Aartum: A platform valuing verified communal benefits

The *Aartum founders group*

Contents

Chapter 1

Preamble

1.1 Cryptocurrency mining as selling environmental damage

Cryptocurrencies will in all likelihood take up a permanent place as means of exchange in the world economy. Although these currencies offer unprecedented opportunities, the practice of securing the network through *mining* based on the *proof-of-work* consensus mechanism is environmentally harmful because of the vast quantities of electricity required for mining. A recent report gave the electricity consumption of global Bitcoin mining as equivalent to that of Argentina[1]. In essence, cryptocurrency miners are producing two products: the distributed ledger that is secured and the greenhouse gases that result from the mining process. Miners are, in effect, converting environmental damage to cryptocurrency value. There are attempts to break this relationship through either using renewable energy for the mining itself or avoiding excessive power consumption by using alternative consensus mechanisms such as a *proof of stake*. The large cryptocurrencies, however, still rely on *proof-of-work*.

1.2 Communal benefit as basis for cryptocurrency value

For a cryptocurrency to have maximum benefit to humanity, the relationship between cryptocurrency value and environmental impact must be inverted from its current state: the value of cryptocurrencies must be linked to real environmental *benefits*. In fact, the most beneficial situation for humanity would be a state of affairs where every token of value is linked, not to an arbitrary waste of resources, but to a communal benefit - whether environmental or otherwise - to the human race and the planet.

For this to be viable we need a new gold standard based on verified outcomes of a set of communal goals. One widely supported articulation of such a set of

[1] https://www.morganstanley.com/ideas/cryptocurrencies-global-utilities

goals is the UN Sustainable Development Goals (SDG). Goal 13 (*Take urgent action to combat climate change and its impacts*) serves as a logical starting point for implementing this idea, as a robust means of verification of the outcomes is already available for greenhouse gas emission reductions.

The process of *mining* in proof-of-work cryptocurrencies serves, *inter alia*, to regulate scarcity and avoid devaluation of the currency through over-supply. It is an essential feature of the system that *mining* must be difficult and require resources because this guarantees the scarcity of the currency and protect its value. As communal benefits such as biosphere protection, reforestation, the reduction of greenhouse gas emissions or eradication of poverty are also difficult to achieve and prove, linking the value of cryptocurrencies to such actions can function as the guarantee of scarcity in the same way as environmental destruction though cryptocurrency mining does.

1.3 Tokenisation as incentivisation

In the era when the gold standard was in use, money used to symbolise an actual object that was deemed to be of value, namely the gold in the vault of a central reserve controlled by a government. Such money is referred to as *representative money* because the money represented the asset, and ownership of the representation was deemed to be ownership of the underlying asset. In a system such as this, a fundamental mismatch existed between the need for liquidity in the economy and the supply of gold because the supply of gold was determined by the rate of mining subject to the constraints of the geology, the state of technology and the availability of resources. The gold standard provided a certain stability to currencies but was counter-productive during, for example, the great recession when the US Federal reserve increased interest rates to prevent the depletion of its gold reserves.

National currencies are no longer representative money, but are what is referred to as “fiat currencies”. The experience with representative money does, however, lead to an interesting though-experiment: The choice of gold as the symbol of value incentivised gold mining and the rate of growth of the money supply was linked to the rate of gold extraction. It follows that the choice of another commodity as the reference point for the means of exchange will place that commodity in the same position that gold occupied. The money supply will then be determined by the rate of production of that commodity or commodities. What if those commodities are not things but actions and states that we all want, such as the achievement of the SDGs? Then the production of those states and the practice of those actions would be incentivised in such a way that the means of producing them would take the place that goldmines occupied at the time when the gold standard was in use.

1.4 Conclusion

It is conceivable that a state of affairs can come to exist where unique cryptographic representations of verified communal benefits function as a symbol of value in a way similar to how paper money represented gold at the time of the gold standard.

Chapter 2

Aartum

2.1 Overview

2.1.1 .

Aartum[1] is a platform originated by the Nova Institute[2] for an ecosystem where communal benefits (such as, conceivably, all SDG outcomes) can be verified, tokenised, reported, traded and retired. In this chapter we set out the Aartum concept in detail, describe the targeted governance structure of the platform, and look at some of the envisioned use cases. A roadmap for the development of *Aartum* is provided later in chapter 4.

2.2 Concept

2.2.1 Verification and tokenisation of achieved outcomes

The basic problem that must be addressed in a blockchain-based ecosystem that tokenises real world outcomes is the accuracy and veracity of the data stored in the blockchain. Blockchain systems themselves are inherently tamper-resistant and transparent - many checks can be done programmatically (at any point in time) to verify that the data on the blockchain has been processed according to the rules of the blockchain. There is, however, no comprehensive way to determine the extent to which the data captured accurately represents the real-world states or events on which they report. The most vulnerable phase in the process of tokenising a real world outcome is where real world data is recorded in the blockchain. Physical verification of the raw data captured on the blockchain must therefore be an integral part of the system.

To address this requirement, the Aartum platform will house a hierarchy of SDG standards and methodologies. The SDG-specific standards will provide the principles on which such verification should be based, and activity-specific

[1] From the root for *earth* (a-r-ṭ) in a large variety of languages including Afrikaans, Arabic, Danish, Dutch, English, German, Hebrew, and, in inverted from, in the languages deriving from Latin (t-r-a)

[2] An independent, South African, not-for-profit company. www.nova.org.za

methodologies will provide detailed procedures for verifiers. All standards and methodologies will be underlined by the Aartum Protocol. This hierarchy of standards and methodologies is discussed below.

2.2.1.1 The Aartum Protocol

The *Aartum Protocol* contains the conceptual framework, definitions and procedures according to which SDG-specific standards come into being. This includes definitions of *valued outcomes*, *activity boundaries*, *ownership* and *additionality* as well as procedures for avoiding double counting and conflicting impacts across SDGs.

2.2.1.1.1 Transparency, reproducibility and triangulation enhance veracity

In order to ensure that tokens uniquely represent specific outcomes in all material aspects, the Protocol requires that the process through which a token came into existence should be transparent and reproducible from the raw data right up to the issuance of the token. This means that data and meta-data on a token's origination and verification process should be stored, and the methods for the transformation of that data should be unambiguous so that it may be repeated by another party to get the same result. Persistence of data or parameters greatly adds to the confidence that third parties can have because it allows for triangulation.

The data collected should provide transparency on five aspects:

- What really happened? (Activities)
- Wouldn't it have happened anyway? (Baseline)
- Who is really responsible? (Agency)
- Are all the relevant outcomes included? (Completeness)
- Is the representation unique? (Representation)

The Protocol further requires that: * Project operators should be identified * The identity of the agent that records the data (whether that is an instrument, an IoT device of a human) must be known * Software components that transform the data should be identified * The object or subject about which the data is recorded must be identified * Both data and meta-data should be stored * Verifiers should be competent, independent parties * The operator should pay for verification but there should be no incentive for any particular outcome * Verifiers should store data and meta-data on the verification process and so that they themselves can be evaluated.

