C_4Coin: The Carbon-Negative Blockchain

Harrison Perl, Tigran Avakyan, Dylan Penn, and Aidan Krakowsky

January 24, 2018
v1.01

"There are a herd of environmental black elephants gathering out there. Global warming, deforestation, ocean acidification, and mass biodiversity extinction just to name four. When they hit, we will claim they were black swans that no one could have predicted, but, in fact, they are black elephants, very visible right now. We're just not dealing with them with the scale and speed that is necessary."

-Adam Sweidan via Thomas Friedman's *Thank You For Being Late*

Legal Disclaimer

CAUTIONARY NOTE REGARDING FORWARD-LOOKING STATEMENTS

THIS WHITE PAPER CONTAINS FORWARD-LOOKING STATEMENTS WITHIN THE MEANING OF THE SECURITIES LAWS. THESE FORWARD-LOOKING STATEMENTS ARE SUBJECT TO A NUMBER OF RISKS AND UNCERTAINTIES, MANY OF WHICH ARE BEYOND CO2KN, INC'S (THE "COMPANY") CONTROL. ALL STATEMENTS BELOW, OTHER THAN STATEMENTS OF HISTORICAL FACTS, INCLUDING THOSE REGARDING STRATEGY, FUTURE OPERATIONS, ESTIMATED REVENUES, PROJECTED COSTS, PROSPECTS, PLANS AND OBJECTIVES, ARE FORWARD-LOOKING STATEMENTS. THE WORDS "WILL," "BELIEVE," "ANTICIPATE," "INTEND," "ESTIMATE," "EXPECT," "PROJECT" AND SIMILAR EXPRESSIONS ARE ALSO INTENDED TO IDENTIFY FORWARD-LOOKING STATEMENTS, ALTHOUGH NOT ALL FORWARD-LOOKING STATEMENTS CONTAIN SUCH IDENTIFYING WORDS. ALL FORWARD-LOOKING STATEMENTS SPEAK ONLY AS OF THE DATE OF THIS WHITE PAPER. THE COMPANY UNDERTAKES NO OBLIGATION TO UPDATE OR REVISE ANY FORWARD-LOOKING STATEMENTS, WHETHER AS A RESULT OF NEW INFORMATION, FUTURE EVENTS OR OTHERWISE. ALTHOUGH THE COMPANY BELIEVES THAT THE PLANS, INTENTIONS AND EXPECTATIONS REFLECTED IN OR SUGGESTED BY THE FORWARD-LOOKING STATEMENTS MADE IN THIS WHITE PAPER ARE REASONABLE, ULTIMATELY, SUCH PLANS, INTENTIONS OR EXPECTATIONS MAY NOT BE MET.

Acknowledgements

The authors would like to acknowledge the contributions of the following individuals who have helped make this project possible:

- Miles Murrough O'Brien
- Aidan Penn
- Ashley Taylor
- Reed Shapiro
- Dave Sag
- Gerhard Diedericks
- Andrew De Bruijn
- Amila Samarabandu
- Sara Egendorf
- Sam Egendorf
- Brooke Singer
- Dazza Greenwood
- Daniel Rosenthal
- Jack Miller
- Leo Leibovitch
- Justin Birenbaum
- Yazan Barghuthi

Contents

1 Introduction

C_4Coin aims to build a carbon-negative public blockchain. The C_4Coin project will achieve this goal by providing the first viable economic incentive to voluntarily retire carbon credits.

Since the Kyoto Protocol in 1997,[1] the world has agreed on carbon credits (one metric ton of CO_2 or equivalent offset) as a mechanism for financially incentivizing conservation efforts. Many regional governments have enacted compliance carbon trading schemes with mixed results.[2,3,4,5] Meanwhile, the voluntary carbon market suffers from oversupply[6] due to the lack of a financial incentive to retire credits.

The C_4Coin network will create this incentive through a two-token model. C_4Coin tokens will each be equivalent to one carbon credit. Initially, these tokens will be backed by carbon credits in existing registries. Exo tokens will function as traditional crypto-assets, usable as fuel for distributed applications (dApps) or simply as a way to store value. A Proof-of-Burn consensus mechanism will link the creation of Exo to the staking and burning of C_4Coin tokens.

Migrating existing carbon credits onto the blockchain as C_4Coin tokens will create several significant benefits. First, the ability to retire C_4Coin through network consensus and earn Exo will give C_4Coin tokens added value compared to traditional credits. Additionally, hosting these credits on a public blockchain will streamline the process of carbon trading, allowing for interoperability between differing standards and reducing transaction fees.

The C_4Coin blockchain will feature a virtual machine similar to Ethereum's, allowing developers to create dApps. Exo tokens will fuel these dApps. Because C_4Coin's consensus mechanism requires retiring carbon credits, the network (and any dApps using it) will be carbon-negative. This innovation improves on existing blockchain technologies, which are inherently wasteful.[7] Given the choice of two blockchains that are otherwise functionally identical, developers should use the environmentally conscious one.

By creating a carbon-negative blockchain economy, C_4Coin will provide a tangible incentive for environmentalism. In the absence of unified government efforts, C_4Coin aims to mobilize individuals and communities to combat climate change.

From this introduction, it should be clear that several aspects of the project require further explanation. This paper will first provide a brief overview of the carbon credit space. Next, it will spell out in detail the problems C_4Coin aims to solve. Finally, the paper will present the technical details of C_4Coin's proposed solution and the team's vision for the project's long-term future.

[1] United Nations Framework Convention for Climate Change, "Kyoto Protocol," Accessed 2017-11-17, http://unfccc.int/kyoto_protocol/items/2830.php.

[2] Alexander Jung, "The EU's Emissions Trading System Isn't Working," Translated by Ella Ornstein, 2012, accessed February 15, 2012, http://www.spiegel.de/international/business/hot-air-the-eu-s-emissions-trading-system-isn-t-working-a-815225.html.

[3] California Air Resources Board, "Compliance Offset Program," Accessed 2017-11-15, https://www.arb.ca.gov/cc/capandtrade/offsets/offsets.htm.

[4] The EU Emissions Trading System (EU ETS), "Use of International Credits," Accessed 2017-11-15, https://ec.europa.eu/clima/policies/ets_en.

[5] Carbon Action Reserve, "Reserve FAQs," Accessed 2017-11-14, http://www.climateactionreserve.org/resources/faqs/.

[6] Environmental Finance, "Low Prices, But High Hopes for the Voluntary Carbon Market," South Pole Group. Accessed 2017-12-08, https://www.southpole.com/news/low-prices-but-high-hopes-for-the-voluntary-carbon-market.

[7] Sebastiaan Deetman, "Bitcoin Could Consume as Much Electricity as Denmark by 2020," 2016, accessed March 29, 2016, https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020.

2 Carbon Credits

This section will provide a brief introduction to carbon offsets. It will cover offset methodologies, the present state of carbon-offset markets worldwide, and the life cycle of carbon offsets within these systems. Readers already familiar with carbon offsets may find it helpful to skim the following until §3.

2.1 Offset Methodologies

Many types of carbon credits exist under the UNFCCC's Clean Development Mechanism (CDM) standards.[8] It would be impractical to discuss the full range of approved carbon-offset methodologies at length here. For the sake of simplicity, this section will examine the following two broad types of carbon offsetting:

1. Avoidance projects prevent future carbon emissions. For example, a renewable energy source may generate energy in excess of its operational requirement and distribute this energy back into the grid. By doing so, the renewable energy source reduces the net energy demand of the grid, thereby decreasing the amount of energy fossil fuel plants must produce. Typically, the owner of the renewable energy source is eligible to earn a carbon credit for every metric tonne of CO_2-equivalent (tCO_2e) of emissions offset in this manner.[9]

2. Sequestration projects remove greenhouse gases that have already been emitted into the atmosphere. When a forestry initiative regenerates formerly degraded land, it can be considered a sequestration project.[10] Sequestration projects make up only a small portion of total approved methodologies across all standards.[11]

As was mentioned above, hundreds, if not thousands, of methodologies exist for sequestration and avoidance projects under a variety of standards.[12] For the purposes of understanding the problems that C_4Coin aims to solve, these two general offsetting methods–avoidance and sequestration–provide sufficient background to understand carbon markets.

2.2 The State of Carbon Markets Today

This section will describe the state of carbon markets worldwide and how the C_4Coin blockchain can improve on the current system.

Carbon trading consists of compliance and voluntary markets. There are two types of compliance markets: Carbon Taxes and Cap-and-Trade schemes.[13] Carbon Taxes require companies to pay a fee based on how much they pollute into the atmosphere. In a Cap-and-Trade system, state regulation requires companies to keep their total carbon emissions below a certain level. If a company is unable to stay below this limit, it must purchase and retire carbon credits.[14] The voluntary

[8]United Nations Framework Convention for Climate Change, "Registry Functions," Accessed 2017-11-16, http://unfccc.int/kyoto_protocol/registry_systems/registry_functions/items/4066.php.

