(B) < 2'000'000'000'000$$

The weights must fulfil the requirements as noted by the fundamentals and limitations, and can be assigned as the author sees fit. As a simple example, consider a maximum block weight of 1'000'000'000, an available ratio of 75% and a targeted transaction throughput of 500 transactions, we could assign the (average) weight for each transaction at about 1'500'000. Block producers have economic incentive to include as many extrinsics as possible (without exceeding limitations) into a block before reaching the targeted block time. Weights give indicators to block producers on which extrinsics to include in order to reach the blocks fullest potential.

2.3 Calculation of the weight function

In order to calculate weight of block B, $TWF(B)$, one needs to evaluate the weight of each transaction included in the block. Each transaction causes the execution certain Runtime functions. As such, to calculate the weight of a transaction, those functions must be analyzed in order to determine parts of the code which can significantly contribute to the execution time and consume resources such as loops, I/O operations, and data manipulation. Subsequently the performance and execution time of each part will be evaluated based on variety of input parameters. Based on those observations, weights are assigned Runtime functions or parameters which contribute to long execution times. These sub component of the code are discussed in Section 2.4.1.

The general algorithm to calculate $\mathcal{W}(E)$ is described in the Section 2.4.

2.4 Benchmarking

Calculating the extrinsic weight solely based on theoretical complexity of the underlying implementation proves to be too complicated and unreliable at the same time. Certain decisions in the source code architecture, internal communication within the Runtime or other design choices could add enough overhead to make the asymptotic complexity practically meaningless.

On the other hand, benchmarking an extrinsics in a black-box fashion could (using random parameters) most centainly results in missing corner cases and worst case senarios. Instead, we benchmark all available Runtime functions which are invoked in the course of execution of extrinsics with a large collection of carefully selected input parameters and use the result of the benchmarking process to evaluate $\mathcal{W}(E)$.

In order to select useful parameters, the Runtime functions have to be analysed to fully understand which behaviors or conditions can result in expensive execution times, which is described closer in section 2.4.1. Not every possible benchmarking outcome can be invoked by varying input parameters of the Runtime function. In some circumstances, preliminary work is required before a specific benchmark can be reliably measured, such

as creating certain preexisting entries in the storage or other changes to the environment.

The Practical Examples Section 2.5 covers the analysis process and the implementation of preliminary work in more detail.

2.4.1 Primitive Types

The Runtime reuses components, known as "primitives", to interact with the state storage. The execution cost of those primitives can be measured and a weight should be applied for each occurrence within the Runtime code.

For storage, Polkadot uses three different types of storage types across its modules, depending on the context:

- **Value**: Operations on a single value.

  The final key-value pair is stored under the key:

  ```
  hash(module_prefix) + hash(storage_prefix)
  ```

- **Map**: Operations on mulitple values, datasets, where each entry has its corresponding, unique key.

  The final key-value pair is stored under the key:

  ```
  hash(module_prefix) + hash(storage_prefix) + hash(encode(key))
  ```

- **Double map**: Just like **Map**, but uses two keys instead of one. This type is also known as "child storage", where the first key is the "parent key" and the second key is the "child key". This is useful in order to scope storage entries (child keys) under a certain `context` (parent key), which is arbitrary. Therefore, one can have separated storage entries based on the context.

  The final key-value pair is stored under the key:

  ```
  hash(module_prefix) + hash(storage_prefix)
    + hash(encode(key1)) + hash(encode(key2))
  ```

It depends on the functionality of the Runtime module (or its sub-processes, rather) which storage type to use. In some cases, only a single value is required. In others, multiple values need to be fetched or inserted from/into the database.

Those lower level types get abstracted over in each individual Runtime module using the `decl_storage!` macro. Therefore, each module specifies its own types that are used as input and output values. The abstractions do give indicators on what operations must be closely observed and where potential performance penalties and attack vectors are possible.

