Byson: Application of Blockchain Technology in the Carpathians

Chaoran Chen
mail@chaoran-chen.de

David Ittah
ittahd@student.ethz.ch

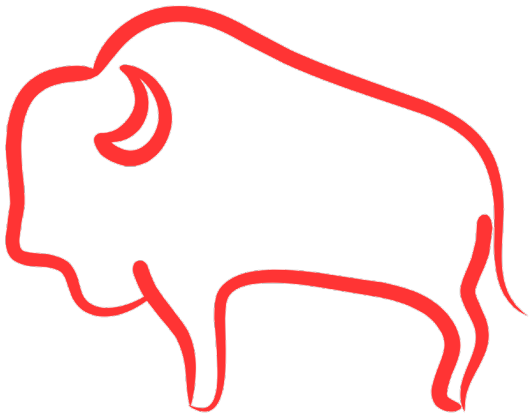
Severin Kranz
severin.kranz@student.unisg.ch

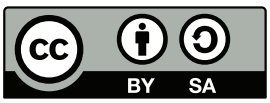
Sergiu Soima
sergiu.soima@gmail.com

Alessandro Tarantola
ataranto@student.ethz.ch

24 April 2019

A. Tarantola and D. Ittah contributed equally to this report.





1 Introduction

1.1 Sustainability and blockchain: The Odd Couple

It was early 2009 when the first Bitcoin network came into existence. At the time, very few suspected how radical an impact this new technology would have on modern society. Ten years later, blockchain and subsequent distributed ledger technologies (DLT) are deployed in innumerable projects and their effectiveness and popularity seem only bound to grow.

A blockchain is a digital record of transactions, a ledger. It is public and accessible to everyone, yet secure, thanks to the method employed for the verification of transactions: the consensus. For a transaction to be valid, the majority of the nodes of the consensus have to agree upon its outcome, making it practically impossible for any individual to modify pieces of information on the chain without all of the nodes knowing about it. The name "blockchain" derives from its method of organizing data: transactions are packed into "blocks", which are connected to each other to form a "chain" by writing the hash of the previous block into the following one.

From the few facts above, it is clear that DLTs hold some interesting properties, such as reliability of the data stored, resilience to attacks and transparency. The connection to sustainability issues, however, remains obscure. To understand it, one has to look at the disruptive change in perspective this new approach brings about. Blockchain is, potentially, a powerful vehicle of decentralization, peer-to-peer collaboration, and alternative governance. It is a means of empowering people, allowing for bottom-up rather than top-down organization schemes. There are many areas in which such an approach proves to be winning, areas like energy distribution, crowdfunding, direct democracy, and donations to charity. The sceptical reader may think that this is just a bunch of promises and unproven claims. However, thousands of projects revolving around blockchain have risen in the past few years, and some of them are already making an impact on the real world. To give some examples: the start-up GridSingularity is creating distributed energy grids where consumers buy and sell energy to their nearest neighbours, exploiting microtransactions on the chain, hence drastically cutting down energy distribution costs; e-Estonia, a project started in 2008 by the Estonian government, safely stores the citizens' most sensitive data, and provides them with a wide range of online services; RootProject uses crowdfunding and a token system (ROOTS) for humanitarian purposes. Moreover, among those who presently employ blockchain, a vast majority reports an increased efficiency in comparison to other available solutions, and almost a fifth believes what they're doing would be impossible without it [1].

Nothing of what has been done so far proves blockchain to be the ultimate solution to these problems, yet significant evidence points in that direction, making it worthy of consideration.

1.2 The challenge

The area of the Carpathians, situated in parts of Romania, Ukraine, and Slovakia, is one of the wildest sites on the old continent. With their 250,000+ hectares of virgin forests just in the Romanian part, these mountains are con-

sidered the lungs of Europe, and host the largest European populations of large mammals such as bears, wolves, chamois, and lynxes. In addition to that, they have recently witnessed the reintroduction of the European bison, a species that was almost extinct just a few decades ago. Such a unique region is definitely worth protecting, something that WWF has been working on in the past years. However, their efforts alone might not be sufficient.

Protecting the environment is not considered an economically rewarding activity by most companies, governments or entrepreneurs, which often shortsightedly push in the opposite direction: destroying nature for the sake of "progress" or economic development. Standing up to economic elites is difficult enough by itself, but the task of monitoring and preserving the area is made even harder for the activists by the lack of an efficient network to track its health. However, there might be a way to tackle all these problems at once: if one could instill into the local population the idea that preserving the environment is really economically beneficial, they might start caring for it.

