CYPRUS COIN (XCY)
WHITE PAPER v. 1.0

@CyprusCoin + Team[1]

Abstract: This White Paper presents the case and plan for *CyprusCoin* (XCY), a fork of TurtleCoin (TRTL). XCY was launched on October 17, 2018 and is proof-of-work minable on Cryptonight v1. CyprusCoin is unique because it embeds CryptoNote's best-in-class privacy technology with the innovations and several network externality benefits from ongoing innovation from the TurtleCoin project. The name Cyprus represents the project's ambitions in the market by providing an untraceable coin product that specifically *offshore* investors globally. The White Paper describes the meaning of offshore in the context of the project, raises a question for community comment about governance of the 2% premine, and presents a vision for the community. Additionally, the White Paper explains the rationale for a rapid emission rate that will lead to 99% of coins being mined within four years of launch. We intend to seek input from the community on the best path to long-term blockchain viability with a four-year PoW cycle.

[1] This White Paper has no single author, and no contributing author wishes attribution. This was a "collabo-written" project that included the CyprusCoin founder, several CyprusCoin team members and was shared for discussion on Discord.

TABLE OF CONTENTS

1. Introduction

CyprusCoin (XCY) is a fork of TurtleCoin and is built on CryptoNote. The project is a fast-emission project aimed at distributing the coins quickly so that users can enjoy the benefits of this implementation of CryptoNote. We stand on the shoulders of many giants before us from these projects. Our code is 100% open source and CyprusCoin will give back to these efforts via open-source repositories. In our white paper, we describe the technical characteristics of our project and the rationale for our decision. We love the technology and are impressed at how the TurtleCoin innovation platform alone has enabled anyone to make a fork of their coin in one hour.[2] This is a point of pride, not shame, because our expertise is not in developing new algorithms: instead, it's implementing a now established best-in-class technology and executing in a unique way.

Although CyprusCoin is deploying a best-in-class privacy coin, the project's differentiator will be in the appreciation for the complex policy and business context we work in. We want to build a system that's optimized for offshore transactions. We'll describe in our white paper of what this means generally, and we invite you to join us as a community member to co-build and bring the vision alive in an interdisciplinary way. We're looking for developers, coders, marketers, lawyers, accountants, money transmitters and everyone that has expertise in this field to join us. We're undertaking a bold proposition to build a community of experts in this field in an anonymous way.

2. Founder vision

The founder of CyprusCoin wants to fix a problem in real life related to offshore money transfers. Although there are a number of large, secure, anonymous financial transaction platforms (e.g., Monero, ZCash), these projects are built to thrive within a 100% crypto world. That's not the world we're in, we're in a fiat world with just a few very, very early adopters. It's up to us to help the suits, stiff necks in NYC understand it—and to help unsophisticated users actually use it. A lot of coins say and want that, the "coin for people." Of course, we share that same vision with thousands of others in the Blockchain. For our professional and personal use, however, we're unsatisfied with progress can from incumbents for one specific piece: enabling use of crypto, anonymously (if they wish), in a fiat world.

2.1 The chasm and the trough

We launched CyprusCoin on October 17, 2018 right as Bitcoin had begun to suffer serious relative declines down to the $4k range as of this writing. Everyone seems confused about why the market has fallen. Instead, we are both relieved and reassured in our belief that there are still real gaps to fix, real problems to address in order to get to the point where regular people (e.g., unsophisticated users in remote locations, perhaps Siberia or Haiti or Malta) can use crypto in a cheap easy way. First, the basic strategic theory as to where we are in this cycle, which we believe fits very well into author's Geoffrey Moore's construct for technology adoption.[3]