Considerations

The storage layout is mostly the same for every primitive type, primarily differentiated by using special prefixes for the storage key. Big differences arise on how the primitive types are used in the Runtime function, on whether single values or entire datasets are being worked on. Single value operations are generally quite cheap and its execution time does not vary depending on the data that's being processed. However, excessive overhead can appear when I/O operations are executed repeatedly, such as in loops. Especially, when the amount of loop iterations can be influenced by the caller of the function or by certain conditions in the state storage.

Maps, in contrast, have additional overhead when inserting or retrieving datasets, which vary in sizes. Additionally, the Runtime function has to process each item inside that list.

Indicators for performance penalties:

- **Fixed iterations and datasets** - Fixed iterations and datasets can increase the overall cost of the Runtime functions, but the execution time does not vary depending on the input parameters or storage entries. A base Weight is appropriate in this case.
- **Adjustable iterations and datasets** - If the amount of iterations or datasets depend on the input parameters of the caller or specific entries in storage, then a certain weight should be applied for each (additional) iteration or item. The Runtime defines the maximum value for such cases. If it doesn't, it unconditionally has to and the Runtime module must be adjusted.

  When selecting parameters for benchmarking, the benchmarks should range from the minimum value to the maximum value, as described in paragraph 2.4.1.
- **Input parameters** - Input parameters that users pass on to the Runtime function can result in expensive operations. Depending on the data type, it can be appropriate to add additional weights based on certain properties, such as data size, assuming the data type allows varying sizes. The Runtime must define limits on those properties. If it doesn't, it unconditionally has to and the Runtime module

must be adjusted.

When selecting parameters for benchmarking, the benchmarks should range from the minimum values to the maximum value, as described in paragraph 2.4.1.

What the maximum value should be really depends on the functionality that the Runtime function is trying to provide. If the choice for that value is not obvious, then it's advised to run benchmarks on a big range of values and pick a conservative value below the `targeted time per block` limit as described in section 2.2.1.

2.4.2 Parameters

The inputs parameters highly vary depending on the Runtime function and must therefore be carefully selected. The benchmarks should use input parameters which will most likely be used in regular cases, as intended by the authors, but must also consider worst case scenarios and inputs which might decelerate or heavily impact performance of the function. The input parameters should be randomised in order to cause various effects in behaviors on certain values, such as memory relocations and other outcomes that can impact performance.

It's not possible to benchmark every single value. However, one should select a range of inputs to benchmark, spanning from the minimum value to the maximum value which will most likely exceed the expected usage of that function. This is described in more detail in section 2.4.1. The benchmarks should run individual executions/iterations within that range, where the chosen parameters should give insight on the execution time. Selecting imprecise parameters or too extreme ranges might indicate an inaccurate result of the function as it will be used in production. Therefore, when a range of input parameters gets benchmarked, the result of each individual parameter should be recorded and optionally visualized, then the necessary adjustment can be made. Generally, the worst case scenario should be assigned as the weight value for the corresponding runtime function.

Additionally, given the distinction theoretical and practical usage, the author reserves the right to make adjustments to the input parameters and assigned weights according to the observed behavior of the actual, real-world network.

Weight Refunds

When assigning the final weight, the worst case scenario of each runtime function should be used. The runtime can then additional "refund" the amount of weights which were overestimated once the runtime function is actually executed.

The Polkadot runtime only returns weights if the difference between the assigned weight and the actual weight calculated during execution is greater than 20%.

2.4.3 Storage I/O cost

It is advised to benchmark the raw I/O operations of the database and assign ”base weights” for each I/O operation type, such as insertion, deletion, querying, etc. When a runtime function is executed, the runtime can then add those base weights of each used operation in order to calculate the final weight.

2.4.4 Environment

The benchmarks should be executed on clean systems without interference of other processes or software. Additionally, the benchmarks should be executed on multiple machines with different system resources, such as CPU performance, CPU cores, RAM and storage speed.

2.5 Practical examples

This section walks through Runtime functions available in the Polkadot Runtime to demonstrate the analysis process as described in section 2.4.1.