In this spirit, WWF has developed the following concept: local hunters, shepherds, etc. could perform a series of actions to help the conservationists, ranging from trail maintenance to installing sensors and IoT devices for the monitoring of the region, receiving a twofold benefit in return. Upon supplying a valid proof, they would be granted an immediate monetary reward, as well as the promise of future development projects for their community, once certain impact goals are met. The money needed would be gathered through donations, and benefactors would be given the possibility to check the effectiveness of their help by having access to the data collected by the (newly) installed sensor network. The challenge is therefore: can we realize this project in the most transparent way possible for donors, locals and WWF? Can blockchain help in achieving this goal? Can we eliminate the need of a trusted third party (in this case WWF) by exploiting the peculiarities and resources of smart contracts? How would the use of tokens, incentive design and multidimensional monetary systems help in the process? What would be the role of IoT devices in providing proofs of actions? And in data collection? In the following, we will present a cohesive solution to these challenging questions.

2 Solution

2.1 Overview

How is *Byson* solving the issues of donor trust and harmonizing communities with their environment? The proposed solution takes a multifaceted approach, at the core of which resides blockchain technology as an incorruptible agent. In using this emerging technology, we can create real trust between donors and WWF, ultimately promoting donations by providing total transparency of WWF's actions, and complete traceability of the donated funds. In addition, a key motivator for recurring donations will be realized by providing direct feedback of the impact the donations had on the environment.

On the other side, we can incentivize the local population to not only participate and contribute to conservation efforts, but also to abstain from harmful actions towards the environment. Direct involvement of individuals will be promoted using immediate monetary rewards but, more importantly, the commu-

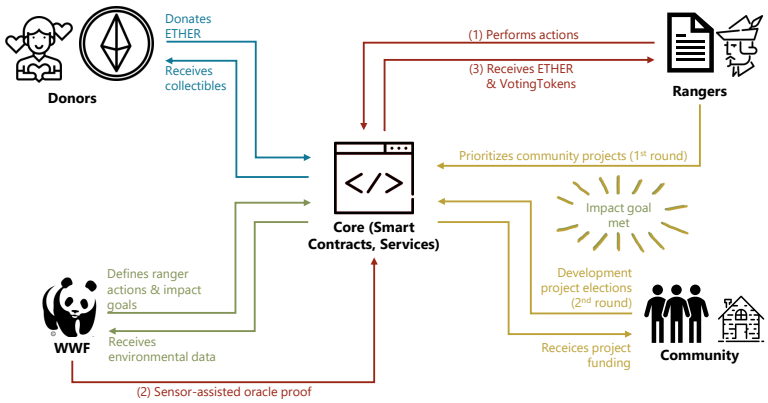


Figure 1: A diagrammatic illustration of the proposed solution, showing the most important interactions between the players and core architecture.

nity as whole will be provided with a stake in the well-being of nature. This is achieved using a positive-feedback loop, linking positive environmental impacts to advancing prosperity of the community. This will propagate twofold to reduce harmful actions on the Carpathian ecosystem. Improving living standards by providing community development aid directly addresses the root causes of some of the harmful behaviour of individuals driven by economic need. Importantly, the community development aid will be conditioned on successfully completing environmental goals. Social pressure can then be a great aide in regard to preventing the infringement of environmental protection measures, once the community as a whole is invested in the care of their environment. Contrasting this to traditional punitive systems, often too difficult to enforce and ultimately ineffective, individuals will be significantly less inclined to perform harmful actions if it comes at the expense of their peers.

2.2 Concept

In this section we will present a detailed solution to the challenge, focusing on each of the four players: donors, rangers, community, and WWF. Figure 1 provides a high-level overview of the interactions between these players.

Donors Donors are a vital resource for any non-profit operation. They come from all over the world with a variety of backgrounds but are unified through their willingness to promote change or protect causes they care about. However, many donors have lost trust in charities and NGOs due to the scandalous and corrupt behaviour by some of the organizations or individuals within them. It is of paramount importance to instill donors with a maximum amount of trust, all the while providing as easy a platform as possible for them to get involved and receive the necessary information to maintain this trust.

This is achieved using the *bioson* app. Donors will be presented with an option to donate funds from their Ethereum wallet to a WWF account managed by the publicly verifiable, independent fund manager sitting on the blockchain.