Project operators should be identified so that the incentives and disincentives of the reputation system can operate. The identity of the agent that records that data enables accountability. Human agents will require a minimum reputation and will have reputation to gain and loose. Identification of instruments and IoT devices will make it possible for verifiers to initially confirm the instrument specifications and then monitor data on-chain. Software components will be handled in a similar way (although more centralised): Software components will be developed to process data in accordance with a specific methodology. The software component will be tested against series of unit tests that accompany the methodology. If it passes, the specific component, identified by its SHA256 hash will be authorised to be used in execution of the relevant methodology. Identifying and storing both data and meta-data about the subject or object observed will enable in situ verification through re-measurement of the same subject or object an also to some extent off-site. Different aspects of project verification can be carried out by different parties and weighted and aggregated through smart contracts. Payment for verification services could be done in a similar way. The same requirements that hold for verification of project activities will also be applied for the verification process.

Is it hardly possible that the first draft of the Protocol, encompassing such a broad scope, will be suitable for all situations. There will be a need to refine and update the standard as more SDG specific standards come into being and as users gain more experience.

2.2.1.2 SDG standards

Each SDG-specific standard defines concepts, procedures and unit of measure relevant to that goal. Standards allow for differentiation and comparison between outcomes because they provide clarity on what is meant by certain terms and what conditions need to be met before a certain claim can be made. Two outcomes that both comply to a standard can be compared in terms of the metrics relevant to that standard.

In order to provide the framework though which the unique significance of an outcome can be articulated, the standards used must provide a way to objectively and transparently describe the dimensions of an activity and provide a procedure for proving the causal link between an activity and an outcome. The dimensions of an activity comprises both what was done, who the agent of each action was and what the consequences of the activity was.

Standards give guidance on how to take something unique (an activity by an agent) and quantify its consequences as something generic. It is normally the consequences of an activity that is quantified.

2.2.1.2.1 Acknowledge historic achievements of existing standards

Although we envision that the *Aartum* community will create blockchain-based accounting standards in future, we acknowledge the significant contribution that existing standards have already made. There are well-established standards with proven track-records that produce environmental credits of various kinds. These standards operate both under the auspices of the United Nations, nation states and local governments but also in the domain of business and civil society organisations. Under these standards, various environmental assets such as certified or verified greenhouse gas emission reductions, water benefit certificates and renewable energy certificates are issued. In general, the communities producing, selling and using these environmental assets are aware of the difference between standards in terms of their inclusion criteria and validation and verification practices. These differences reflect in the price of the commodity - typically higher levels of certainty (i.e. more stringent standards and verification practices) and more co-benefits reflect in higher prices for the environmental assets. The *Aartum Protocol* will provide the framework by which assets created against these standards can be tokenised while avoiding double counting. Articulation with existing standards are further discussed in [chapter 3] of this document.

2.2.1.3 Methodologies

2.2.1.3.1 .

Of particular importance is the procedure for the development of methodologies. A methodology targets a specific outcome expressed in a unit of measure defined by a SDG-specific standard.

Methodologies specify rules for processing raw data into SDG-related outcomes expressed in specific units of measure. A methodology will take the form of a humanly readable component and a software component. The humanly readable component will be document giving guidance on applicability of the methodology including its alignment to a SDG-specific standard and providing the definitions of entities, states and activities units to be quantified. It will also provide a procedure for establishing the baseline scenario (additionality) as well as the procedures for monitoring.

The software component of a methodology will consist of a series of tests that can be used to unit test transaction processors to ensure that the transaction processors produce valid responses in accordance with the methodology. Such a unit test must contain valid and invalid data to ensure that the transaction processor not only produces correct results from valid data but also that it correctly ignores invalid data. A new methodology need not include a transaction processor but only a unit test that can be used to test a transaction processor.

Every software component in the ecosystem will have an identity which may be an MD5-hash. A transaction processor can be registered after passing the unit test. The provenance of each unit, including the specific transaction processor that performed the processing of the raw data, can therefore be recorded. This transparency strengthens the total quality.

A unit of any pure PoW cryptocurrency represents nothing in the world outside the blockchain except the application of processing power with the accompanying opportunity cost and environmental impact. This is often viewed as a feature but may also be the cause of the inherent instability evident in such currencies. On the other hand, a cryptographic token of a communal benefit (such as a positive environment or social impact) makes reference to empirical phenomena. Such a token represents a claim to causality where an agent claims to be the cause of changes in real-world states. Such a claim will necessarily involve quantification of states and activities.

All quantification is expressed in a specific unit of measure according to some scale. The simplest scale just records the presence or absence of a single property. For any quantification to take place, observations of the empirical phenomena must be made and encoded as data. In all likelihood, aggregation and secondary transformations of this data will also take place in order to arrive at a final quantification in the relevant unit of measure.

For a measure to be a measure of *impact*, it must also include an estimate of what the situation would have been had the agent not undertaken the activity that lead to the changes in real-world states. Such a reference level is per definition counterfactual.

2.2.2 Trading tokenised outcomes

2.2.2.1 Determining the value of a token

The value of a *utility token* is a function of the community of users' assessment of the future willingness and ability of a service provider to exchange the token for a service, combined with their assessment of their own and others' desire for the service in future[3]. The value of an *equity token* is a function of the community of users' perception of the enduring value of the asset and the future enforceability of the rights represented by ownership of the token.

The way in which the value of a cryptographic token of an accomplished real-world outcome is determined, bears likeness to that of utility tokens as well as equity tokens: it is a function of the community of users' estimation of the significance of such an outcome, their evaluation of the likelihood that such a token indeed uniquely represents the specific outcome in all material aspects, and the likelihood that a claim to be the cause of such an outcome will have value in future.

A central problem to be solved for *Aartum* to be used as a general means of exchange is how to determine the relationship between the specific SDG-related units of measure (such as tonne CO-2- equivalent for Goal 13) and the face value (in ART) assigned to that outcome at issuance (for a discussion on fungibility, please refer to the discourse at the end of the chapter). The relationship between face value and the true underlying value (purchasing power) of any currency is a dynamic phenomenon, e.g. inflation means that although the face value of money does not change, its underlying purchasing power decreases over time. The value of a token of an SDG-related outcome will change with the community of users' perception of the value of that outcome, their anticipation that other people will value it in future and their trust in the uniqueness, certainty and accuracy of its representation of the outcome it claims to represent.

The relationship between the face value (ART) of an *Aartum* token and the specific SDG-related units of measure is similar to the relationship between the face value of a stamp and its value to a collector. In normal usage (i.e. for posting a letter), the value of a stamp is its face value but a certain stamp may be worth much more to a collector due to some specific property of that stamp (e.g. its scarcity or being part of a batch with a rare printing mistake).

When *Aartum* is issued the token will contain details of the provenance, the verification process and a quantification of the SDG-related outcome achieved in its appropriate unit of measure. In addition to this it will have a face value in units of ART. That face value will be calculated from the mean of the recent transactions for comparable outcomes.

[3] A currency can of course be viewed as the most generic utility token of all.