In order for certain benchmarks to produce conditions where resource heavy computation or excessive I/O can be observed, the benchmarks might require some preliminary work on the environment, since those conditions cannot be created with simply selected parameters. The analysis process shows indicators on how the preliminary work should be implemented.

2.5.1 Practical Example #1: `request_judgement`

In Polkadot, accounts can save information about themselves on-chain, known as the ”Identity Info”. This includes information such as display name, legal name, email address and so on. Polkadot offers a set of trusted registrars, entities elected by a Polkadot public referendum, which can verify the specified contact addresses of the identities, such as Email, and vouch on whether the identity actually owns those accounts. This can be achieved, for example, by sending a challenge to the specified address and requesting a signature as a response. The verification is done off-chain, while the final judgement is saved onchain, directly in the corresponding Identity Info. It’s also note worthy that Identity Info can contain additional fields, set manually by the corresponding account holder.
Information such as legal name must be verified by ID card or passport submission.

The function `request_judgement` from the `identity` pallet allows users to request judgement from a specific registrar.

```
(func $request_judgement (param $req_index int) (param $max_fee int))
```

- `req_index`: the index which is assigned to the registrar.

- `max_fee`: the maximum fee the requester is willing to pay. The judgement fee varies for each registrar.

Studying this function reveals multiple design choices that can impact performance, as it will be revealed by this analysis.

Analysis

First, it fetches a list of current registrars from storage and then searches that list for the specified registrar index.

```
let registrars = <Registrars<T>>::get();
let registrar = registrars.get(reg_index as usize).and_then(Option::as_ref)
  .ok_or(Error::<T>::EmptyIndex)?;
```

Then, it searches for the Identity Info from storage, based on the sender of the transaction.

```
let mut id = <IdentityOf<T>>::get(&sender).ok_or(Error::<T>::NoIdentity)?;
```

The Identity Info contains all fields that have a data in them, set by the corresponding owner of the identity, in an ordered form. It then proceeds to search for the specific field type that will be inserted or updated, such as email address. If the entry can be found, the corresponding value is to the value passed on as the function parameters (assuming the registrar is not "stickied", which implies it cannot be changed). If the entry cannot be found, the value is inserted into the index where a matching element can be inserted while maintaining sorted order. This results in memory reallocation, which increases resource consumption.

```
match id.judgements.binary_search_by_key(&reg_index, |x| x.0) {
  Ok(i) => if id.judgements[i].1.is_sticky() {
    Err(Error::<T>::StickyJudgement)?
  } else {
    id.judgements[i] = item
  },
  Err(i) => id.judgements.insert(i, item),
}
```

In the end, the function deposits the specified `max_fee` balance, which can later be redeemed by the registrar. Then, an event is created to insert the Identity Info into storage. The creation of events is lightweight, but its execution is what will actually commit the state changes.

```
T::Currency::reserve(&sender, registrar.fee)?;
<IdentityOf<T>>::insert(&sender, id);
Self::deposit_event(RawEvent::JudgementRequested(sender, reg_index));
```

Considerations

The following points must be considered:

- Varying count of registrars.
- Varying count of preexisting accounts in storage.
- The specified registrar is searched for in the Identity Info. An identity can be judged by as many registrars as the identity owner issues requests for, therefore increase its footprint in the state storage. Additionally, if a new value gets inserted into the byte array, memory get reallocated. Depending on the size of the Identity Info, the execution time can vary.
- The Identity Info can contain only a few fields or many. It is legitimate to introduce additional weights for changes the owner/sender has influence over, such as the additional fields in the Identity Info.

Benchmarking Framework

The Polkadot Runtime specifies the `MaxRegistrars` constant, which will prevent the list of registrars of reaching an undesired length. This value should have some influence on the benchmarking process.