[9]United Nations Framework Convention on Climate Change (UNFCCC) Clean Development Mechanism (CDM), "CDM Methodology Booklet," 2016, 7, https://cdm.unfccc.int/methodologies/documentation/1611/CDM-Methodology-Booklet_fullversion.pdf.

[10]Ibid., 8.

[11]Ibid., 9-12.

[12]See Ex. 1 for a list of Standard-Setting Bodies

[13]Lawrence H Goulder and Andrew R Schein, "Carbon Taxes Versus Cap and Trade: a Critical Review," *Climate Change Economics* 4, no. 03 (2013): 1350010.

[14]Robert N Stavins, "Experience With Market-Based Environmental Policy Instruments," *Handbook of environmental economics* 1 (2003): 355–435.

market, by contrast, is reliant on altruistic motives. Voluntary credits tend to be cheaper and more plentiful due to more relaxed standards.

Including compliance and voluntary markets, the price of a carbon credit ranges from $1 to over $130 per credit.[15] Conjoining separate markets could eventually contribute to a more uniform price globally. This prospect appears increasingly likely as China (pilot system trading around $2.00)[16] seeks to link to California's Cap-and-Trade system (currently trading at $15.40),[17] which is also considering linking with Quebec ($14.75)[18] and other Canadian provinces.

The largest carbon trading systems in the world are compliance markets, with over $52 billion in worldwide trading as of 2017.[19] Compliance markets exist in a number of governments throughout the world (Ex. 2). The European Union's market is particularly robust. Currently the world's largest, it is soon expected to be second to China's Cap-and-Trade system which launched in December 2017.[20]

There are a number of challenges associated with participating in compliance systems, perhaps the foremost of which is that compliance markets are not standardized worldwide. Instead, each government has its own stringent, disparate regulations as to what qualifies as a carbon credit that can be traded, auctioned, or retired. As a result, compliance markets struggle to operate across borders.[21,22]

The voluntary carbon market features around $200 million of yearly trading worldwide, with a volume of about 65 million metric tonnes and an average global price of $3 per metric tonne.[23] Any individual hoping to offset their carbon footprint can purchase carbon credits on the voluntary market.[24] Voluntary carbon credits are verified by a number of standard-setting bodies (Ex. 1). Retiring a voluntary carbon credit would not qualify for compliance purposes, but one could voluntarily purchase and retire a compliance credit.

The voluntary market represents a major growth opportunity. If just 17% of the potential global voluntary carbon market were developed, it would be larger than all of the world's compliance markets put together.[25] Moreover, by entering the voluntary market, individuals and small businesses–although not covered by Cap-and-Trade or Carbon Tax schemes–can contribute enormously toward meeting the world's emissions reduction targets.

[15] World Bank, *State and trends of carbon pricing 2015* (World Bank Publications, 2015).

[16] International Carbon Action Partnership, "China - Guangdong pilot system," Accessed 2017-11-12, https://icapcarbonaction.com/en/?option=com_etsmap&task=export&format=pdf&layout=list&systems[]=73.

[17] Climate Policy Initiative, "California Carbon Dashboard," Accessed 2017-11-13, http://calcarbondash.org.

[18] International Carbon Action Partnership, "Canada - Québec Cap-and-Trade System," Accessed 2017-11-12, https://icapcarbonaction.com/en/?option=com_etsmap&task=export&format=pdf&layout=list&systems[]=73.

[19] World Bank, "Carbon Pricing Dashboard, 2016," Accessed 2017-11-10.

[20] Ken Silverstein, "China Launches a Cap-and-Trade Program to Cut Carbon Emissions," 2017, accessed December 23, 2017, https://www.environmentalleader.com/2017/12/china-launches-cap-trade-program-cut-carbon-emissions/.

[21] California Air Resources Board, "Compliance Offset Program."

[22] The EU Emissions Trading System (EU ETS), "Use of International Credits."

[23] Steve Zwick, "Building on Paris, Countries Assemble The Carbon Markets Of Tomorrow," 2016, accessed November 9, 2017, http://www.ecosystemmarketplace.com/articles/building-on-paris-countries-assemble-the-carbon-markets-of-tomorrow/.

[24] Carbon Trade Exchange, "What is CTX?," Accessed 2017-11-16, http://www.ctxglobal.com/about/.

[25] Compliance markets encompass 7 GtCO2e, or approximately 12% of global emissions according to Kossoy et. al "State and Trends," 21. Therefore, total global emissions are roughly 58 GtCO2e annually and 15% of 51 is 7.7.

2.3 Issuance, Verification, Trading, and Retirement

This section will provide an overview of how a carbon-offset project developer complies with the established protocols.[26,27]

A project developer begins by identifying a potential carbon-offset project. Once a potential project has been identified, the developer must contract a third party to conduct a baseline greenhouse gas (GHG) study.[28] This study measures the amount of carbon emitted under a "business-as-usual" scenario, before the offsetting project is operational.

Upon completion of the baseline GHG study, the project developer is required to submit a methodology document for the offset project.[29] The methodology document details the results of the baseline GHG study and puts forth a list of proposed actions that will reduce total GHG output relative to the baseline scenario. Methodology documents must be submitted to a standard-setting body for approval.[30] This approval process is rigorous and may involve several rounds of revision. If a new methodology is approved, it is registered in the standard-setting body's database as a verified methodology.[31] Verified methodologies can be re-used in the future as long as they are adjusted to meet the specific conditions of the new offset project.[32]

Next, the developer must complete a Project Design Document (PDD). A PDD explains a specific application of a verified methodology. The developer must submit the PDD for validation by an accredited third party. Upon validation, the project can be registered in the standard-setting body's project database.[33]

Once a project has been registered, the developer must create a monitoring plan.[34] This plan contains specific instructions enabling a third-party verifier to observe the project and determine the amount of GHGs mitigated. Upon submission of the monitoring plan, the standard-setting body coordinates with the third-party verifier to set up an in-person audit of the offset project. This carbon audit is based on the instructions laid out in the monitoring plan.

After a project has been audited, the third-party verifier reports back to the standard-setting body, comparing the project's actual performance with the predicted performance detailed in the methodology proposal and PDD. The standard-setting body issues one carbon credit into the developer's account for each metric ton of GHGs that the project actually offsets.

For the developer to sell credits to another entity, the buyer must also have a registry account. Transactions between registry accounts typically cost a fee. Credits held in a registry account can be sold, held as financial assets, or retired.

Retirement transactions are similar to sales. However, a buyer does not need

[26] Much of this section is written by Reed Shapiro, the Director of Business Development at Carbon Credit Capital (CCC). This writing does not necessarily reflect the opinions of CCC. His expertise is a trustworthy source due to his years of experience in the carbon-offset industry. Any inaccuracies created during the editing process are the responsibility of the C4Coin authors.

[27] United Nations Framework Convention on Climate Change (UNFCCC) Clean Development Mechanism (CDM), "CDM Methodology Booklet."

[28] United Nations Framework Convention for Climate Change (UNFCCC) Clean Development Mechanism (CDM), "CDM accreditation standard," Accessed 2017-11-10.

[29] United Nations Framework Convention for Climate Change (UNFCCC) Clean Development Mechanism (CDM), "Propose a new methodology," Accessed 2017-11-14.

[30] Ibid.

[31] Ibid.

[32] United Nations Framework Convention on Climate Change (UNFCCC) Clean Development Mechanism (CDM), "CDM Methodology Booklet."

[33] United Nations Development Programme, "Clean Development Mechanism, a User's Guide," 2003. http://www.undp.org/content/undp/en/home/librarypage/environment-energy/climate_change/mitigation/undp_cdm_manual.html.

[34] Carbon Action Reserve, "Program and Project Documents," Accessed 2017-11-15, http://www.climateactionreserve.org/how/program/documents/.

a registry account if they intend to retire credits immediately after purchasing. Typically, the buyer specifies a number of credits they would like to retire, and the project developer invoices them at an agreed price per credit. Once paid, the developer schedules the retirement of the purchased credits with the standard-setting body or registry. These credits are identified by serial number and permanently removed from circulation.

3 Problems

3.1 Ecological

Climate change is causing a global ecological crisis. Greenhouse gases trapped in the atmosphere are raising Earth's average temperature and devastating the environment. Glaciers are melting. Sea levels are rising. Precipitation levels are shifting, leading to historic droughts around the world.[35] Warmer waters are strengthening hurricanes.[36] It is difficult to look at the evidence and conclude that climate change is a hoax or non-issue, but millions of Americans remain skeptical,[37] adding to the challenge of organizing climate-conservation action.