Consider the following example: There is a marked preference in the market for voluntary greenhouse gas emission reductions (VERs) from specific project types and areas of origin. Such VERs routinely fetch higher prices compared to other project types or areas of origin. With a transaction history of trades of VERs of different types, it is possible to predict the price that a specific VER is likely to fetch based on its proporties. *Aartum* will provide a platform where offers and bids for specific tokens (i.e. specific goal, activity type, methodology, units of measure, areas of origin or level of verification) can be made and executed. An offer would be when the owner of a specific token offers the token for sale for a specific fraction or, more likely, a multiple of its face value. When a bid is made and a trade takes place, this data will serve as evidence that the community values a specific set of properties more. When a new issuance taken place, the face value of the new issuance would be such that it would not sell immediately at a markup or discount - i.e. based on the history of trades, the prediction model would attempt to allocate the *correct* face value to the token.

The core of the *Aartum* ecosystem is the *Aartum protocol* which describes the core concepts and principles of accounting for SDG-related outcomes and will form the basis for 16 SDG-specific standards. Each unit of Aartum will remain linked to a specific SDG-aligned outcome expressed in a unit of measure defined by an approved methodology. The reference to the unique provenance of each unit is maintained as part of each token by including the reference and hash of the issuance transaction. This reference will provide access to the provenance blockchain of the project where the user may verify the SDG goal, the specific standard, unit of measure and details of the the verification process. A unit of *Aartum* is therefore literally a token of the achievement of an SDG-aligned outcome.

2.3 Governance

To be sustainable in the long term, *Aartum* will have to belong to a community and not be monopolised by particular interests. *Aartum* will therefore be constituted so as to provide the platform for such a collaborative community to come into being and to create the standards and tokens that will facilitate activities in pursuit of the SDGs on the scale needed. We specifically aim to create a system that is open to contribution by all but biased by design to ever improving quality. This has important implications for identity and reputation management of collaborators because incentives for meaningful contributions and disincentives for bad behaviour are built into the system. Changes to standard, methodologies, procedures as well as software version will be effected by voting. Voting will be weighted by domain-specific reputation which is built up through peer-assessed contribution.

The Aartum governance regime thus rests on three pillars: openness, identity and reputation. Each is elaborated upon below.

2.3.1 Openness

2.3.1.1 .

Aartum's vision is that of a universally accessible, widely trusted and comprehensive ecosystem where real communal benefits function as the symbol of value. It is conceivable that there would be an advantage in the short term to one entity keeping control over the development of the platform. This would greatly simplify decision-making but also tie the platform to the fate of a single entity. Granting control to a consortium is also an option. Many very large and successful project are managed as such, e.g. Hyperledger, the X project and the Open Container Initiative. A consortium does increase the complexity of decision-making compared to an individual entity but it provides better adoption into the market. In the design of *Aartum* we choose, for a fundamentally open governance model with the provision that influence will be proportional to peer-reviewed contribution. We refer to this as *reputation.* This means concretely that participation is open to anyone but that a participant's ability to influence consequential decisions is based on their prior contribution to the ecosystem. Fundamental openness does does not preclude the organisation of consensus-seeking meetings or groups but it will prevent a smaller group from gaining permanent control over the ecosystem.

The *Aartum* transaction platform will be accessible free of change through a web and mobile wallet. This is fairly standard for most public blockchains. A distinctive aspect of the *Aartum* platform is that it is open to all contributors but that the power of contributors to influence the development of the platform is determined by their domain-specific reputation that is gained over time through peer-assessed contributions. Contributions can take the form of, *inter alia*, commenting on project documentation, ground truthing, project assessments or participation in the draughting of new methodologies and protocols or the revision of existing ones.

Contributions will either be participation in *operation*, *co-creation* or *decision making.* Participation in the *operation* of the platform will be where a person or entity fulfils some of the regular tasks on the platform. This may relate to the technical operation of the nodes in the blockchain network but also to the activities related to validation and verification of projects and outcomes. Participation in *co-creation* means that a person or entity contributes a partial or complete standard, methodology, procedure or software component to the platform. This contribution must be evaluated, tested and refined by peers and eventually incorporated into the platform after a voting process (*decision making*). In all these forms of participation, reputation will play an important role. This is further elaborated under section [2.3.2 Identity and reputation management]. Openness does not mean that anyone can engage in all these activities regardless of past contribution, but that there is an entry level that is open to everyone and that, in principle, everyone can potentially build up reputation and be included in decision-making processes of increasing consequence. This means that every contributor will have to start by making relatively modest contributions before participating in more consequential decisions.

2.3.2 Identity

Another core design decision that has to be taken at the start of the project is the way in which identity and reputation is managed within the ecosystem.

The *Aartum* ecosystem has to make provision for the whole spectrum of opacity of identity ranging from complete anonymity to verified identity. Users who engage in day-to-day transactions require the protection of their privacy. On the other hand, the community will require full transparency of identity from project owners who operate projects that produce verified communal benefits that will be tokenised as *Aartum.* The same also applies for verifiers. The level of identity disclosure will differ for every use case, e.g. the use of *Aartum* for environmental compliance will obviously require that the identity of the complying party must be verified. Table 1 shows how confidentiality requirement escalate by level of privilege increases.

Table 2.1: Confidentiality requirement by level of priviledge

Use case	**Identity requirement**
Buy, sell, transfer *Aartum*	Private and confidential
Contribute to methodologies	Profile: user choice
Accounting and reporting	Profile: user choice
Compliance	Verified real-world identity
Project verification	Verified real-world identity
Project operation	Verified real-world identity
Vote on changes in standards	Profile with voting rights, secret vote

There are also cases where the users will be free to choose their level of identity disclosure. This will be the case for contributing texts or code or making comments and suggestions. User may contribute under a pseudonym and still gain reputation because anonymity and privilege represent different dimensions and the reputation of a contributor is should as far a possible reflect only the quality and quantity of their work. Anonymous users will be allowed to earn reputation that includes voting the acceptance of new standards, methodologies and transaction processors.

2.3.2.1 Protection of privacy in transactional use of *Aartum*

Transaction in *Aartum* will necessarily rely on a UTXO model because each token represents a concrete verified outcome related to a SDG. This means that a single token can potentially be traced through a series of transactions. This problem is present in other applications that use a UTXO (such as Bitcoin). To counter this, the *Aartum* platform will implement *CoinJoin* or a similar protocol that combines and mixes UTXOs in the creation of new transactions is such a way that the exact parties participating in individual transactions are obscured. We foresee that the user will be able to control settings related to this mechanism in their wallets.

2.3.3 Reputation

2.3.3.1 .

The value of a token of an accomplished real-world outcome will be enhanced if the process though which such token is created and traded contains strong incentives for compliance and strong disincentives for anti-social behaviours. A similar mechanism is used to protect the value of traditional PoW cryptocurrencies where there are strong disincentives for launching a so-called 51 percent attack since the attack is likely to cost more than anything that can be gained from it. Proof-of-stake blockchains require users to stake a certain amount of currency for the privilege to perform certain transactions and may withhold the staked amount in cases where users flaunt the rules.

In the case of tokens that represent real-world outcomes, persistence of identity and persistence of data will function as incentives and disincentives. Persistence of data has already been discussed under *Transparency, reproducibility and triangulation enhance veracity*. If data is persistent and public, fraud may be uncovered at any time after the fact.