The benchmarking implementation of for the function *request_judgement* can be defined as follows:

Algorithm 2.1 Run multiple benchmark iterations for *request_judgement* Runtime function

Output: $\mathcal{W}$

Init collection = {}

for $amount \leftarrow 1, MaxRegistrars$ **do**
  GENERATE-REGISTRARS($amount$)
  $caller \leftarrow$ CREATE-ACCOUNT("CALLER", 1)
  SET-BALANCE($caller$, 100)
  $time \leftarrow$ TIMER(REQUEST-JUDGEMENT(RANDOM($amount$), 100))
  ADD-TO($collection$, $time$)
end for

$\mathcal{W} \leftarrow$ COMPUTE-WEIGHT($collection$);
return $\mathcal{W}$

- GENERATE-REGISTRARS($amount$)

- Creates *number* of registrars and inserts those records into storage.

- CREATE-ACCOUNT(*name*, *index*)

  - Creates a Blake2 hash of the concatenated input of *name* and *index* representing the address of a account. This function only creates an address and does not conduct any I/O.

- SET-BALANCE(*account*, *balance*)

  - Sets a initial *balance* for the specified *account* in the storage state.

- TIMER($function$)

  - Measures the time from the start of the specified $function$ to its completion.

- REQUEST-JUDGEMENT($registrar\_index$, max_fee)

  - Calls the corresponding *request_judgement* Runtime function and passes on the required parameters.

- RANDOM(*num*)

  - Picks a random number between 0 and *num*. This should be used when the benchmark should account for unpredictable values.

- ADD-TO(*collection*, *time*)

  - Adds a returned time measurement (*time*) to *collection*.

- COMPUTE-WEIGHT(*collection*)

  - Computes the resulting weight based on the time measurements in the *collection*. The worst case scenario should be chosen (the highest value).

2.5.2 Practical Example #2 payout_stakers

Analysis

The function `payout_stakers` from the `staking` Pallet can be called by a single account in order to payout the reward for all nominators who back a particular validator. The reward also covers the validator's share. This function is interesting because it iterates over a range of nominators, which varies, and does I/O operation for each of them.

First, this function makes few basic checks to verify if the specified era is not higher then the current era (as it is not in the future) and is within the allowed range also known as "history depth", as specified by the Runtime. After that, it fetches the era payout from storage and additionally verifies whether the specified account is indeed a validator and receives the corresponding "Ledger". The Ledger keeps information about

the stash key, controller key and other informatin such as actively bonded balance and a list of tracked rewards. The function only retains the entries of the history depth, and conducts a binary search for the specified era.

```
let era_payout = <ErasValidatorReward<T>>::get(&era)
  .ok_or_else(|| Error::<T>::InvalidEraToReward)?;

let controller = Self::bonded(&validator_stash).ok_or(Error::<T>::NotStash)?;
let mut ledger = <Ledger<T>>::get(&controller).ok_or_else(|| Error::<T>::NotControlle

ledger.claimed_rewards.retain(|&x| x >= current_era.saturating_sub(history_depth));
match ledger.claimed_rewards.binary_search(&era) {
  Ok(_) => Err(Error::<T>::AlreadyClaimed)?,
  Err(pos) => ledger.claimed_rewards.insert(pos, era),
}
```

The retained claimed rewards are inserted back into storage.

```
<Ledger<T>>::insert(&controller, &ledger);
```

As an optimization, Runtime only fetches a list of the 64 highest staked nominators, although this might be changed in the future. Accordingly, any lower staked nominator gets no reward.

```
let exposure = <ErasStakersClipped<T>>::get(&era, &ledger.stash);
```

Next, the function gets the era reward points from storage.

```
let era_reward_points = <ErasRewardPoints<T>>::get(&era);
```

After that, the payout is split among the validator and its nominators. The validators receives the payment first, creating an insertion into storage and sending a deposit event to the scheduler.

```
if let Some(imbalance) = Self::make_payout(
  &ledger.stash,
  validator_staking_payout + validator_commission_payout
) {
  Self::deposit_event(RawEvent::Reward(ledger.stash, imbalance.peek()));
}
```