This challenge is worsened by the fact that working to halt or reverse climate change is expensive.[38] Even businesses that accept the reality of the problem have no incentive to change their usual practices as they could lose profits and fall behind competitors. The current state of business optimizes for maximum immediate profit, leaving little room for environmental concerns.[39]

3.2 Political and Economical

Each compliance market around the world is crafted by a different set of legislators with different challenges and motivations in mind. This type of inconsistency creates difficulties when confronting any global issue on an inter-governmental level.

Additionally, carbon credits can appear to stifle the economy. Politicians don't want bad press for proposing policies that restrict economic growth, and businesses don't want extra expenses. In many countries, politicians are reliant on the business community for funding.[40] Moreover, a large segment of the voting population refuses to accept the reality of climate change.[41] These challenges make it difficult for politicians to advocate for carbon regulations, further hindering the development of compliance markets.

Environmental degradation is an external cost insufficiently incorporated into mainstream economics. Therefore, a market-driven approach can successfully combat climate change only if a financial incentive exists to protect the environment.

[35] Terrell Johnson, "California Isn't Alone: Historic Droughts Happening Around The World," 2015, accessed July 28, 2015, https://weather.com/science/environment/news/california-historic-drought-world-brazil-africa-korea.

[36] Michael E. Mann, Thomas C. Peterson Peterson, and Susan Joy Hassol, "What We Know About the Climate Change-Hurricane Connection," 2017, accessed September 8, 2017, https://blogs.scientificamerican.com/observations/what-we-know-about-the-climate-change-hurricane-connection/.

[37] Cary Funk and Brian Kennedy, "The Politics of Climate," 2016, accessed November 10, 2017, http://www.%20pewinternet.%20org/2016/10/04/the-politics-of-climate.

[38] Climate Policy Info Hub, "The Costs of Mitigation: An Overview," Accessed 2017-11-10, http://climatepolicyinfohub.eu/costs-mitigation-overview.

[39] Wikipedia, "Dodge v. Ford Motor Co.," Accessed 2017-11-07, https://en.wikipedia.org/wiki/Dodge_v._Ford_Motor_Co..

[40] Federal Election Commission, "2018 Political Action Committee Summary by Type," Accessed 2017-11-12, http://classic.fec.gov/disclosure/pacSummary.do?cf=phome.

[41] Funk and Kennedy, "The Politics of Climate."

3.3 The Wasteful Nature of Blockchain Consensus

Proof-of-Work (PoW) consensus is wasteful.[42] PoW deters malicious actors from engaging with the network by requiring expensive CPU (or GPU) resources to participate.[43] It has been predicted that the Bitcoin network will consume more electricity per year than the country of Denmark by 2020.[44] This figure does not account for the resources expended purchasing the required computer chips.[45]

Any environmentally conscious project cannot reasonably be created on such a wasteful network. It is essential for any carbon token solution to present a green consensus mechanism.

4 Network Architecture

This section describes the proposed network architecture for C_4Coin. The C_4Coin blockchain approaches the problems spelled out in Section 3 from an infrastructural perspective. First, a public blockchain can solve several inefficiencies in carbon markets. Specifically, a distributed carbon registry would significantly lower the costs of trading and retiring credits by removing the need for transactional oversight. Furthermore, immutable blockchain records contain the entire history of each credit on the system. Tokenizing credits migrated from multiple existing registries onto one blockchain enables interoperability between carbon standards on one market interface.

Most importantly, the C_4Coin Proof-of-Burn consensus mechanism resolves the voluntary carbon market's biggest failure: a lack of incentive to retire credits. This market failure results in an oversupply of carbon credits.[46] By creating this missing incentive, currently unusable credits gain utility and an entire economy can be built on combating climate change. For the C_4Coin blockchain to be carbon-negative, C_4Coin tokens used in consensus must be burned. This ensures the carbon credits that the tokens represent cannot be spent twice, and that users earning Exo through consensus have done verifiable work to benefit the environment.

The C_4Coin solution is market-driven and does not depend on innovative ecological science. Rather, the C_4Coin solution depends only on the fact that increasing the retirement of carbon credits will help curb global warming. As the supply of carbon credits decreases, the price will rise.[47] This increased price will incentivize investment in carbon mitigation technologies as previously economically unfeasible methods become profitable.

[42] Marc Pilkington, "11 Blockchain technology: principles and applications," *Research handbook on digital transformations*, 2016, 225.

[43] Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2008.

[44] Deetman, "Bitcoin Could Consume as Much Electricity as Denmark by 2020."

[45] John Leonard, "Cryptocurrency Miners Are Hiring Boeing 747s to Deliver GPUs," 2017, accessed July 31, 2017, https://www.theinquirer.net/inquirer/news/3014813/cryptocurrency-miners-are-hiring-boeing-747s-to-deliver-gpus.

[46] Environmental Finance, "Low Prices, But High Hopes for the Voluntary Carbon Market."

[47] Adam Smith and John Ramsay McCulloch, *An Inquiry into the Nature and Causes of the Wealth of Nations* (A. / C. Black / W. Tait, 1838), Book 1, Ch 7.

The remainder of this section will detail:

1. How off-chain carbon credits can be represented as digital tokens,
2. How C_4Coin tokens are traded on the network,
3. How this public blockchain achieves network consensus,
4. How the monetary policy for Exo tokens will be managed, and
5. How network development will be governed.

4.1 Carbon Token Generation and Retirement

This section will describe how C_4Coin tokens will be generated initially. Section 4.5.1 will discuss future methodologies for generating C_4Coin tokens.

Because one C_4Coin is equivalent to one carbon credit, it is important to determine which carbon-offset methodologies generate C_4Coin tokens. Due to the difficulty of measuring and verifying carbon offsets, the network will utilize existing carbon registries'[48] data to issue C_4Coin tokens. This will be accomplished by working with carbon-offset project developers to auction off their registry account balances in the form of C_4Coin tokens. These tokens represent claims to retire existing credits in carbon-offset project developers' registry accounts. As each of these C_4Coin tokens is retired (burned) in PoB consensus, the project developer will retire the off-chain counterpart.

These auctions will make C_4Coin tokens available to anyone interested in joining the network. Since the origin of a carbon credit is important for determining its value, each of these auctions will be started by a generation transaction. This transaction stores a hash of the following data:

- The generator's public address,
- The number of carbon credits,
- The date of the auction,
- The location of the project that generated the credits,
- The identifier of the methodology used to create the tokens, and
- The signed auction agreement (explained below).

Auction participants bid and, if the reserve is met, receive C_4Coin tokens in their wallets at the close of the auction. However, this method of issuing C_4Coin tokens will not work if the off-chain data cannot be trusted. This issue raises two distinct problems:

1. Identity theft, and
2. Double-selling existing carbon credits.

If a malicious actor claimed false ownership of existing registry accounts, they could sell credits that they do not own. To prevent such identity theft, the issuance system should implement an oracle that provides data veracity through Proof-of-Existence and an attestation mechanism. One possible candidate for a decentralized

[48]See Exhibit 2 for a list of carbon registries.

oracle is ChainLink.[49] When a project developer wants to open an account, they will be required to retire one carbon credit and put a unique challenge hash provided by the network in the comment section. By comparing the resulting public receipt to the challenge, the data from the oracle can be used to verify account ownership.

When the auction ends, the carbon-offset project developer will be paid for their existing credits but retain control of their registry account. Even though participants will have received C_4Coin tokens, there must be enough off-chain credits reserved for each auctioned C_4Coin token. However, carbon-offset project developers could be tempted to double-sell the existing credits – thereby leaving the auctioned tokens without backing.

To disincentivize double-selling opportunities, all auctions will include a legally-enforceable auction agreement. This agreement will include a per-credit penalty if the registry account owner does not retire credits within the given time-limit. If a malicious carbon-offset project developer tokenizes the same set of credits twice or fails to retire off-chain credits when their digital counterparts are retired, the system can determine any discrepancies between the value of the project developer's registry account retirements and the value represented on-chain. These discrepancies will be easily identifiable because both sets of data are publicly available. This verifiability makes it extremely difficult for project developers to successfully perpetuate fraud.

To automatically detect retirement fraud, a dApp will be built to report C_4Coin retirements on a regular interval. First, it will calculate the amount of C_4Coin burned in network consensus. Then, it will provide a report to carbon-offset project developers indicating the amount of off-chain carbon credits to retire. It will also be possible to attribute specific amounts of retired credits to particular identities. A public receipt for each of these retirement transactions will be posted by the existing registry and bound by the oracle using the same Proof-of-Existence protocol. Thus, carbon-offset project developers not in compliance can be charged penalties and prevented from selling additional credits. Furthermore, users can verify that the blockchain is achieving its stated goals.