Persistence of data can, however, only function as an incentive if identity is persistent and valuable. An open system aimed at mass participation cannot practically regulate the creation of new identities (i.e. new users). It is thus conceivable that a user may create numerous identities. Users will embrace a persistent identity if there are advantages to having a persistent identity such as when reputation can be gained over time and that reputation is the key to exerting influence and unlocking value. For reputation to function as incentive, reputation must be valuable and it must be expensive. The reputation needed to be an originator or a verifier should be valuable and expensive so that the loss of reputation associated with the eventual discovery of fraud will represent a real and substantial loss of value. Similarly, the reputation gained from long-standing compliance should unlock increasing value for its owner.

Reputation can therefore function as both incentive (i.e. it enables unlocking of value) and disincentive (i.e. its loss represent an expense) in the same way as staking functions in proof-of-stake blockchains.

Users who want to contribute to *Aartum* by participating in the creation of standards, methodologies and transaction processors will have a profile that may contain any level of detail that they choose. Reputation will be awarded to an identity based on the quality, quantity and duration of contributions and influence will be proportional to reputation. Identity in this context is essentially just a public key - private key combination that is linked to a profile. Nothing stops a users from opening more than one profile but then these profiles will acquire reputation independently.

In order ensure quality and full transparency of provenance, originators of SGD-related outcomes (i.e. project operators) must be positively (legally) identified. For the same reasons, the identity of verifiers must be known.

Reputation will be gained through peer-assessed contribution. Reputation will enable a user to rise though a hierarchy of influence and privilege. To a certain extent we will emulate the reputation model used on stackoverflow.com[4]. Any user will be able to comment on proposals code and texts. More reputation will be required to rate, upvote or downvote a contribution. Formal voting for the acceptance of new methodologies require domain specific reputation, i.e. will be done by users who have contributed though comments, reviews and proposals to that specific knowledge domain.

Users with proven expertise and commitment will be voted into specific positions such as moderators or coordinators of working groups or even ambassador for a specific SDG or the *Aartum* platform as a whole.

Reputation will decay over time to incentivise continued involvement and to prevent a situation where a users that looses touch with the development of the platform continues to hold very large voting rights for a large contribution made years or decades before.

2.4 Envisioned use cases

We envision that users will be able to use *Aartum* in a variety of ways. We specifically want to make *Aartum* applicable to any situation where verified accounting of SDG-related outcomes is needed.

2.4.1 Voluntary SDG or environmental contribution

As a unit of *Aartum* represents a unique, completed and verified SDG-related outcome, *Aartum* can be collected by individuals or entities as a form of voluntary SDG or environmental contribution. A special transaction type (the *retirement transaction*) will allow a unit of *Aartum* to be retired (permanently taken out of circulation). The retirement transaction preserves a record of the person responsible for the retirement (if the user chooses so) and the details of the unit (SDG goal, unit of measure, number of units, reference to issuance transaction). In such a way a user can build up a portfolio of the outcomes which they are responsible for (as the retiree is the end of the causal chain, it it the retiree who is ultimately responsible for the outcome).

Retirement transactions are publicly visible (although the retiree can determine how much information will be shared) and may be incorporated into social media through an API or special retirement registry browser. This will serve individuals, businesses or other entities who want to communicate their environmental or social impact to the public in a specific, permanent and verifiable way.

2.4.2 Accounting and public reporting

As *Aartum* will be based on a hierarchy of standards with clear procedures for verification, *Aartum* will also be suitable for accounting and public reporting of SDG-aligned outcomes even in cases where the activities that give rise to these outcome are not additional (i.e. are part of the normal business of an entity) and therefore not suited to be issued as tradable units. This may be particularly suited to businesses who want to demonstrate the positive impact

[4] https://stackoverflow.com/help/whats-reputation

of their day-to-day business. This will be particularly useful in the field of *Impact Investing*, where investors evaluate both the profitability and social or environmental impact of an investment.

2.4.3 Offsetting

Aartum also offers individuals and businesses the opportunity not only for voluntary contribution but also for offsetting. Offsetting differs from voluntary contribution because in the case of offsetting, two outcomes are compared namely an (negative) outcome related to the actions of the offsetting party (like the greenhouse gas emissions of an individual or business) and a comparable (positive) outcome meant to counterbalance the negative outcome (like a greenhouse gas emission reduction or sink). Offsetting means demonstrating that a specific negative outcome has been compensated for by another comparable beneficial outcome of a similar or larger magnitude resulting from an activity that has been specifically undertaken for the sake of the beneficial outcome. It is important to show that the owner of the negative outcome and the owner of the positive outcome is the same.

2.4.4 Asset-based currency

Every unit of *Aartum* is associated with a specific number of outcomes in a unit of measure related to one of the SDGs but also has a face value (in units of *ART*). The face value will be allocated at issuance reflecting the weighted desirability of the unit, given its properties, at the time of issuance. This means that users will also be able to use *Aartum* as a general currency in the same way as other cryptocurrencies. Although *Aartum* necessarily has a UTXO architecture, we envision that the *Aartum* wallet will give an account-like feel if the user prefers it. The wallet will also include a mixing mechanism to mix or join UTXOs in larger units and improve anonymity.

2.4.5 Environmental compliance

Aartum is supremely suited for use as amechanism for environmental regulation because it provides a permanent record of very specific SDG-aligned outcomes.

Consider the following example: The regulator of a watershed grants a water-use licence to a specific business. A condition of the water-use license is that the business delivers a specific number of water benefit certificates from a specific activity type in that watershed annually. A local NGO operates a wetland restoration project that is already registered to generate *Aartum* under *Goal 6: Ensure access to water and sanitation for all.* The business enters into an agreement with the NGO to buy the *Aartum* that it will then deliver to the regulator. If the *Aartum* produced by this project does not represent enough of the specific unit of measure that the regulator requires (say, tonnes of sediment removed per annum), then the business may develop and register their own project to make up for the shortfall and even sell any excess *Aartum* from that project. The regulator retires the *Aartum* at the end of the year and can therefore unambiguously show the impact of its regulatory efforts in specific and relevant units (e.g. tonnes of sediment avoided per annum form the specific watershed).

The same process will also apply for many other allowances, such as emission- or extraction licences, or the use of any other ecosystems service.

2.4.6 Outcomes-based government

Because each unit of *Aartum* will be a token of the achievement of a specific SDG-aligned outcome, it represents the opportunity for governments to invest directly in desirable outcomes in a way that minimises bureaucracy and allows for maximum market freedom and efficiency. We envision a scenario where governments can budget directly for a specific outcome and, through a smart contract, pay only for that outcome or nothing at all.

A government agency could contribute to the *Aartum* community though the creation of specific standards, methodologies and procedures related to its mandate and then buy outcomes that meet those standards. Since the provenance is included in the token, a government agency can make sure to only buy tokens generated within its own jurisdiction. In such a way the traditional competence of governments (making rules en overseeing compliance) and the private sector (efficient implementation) can both be leveraged.