Then, the nominators receive their payout rewards. The functions loops over the nominator list, conducting an insertion into storage and a creation of a deposit event for each of the nominators.

```
for nominator in exposure.others.iter() {
  let nominator_exposure_part = Perbill::from_rational_approximation(
    nominator.value,
    exposure.total,
  );

  let nominator_reward: BalanceOf<T> = nominator_exposure_part * validator_leftover_payout;
  // We can now make nominator payout:
  if let Some(imbalance) = Self::make_payout(&nominator.who, nominator_reward) {
    Self::deposit_event(RawEvent::Reward(nominator.who.clone(), imbalance.peek()));
  }
}
```

Considerations

The following points must be considered:

- The Ledger contains a varying list of claimed rewards. Fetching, retaining and searching through it can affect execution time. The retained list is inserted back into storage.

- Looping through a list of nominators and creating I/O operations for each increases execution time. The Runtime fetches up to 64 nominators.

Benchmarking Framework

Definition 15 *History Depth indicated as `MaxNominatorRewardedPerValidator` is a fixed constant specified by the Polkadot Runtime which dictates the number of Eras the Runtime will reward nominators and validators for.*

Definition 16 *Maximum Nominator Rewarded Per Validator indicated as MaxNominatorRewardedPerValidator specifies the maximum amount of the highest-staked nominators which will get a reward. Those values should have some influence in the benchmarking process.*

The benchmarking implementation for the function *payout_stakers* can be defined as follows:

Algorithm 2.2 Run multiple benchmark iterations for *payout_stakers* Runtime function

Output: $\mathcal{W}$

Init collection = {}

for $amount \leftarrow 1, MaxNominatorRewardedPerValidator$ **do**
  for $era\_depth \leftarrow 1, HistoryDepth$ **do**
    $validator \leftarrow$ GENERATE-VALIDATOR()
    VALIDATE($validator$);
    $nominators \leftarrow$ GENERATE-NOMINATORS($amount$)
    for $nominator \in nominators$ **do**
      NOMINATE($validator$, $nominator$)
    end for
    $era\_index \leftarrow$ CREATE-REWARDS($validator$, $nominators$, era_depth)
    $time \leftarrow$ TIMER(PAYOUT-STAKERS($validator$), era_index))
    ADD-TO($collection$, $time$)
  end for
end for

$\mathcal{W} \leftarrow$ COMPUTE-WEIGHT($collection$)
return $\mathcal{W}$

- GENERATE-VALIDATOR()
  - Creates a validators with some unbonded balances.
- VALIDATE($validator$)
  - Bonds balances of *validator* and bonds balances.
- GENERATE-NOMINATORS($amount$)
  - Creates the *amount* of nominators with some unbonded balances.
- NOMINATE($validator$, $nominator$)
  - Starts nomination of *nominator* for *validator* by bonding balances.
- CREATE-REWARDS($validator$, $nominators$, era_depth)
  - Starts an Era and creates pending rewards for *validator* and *nominators*
- TIMER($function$)
  - Measures the time from the start of the specified $function$ to its completion.
- ADD-TO($collection$, $time$)

- Adds a returned time measurement (*time*) to *collection*.

- COMPUTE-WEIGHT(*collection*)

  - Computes the resulting weight based on the time measurements in the *collection*. The worst case scenario should be chosen (the highest value).

2.5.3 Practical Example #3: `balances`

The *transfer* function of the `balances` module is designed to move the specified balance by the sender to the receiver.

Analysis

The source code of this function is quite short:

```
let transactor = ensure_signed(origin)?;
let dest = T::Lookup::lookup(dest)?;
<Self as Currency<_>>::transfer(
  &transactor,
  &dest,
  value,
  ExistenceRequirement::AllowDeath
)?;
```

However, one need to pay close attention to the property `AllowDeath` and to how the function treat existingand non-existing accounts differently. Two types of behaviors are to consider:

- If the transfer completely depletes the sender account balance to zero (or bellow the minimum "keep-alive" requirement), it removes the address and all associated data from storage.