4.2 Carbon-Offset Tokens: C_4Coin

This section will discuss the structure of C_4Coin tokens. C_4Coin will be implemented using an ERC223 token interface, with one token corresponding to one metric ton of carbon offset. These tokens will also be composed of a hash of metadata, A, indicating:

- The project developer's public key, and
- The identifier of the auction generation transaction (§4.1) used to create the tokens.

While the PoB mechanism is insensitive to metadata, metadata will allow the network infrastructure to host both the voluntary and compliance markets. By linking token creation with methodology metadata (establishing token origins), users will be able to identify which tokens meet their requirements. However, the inclusion of this data in the tokens will mean some transactions may involve conflicting metadata.

To illustrate, suppose a user decides to send 7 tokens. Their wallet consists of 5 tokens with metadata A_1 and 5 tokens with metadata A_2, where A_1 and A_2 represent metadata identifying different methodologies. Given the metadata conflict, the user

[49] Steve Ellis, "ChainLink - A Decentralized Oracle Network," 2017-09-04, https://link.smartcontract.com/whitepaper.

must either send two transactions and pay two transaction fees, or the metadata must transform to reflect both origins. Since the ultimate goal is to determine the origin of the tokens and avoid unnecessary fees, the tokens should be sent with new metadata, B, that consists of:

- The sender's public address,
- The composite transaction identifier,
- The date of the current transaction, and
- The number of times metadata has been replaced on these tokens.

Continuing the example, if the user decided to send 5 tokens with metadata A_1 and 2 tokens with metadata A_2, the recipient would receive 7 tokens of metadata B_1. Since metadata B_1 contains information identifying the transaction in which tokens were combined, mapping algorithms will be able to determine the composition of tokens with metadata B.

Wallet solutions may either store a user's tokens in their aggregated form (metadata B), or in the form of some number of tokens, W, with metadata A_1, X tokens with metadata A_2, Y tokens with metadata B_1, Z tokens of metadata B_2 and so on. If a user wants to turn tokens with metadata B into tokens with metadata $A_1, \ldots, A_z$, the generation API will support "unpacking" by mapping the submitted tokens, removing them from circulation, and reissuing tokens with clean metadata. A fee will be charged based on the difficulty of the mapping transaction.

4.3 Proof-of-Burn Consensus

This section will describe the C_4Coin consensus mechanism. It will begin with an overview of the Ouroboros Proof-of-Stake protocol, the basis for C_4Coin's proposed implementation. This section will then discuss the modifications necessary to implement Proof-of-Burn within Ouroboros and the resulting crypto-economic analysis.

4.3.1 Ouroboros

Currently, several proven Proof-of-Stake protocols exist.[50] C_4Coin will develop a Proof-of-Burn protocol based on Ouroboros Proof-of-Stake.[51]

Proof-of-Stake (PoS) balances incentives by rewarding nodes who host the network. The trustworthiness of a given node is measured by the absolute stake (the number of tokens) it is willing to forfeit for malicious actions. For as long as a node stakes (places assets into escrow) without acting maliciously, it will receive block and gas rewards proportional to its relative stake. Relative stake is a dynamic number that is a function of absolute stake over total network stake per epoch, where an epoch is a constant length sequence of blocks using the same validators. Block rewards issue new currency into circulation based on the network's monetary policy, whereas gas rewards are based on collected transaction fees. If a node acts maliciously, its absolute stake is slashed.

The Ouroboros protocol uses a predefined set of validators (nodes) at the genesis block. These validators act as the initial committee and electors, proposing blocks onto the chain. During the initial epoch, a dynamic committee-selection mechanism will be applied based on the assumption that at least one-third of the validators are

[50] Ouroboros and Snow White are two good examples.

[51] Aggelos Kiayias et al., "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Annual International Cryptology Conference* (Springer, 2017), 357–388.

honest.[52] The committee for each subsequent epoch will be selected by a subset of the electors.

Once a committee is selected, a verifiable random function (VRF) is used to determine if each proposer can propose a block in that slot given their relative stake. Slot assignment is determined by a secure, multi-party signing protocol defined by the Ouroboros protocol.[53]

The Ouroboros protocol is a synchronous protocol with an upper time limit for which any honest stakeholder can communicate with any other stakeholder. Each slot represents an opportunity for a stakeholder to be selected to mint a block. When a slot leader's time arrives, they generate a block to commit to the blockchain. At this time, relevant rewards will be accumulated by each user upon completion of the epoch. Each participant will receive both block and gas rewards.

4.3.2 Design

The primary difference between the Ouroboros Proof-of-Stake protocol and C_4Coin's protocol is that the former uses a one-token model while the latter uses a two-token model. In Ouroboros, a user's stake and rewards are denominated in the same tokens. Instead, C_4Coin will be burned for rewards of a different token, Exo.

When a user decides to mint Exo, they will send C_4Coin to a bond smart-contract. This contract will decay the staked tokens to determine a user's proportional reward distribution. Rewards will be received when the bond contract depletes the stake or when the stake is removed. The amount of C_4Coin staked will define the user's absolute stake, which will decay throughout the life-cycle of participation. This absolute stake can be used to determine the relative stake, which leads to the following rewards function:

Rewards per Minter S_{rel} is the relative stake and corresponds to the probability a minter with address m in a committee c will be chosen to propose a block in an epoch e:

$$S_{rel}(c, m) = \frac{c[m].Stake}{CommitteeStake(c)}$$

where

$$CommitteeStake(c) = \sum_{i=1}^{|c|} c[i].Stake$$

Once a minter is selected and creates a block the total rewards are accumulated into the bond-smart contract using a coinbase transaction. Given a block and a minter the rewards can be computed as:

$R = R_{block} + R_{gas}$ where R_{block} and R_{gas} are the block and gas rewards.

Block rewards depend on the epoch number, and will be defined by Exo's monetary policy (§4.4). Gas rewards depend on the amount of gas used by dApps on the

[52] Kiayias et al., "Ouroboros: A provably secure proof-of-stake blockchain protocol."

[53] Ibid.

network. The longer the commitment time, the more a minter will accumulate gas rewards.

An optimal decreasing monotonic function will be determined to ensure a user's C_4Coin stake is exhausted during the life-cycle of participation. The next two subsections explain how two types of decay–exponential decay and linear decay–might work.

4.3.3 Exponential Decay

If C_4Coin decays at an exponential rate, a user's absolute stake gradually decreases over a sequence of slots throughout epochs according to the following function:

$$S(s) = S_0 e^{-\lambda s \Delta t}$$

where S_0 is the initial amount staked, λ is the age factor and Δt is the slot interval taken as a constant.

The stake decay function $S(s)$ represents the absolute stake of a minter, $c[m].Stake$, as a function of slot number. As slots are proposed, the slot count is incremented and the absolute stake is decremented according to the decay function.

The block time between slots can be modeled as a constant, Δt. If there are $s = k$ slots from the initial stake time, $t_0 = 0$, the absolute stake will decay until a minimum stake S_{min} is reached:

$$S_{min} = S_0 e^{-\lambda s \Delta t}$$

Therefore, given an initial stake amount, the finite staking duration can be derived by solving for the number of slots k:

$$k = \frac{-ln \frac{S_{min}}{S_0}}{\lambda \Delta t}$$

Staking more C_4Coin will therefore require a longer stake duration.

To encourage longer staking times and increase network participation, a constant divider can be added, $\rho > 1$, against the decay constant, effectively increasing the staking time.

$$\rho k = \frac{-\rho ln \frac{S_{min}}{S_0}}{s \lambda \Delta t}$$

$$S(s) = S_0 e^{\frac{-\lambda}{\rho s \Delta t}}$$

However, the initial absolute stake, S_0, must be adjusted to a new initial stake amount, $S_\emptyset$, to maintain the same total decay amount and eligibility for reward:

$$S_0 \int e^{-\lambda t} dt = S_\emptyset \int e^{-\lambda \rho t} dt$$

Solving for for the adjusted initial stake:

$$S_\emptyset = S_0 \frac{\int e^{-\lambda t} dt}{\int e^{-\lambda \rho t} dt}$$

$$S_\emptyset = S_0 \rho$$

This would create incentives for minters with varying stakes to select longer staking durations.