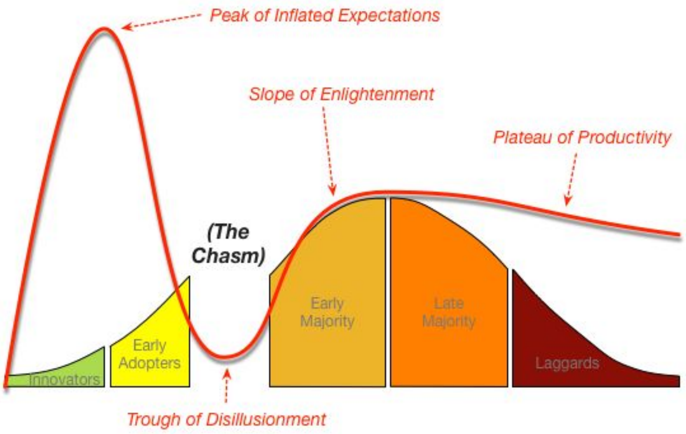

Fig 1. Geoffrey Moore's "chasm" construct can be applied to any tech industry

We believe that the Chasm for us to cross in crypto is the inability to connect crypto and fiat in a meaningful way for users. CyprusCoin's idea was born on a meeting in Cyprus where several businessmen and offshore finance advisers were discussing safe management of investment funds, and the need to make remittance payments to family members without the complexity of banking institutions. It's not just coders involved in a project like this: we're

[2] TurtleCoin, "Altcoin 101 — Create a Cryptonote Privacy Coin Clone in One Hour," *Medium,* Jul 9, 2018 available at https://medium.com/@turtlecoin/altcoin-101-create-a-cryptonote-privacy-coin-clone-in-one-hour-f14bff7eb2fd

[3] *See* West Stringfellow, Chrossing the Chasm Summary and Review, *Medium,* Jan 4, 2018, available at https://medium.com/west-stringfellow/crossing-the-chasm-summary-and-review-9cfafdac9180

parties sitting on different sides of what Geoffrey Moore calls the "chasm." Those of us that code, develop and are using blockchain are all "early adopters," on the left side. We're in a bubble. In order for our industry to climb out of the trough of disillusionment it has to find a way to get the early adopters *outside* our bubble; or to bring our efforts across to the other side. The chasm won't connect itself. It's up to the miners, innovators, creators to bridge the gap to the Early Majority, to bring them to our side. Similarly, our community needs to become more interdisciplinary and think about this as solely a technical problem, and we're going to have to build some temporary technical/human interfaces.

2.2 Our test case

Cyprus is a very popular offshore investment destination and it has already provided a forum for blockchain experts, businesspeople and others to confer about how to build an ecosystem that accommodates crypto, fiat, offshore, but take it one step further: do it as a community project rather than a top-down initiative. We've named the project CyprusCoin in tribute to the opportunity that our meetings in Cyprus brought to use the project. The coin and project are by no means limited to Cyprus. It is, however, one of the first markets where we wish to test.

2.3 What is an "offshore" focus

CyprusCoin focuses on offshore interests—so what does this mean? First and foremost it means that CyprusCoin's team is looking at a real business need and bringing a cryptoasset to help solve it, not vice versa. It's a mission to facilitate the intersection of crypto and fiat, and to do so in key offshore markets where user anonymity can be assured. We have not yet heard of another privacy coin that has undertaken such an initiative (if such a project exists we would welcome collaboration).

In the fiat world, "offshore" refers to a bank account that's not in the jurisdiction where the person usually lives. Offshoring is a broad concept but important to understand. Increasingly, people of all wealth levels travel for work and many of us send remittances home to less fortunate family members abroad. For the people of wealth and the impoverished alike, the end goal for their transfer is not to retain a cryptoasset—it's just the opposite. Both sender and receiver of the remittances sent every day from North to South or East to West are converted into Fiat. In accounting and business ledgers worldwide, all of these are generally classified as "offshore."