This fund manager is an Ethereum smart contract with a very specific set of allowed operations (more on this in section 2.3.1). For every donation made, the user can pull up a breakdown of what kind of tasks or operational costs the money was spent on, letting them know that their contributions are put to good use without the need to consult third party analyses of organizational spending. Additionally, a dashboard will be available, showing the progress made over time on the impact goals defined by WWF, affirming to the donor that their contributions are vital and can effect change. Another screen will allow the user to query and display a variety of scientific data gathered by the project trough sensors, satellites, or personnel, allowing them to dive deeper into the issue and really feel as though they are part of the project. Examples of this include bison location tracking, forest satellite images, and other environmental data.

To reward generous benefactors for their donations, we have established a collectible Wildlife token system. These are unique tokens representing an animal (such as a bison, bear, fox, bird, ...), whose appearance is determined by DNA, and which can be traded and bred (limited so as not to create a flood of them). Such tokens can be viewed and managed through the app as well. Adding gamification to the donation system can further increase the perceived value of donating. For a special class of tokens such as the bison, the token will be linked to a real-life animal, creating an emotional bond similar to those of other benevolent guardian systems.

Rangers Much of the local populace in the Carpathians is engaged in outdoor work such as farming, herding, logging etc.[2]: a currently untapped resource that could provide a massive boost to conservation efforts. Often, the income obtainable from these activities is by no means lavish and can present a challenge to make ends meet. As such, opportunities to gain additional income are sometimes seized without much consideration for legality or environmental impact (e.g. poaching). Both of these issues must be tackled in order to achieve a healthy co-dependant environment for both humans and nature.

A solution to these problems is provided by the *CryptoRanger* app. Users registering through the app as rangers will be notified with an up-to-date list of available tasks which they can register for and will have to complete within a certain time frame. This will avoid two people attempting to perform the same task, while also making sure the task is not indefinitely blocked off. A limit on the number of simultaneously registered tasks should prevent any severe "task hogging". Upon completion of a task, the ranger will provide any collected data as-well as the required proof through the app. The main proof mechanism we foresee for this system will be the *sensor-assisted oracle proof*. Using this system will significantly simplify the task of the human oracle by running a series of automated checks and presenting any available relevant information. Examples of this can include GPS-location tracking in the app if the task is required to be performed at a specific location or within a certain region. Location- & time-stamped pictures can be authenticated by forcing the user to take them through the app at the right location and time. Tasks relating to sensors can present sensor data to the oracle if this helps verify an action. Once the task has been verified as completed, the cash reward in form of ether is automatically disbursed to the user's account. Additionally, the ranger is rewarded with a certain number of voting tokens which will increase their say in community

development decisions (see next section). Lastly, *CryptoRanger* aims at further strengthening the rangers' bond with nature by providing them with detailed information about the progression of the aforementioned impact goals.

Community For the initiative to be successful, it is important to take special care in involving the local communities. Providing development aid can certainly improve the lives of their members, but we need to go further than that and let the community self-determine its priorities on where investments are most needed.

This approach works hand in hand with the presented concept. The fundraising of development projects will be tied directly to the general donations. For each donation the benefactor can set the percentage of funds going directly into the conservation fund, while the remainder will go into the development fund. A certain default split will be encouraged to ensure enough funding for the community↔nature mechanism to work. Project proposals will come directly from the community, e.g. one could imagine an open submission system with an advisory council evaluating feasibility, cost, and time frames of proposals, while WWF can of course propose suitable projects as well. The process will be ongoing, allowing new proposals to be added at any time.

The voting system takes on a key role in both involving the community and incentivizing WWF↔Ranger cooperation. In a first phase, members having earned voting tokens will be able to back proposals by pledging a portion of their tokens towards one or more (or none) of the projects of their liking. Votes can be redistributed until the end of this phase, to account for new proposals and changes of mind. The next phase is triggered upon reaching one of the major impact goals, upon which members will be notified that this first voting round will end within a certain time-frame (e.g. a week). The top three projects are then submitted to a democratic ranked-choice vote. That means in the second round every member of the community will have an equal say, and the voting system was chosen to maximize consensus by finding the option that the most people can agree on. A quick overview of *ranked-choice* voting goes as follows:

- Each voter ranks as many or few options as they want according to their preference.
- Allocate one vote to every voter's first choice.
- As long as no option has a majority ($> 50\%$), repeat:
  - ↻ Eliminate the option in the last place and attribute each of those votes to the voter's next choice in the ranked list (if any).
- Declare the majority option the winner.