4.3.4 Linear Decay

If C_4Coin decays at a linear rate the decay function is:

$$S(s) = S_0 - B_r s \Delta t$$

The pledged stake, S_0, and the burn rate, B_r, will be chosen by the minter. The number of slots required to deplete a user's stake can be determined using the initial stake amount.

$$k = \frac{S_0}{B_r \Delta t}$$

where the burn rate must be

$$B_{min} \leq B_r \leq B_{max}$$

The maximum burn rate, B_{max}, gives the shortest duration, or minimum number of slots k_{min}. Since users will stake varying amounts of C_4Coin, the maximum burn rate should be parametric to the initial amount staked. For larger stakes, the burn-rate must be proportionally increased by a constant scaling factor $n > 1$.

$$B_{max} S_0 = n S_0$$

A maximum amount of steps k_{max} can be used to create an upper-bound on staking duration.

$$k_{max} = \frac{S_0}{B_{min}\Delta t}$$

After each slot, the slot count is incremented, effectively decreasing a user's absolute stake. This continues until the stake reaches zero. By holding rewards in a bond contract until a user's entire staking life cycle has ended, disincentives can be maintained. Minters can withdraw their stake early (between epochs) at the cost of some of their gas rewards.

4.4 Network Tokens: Exo

The goal of this section is to open a dialogue about C_4Coin's monetary policy. The monetary policy proposed in this section is based on Ethereum Classic, but is currently under development. Community feedback will be paramount for composing an ideal policy.

Exo is the utility token used to run the C_4Coin network. It is a disinflationary crypto-asset, meaning that it reduces to a near-zero inflation rate within two decades. A finite amount of Exo will be created in the genesis block, and will be based on the amount distributed in the pre-sale auctions. An estimated 10,000,000 Exo tokens will be circulated initially, with an estimated 70,000,000 to be generated overall. The intention is to distribute 100% of the initial 10,000,000 Exo in pre-launch auctions of C_4Coin. The actual amount distributed may vary depending on how many ITO auction stretch goals are reached (§4.5.4).

Annual block rewards (the base amount of Exo received for successfully proposing a block) will decrease by 10% per era (about 2.4 years). Each era will contain 5,000,000 epochs.

Since Exo will be required to run smart contracts on the C_4Coin blockchain, this demand for Exo will help to regulate the network's market. A finite supply of Exo will exist, adding to positive pressure on the price of Exo over time. As the price increases, more users will be incentivized to generate and burn C_4Coin to earn Exo.

Topics for further discussion include:

1. How many Exo tokens should be made available in the ITO?
2. Should there be a finite number of Exo tokens? If so, how many?
3. How many decimal places should Exo tokens have?
4. How should Exo block rewards be calculated?
5. What should smaller denominations of Exo be named?

4.5 Network Development

This section will describe the planned development of the C_4Coin project. Significant development work will be required for the C_4Coin network to become self-sufficient. Beyond the development covered in Sections 4.1 through 4.4, the network must be a legally compliant entity with decentralized governance. Since this network fundamentally relies on its users agreeing that C_4Coin tokens are valuable, the methods that generate C_4Coin tokens must be trusted.

The C_4Coin blockchain relies on off-chain data for operation. This reliance creates a trust issue in that data can be fabricated. Initially, the C_4Coin team will identify trustworthy entities to generate tokens. However, the trust established will rely on the enforceability of agreements between C_4Coin token generators (carbon-offset project developers) and the network. Thus, the network must be a compliant entity. In the long term, it would be best if these agreements were made by the entire network.

In lieu of issuing a significant percentage of network tokens to themselves, the C_4Coin team will collect a fee on Exo rewards. These funds will be used to support the continued development of features including a distributed governance system and a self-amenable consensus mechanism. Once a stable governance mechanism is implemented, the original C_4Coin team will turn over all network operations to the users, resulting in a decentralized network.

The remainder of this section will begin by discussing how C_4Coin generation methods will be managed and how decisions will be made. It will then present the implementation roadmap for proof-of-concept before finally discussing the planned ITO strategy.

4.5.1 New C_4Coin Generation Methodologies

The most important aspect of any C_4Coin token generation method is that the network agrees it represents valuable work. This paper's initial contention is that climate change is a significant enough issue that people should agree work performed to mitigate the problem is valuable. However, there are many ways to measure the value of work done to protect the environment. Therefore, the network needs a mechanism to determine which methods are approved to generate C_4Coin.

A whitelist will be implemented to discern which methodologies can generate C_4Coin tokens. By adding methods to or removing methods from the list, different incentives can be implemented. A possible method for making decisions about which tokens should be added to or removed from the list is discussed in §4.5.2.

4.5.2 Proposed Reputation System

The proposed Reputation System will be a dApp allowing for collective decision-making among nodes. Because significant network development is required post-launch, the C_4Coin team will initially maintain control of major decisions. However, the team is committed to soliciting community input before making any deviations from the plan presented in this paper. Specific goals for the reputation system include:

1. Maintaining network stability,
2. Encouraging user involvement in network consensus, and
3. Granting small (in terms of financial value) network participants useful influence relative to large network participants.

One proposed solution is presented below:

Change is a reputation token that allows users to vote on network decisions. Change will be non-transferable and only represents voting power for a node. When a node participates in consensus, it will receive Change tokens. The more blocks proposed, the more Change a node will receive, up to a maximum. When a node stops hosting the network, Change they have amassed will rapidly decay, requiring nodes to remain active to influence the network.

In time, the goal is to link all network-wide decision-making to this tool (or something like it as determined by the community as the project develops). Decisions this system will control include:

1. Whitelisting C_4Coin generation methodologies,
2. Determining the demurrage and/or value in consensus of different types of C_4Coin,
3. Amending Exo monetary policy, and
4. Implementing new network consensus mechanisms.

A foundational reputation system as proposed above may be used to implement additional governance mechanisms. For example, Ryan Zurrer has suggested a method for determining the reputation of carbon-offset verifiers.[54] Such a model could decentralize the identification of which verifiers are most trustworthy.

4.5.3 Implementation Roadmap

The proof-of-concept roadmap consists of five milestones. Roughly four to eight weeks of development will be required to achieve each milestone.

The first milestone is to establish a continuous integration process on a test network for the C_4Coin blockchain. Parity's implementation of Ethereum will be used for Proof-of-Concept due to its modular consensus interface. This codebase will allow agile changes to both network and application layer code as the network is tested.

The second milestone is to implement Proof-of-Burn with a supply of C_4Coin tokens from an existing registry. Validator contracts will be integrated and modified to interface with bond smart-contracts that pay rewards in Exo. Additionally, the whitelist filter discussed §4.5.1 will be created to determine which tokens are allowable in network consensus.

The third milestone is to begin work on the auction portal backend. Development of this backend API will focus on integrating a decentralized oracle such as ChainLink. Additionally, the API will manage auction agreements generating C_4Coin as described in §4.1.

The fourth milestone is to integrate a payment gateway into the backend API. This gateway will allow buyers to purchase C_4Coin using Bitcoin, Ether, and USD. Potential implementations include GDAX, CoinBase, Stripe, and/or Braintree.

The fifth milestone is to develop the auction portal dApp. This dApp matches bidders to sellers based on a sealed-bid auction smart contract. In the interest of performance, matching may be done on a state channel using the 0x protocol.[55]

4.5.4 Initial Token Offering Strategy

The C_4Coin Initial Token Offering (ITO) is designed to raise capital to finish developing Minimum Viable Product (MVP) in compliance with securities laws in the United States of America.

[54] Ryan Zurrer, "Carbon Token Ecosystem - White Paper," accessed November 8, 2017, https://docs.google.com/document/d/1fNxBRcdYR7Ug5y208K-VPDhDk_IHjm8Sli3It8JduDI/edit.

[55] https://0xproject.com/

The Securities Exchange Commision (SEC) recently clarified its stance[56] on crypto-assets in its investigation of the DAO. In this investor bulletin, the SEC advises against investing in Initial Coin Offering (ICO) opportunities because they are not protected by the Securities Exchange Acts of 1933 and 1934. More importantly, the SEC noted that it will review each token offering separately to determine the character of the tokens. The SEC acknowledges that while the tokens sold by the DAO were considered equity, tokens in general do not have to contain the characteristics of a security. Notably, the SEC is able to make these determinations from existing law.

Neither C_4Coin nor Exo is intended to be structured as a security. Furthermore, there is no intention to sell Exo tokens at this time.

The U.S. Treasury Department enforces the Bank Secrecy Act and the Anti-Money Laundering regulations via the Financial Crimes Enforcement Network (FinCEN) for Money Services Businesses.[57] Specifically, issues arise when one becomes an Administrator or Exchanger of a Convertible Virtual Currency. Due to the need for continued network development post-launch, the C_4Coin team may be considered an Administrator (and potentially an Exchanger) of a Convertible Virtual Currency.