In the crypto world, "offshore" has no fixed concept and in fact may be an oxymoron. After all, the minute somebody uses a cryptoasset or converts fiat to a cryptoasset they may in a technical sense be "offshoring" because there are keys, bits, bytes, blockchains, etc all over the world once the conversion is done. Still, the lack of any crypto equivalence for "offshoring" concepts in crypto is unhelpful for bridging the gap and fixing the real problems of users who work regularly with bankers, lawyers, accountants and others who still deal in fiat. Because of this, we apply the "offshore" term to our mission because it assists in bringing a concept that's familiar to fiat (offshore) and create the equivalent of legal, contractual and ideally blockchain-ified processes to translate crypto into offshore fiat needs. Our team has real needs for this product that we are co-developing, and we want to build and deliver it for their own use. On this level we hope that our users will discover a coin that is fun to mine, and that we are setting up on fairness principles—but which has a much broader, long-term use case in mind.

2.4 Rough consensus & running code

The team is comprised entirely of *unpaid* community contributors who bring their expertise in coding, marketing, e-commerce, privacy, and law and regulatory affairs. Like many crypto projects, our ages, geographic, academic qualifications and experience span the spectrum.

In earlier drafts of this paper the team provided some high-level descriptions of their academic qualifications (a commonly requested thing). Ultimately, that was scrapped. We're going to have the chance to know each other (sort of, as much as anonymous collaborators do) without the baggage of academic labels. Establishing new a way to work with each other in a meritocracy (where what you've done with us matters, not what your resume says) is not easy, but our predecessors in the Internet have been doing it at the IETF for almost 30 years. David Clarke famously declared, “We reject: kings, presidents, and voting. We believe in: rough consensus and running code."[4] There’s no need to even try and rewrite Professor Clark’s 1995 statement; it worked great in 1995 and it’s just as good for us today. Rough consensus and running code does not require KYC.

2.5 Team members anonymity—why it’s important

In this section we deviate from typical coin white paper conventions to address a policy issue that is related to CyprusCoin’s governance: a deeper explanation for why the main dev team is anonymous. Also: *no,* this is not the part where we ask you to trust us. Instead we want you to understand why anonymity of the team and project collaborators is a key for building long-term user trust.

First, we have to admit that anonymity is fleeting and may be impossible in the long run. But here’s one reason team anonymity is an aspiration worth keeping: we believe that it is important for *any* privacy coin to protect identities and details of the development team. Yes, there is a loss of trust that may occur by not having the biographies of team members posted to give a warm feeling of “experience.”

We understand and support the proposition that developer and team anonymity raises concerns with users about motivations. Yet dev anonymity should be core to any privacy coin project because of the long-term benefits to users (unless there is a fundamental change in the way U.S. jurisdiction operates; we’re not optimistic). XCY *users* want to remain anonymous. For that to occur in the long term, two things need to happen: *(i)* the technology must support anonymity and *(ii)* the coin’s organization itself should be be anonymous (as much as possible).

The first is addressed by our technology choice. We address the second point, in part, by team anonymity. This helps users because it weakens any government's ability to attach *jurisdiction* to the individual or entity that controls the coin. Although invasive government surveillance is a global problem, the U.S. authorities in particular are famous amongst strongly armed entities—even outside the United States—for obtaining information that's never even been in the United States.

For several decades (since the 1970s) the aspirations of companies all over the world to protect customers from U.S. inquiry have been thwarted by the “long arm of the law” in the United States. Questions of international jurisdictional authority make lawyers and bankers rich, and everyone else including users unhappy and angry. However, telling the U.S to “f-off” if the authorities come knocking, as many of us in the crypto world would want to won’t work. To win, we have to step up the game, not ignore it or pretend that we can just wander around it.

The US legal system’s self-declared ability to obtain information—computerized or not—located outside US borders in defiance of local laws predates the Internet. In a 1976 federal case (resolved in 1981), *United States v. Field,* the federal government wanted to take action against suspected criminals who might be importing drugs from South America to United States via Germany. Even with the core of activities occurring outside the U.S. territory, the court found jurisdiction stating that it “simply cannot approve the proposition that United States criminal investigations must be thwarted whenever there is conflict with the interest of other states.”[5]In *United States v. Bank of Nova Scotia*, an appeals court ruled (8 years later) that the US government could request information *of any kind* from a company as long as it had a subsidiary on US soil. In this particular case, a Canadian bank was forced to turn over a customer’s records because it had a branch in the US. None of the records were stored in the US, and providing the information even violated the laws of the Cayman Islands and the Bahamas, where the records were actually kept.[6]