- If recipient account has no balance, the transfer also needs to create the recipient account.

Considerations

Specific parameters can could have a significant impact for this specific function. In order to trigger the two behaviors mentioned above, the following parameters are selected:

Type		From	To	Description
Account index	`index` in...	1	1000	Used as a seed for account creation
Balance	`balance` in...	2	1000	Sender balance and transfer amount

Executing a benchmark for each balance increment within the balance range for each index increment within the index range will generate too many variants (1000×999) and highly increase execution time. Therefore, this benchmark is configured to first set the balance at value 1'000 and then to iterate from 1 to 1'000 for the index value. Once the index value reaches 1'000, the balance value will reset to 2 and iterate to 1'000 (see algorithm 2.5.4 for more detail):

- `index`: 1, `balance`: 1000
- `index`: 2, `balance`: 1000
- `index`: 3, `balance`: 1000
- ...
- `index`: 1000, `balance`: 1000
- `index`: 1000, `balance`: 2
- `index`: 1000, `balance`: 3
- `index`: 1000, `balance`: 4
- ...

The parameters itself do not influence or trigger the two worst conditions and must be handled by the implemented benchmarking tool. The $transfer$ benchmark is implemented as defined in algorithm 2.5.4.

Benchmarking Framework

The benchmarking implementation for the Polkadot Runtime function $transfer$ is defined as follows (starting with the MAIN function):

Algorithm 2.3 Run multiple benchmark iterations for *transfer* Runtime function

Output: *collection*: a collection of time measurements of all benchmark iterations

```
function Main
    Init collection = {}
    Init balance = 1′000

    for index ← 1, 1′000 do
        time ← Run-Benchmark(index, balance)
        Add-To(collection, time)
    end for

    Init index = 1′000
    for balance ← 2, 1′000 do
        time ← Run-Benchmark(index, balance)
        Add-To(collection, time)
    end for

    W ← Compute-Weight(collection)
    return W
end function

function Run-Benchmark(index, balance)
    sender ← Create-Account("caller", index)
    recipient ← Create-Account("recipient", index)
    Set-Balance(sender, balance)

    time ←Timer(Transfer(sender, recipient, balance))
    return time
end function
```

- Create-Account(*name*, *index*)

  - Creates a Blake2 hash of the concatenated input of *name* and *index* representing the address of a account. This function only creates an address and does not conduct any I/O.

- Set-Balance(*account*, *balance*)

  - Sets a initial *balance* for the specified *account* in the storage state.

- Transfer(*sender*, *recipient*, *balance*)

  - Transfers the specified *balance* from *sender* to *recipient* by calling the corresponding Runtime function. This represents the target Runtime function to be benchmarked.

- Add-To(*collection*, *time*)

  - Adds a returned time measurement (*time*) to *collection*.

- Timer(*function*)

  - Measures the time from the start of the specified *function* to its completion.

- Compute-Weight(*collection*)

  - Computes the resulting weight based on the time measurements in the *collection*. The worst case scenario should be chosen (the highest value).

2.5.4 Practical Example #4

The `withdraw_unbonded` function of the `staking` module is designed to move any unlocked funds from the staking management system to be ready for transfer. It contains some operations which have some I/O overhead.

Analysis

Similarly to the `payout_stakers` function (2.5.2), this function fetches the Ledger which contains information about the stash, such as bonded balance and unlocking balance (balance that will eventually be freed and can be withdrawn).

```
if let Some(current_era) = Self::current_era() {
  ledger = ledger.consolidate_unlocked(current_era)
}
```

The function `consolidate_unlocked` does some cleaning up on the ledger, where it removes outdated entries from the unlocking balance (which implies that balance is now free and is no longer awaiting unlock).

```
let mut total = self.total;
let unlocking = self.unlocking.into_iter()
  .filter(|chunk| if chunk.era > current_era {
    true
  } else {
    total = total.saturating_sub(chunk.value);
    false
  })
  .collect();
```