Consider the following example: A government health agency operates an integrated TB control programme in a specific region. This activity resorts under *Goal 3: Ensure healthy lives and promote well-being for all at all ages.* As a part of this programme it implements the World Health Organisation's DOTS (directly observed treatment short course) method to ensure patients adhere to their prescribed treatment. In addition to operating the programme from existing government facilities, the agency also creates a smart contract that buys and retires *Aartum* from DOTS outcomes within its jurisdiction. The agency can do this because it is satisfied that the methodology used to accredit providers and record and verify the outcomes meet its own internal quality standards, because the agency itself contributed the methodology to the *Aartum* community. It also remains active in the review of project registrations and the verification of outcomes. In this way private health facilities and NGOs can provide the service in areas where there are no current government facilities. The agency's own annual reporting is simplified by the fact that it only pays for verified outcomes and can report the exact number of outcomes. All this is achieved without the onerous procurement processes that are usual in the public sector. The creation of procedures and methodologies means that similar programmes can be implemented by other agencies or even private donors world-wide.

2.4.7 Conservation of pristine areas

Goal 14 and 15 are to *Conserve and sustainably use the oceans, seas and marine resources for sustainable development* and to *Protect, restore and promote sustainable use of terrestrial ecosystems, sustainably manage forests, combat desertification, and halt and reverse land degradation and halt biodiversity loss.* The fact that naturally pristine areas have little direct monetary value if they remain pristine is a difficult economic problem. We foresee that *Aartum* can be used to create standards for the maintenance of environmental integrity for specific ecosystem types. Owners or caretakers of vulnerable ecosystems can then generate *Aartum* from the maintenance or rehabilitation of such areas. This will enable individuals and other entities to directly contribute to the conservation of vulnerable ecosystems and at the same time provide an income to owners or caretakers of vulnerable ecosystems as an alternative to the direct (extractive) economic exploitation thereof.

2.4.8 Gaming

We foresee that *Aartum* could be integrated in gaming, in particular in world-building games where *Aartum* provides an interesting link between the real world and the world of the game. World-building games can be structured is such a way that the outcomes represented by *Aartum* token play a similar role in the world of the game as it does in real life, e.g. a player would need a small amount of *Aartum* from Goal 1 to prevent their population in the game-world to suffer starvation.

–>

2.5 Discourse: The ideal of trustless transactions

Cryptocurrencies strive to enable trustless transactions. Trustlessness is achieved by removing all but a single link between the symbolic world represented by the data on the blockchain and the material everyday world of the users. Pure (proof-of-work) cryptocurrencies are successful because they value only a single linkage to the real world namely processing power and because that linkage to the real world can be incorporated into the symbolic world of the blockchain in a way that cannot be forged[5].

An approach that values real-world effects faces the challenge of how real-world activities and states are converted to data and stored on the blockchain. It is clear that a stronger link to reality requires a stronger concept of the identity of the originator of the benefits and a concept of verification which incorporates real-world observations. This raises the question as to whether such a system can also satisfy the ideal of trustless transactions.

Linking the value of cryptocurrencies to proof of communal global benefits brings to the fore an aspect that have to date been under-emphasised in the cryptocurrency market, namely the difference between faith and trust. We use faith to refer to that form of confidence that is orientated on another person or on the future state of affairs while trust means the belief that a certain state of affairs is what it appears to be. Trust therefore functions on the level of the transaction, while faith functions at the level of the currency.

It has been said that *the value of any currency is largely a matter of faith*[6]. because a buyer's willingness to pay reflects their assessment of the probability that another buyer will value that commodity and currency in future. An aggregate indicator of level of faith of a certain community (market) in a currency is

[5] The emergence of mining pools has in the mean time demonstrated the limits of this approach.

[6] JACQUES PLAUT, https://bit.ly/2Nxpre3

provided by the interest rate, the inflation rate and the inter-currency exchange rates.

The emergence of distributed ledger technology has been called a revolution in trust since completely unknown parties can transact without the needing to trust or even know each other in any way. Although it may be technically true that no trust is needed for transactions in the virtual realm, especially with mechanisms such as smart contracts, it is not true that no faith is needed. Trustless does not mean certain with regard to value because value is always a perception of an individual (or, in aggregate, a market). The user trusts the network and needs faith that the currency they holds today will still be desired by other people as a means of exchange in future. The massive volatility in the value of cryptocurrencies shows that this faith is sometimes unfounded and that in some cases users had too much faith.

It is important to understand that a trustless system is actually a trusted system made up of untrusted members and that the certainty created is only valid in the system and on condition that the system itself is trusted. In a trustless system the user trusts the system itself and therefore does not need to trust the members as far as the veracity of a single transaction is concerned. There are reasons to trust the major cryptocurrencies but absolute certainty is not an option. Whether there is reason to have faith in the major cryptocurrencies is entirely a different matter. It is not unlikely that the faith in the major cryptocurrencies will be eroded by continued awareness of the gratuitous waste of resources necessitated by cryptocurrency mining.

Cryptocurrencies based on environmental or social impacts assets require little trust but require slightly more faith. As with all cryptocurrencies, the end-user has to trust the system. In addition to this, the end user has to trust the verifier of the benefits. A system of proofs and guarantees of the underlying environmental assets that is open to verification by the end-user is therefore needed to keep the quantum of trust as low as possible.

The pretence that the major cryptocurrencies enable trustless transactions can therefore not be understood to refer in any way to the value and usability of the currency but only the that veracity of transactions. With a suitable consensus mechanism, a currency based on verified communal benefits can be trustless as well.

2.6 Discourse: On fungibility

The basic problem of a fungible token of real-world outcomes is that the outcomes are unique and that fungibility is, per definition, the removal of uniqueness.

The following example illustrates the problem: The value of a fungible token of an SDG-related outcome, say of the avoidance of one tonne of CO_2 (a carbon credit), gravitates towards the minimum value of that outcome in the market. This is because buyers have no reason to believe that a fungible carbon credit will have any of the properties of a premium credit. Suppliers will therefore be motivated to tokenise their most unattractive credits first. In practise the price of carbon credits vary widely[7]. This variation is determined by the specifics of the provenance including the quality of verification, the project type, location and especially the co-benefits resulting from the project. A fungible carbon credit destroys the most important drivers of the price of carbon credits.

Numerous attempts[8] have been made to create cryptographic representations of environmental assets like carbon credits in order to make these assets more liquid. To date these efforts has not yet lead to mass adoption in the market. Given that fungible tokens of a specific outcomes like environmental assets can be expected to gravitate towards the lowest price for that class of asset, this approach does not hold much promise and tokenisation will destroy value for all but the lowest quality assets. The only application for such token are for environmental compliance where the buyer is forced to buy the assets and may not be interested in anything but a single property. The current situation for environmental assets like carbon credits is that, except for compliance purposes, these assets are non-fungible and developers and resellers emphasise the specific properties and co-benefits of their project in order to achieve better prices. Giving up on the ideal of fungibility therefore means that the *status quo* continues and that tokenisation does not make much sense. This also means that the opportunity to accelerate of demand for such assets is missed.