The benefit of having these two separate voting rounds is to combine the goal of incentivizing rangers to perform tasks by having a greater say in the selection of projects to be implemented, all the while still retaining a fair democratic process by leaving the ultimate decision up to everyone in the community.

After the voting is completed, the money necessary to implement the winning project will be pledged towards it from the development aid fund. If the funds are insufficient at the moment, the income stream from future donations will be pledged towards this project until enough has been collected. The responsible

party for implementing the project can then decide whether to start immediately with the limited funds or wait until all the funds have been collected. Ultimately, the benefits the community will experience, conditioned upon the completion of sustainability impact goals, will create a strong bi-directional bond between communities and nature benefiting everyone.

WWF Naturally, WWF can benefit greatly from implementing these measures. Not only can the increased manpower help to cover vastly more ground than would otherwise be possible, and thus significantly boost the available information allowing WWF to be more reactive, but additionally this solution would provide a convenient way of collecting the data and making it available to WWF as well as interested members of the public. This, along with the verifiable & traceable fund managing will ultimately be a great boon to the public image and trust of the World Wildlife Foundation.

2.3 Technical Implementation

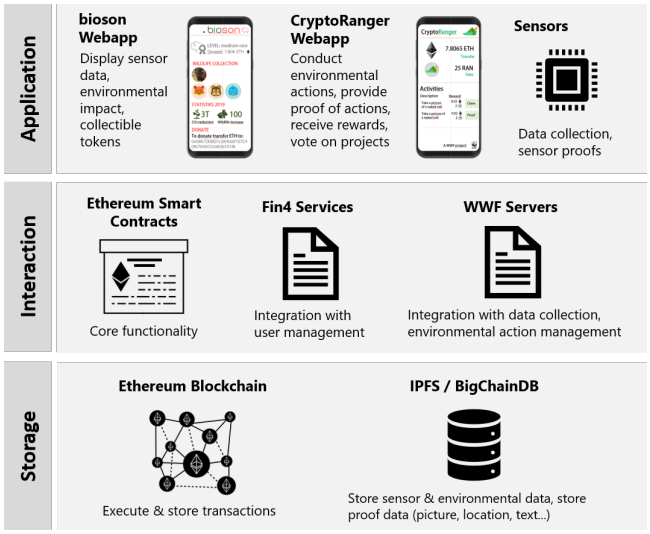


Figure 2: High- to low-level components of the Byson project: front-facing user apps, core functionality & services, and underlying technology.

2.3.1 Smart contracts

Our four smart contracts are the core of the whole architecture. As such, they take care of the most crucial aspects of the project: a *FundManager* is in charge of receiving donations, distributing ether for operational costs and confirmed ranger actions, as well as releasing money stored in the community pot upon reaching an impact goal; a *Collectibles* contract handles the generation and distribution of wildlife tokens; the*Hunters* contract deals with ranger actions and their booking, claiming and proving; *Voting* generates and distributes voting tokens, and manages elections. Their precise role and mutual relationships will be made clear in the following paragraphs.

Collectibles The main task of this contract is to generate non-fungible tokens according to the ERC721 standard. Such tokens can only be minted by the *FundManager*, which triggers the minting right after receiving a donation. Upon initiation of the minting process, a new DNA is produced in a pseudo-random fashion, based on hashing the donor's address and the number of tokens they already own. The genetics of the wildlife token will determine the animal's species (bison, bear, fox or bird) and appearance.

Hunters The core functionality of the ranger task system is implemented by this smart contract. Each task is stored in the contract with the following information: the reward in ether, the reward in voting tokens, a description, an associated ranger, and a status indicator (*active*,*claimed* or *completed*). Let us depict the life-cycle of a task in a schematic way, maintaining our focus on the role of rangers during the process:

1. WWF employees generate a task through the *createActivity* function. Access rights to this API function are restricted and managed by the *Administrable* contract, a vital component in order to prevent unauthorized disbursement of funds. The task list is then updated with the newly created task, which becomes *active*, and is available for everyone to consult.

2. Rangers can then call the *bookActivity* function to prevent other users from performing a task they are planning on completing. Such a task becomes inactive and is now associated to the calling ranger's Ethereum address.