This function does a check on wether the updated ledger has any balance left in regards to staking, both in terms of locked, staking balance and unlocking balance. If not amount is left, the all information related to the stash will be deleted. This results in multiple I/O calls.

```
if ledger.unlocking.is_empty() && ledger.active.is_zero() {
  // This account must have called `unbond()` with some value that caused the active
  // portion to fall below existential deposit + will have no more unlocking chunks
  // left. We can now safely remove all staking-related information.
  Self::kill_stash(&stash, num_slashing_spans)?;
  // remove the lock.
  T::Currency::remove_lock(STAKING_ID, &stash);
  // This is worst case scenario, so we use the full weight and return None
  None
```

The resulting call to `Self::kill_stash()` triggers:

```
slashing::clear_stash_metadata::<T>(stash, num_slashing_spans)?;
<Bonded<T>>::remove(stash);
<Ledger<T>>::remove(&controller);
<Payee<T>>::remove(stash);
<Validators<T>>::remove(stash);
<Nominators<T>>::remove(stash);
```

Alternatively, if there's some balance left, the adjusted ledger simply gets updated back into storage.

```
// This was the consequence of a partial unbond. just update the ledger and move on.
Self::update_ledger(&controller, &ledger);
```

Finally, it withdraws the unlocked balance, making it ready for transfer:

```
let value = old_total - ledger.total;
Self::deposit_event(RawEvent::Withdrawn(stash, value));
```

Parameters

The following parameters are selected:

Type		From	To	Description
Account index	`index` in...	0	1000	Used as a seed for account creation

This benchmark does not require complex parameters. The values are used solely for account generation.

Considerations

Two important points in the `withdraw_unbonded` function must be considered. The benchmarks should trigger both conditions

- The updated ledger is inserted back into storage.
- If the stash gets killed, then multiple, repetitive deletion calls are performed in the storage.

Benchmarking Framework

The benchmarking implementation for the Polkadot Runtime function `withdraw_unbonded` is defined as follows:

Algorithm 2.4 Run multiple benchmark iterations for $withdraw_unbonded$ Runtime function

Output: $\mathcal{W}$

function MAIN
  Init collection = {}

  for $balance \leftarrow 1, 100$ **do**
    $stash \leftarrow$ CREATE-ACCOUNT("STASH", 1)
    $controller \leftarrow$ CREATE-ACCOUNT("CONTROLLER", 1)
    SET-BALANCE($stash$, 100)
    SET-BALANCE($controller$, 1)
    BOND($stash$, $controller$, $balance$)
    PASS-ERA()
    UNBOND($controller$, $balance$)
    PASS-ERA()
    $time \leftarrow$TIMER(WITHDRAW-UNBONDED($controller$))
    ADD-TO($collection$, $time$)
  end for

  $\mathcal{W} \leftarrow$ COMPUTE-WEIGHT($collection$)
  return $\mathcal{W}$
end function

- CREATE-ACCOUNT($name$, $index$)

  - Creates a Blake2 hash of the concatenated input of *name* and *index* representing the address of a account. This function only creates an address and does not conduct any I/O.

- SET-BALANCE($account$, $balance$)

  - Sets a initial *balance* for the specified *account* in the storage state.

- BOND($stash$, $controller$, $amount$)

  - Bonds the specified *amount* for the *stash* and *controller* pair.

- UNBOND($account$, $amount$)

  - Unbonds the specified *amount* for the given *account*.

- Pass-Era()

  - Pass one era. Forces the funtion *withdraw_unbonded* to update the ledger and eventually delete information.

- Withdraw-Unbonded(*controller*)

  - Withdraws the the full unbonded amount of the specified *controller* account. This represents the target Runtime function to be benchmarked

- Add-To(*collection*, *time*)

  - Adds a returned time measurement (*time*) to *collection*.