A possible approach to overcoming the tension between fungibility and thus liquidity on the one hand and uniqueness on the other is to issue a separate token for each quantifiable benefit from the same activity in their relevant units of measure but to allocate a face value to each unit in addition to its relevant unit of measure. The face value serves as a common denominator for interchange between different units of measure.

Generation of a separate token for each quantifiable benefit is possible where standards and methods exist to quantify each benefit. The purpose of the *Aartum* platform is to eventually be support the quantification of outcomes related to all the SDGs. This will however be limited in the short term as standards and methods are being developed. Tokenising those benefits for which methods are readily available is an improvement on the one-dimensional approach but it may represent a loss of value for some projects with benefits that are present but difficult to quantify or properties that make them valuable that are not related to specific outcomes. An example of such a property is the location of the project. The allocation of a face value determined by market forces at the time of issuance may overcome this loss of value bought about by tokenisation to some extent.

Following this approach, one has to choose between issuing multi-dimensional tokens or issuing a separate token for each quantifiable benefit from the same activity. Market forces will determine the rate of exchange between tokens representing different types of outcomes (either separately or in a multi-dimensional token) in the same way as it does for fiat currencies. Data from inter-outcome exchanges will be used to allocate a face value (in ART) at the time of issuance. Face value therefore functions as the recommended exchange rate based in a

[7] see the *State of the Voluntary Carbon Markets report* at https://www.forest-trends.org/sovcm2019/.

[8] For example *Veridium*, *Carbon Coin*, *Earth Token*, *Solar Coin*, *ixo* and the *Regen Network*

common denominator (ART) at the time of issuance. Ideally a unit will not trade above of below its face value immediately after issuance.

Chapter 3

Technical implementation

In this chapter we outline the proposed technical implementation of the core design of the platform. Section 3.1 discussed the collaboration platforms to be used. Section 3.2 gives an overview of the design on the Aartum Accounting Blockchain and Section 3.3 does the same for the Aartum Trading Blockchain.

3.1 Collaboration

The development of the *Aartum* platform will involve development of text (Standards, methodologies, procedures, training material) and the development of computer code. There are different best practices for collaborative work in these two fields.

For collaborative writing we will use a wiki[1] because it is simple and easy to use. It will allow anyone to contribute to the writing of a documents (e.g. methodology/standard), regardless of reputation. Users will be able to make contributions anonymously or associated with a certain identity. Mature pieces developed in this way will then submitted for inclusion in the official standards, methodologies or procedures. Inclusion will be determined through a reputation-weighted voting process.

For collaborative development of computer code we will use a git repository housed on www.github.com/aartum.

3.2 Aartum Accounting Blockchain

3.2.1 Overview

This part of the paper sets out the design and functioning of the Accounting Blockchain (hereafter abbreviated as AccB) on a technical level - complete with Protocol Buffers [2] where necessary.

[1] "A wiki is a knowledge base website on which users collaboratively modify content and structure directly from the web browser". See https://en.wikipedia.org/wiki/Wiki

[2] See https://developers.google.com/protocol-buffers

3.2.2 Architecture

The Aartum platform is built upon the Hyperledger Sawtooth architecture. Sawtooth stores blockchains as addressable Merkle-Radix trees divided into namespaces. The namespace to which a transaction belongs is indicated by the first three bytes of its 35-byte address. The use of the remaining 32 bytes is up to the designers' considerations. Aartum's implementation of the Sawtooth architecture, including namespace design and transaction families, for the platform's Accounting Blockchain is set out below.

3.2.3 Namespaces

The AccB will launch wih 21 namespaces:

- seventeen namespaces for the development of standards and their related methodologies
- one namespace for the management of activities
- one namespace for the management of identities
- one namespace for hosting and refining the Aartum Core Protocol
- one namespace for hosting and refining the Aartum Constitution

Each of these is discussed in more detail below.

3.2.3.1 *standards* namespaces

The platform will launch with seventeen namespaces for standards - one for each SDG:

3b3657 (standards-SDG1-a: 3b365700...x30...00 - 3b3657ff...x30...ff)
5c21e3 (standards-SDG2-a: 5c21e300...x30...00 - 5c21e3ff...x30...ff)
28ad00 (standards-SDG3-a: 28ad0000...x30...00 - 28ad00ff...x30...ff)
1884f2 (standards-SDG4-a: 1884f200...x30...00 - 1884f2ff...x30...ff)
130a1e (standards-SDG5-a: 130a1e00...x30...00 - 130a1eff...x30...ff)
b65d18 (standards-SDG6-a: b65d1800...x30...00 - b65d18ff...x30...ff)
6d9c76 (standards-SDG7-a: 6d9c7600...x30...00 - 6d9c76ff...x30...ff)
804ad0 (standards-SDG8-a: 804ad000...x30...00 - 804ad0ff...x30...ff)
8b47e5 (standards-SDG9-a: 8b47e500...x30...00 - 8b47e5ff...x30...ff)
0006fc (standards-SDG10-a: 0006fc00...x30...00 - 0006fcff...x30...ff)
57e6e6 (standards-SDG11-a: 57e6e600...x30...00 - 57e6e6ff...x30...ff)
498a30 (standards-SDG12-a: 498a3000...x30...00 - 498a30ff...x30...ff)
7a5dc5 (standards-SDG13-a: 7a5dc500...x30...00 - 7a5dc5ff...x30...ff)
a646dd (standards-SDG14-a: a646dd00...x30...00 - a646ddff...x30...ff)
8591ab (standards-SDG15-a: 8591ab00...x30...00 - 8591abff...x30...ff)
3cacc1 (standards-SDG16-a: 3cacc100...x30...00 - 3cacc1ff...x30...ff)
71ea34 (standards-SDG17-a: 71ea3400...x30...00 - 71ea34ff...x30...ff)

These namespaces will store all transactions pertaining to the development and (continuous) refinement of the standard and the methodologies associated with the measurement of an activity's achievement of one or more outcomes related to the SDG.

The two bytes (four characters) following the three bytes of a standard's namespace will be used to organise the namespace by outcome; this allows for up to

65536 outcomes (targets) to be defined under each SDG. The first byte following the two bytes of an outcome's namespace will be used for the version management of the outcome's standard/definition, allowing up to 256 revisions of a definition. The first byte following the version byte of an outcome's standard will be used to divide the remaining namespace according to the methodologies pertaining to the specific version of the outcome's definition/standard, allowing up to 256 methodologies under each outcome definition version.

For example, methodology 23 (17h) for definition version 3 (03h) of outcome 145 (91h) under SDG 4 will occupy the addresses 1884f2.0091.03.17.00...x26...00 - 1884f2.0091.03.17.ff...x26...ff.

3.2.3.2 *activities* namespace

The *activities* namespace will initially comprise only one address prefix, namely '3d3500' (human name 'activities-001'). It will store all transactions pertaining to the management of projects and activities, i.e. registration, evaluation, certificate issuances, etc. Address prefixes '7120e0', '1dac2b', 'aafeb6', 'ad0f43', '2afd27', '935f91', '4bbe52', '02cc20', '08aecf', '64aacd', '7606c0', '7ab7c2', 'fcbd0', '9ee9c7', 'c1cd63', '0caa6c', 'beeed3', 'c086d6' and 'd288cd', will be reserved for potential future use (i.e. as "activities-002", "activities-003", etc.), but will not be activated until the '3d3500' address space is filled to capacity, if ever.