These regulations do not apply to C_4Coin if it is not considered a Convertible Virtual Currency by FinCEN. However, it is also possible that the project may be exempt under the "Integral Exception."[58] The primary strategy is to request an administrative ruling from FinCEN first regarding the classification of C_4Coin and second arguing for exemption under the integral clause. A ruling in C_4Coin's favor would be an enormous public relations opportunity.

Contingencies exist if the FinCEN ruling is not in the project's favor. Specifically, it may be possible to structure the ITO Auctions as gift certificates. In a worst case scenario, C_4Coin may have to incorporate in Switzerland and avoid soliciting investment from U.S. citizens in the ITO. This strategy has been successfully implemented by several prominent ITO projects.[59] However, C_4Coin can benefit from the protections offered by U.S. capital markets.

The C_4Coin ITO will use the auction system described in §4.1 with one important difference: when carbon credit auctions reach a stretch goal price, participants will be rewarded with Exo tokens in addition to the C_4Coin they purchased. Because Exo is never sold by the C_4Coin team, whether or not the token represents a security is not an issue for the ITO. The ITO auctions will feature a curated selection of carbon credits from reputable project developers. Several rounds of C_4Coin ITO auctions will be completed by the end of summer 2018.

A final unique feature of the C_4Coin project will be the Regulation A+ equity crowdsale conducted instead of a token pre-sale. CO2KN, INC, a Delaware corporation developing the C_4Coin blockchain, will offer a significant amount of equity to early adopters to ensure these users have influence in early governance decisions as a distributed system is established.

[56] U.S. Securities and Exchange Commision, "Investor Bulletin: Initial Coin Offerings," 2017-06-25, https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings.

[57] Department of the Treasury Financial Crimes Enforcement Mechanism, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," 2013-03-18, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

[58] US Federal Statute, *31 C.F.R. § 1010.100(ff)(5)(ii)(F)*.

[59] Hugo Miller, "Welcome to Crypto Valley," 2017, accessed November 10, 2017, https://www.bloomberg.com/news/articles/2017-10-10/welcome-to-crypto-valley.

5 Technological Challenges

Section 3 surveyed the various problems–ecological, political, and economic–that C_4Coin will solve. This section describes two technological challenges C_4Coin faces to provide a viable solution to the problems outlined above. Namely,

1. It is difficult to ensure the veracity of off-chain data, and
2. Public blockchains present unique scalability issues.

This section will elaborate on these two challenges and how they apply to C_4Coin.

5.1 Maintaining Data Veracity

Maintaining data veracity is the process of continuously ensuring data accurately reflects reality. While blockchain makes it easier to determine whether data has changed, the question as to whether the initial data was valid remains a problem. No matter how precisely carbon-offset measurements are implemented, there are methods for fraudulently modifying off-chain data sources.[60] Too many spurious tokens in circulation would dilute the value of valid tokens and discourage user trust in the network. Trusted token generators beholden to network users can alleviate this issue (§4.5.1).

Another potential data veracity issue concerns hard forks of the blockchain. If irreconcilable differences arise between proposed next blocks, a hard or soft fork occurs. The resulting blockchains contain identical data for all blocks prior to the fork (Ex. 4). The divergence must be resolved by the network protocol (soft fork), otherwise a new network emerges (hard fork). Hard forks are especially problematic for C_4Coin, as tokens on the new network would represent competing claims to retire the same off-chain carbon credit. It may be possible to mitigate this issue with the legal agreements discussed in §4.1.

5.2 Scalability

Blockchains present two unique scalability issues that limit user adoption. The first problem involves the size of the blockchain. A blockchain continues to grow in size as transactions are verified in each new block. For example, just over two years after launch, it is now impossible to expect rewards when hosting a full Ethereum node on consumer hardware.[61] Hosting such a system on an embedded or cellular device is currently impossible. While the late-stage exponential growth of processing power may allow hardware to keep up with these constraints, a more scalable solution is necessary. Cutting-edge theories are trending towards hash-graph technologies (such as Iota[62]) to solve scalability, but these implementations remain experimental, still rely on PoW, and cannot run smart contracts because they lack a virtual-machine implementation.

The second scalability issue facing this project is the limitation on Transactions Per Second (TPS). Public blockchains have significantly lower TPS than payment systems such as credit cards (Ex. 3). TPS limitations present an issue for the

[60] Shusuke Murai, "GPS 'Spoofing' is No Joke: Dangers of GPS Data Hacking Realized," 2017, accessed November 28, 2016, http://www.govtech.com/security/GPS-Spoofing-is-No-Joke-Dangers-of-GPS-Data-Hacking-Realized.html.

[61] 5chdn, "What are the Ethereum Disk Space Needs: Response," 2016, accessed November 6, 2017, https://ethereum.stackexchange.com/questions/143/what-are-the-ethereum-disk-space-needs.

[62] Serguei Popov, "The tangle," *IOTA*, 2016,

C_4Coin blockchain, which would ideally grow to support a variety of marketplaces and applications.

Since much larger, established blockchain projects face these same scalability issues,[63] the C_4Coin blockchain can launch and grow successfully with current technology. Future resources may be contributed to broader open source projects tackling these scalability challenges. Solving blockchain scalability is outside of the initial scope of the project and not essential to achieving C_4Coin's core value proposition. Nonetheless, these issues must remain on the project's long-term radar.

6 Conclusion

C_4Coin is an innovative project with the potential to combat climate change globally. Incentivizing individuals and communities to voluntarily clean up the atmosphere presents the most realistic opportunity to protect the earth. Using a unique business model, this project can be completed in a way that rewards initial investors while working towards the long-term goal of distributed political action. While there are significant challenges associated with the project, the team is confident that they can be overcome through dedication and community support.

[63] Alyssa Hertig, "The $28-Billion Challenge: Can Ethereum Scale to Meet Demand?," 2017, accessed June 30, 2017, https://www.coindesk.com/28-billion-challenge-can-ethereum-scale-meet-demand/.

7 Contact Information

For any inquiries related to the C_4Coin blockchain, please contact:

Harrison Perl
harrison@c4coin.org
1(917) 575-4134
Or
info@c4coin.org

8 Exhibits

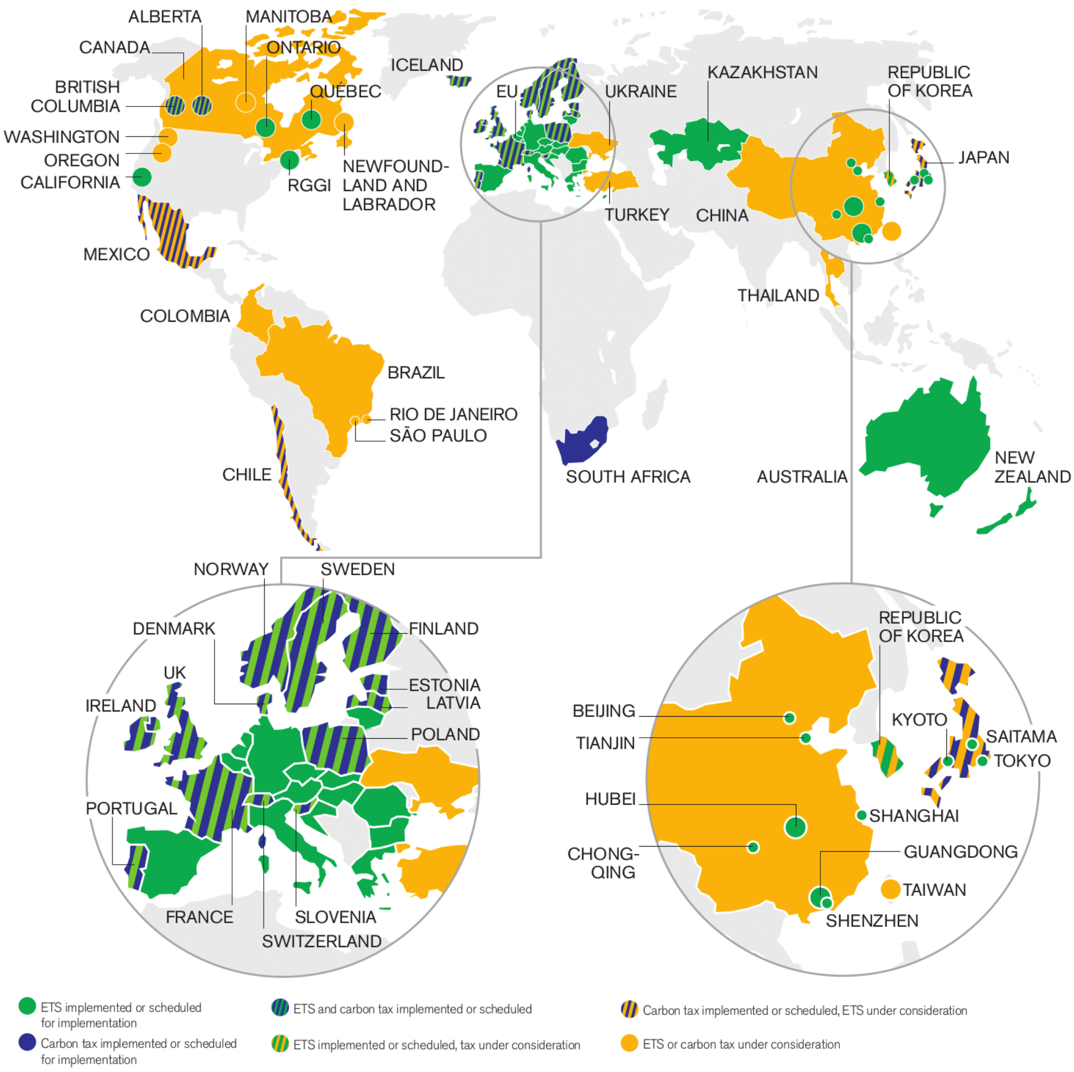
8.1 Exhibit 1

List of Voluntary Standard Setting Bodies

Number	Entity	Website
1	Verified Carbon Standard (VCS)	http://www.v-c-s.org
2	American Carbon Registry (ACR)	http://americancarbonregistry.org
3	REDD+	http://www.un-redd.org
4	Clean Development Mechanism (CDM)	http://cdm.unfccc.int/index.html
5	CCBA	http://www.climate-standards.org
6	Gold Standard	https://www.goldstandard.org
7	Climate Action Reserve (CAR)	http://www.climateactionreserve.org

8.2 Exhibit 2

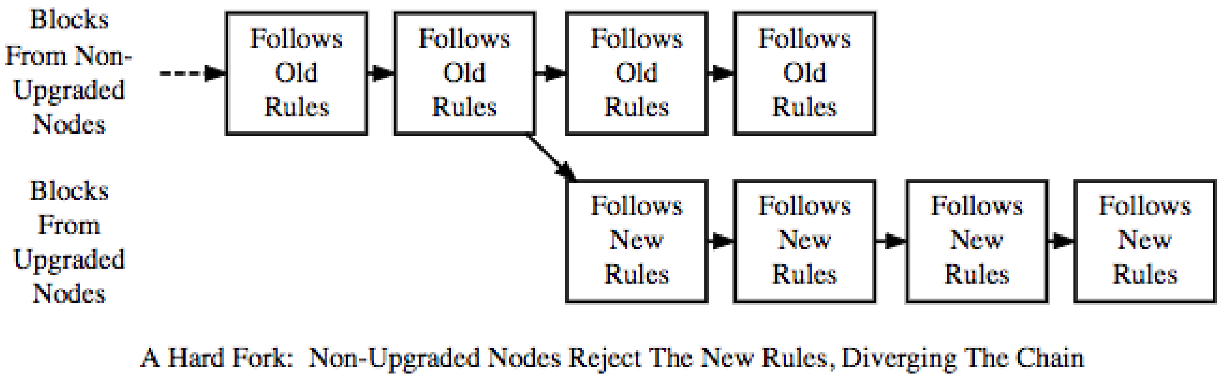
Chart of Compliance Carbon Markets[64]



[64]World Bank, “Carbon Pricing Dashboard, 2016.”

8.3 Exhibit 3

Hard Forks[65]



8.4 Exhibit 4

Comparison of current, approximate practical and theoretical TPS for Bitcoin, Ethereum, and Visa circa summer 2017.[66]

Technology	Practical TPS	Theoretical TPS
Bitcoin	3-4	7
Ethereum	15	30
Visa	1,667	56,000

[65]Investopedia.com, "Hard Fork," 2017. Accessed 2017-11-15, https://www.investopedia.com/terms/h/hard-fork.asp.

[66]Jan Vermeulen, "Bitcoin and Ethereum vs Visa and PayPal - Transactions per second," 2017, accessed November 10, 2017, https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html.

9 Definitions

- **Application Programming Interface (API):** A set of clearly defined methods of communication between various software components.
- **Bitcoin:** The first decentralized cryptocurrency, which was launched in 2009 by Satoshi Nakamoto. It uses a **Proof-of-Work Consensus Mechanism**.
- **Blockchain:** a method for coalescing a single source of objective sequential data amongst a distributed network.
- **Block:** A file containing a designated amount of compound data.
- **C_4Coin:** a tradable **Carbon Credit** built on the **C_4Coin Blockchain**.
- **Cap-and-Trade:** A carbon trading system under which companies must purchase credits to counteract emissions above a regulatory maximum. (See 2.1.2)
- **Carbon Credit:** A certificate that represents one metric tonne of CO_2 or equivalent offset.
- **Carbon Credit Registry:** A body denoting who retired **Carbon Credits** and confirming that individual credits comply with the registry's specific standards.
- **Carbon Tax:** A government tax on greenhouse gas emissions. (See 2.1.2)
- **CO2KN (Pronounced "See-Oh-Token"):** The company operating the **C_4Coin Blockchain**.
- **Coinbase transaction:** The first transaction in the creation of a new **Block**. Only **Miners** can make this transaction. There is no input into this transaction, instead this transaction is the block rewards.
- **Compliance Carbon Market:** Government-mandated systems for reducing emissions like **Cap-and-Trade** or **Carbon Taxes**. (See 2.1.2 and Ex. 2)
- **Consensus Mechanism:** The algorithm by which a distributed **Blockchain** comes to agree on the data to be added to the next **Block** for the purposes of immutable storage.
- **Crypto-asset:** A unique piece of data with provable ownership.
- **Cryptocurrency:** A digital currency using encryption to regulate the generation of units of currency and verify transactions.
- **Decentralized Application (dApp):** An application that runs on a distributed **Blockchain** rather than a centralized server.
- **Epoch:** a sequence of **Blocks** using the same validators.
- **Ethereum:** A **Blockchain** that allows users to build smart contracts and **dApps**. It was launched in 2015 and currently uses a **Proof-of-Work Consensus Mechanism**.
- **Exo:** A network token on the **C_4Coin Blockchain** that **Smart Contracts** must use as a fuel to continue running. (See 4.4)

- **Fork:** A fork is when some **Nodes** agree on one **Block** while other **Nodes** agree on a different **Block**. This creates two **Blockchains** run by two groups of **Nodes**, but they have the same history. (See Exhibit 3)
- **Genesis Block:** The first **Block** in a **Blockchain**.
- **Initial Token Offering (ITO, a.k.a. ICO):** The first time a **Crypto-asset** is made available for sale.
- **Miner:** An individual operating a **Node** organizing **Blocks** in a **Proof-of-Work Consensus Mechanism**. **Miners** use computer processing power as a resource to determine the next **Block** and obtain rewards. The term is sometimes used to describe users who organize **Blocks** in other **Consensus Mechanisms** as well.
- **Minter:** An individual operating a **Node** organizing **Blocks** in a **Proof-of-Burn Consensus Mechanism**. (See 4.3)
- **Node:** A computer that hosts an entire **Blockchain** and organizes **Blocks**.
- **Proof-of-Burn (PoB):** A **Consensus Mechanism** proposed by Iain Stewart where **Proof-of-Work** is simulated by spending **Crypto-Assets** instead of real-world resources.
- **Proof-of-Stake (PoS):** A **Consensus Mechanism** where users put **Crypto-Assets** into escrow. If a user's **Node** behaves honestly and without malfunctions, they receive a reward. If they fail to do so, they lose the staked **Crypto-Assets**.
- **Proof-of-Work (PoW):** A **Consensus Mechanism** where users who organize **Blocks** must use CPU or GPU power to solve complex cryptographic codes to win **Blocks**. This process is resource-intensive. (See 3.3).
- **Retired:** A term used to describe **Carbon Credits** that have been applied as emission reductions and can no longer be traded.
- **Smart Contract:** A contract that is run by a computer with no human input. These programs form the foundation of **dApps**. Most common on the **Ethereum** platform.
- **Solidity:** A programming language on **Ethereum** similar to JavaScript, which allows for writing **Smart Contracts**.
- **Voluntary Carbon Market:** A carbon market where businesses or individuals can buy and retire **Carbon Credits** of their own volition. (See 2.1.2)

References

5chdn. “What are the Ethereum Disk Space Needs: Response.” 2016. Accessed November 6, 2017. https://ethereum.stackexchange.com/questions/143/what-are-the-ethereum-disk-space-needs.