- Timer($function$)

  - Measures the time from the start of the specified $function$ to its completion.

- Compute-Weight(*collection*)

  - Computes the resulting weight based on the time measurements in the *collection*. The worst case scenario should be chosen (the highest value).

2.6 Fees

Block producers charge a fee in order to be economically sustainable. That fee must always be covered by the sender of the transaction. Polkadot has a flexible mechanism to determine the minimum cost to include transactions in a block.

2.6.1 Fee Calculation

Polkadot fees consists of three parts:

- Base fee: a fixed fee that is applied to every transaction and set by the Runtime.
- Length fee: a fee that gets multiplied by the length of the transaction, in bytes.
- Weight fee: a fee for each, varying Runtime function. Runtime implementers need to implement a conversion mechanism which determines the corresponding currency amount for the calculated weight.

The final fee can be summarized as:

$$\begin{aligned} fee = &\, base\ fee \\ &+ length\ of\ transaction\ in\ bytes \times length\ fee \\ &+ weight\ to\ fee \end{aligned}$$

2.6.2 Definitions in Polkadot

The Polkadot Runtime defines the following values:

- Base fee: 100 uDOTs
- Length fee: 0.1 uDOTs
- Weight to fee conversion:

$$weight\ fee = weight \times (100\ uDOTs \div (10 \times 10'000))$$

  A weight of 10'000 (the smallest non-zero weight) is mapped to $\frac{1}{10}$ of 100 uDOT. This fee will never exceed the max size of an unsigned 128 bit integer.

2.6.3 Fee Multiplier

Polkadot can add a additional fee to transactions if the network becomes too busy and starts to decelerate the system. This fee can create an incentive to avoid the production of low priority or insignificant transactions. In contrast, those additional fees will decrease if the network calms down and it can execute transactions without much difficulties.

That additional fee is known as the `Fee Multiplier` and its value is defined by the Polkadot Runtime. The multiplier works by comparing the saturation of blocks; if the previous block is less saturated than the current block (implying an uptrend), the fee is slightly increased. Similarly, if the previous block is more saturated than the current block (implying a downtrend), the fee is slightly decreased.

The final fee is calculated as:

$$final\ fee = fee \times Fee\ Multiplier$$

Update Multiplier

The `Update Multiplier` defines how the multiplier can change. The Polkadot Runtime internally updates the multiplier after each block according the following formula:

$$\begin{aligned} diff &= (target\ weight - previous\ block\ weight) \\ v &= 0.00004 \\ next\ weight &= weight \times (1 + (v \times diff) + (v \times diff)^2/2) \end{aligned}$$

Polkadot defines the `target_weight` as 0.25 (25%). More information about this algorithm is described in the Web3 Foundation research paper: `https://research.web3.foundation/en/latest/polkadot/Token%20Economics.html#relay-chain-transaction-fees-and-per-block-transaction-limits`.

Chapter 3

Consensus

3.1 BABE digest messages

The Runtime is required to provide the BABE authority list and randomness to the host via a consensus message in the header of the first block of each epoch.
The digest published in Epoch $\mathcal{E}_n$ is enacted in $\mathcal{E}_{n+1}$. The randomness in this digest is computed based on the all the VRF outputs up to including Epoch $\mathcal{E}_{n-2}$ while the authority set is based on all transaction included up to Epoch $\mathcal{E}_{n-1}$.
The computation of the randomeness seed is described in Algorithm 3.1 which uses the concept of epoch subchain as described in host specification and the value d_B, which is the VRF output computed for slot s_B.

Algorithm 3.1 EPOCH-RANDOMNESS($n > 2$: epoch index)

1: **Init** $\rho \leftarrow \phi$
2: **for** B in SUBCHAIN($\mathcal{E}_{n-2}$) **do**
3: $\quad \rho \leftarrow \rho || d_B$
4: **end for**
5: **return** BLAKE2B(EPOCH-RANDOMNESS$(n-1)||n||\rho$)