3. After performing the action, the ranger calls *sendProof*, stating the task has been carried out and providing the contract with the hash of his proof. All the proof data is stored off-chain to prevent inhibitive blockchain processing costs. If another ranger were to try to claim the reward for a task they did not book, the claim would automatically be rejected. Following a legal claim, the activity is marked as claimed.

4. As a last step, a WWF employee accepts or rejects the proof, aided by sensor data as described in the Solution section. In the first case, the *Voting* and *FundManager* contracts are invoked: the former mints the right number of voting tokens and sends them to the ranger, the second one dispenses the due ether. The activity is now completed! In the second case, our task becomes active again and is newly assigned to no one. Its life-cycle can start again.

Voting This contract is responsible for two main functions: generating and distributing voting tokens and managing elections. The generation and distribution have been covered in the previous paragraph, so we will focus on elections. Although the mechanism we would embrace is that of the "ranked choice", exposed in the Community paragraph, we hereby present the limited implementation of the voting system currently in our code.

Proposals for community projects are created by WWF employees or other certified individuals (we will generically call them "admins" from now on). Once stored, they are public. At any time, an owner of voting tokens can place some of them in the "ballot" of his favourite proposal. He can vote for more than one of them, as long as his balance is positive. Once the voting has happened,

admins can stop the election by calling *endVoting*. Elections are now over, *FundManager* is called and sends the due amount of ether to the winner, i.e. simply the proposal with the most votes.

FundManager The *FundManager* can be regarded as the centre of this smart contract ecosystem, being the only one that communicates with all of the others.

Its first responsibility is accepting donations. While doing so, it also triggers the distribution of collectible wildlife tokens, calling *Collectibles*. Secondly, if requested to by *Hunters*, it adequately rewards the rangers for the actions they have performed. Thirdly, it is this contract that releases the community development funds after the completion of an election, when called by *Voting*. Apart from interacting with other contracts, it gives WWF the chance to withdraw part of the funds to cover their costs (paying employees, buying new equipment,etc.), upon stating what that money will be used for (see function *payOpCosts*). The stored funds and their movements are completely traceable and visible to everybody, thanks to the API functions *getConFund* and *getDevFund*.

Bonus: Administrable As touched on before, access rights to critical API functions are managed by the *Administrable* contract. Functions marked as restricted can only be invoked by authorized admins. This could be some WWF employees, appointed members of the community, or contractors taking on a managerial role. Several access levels could be implemented for this in the future. The special project manager is then able to grant or revoke access rights to admins, or transfer the project manager role to a successor. This concludes the description of the most important contracts, their roles and how they interact with one another.

2.3.2 Front-end

The front end of this architecture consists of two applications, designed to be run on smartphones and make the interaction of the final user with the chain as easy and painless as it can get: *CryptoRanger* for local users, and *bioson* for donors all over the world. They have been comprehensively described in the Solution section.
So far, no interface has been developed in the context of this project that would allow WWF employees to perform their set of actions.

2.3.3 Fin4

The fin4 platform was initially meant to be one of the gears of this machinery, thanks to its promising features: intuitive user-management and seamless token generation. However, the complications encountered when trying to interface it with the smart contracts and the front-end under time pressure, forced us to develop alternative solutions, relying mostly on smart contracts directly. We do not see any reason why this couldn't change in the future to include Fin4 in our architecture.

2.3.4 Data storage

When it comes to DLT systems, data storage is well-known to be one of the more difficult topics. Storing high volumes of data on the chain is counter-productive in most cases, due to the high cost and intrinsic difficulty of adding information, let alone modifying it.

In our case, it is apparent that not all of the generated sensor data can be stored on the chain. Hence, the optimal solution currently seems to be a fitting coexistence of old and new technology. All of the sensitive data, like transactions, balances, addresses of users, hashes of proofs and so on, will be kept secure on the distributed ledger; sensor data, proofs and anything else that's meant to be publicly available will be put into the InterPlanetary File System (IPFS). IPFS has the peculiar feature of allowing no copies of the same file throughout its nodes. As handy as this might be for the functionality and speed of the service, it may pose some problems if a node was to go down: all the data it contained would be lost. Since what is stored in IPFS is by no means secret, we believe that the easiest solution is also the best here: WWF could backup in its private servers whatever data it wants to protect from the risk of loss. Data with scientific value awaiting to be processed could, for example, fall into this category. Another alternative could have been using BigChainDB, which is definitely more fault tolerant. However, as stated, we decided to go for the simpler solution, and hence adopted IPFS.