Each project or activity registering on the platform will get its own sub-namespace under the then-current *activities* namespace. The sub-namespace will be indicated by the first 14 characters (i.e. seven bytes) following the three-byte prefix of the main *activities* namespace. This will thus allow a total of 7.205759e+16 (2^(7*8)) projects and activities to register and operate under each main activities namespace (i.e. under each of the 'activities-001', 'activities-002' etc. namespaces). The remaining 25 bytes of the address space of each project/activity will be available for the activity-related transactions.

3.2.3.3 *identities* namespace

The *identities* namespace will initially comprise only the '5e8b8d' address prefix, named 'identities-001'. It will store all transactions pertaining to the management of identities on the , i.e. registration, reputation, etc. Address prefixes 'd8b2cf', 'bdc789', '2abce4', '16cc32', '15fa7c', 'e75006', '97a422', '2b7127', '7b8890', '325d64', '88e867', '17134d', 'a7b023', '036f15', 'b0f08e', '0ff46e', '0d692e', 'ca101e' and 'c90d53' will be reserved for potential future use, but will not be activated until the 'identities-001' namespace is filled to capacity, if ever.

As with the *activities* namespace, the *identities* namespace will be subdivided - each identity on the platform will receive its own sub-namespace. These namespaces will be differentiated through the first nine bytes (i.e. 18 characters) following the three-byte prefix of the then-current identities namespace, allowing the system to distinguish between 4.722366e+21 unique participants. Note that an identity can represent an individual or a group of individuals (e.g. a company or workgroup) acting as one entity. The remaining 23 bytes of the address space of each participant will be used for transactions pertaining to reputation management etc.

3.2.3.4 *protocol* namespace

This namespace will be used to host and update the core Aartum Protocol that defines the process and requirements for defining new standards and developing new methodologies.

3.2.3.5 *constitution* namespace

This namespace will be used to host and update the Aartum Constitution (rules for participation and contribution).

3.2.4 Transaction families

The standards, activities and identities namespaces will each have an associated, eponymous transaction family (txf). In addition to these, there will also be transaction families dedicated to proposal handling and voting.

Each of these is discussed in more detail below.

3.2.4.1 *identities* txf

The *identities* txf revolves around the -identity- object class, which will have at least the following attributes:

- username (a platform-unique, human readable identifier, customisable)
- identifier (a platform-unique, nine-byte system identifier, non-customisable)
- key (hash of passphrase)
- national identity / PoPP (only required for participation in certain domains)
- domain-specific reputation

3.2.4.2 *standards* txf

The *standards* txf will contain all transactions necessary to manage objects of the *standard* class. The latter will have the following attributes:

- identifier (a namespace-unique, two-byte identifier)
- SDG category (identifier of the SDG under which it is categorised)
- definition

3.2.4.3 *methodologies* txf

The *methodologies* txf will be used to manage objects of the *methodology* class, which will have at least the following attributes:

- identifier (a namespace-unique one-byte identifier)
- identifier of targeted standard
- content

3.2.4.4 *activities* txf

The *activity* class has the following attributes:

- identifier (a namespace-unique, nine-byte identifier)
- identifier of owner
- project design document (PDD)
- identifiers of targeted outcomes
- identifiers of chosen methodologies

An example of what the *activity* protobuff can look like:

```
message activity {
  required string id = 1;
  required int32 name = 2;
  optional string description = 3;
  optional string ownerID = 4;
  optional string dateRegistered = 5;
  optional string startDate = 6;
  optional string endDate = 7;
  optional int32 outcomeTargets = 8;
}
```

The *activities* txf will contain all transactions necessary to manage objects of class *activity*, such as:

- activity registration
- submission of activity audit
- issuance of credit certificate
- closing activities

Further preliminary protobuffs for transactions in this family:

```
message txRegisterActivity {
  required transaction transaction = 1;
  required activity details = 2;
}

message txCaptureData {
  required transaction transaction = 1;
  required string data = 2;
}

message evaluation {
  required string aspect = 1;
  required int32 score = 2;
  optional string additionalInfo = 3;
}

message txSubmitEval {
  required transaction transaction = 1;
  required string evaluatorID = 2;
  repeated evaluation evaluation = 3;
  optional string additionalInfo = 4;
}

message creditCertificate {
  required string activityID = 1;
  required string dateIssued = 2;
  required string outcomeRealised = 3;
  required int32 creditsEarned = 4;
}

message txIssueCert {
  required transaction transaction = 1;
  required creditCertificate certificate = 2;
}
```

3.2.4.5 *proposals* txf

The Aartum platform is not centrally controlled by any single entity, but is collaboratively managed by a fluid community of participants. As such, all changes to methodologies, standards definitions, software etc. will be preceded by a process of proposal submission and approval through voting. The transaction family managing the submission of proposals and their subsequent voting processes will thus be running on all namespaces across AccB.

The *proposal* object class has the following attributes:

- identifier
- identifier of proposer
- type (e.g. does it propose a change to a methodology or a new software feature)
- content

Proposals will be submitted in smart contract-like transactions recording the votes in favour of the proposal and the votes against the proposal. The proposed change will only be applied if the voting process closed with a positive outcome.

Preliminary protobuffs for the vote class and vote transactions:

```
message vote {
  required voteTypes type = 1 [default = AART_PER_CRED];
  required string voterID = 2;
  optional string smartContractID = 3;
}

message txSubmitVote {
  required transaction transaction = 1;
  repeated vote vote = 2;
}
```

3.3 Aartum Trading Blockchain

3.3.1 Overview

This part of the paper sets out the design and functioning of the Trading Blockchain (hereafter abbreviated as TrB) on a technical level - complete with protobuffs etc. where necessary.

3.3.2 Architecture

The Aartum platform is built upon the Hyperledger Sawtooth architecture. Sawtooth stores blockchains as addressable Merkle-Radix trees divided into namespaces.

3.3.3 Namespaces

In Sawtooth the namespace to which a transaction belongs is indicated by the first three bytes of its 35-byte address; the use of the remaining 32 bytes is up to the designers' considerations. Aartum will use the first eight bytes following the three bytes of the namespace address to subdivide the namespace according to token issuances; in effect, each token issuance will thus have its own sub-trading chain. Each of these sub-trading chains will have smart contracts which will automatically close the chain once all units under the issuance have been retired. This will enable easier blockchain bloat management by pruning subchains once all tokens on the chain have been retired.

TrB will launch with only one active top-level namespace. This will be considered as the beta trading chain. Once the beta phase has come to a conclusion, a new top-level namespace will be activated and all new token issuances will thereafter occur under the new top-level namespace. New top-level namespaces will hereafter only be activated once the current one has been filled to capacity (if ever), i.e. once there are no unused namespaces left for new token issuances.

3.3.4 Transaction families

3.3.4.1 *chains* txf

TrB will employ a customised version of Sawtooth's built-in chain management transaction family.