Baliga, Arati. *Understanding blockchain consensus models.* Technical report. Tech. rep., Persistent Systems Ltd, Tech. Rep, 2017.

BitInfoCharts. “Bitcoin Block Time historical chart.” Accessed 2017-12-06. https://bitinfocharts.com/comparison/bitcoin-confirmationtime.html#3m.

California Air Resources Board. “Compliance Offset Program.” Accessed 2017-11-15. https://www.arb.ca.gov/cc/capandtrade/offsets/offsets.htm.

Carbon Action Reserve. “Program and Project Documents.” Accessed 2017-11-15. http://www.climateactionreserve.org/how/program/documents/.

———. “Reserve FAQs.” Accessed 2017-11-14. http://www.climateactionreserve.org/resources/faqs/.

Carbon Trade Exchange. “What is CTX?” Accessed 2017-11-16. http://www.ctxglobal.com/about/.

Climate Policy Info Hub. “The Costs of Mitigation: An Overview.” Accessed 2017-11-10. http://climatepolicyinfohub.eu/costs-mitigation-overview.

Climate Policy Initiative. “California Carbon Dashboard.” Accessed 2017-11-13. http://calcarbondash.org.

Deetman, Sebastiaan. “Bitcoin Could Consume as Much Electricity as Denmark by 2020.” 2016. Accessed March 29, 2016. https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020.

Department of the Treasury Financial Crimes Enforcement Mechanism. “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.” 2013-03-18. https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

Ellis, Steve. “ChainLink - A Decentralized Oracle Network.” 2017-09-04. https://link.smartcontract.com/whitepaper.

Environmental Finance. “Low Prices, But High Hopes for the Voluntary Carbon Market.” South Pole Group. Accessed 2017-12-08. https://www.southpole.com/news/low-prices-but-high-hopes-for-the-voluntary-carbon-market.

Federal Election Commission. “2018 Political Action Committee Summary by Type.” Accessed 2017-11-12. http://classic.fec.gov/disclosure/pacSummary.do?cf=phome.

Funk, Cary, and Brian Kennedy. “The Politics of Climate.” 2016. Accessed November 10, 2017. http://www.%20pewinternet.%20org/2016/10/04/the-politics-of-climate.

Goodman, LM. *Tezos—a self-amending crypto-ledger White paper*, 2014.

Goulder, Lawrence H, and Andrew R Schein. “Carbon Taxes Versus Cap and Trade: a Critical Review.” *Climate Change Economics* 4, no. 03 (2013): 1350010.

Hertig, Alyssa. “The $28-Billion Challenge: Can Ethereum Scale to Meet Demand?” 2017. Accessed June 30, 2017. https://www.coindesk.com/28-billion-challenge-can-ethereum-scale-meet-demand/.

International Carbon Action Partnership. “Canada - Québec Cap-and-Trade System.” Accessed 2017-11-12. https://icapcarbonaction.com/en/?option=com_etsmap&task=export&format=pdf&layout=list&systems[]=73.

———. “China - Guangdong pilot system.” Accessed 2017-11-12. https://icapcarbonaction.com/en/?option=com_etsmap&task=export&format=pdf&layout=list&systems[]=73.

Investopedia.com. "Hard Fork." 2017. Accessed 2017-11-15. https://www.investopedia.com/terms/h/hard-fork.asp.

Johnson, Terrell. "California Isn't Alone: Historic Droughts Happening Around The World." 2015. Accessed July 28, 2015. https://weather.com/science/environment/news/california-historic-drought-world-brazil-africa-korea.

Jung, Alexander. "The EU's Emissions Trading System Isn't Working." Translated by Ella Ornstein. 2012. Accessed February 15, 2012. http://www.spiegel.de/international/business/hot-air-the-eu-s-emissions-trading-system-isn-t-working-a-815225.html.

Kiayias, Aggelos, Alexander Russell, Bernardo David, and Roman Oliynykov. "Ouroboros: A provably secure proof-of-stake blockchain protocol." In *Annual International Cryptology Conference*, 357–388. Springer, 2017.

Leonard, John. "Cryptocurrency Miners Are Hiring Boeing 747s to Deliver GPUs." 2017. Accessed July 31, 2017. https://www.theinquirer.net/inquirer/news/3014813/cryptocurrency-miners-are-hiring-boeing-747s-to-deliver-gpus.

Mann, Michael E., Thomas C. Peterson Peterson, and Susan Joy Hassol. "What We Know About the Climate Change-Hurricane Connection." 2017. Accessed September 8, 2017. https://blogs.scientificamerican.com/observations/what-we-know-about-the-climate-change-hurricane-connection/.

Miller, Hugo. "Welcome to Crypto Valley." 2017. Accessed November 10, 2017. https://www.bloomberg.com/news/articles/2017-10-10/welcome-to-crypto-valley.

Murai, Shusuke. "GPS 'Spoofing' is No Joke: Dangers of GPS Data Hacking Realized." 2017. Accessed November 28, 2016. http://www.govtech.com/security/GPS-Spoofing-is-No-Joke-Dangers-of-GPS-Data-Hacking-Realized.html.

Nakamoto, Satoshi. *Bitcoin: A peer-to-peer electronic cash system*, 2008.

Pilkington, Marc. "11 Blockchain technology: principles and applications." *Research handbook on digital transformations*, 2016, 225.

Popov, Serguei. "The tangle." *IOTA*, 2016.

Silverstein, Ken. "China Launches a Cap-and-Trade Program to Cut Carbon Emissions." 2017. Accessed December 23, 2017. https://www.environmentalleader.com/2017/12/china-launches-cap-trade-program-cut-carbon-emissions/.

Smith, Adam, and John Ramsay McCulloch. *An Inquiry into the Nature and Causes of the Wealth of Nations.* A. / C. Black / W. Tait, 1838.

Statute, US Federal. *31 C.F.R. § 1010.100(ff)(5)(ii)(F).*

Stavins, Robert N. "Experience With Market-Based Environmental Policy Instruments." *Handbook of environmental economics* 1 (2003): 355–435.

The EU Emissions Trading System (EU ETS). "Use of International Credits." Accessed 2017-11-15. https://ec.europa.eu/clima/policies/ets_en.

The Fiji Times ONLINE. "5 Islands Disappear." 2017. Accessed 2017-11-12. http://www.fijitimes.com/story.aspx?id=353017.

United Nations Development Programme. "Clean Development Mechanism, a User's Guide." 2003. http://www.undp.org/content/undp/en/home/librarypage/environment-energy/climate_change/mitigation/undp_cdm_manual.html.

United Nations Framework Convention for Climate Change. "Kyoto Protocol." Accessed 2017-11-17. http://unfccc.int/kyoto_protocol/items/2830.php.

———. "Registry Functions." Accessed 2017-11-16. http://unfccc.int/kyoto_protocol/registry_systems/registry_functions/items/4066.php.

United Nations Framework Convention for Climate Change (UNFCCC) Clean Development Mechanism (CDM). "CDM accreditation standard." Accessed 2017-11-10.

United Nations Framework Convention for Climate Change (UNFCCC) Clean Development Mechanism (CDM). "Propose a new methodology." Accessed 2017-11-14.

United Nations Framework Convention on Climate Change (UNFCCC) Clean Development Mechanism (CDM). "CDM Methodology Booklet." 2016. https://cdm.unfccc.int/methodologies/documentation/1611/CDM-Methodology-Booklet_fullversion.pdf.

U.S. Securities and Exchange Commision. "Investor Bulletin: Initial Coin Offerings." 2017-06-25. https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings.

Vermeulen, Jan. "Bitcoin and Ethereum vs Visa and PayPal - Transactions per second." 2017. Accessed November 10, 2017. https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html.

Wikipedia. "Byzantine Fault Tolerance." Accessed 2017-11-07. https://en.wikipedia.org/wiki/Byzantine_fault_tolerance.

———. "Dodge v. Ford Motor Co." Accessed 2017-11-07. https://en.wikipedia.org/wiki/Dodge_v._Ford_Motor_Co..

World Bank. "Carbon Pricing Dashboard, 2016." Accessed 2017-11-10.

———. *State and trends of carbon pricing 2015.* World Bank Publications, 2015.

Zurrer, Ryan. "Carbon Token Ecosystem - White Paper." Accessed November 8, 2017. https://docs.google.com/document/d/1fNxBRcdYR7Ug5y208K-VPDhDk_IHjm8Sli3It8JduDI/edit.

Zwick, Steve. "Building on Paris, Countries Assemble The Carbon Markets Of Tomorrow." 2016. Accessed November 9, 2017. http://www.ecosystemmarketplace.com/articles/building-on-paris-countries-assemble-the-carbon-markets-of-tomorrow/.