3 Conclusion

Even though our solution has been laid out in this document, the project remains at a very early stage. Some reflection is still required on various minor issues and their fixing. Moreover, it is not deniable that some things might not stand up to the expectations in the real world. Finally, we do not dare to claim our solution to be the optimal one. A lot of improvement can be thought of, and we ourselves will propose some shortly. Besides all of these caveats, we still believe in the tremendous potential of this project and support it fully. We will address each question in the following order:

- What adjustments can be made and what could go wrong?
- What future developments do we foresee for this project?

Adjustments and possible problems

First of all, it is well known that blockchain is a very young technology. As such, its full potential is still unexplored, it is harder to find experienced programmers for the coding and maintenance and tailoring the solution to the specific problem can take longer than it would with more widespread techniques. Furthermore, in our case, the interaction with the fin4 platform has proven to be less immediate than expected. Lastly, the smart contracts need a thorough revision before they can be deployed on the chain: their efficiency and correctness are of vital importance for the end result.

Despite this, we believe the main challenges for such a project are not technical, but social. In the first place, this alternative governance system can only sustain itself if enough people embrace the cause and profitably make use of

the platform on a regular basis. A lukewarm or negative welcome by the local community would inevitably lead to the premature death of the project. In the second place, a vital role will be played by WWF and their ability to handle the designing of the tasks and the selection of the rangers. We know that the project should not, at least in the very beginning, be open to everyone, and the range of tasks should be very limited. The most delicate actions should never be carried out by untrained personnel, as it could cause more harm than good. Preventing this from happening will be one of WWF's major responsibilities. Lastly, the "business model", with its concepts of gamification, tokenization and incentive design might be borrowed by companies for profit. Tackling this possibility is, however, not our concern, as it clashes with the "open source" spirit of this project.

Future developments and open questions

The aspects that require the most careful thinking are two: the allowed mechanisms for proving claimed actions and the token design. As far as the former is concerned, should we allow for social proof? If so, how do we prevent people from convincing peers to confirm unperformed actions by offering them a reward? A possible solution, which involves the use of a new token, will be outlined in the next paragraph. Even so, if we did not want to allow for social proofs, would the presence of an oracle (most likely WWF) be the only possibility? Or the best one? Could sensor proof totally replace the previously existing types, once the IoT network is up and running? This seems unlikely.

Let's now address the second question: tokenization. In our current model, only two currencies are required: ether and voting tokens. Could we add more tokens to make the project evolve towards a multidimensional currency system? Which ones are the most suited? A promising one could be a "reputation token" (let's call it RepuTo for brevity). For example, rangers could receive some RepuTo while joining the platform. Later on, when they want to perform an action, they'd have to "stake" part of their reputation to register for it. They would then get back more of it, say twice the staked quantity, once such task is successfully confirmed. This would open to a bunch of possibilities, including social proofs and ranking of the tasks. Provers would have to undergo the same mechanism of stake and reward, therefore losing RepuTo for confirming unperformed/badly executed tasks, thus increasing security. In addition to that, tasks might be ranked, so as to give access to harder tasks only to trustworthy rangers with high reputation.

One last sensitive question is the scope of the project. Do we want just the locals to help, or should we encourage anyone willing to? This would include also tourists and, in general, people who might not really need the extra income. So the problem reduces to: do we give more importance to the environment, and hence welcome all helping hands, or pursue the development and well-being of the communities in the Carpathians through a stronger bond with the nature surrounding them? We support the second line of thought, but this doesn't mean the problem shouldn't be up to debate.

The time for action is now

At the end of the day, one thing has to be clear. We firmly believe that an objective analysis of what has been depicted in the previous pages can only lead to one conclusion: that the advantages of this approach largely outweigh the drawbacks. If there has ever been a time to act for a cleaner, greener, better future, this is certainly it. Should history prove us wrong, we will not regret trying.

Disclaimer

The solution described in this paper is primarily conceptual in nature. As such, the code produced during the hackathon event is merely a quick and incomplete implementation of the presented solution.

References

[1] Doug J. Galen et al. Blockchain for social impact. Technical report, Stanford Graduate School of Business, 2018.

[2] Zoltán Gál et al Iván Illés. Socio-economic analysis of the carpathian area. Technical report, Hungarian Academy of Sciences, 2007.