Some preliminary protobuffs for members of the *chains* transaction family are given below:

```
message transaction {
  required string id = 1;
  required transactionTypes type = 2;
  optional int32 hook = 3;
}

message txOpenChain {
  required transaction transaction = 1;
  required string chainID = 2;
  optional chainType chainType = 3;
}

message txCloseChain {
  required transaction transaction = 1;
}

message txAddSmartContract {
  required transaction transaction = 1;
  repeated smartContract contract = 2;
}

message txCloseSmartContract {
  required transaction transaction = 1;
  repeated string smartContractID = 2;
}
```

A note on slot 'hook' for objects of class 'txOpenChain': there can be only one instance of this class in the entire chainverse with a null 'hook', namely the genesis block of the entire chain verse (a.k.a. the 'big bang' block); all other instances of this class should have a hook specified. In the case of project data chains, the hook should be the chain ID of the last project data chain initiated before this one. In the case of trading chains, the hook should be the pdChainID-txID of the certificate issuance from which the chain was born.

3.3.4.2 *tokens* txf

Examples of what some members of this transaction family may look like:

```
message coin {
  required string id = 1;
  required int32 value = 2;
  required string ownerID = 3;
  required string chainID = 4;
}

message txIssueCoin {
  required transaction transaction = 1;
  required string txIDissuance = 2;
  optional coin coin = 3;
}

message txSplitCoin {
  required transaction transaction = 1;
  required string destroyedCoinID = 2;
  repeated coin newCoins = 3;
}

message txMergeCoins {
  required transaction transaction = 1;
  repeated string destroyedCoinIDs = 2;
  repeated coin newCoin = 3;
}

message txTransferCoin {
  required transaction transaction = 1;
  repeated string destroyedCoinID = 2;
  repeated coin newCoin = 3;
}

message txRetireCoin {
  required transaction transaction = 1;
  repeated coin coin = 2;
}
```

Chapter 4

Roadmap

The development of the *Aartum* platform will follow a phased approach starting with tokens representing greenhouse gas emission reductions and partnerships to achieve the global goals. It aims to develop over time to cover all SDG outcomes. The envisioned roadmap is set out below.

4.1 Public introduction

The platform starts with the launch of the *Aartum* website (www.aartum.io) and the publication of the whitepaper (the document you are reading now) in which the concept of tokens of value linked to SDG outcomes is thoroughly explained. The whitepaper will include a roadmap as well as a call for collaborators.

4.2 Draught and pilot Aartum Protocol

The framework according to which metrics for outcomes (both enabling and final) is defined, as well as the generic process for verifying the achievement of those outcomes, must be carefully designed at the start of the process. During this phase, a working group will be established for draughting the *Aartum Protocol*. Once draughted, it will be piloted for SDG 13. See <> for more detail.

4.3 Establish working groups for development of other standards and methodologies

A successful pilot of the Aartum Protocol will end in a standard and at least one methodology for SDG 13. Working groups will subsequently be established to draught standards and methodologies for all the other SDGs.

4.4 Launch alpha-version of Accounting Blockchain (AB)

The Aartum Protocol will be implemented on a blockchain called the Accounting Blockchain. The launch of this blockchain is an important milestone. A closed working group will initially be established to develop and test the AB. Once ready, an alpha-version will be launched to the public together with a whitepaper describing the technical aspects thereof in detail. From this point onwards, the public will be able to contribute to the further development of the chain. See <> for a more elaborate discussion of the Accounting Blockchain.

4.5 Launch alpha-version of Trading Blockchain (TB)

The Trading Blockchain will enable the currency-like trading of tokens issued on the Accounting Blockchain (refer to <> for more detail). As with the AB, the initial development and testing of the TB and its API will be conducted by a closed working group. Once the alpha version is launched, the public will be free to participate in the further development thereof. The alpha-version of the TB will be launched together with a small set of user interfaces, such as a wallet app for mobile devices (smart phones, tablets etc.) and a web-based wallet. Additional interfaces to the TB will be added over time to, for example, allow integration with point of sale (POS) systems. The launch of the alpha version of the Trading Blockchain will be accompanied by a technical whitepaper describing its internal workings.

4.6 Social media integration

Social media integration is an important aspect of the strategy to create value for verified SDG outcomes. The ability to link a social media profile (e.g. Twitter, Facebook and Instagram) to a profile on the Aartum platform means that people will be able to make their personal contributions towards achieving the SDGs (i.e. the SDG tokens that they retired) visible to others through their social media. This has the potential to popularise and normalise SDG contributions through retirement of verified SDG outcome tokens. This process will start as soon as the alpha version of the TB launches, but will be developed continuously as the social media landscape is an ever-changing one.

4.7 Launch beta-versions of AB and TB

Public voting rounds will determine when the alpha-testing phases for both chains will be concluded and the beta-testing phases commence.

4.8 Fiat and cryptocurrency exchanges

The exchangeability of Aartum for other crypto- and fiat currencies will allow Aartum to be accepted as a currency in point-of-sale systems around the world.

The process of getting Aartum listed on major public exchanges will commence once the beta-versions of both the AB and the TB have been launched.

4.9 Customisation and Gamification

Once the TB is launched the development of customisation options will begin. We aim to give entities the ability to obtain tokens and customise these for their own purposes such as giving token holders certain privileges within their own business systems (e.g. VIP access, discounts and loyalty points). We also plan to make the platform integrable with games so that the SDG tokens may be used in games as points, “power-ups” or currency. This offers an interesting option especially in city-building/world-simulation games where improvements in the virtual world are linked to improvements in the real world, so that such a game becomes more than just a game and rather a symbol of real impact.

Chapter 5

Glossary

API Application programming interface

Blockchain A data structure made up of a growing list cryptographically linked of records (referred to as blocks). Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). See https://en.wikipedia.org/wiki/Blockchain

Blockchain ecosystem A system of entities and practises that emerge around a blockchain-based platform

Blockchain platform A system of software and data storage components that allow users to achieve a specific goal.

CoinJoin Protocol that anonymises unspent transaction outcomes (UTXO) through mixing https://www.skycoin.com/docs/dev-docs/guides/transactions/#coinjoin-hardening.

Crypto-asset A cryptographic token stored in a blockchain the signifies that ownership of as asset

Equity token Token that represents

Impact Investing Impact investing refers to investments intended to generate a measurable social or environmental benefits in addition to financial returns

IoT device A device connected to a network that has a unique identifier (UID). Such a device has the ability to transfer data over a network without requiring human-to-human or human-to-computer. https://en.wikipedia.org/wiki/Internet_of_things

Proof-of-stake (PoS) The mechanism to select the node that submits the next block in a blockchain network based in that node's holdings

Proof-of-work (PoW) The mechanism employed secure a blockchain network and select the node allowed to submit the next block based on a piece of data which is costly to produce but easy for others to verify.

Smart contract Executable code stored on a blockchain that automatically executes a transaction (typically the transfer of a cryptographic asset) when its conditions are met.

Transaction processors A software component that changes the state of a ......

Utility tokens A cryptographic token that grants the owner access to a certain service. See https://blockgeeks.com/guides/utility-tokens-vs-security-tokens/

UTXO Unspent transaction output

VER Voluntary Emission Reductions