Personal jurisdiction: it’s important to understand that if the U.S. government (or any government) is seeking data about financial information of an individual, they will subpoena the people, officers, entities and organizations involved. Even though XCY data is anonymous, unavailable to be hacked, and untraceable, the last thing that we want (as contributors to the project) is to be subpoenaed and interrogated by *any* government about the technology, about any user, etc. That’s why we need to think of anonymity at another level beyond technology. The point is that American law enforcement in particular (but other regimes as well) frequently act as bullies when it comes to getting data of private citizens. They get to the data by getting through people or institutions connected with it.

[4] Paulina Borsook, How Anarchy Works, Wired, Oct 1, 1995 available at https://www.wired.com/1995/10/ietf/

[5] *See United States v. Kenneth Charles Feld, et. al.*, 514 F.Supp 283 (E.D.N.Y. 1981)

[6] *See U.S. v. Bank of Nova Scotia*, 740 F.2d 817 (U.S.C.A. 11th Cir. 1984)

2.6 Anonymity commitment

CyprusCoin makes the following commitment to its users:

XCY will not give any personal data concerning users to any government, ever.

By forging a meaningful but anonymous, collaborative team, we're able to provide an additional layer of protection in the cat vs mouse game between governments and technology. Join our team to help make this commitment a reality.

3. Premine & governance

The premine consists of 760,000 XCY (2% of total 38MM). The purpose of the premine is to be used in development activities of the coin. Any community-based coin should be concerned with premines; if the premine is used for the development and investment on the coin, that's good for the project. The problem is that communities frequently don't believe or trust that the developers will spend coins on the project rather than on themself. We see so many developers get in fights with their community concerning trust and premines.

As we've stated at the outset, *we consider the lack of trust as a feature of the blockchain, not a bug.* But in reality, the problem to be solved with the premine is as old as kingdoms, churches, states and firms. For example, the phrase "separation of church and state," obviously, comes from the desire of the public to worship who and how they wish without having the state make the decision for them. Within a state, it's the separation of powers between the executive, judicial, and lawmaking powers (or other branches); with in a firm, it's the treasury department/CEO, the legal departmen/CEO. Ultimately, the church has the Pope or other anointed leader; the governments have their President or Prime Minister; and companies have the CEO.

We think that this structure is not something that we need to overthink, we for now, we just bring it to the blockchain: separation of church & state. Short of building a fancy automated intelligence system that can manage this for us, to our knowledge this conundrum of how to fund development of a community coin without any outside investors nor any ICO is an open challenge. It is even more complicated with a privacy coin and an anonymous development team. We took a very moderate approach by setting aside a relatively small amount (2%) nd as a premine, but we want to address the premine trust question in a novel way. Our mechanism for governance of the premine will be a combination of: *(i)* third-party control of premine keys and *(ii)* transparency on expenses (transactions involving the premine); and *(iii)* compliance with rules. This is not a task that can easily be done without the aid of a third party so we intend to seek assistance in this regard.

3.1 RFP for control of third-party control of premine keys

As a fundamental separation of church and state, the founder or lead developer should never hold the keys to the premine. Like any passionate leader, the founder (and team) want to be able to make management decisions and execute on them without a committee or a bureaucracy. We believe that we can solve most of this if we can trusted institution or a set of trusted humans willing to carry this task out on CyprusCoin's behalf, for a fee (which would also be transparent).

We don't know how we'll go about this yet in detail, but in 1Q19 we intend to publish a *Request for Proposals* (RFP) in our Discord channel and request submissions from the community for the management of the keys as a portion of payment from the wallet itself (e.g., management in exchange for a 10% fee). We hope that some Blockchain law firms, accounting firms, or other recognizable groups will express interest. Although the ultimate selection will remain with the founder, the process will be published on Discord and available for comment.

> ***Note:*** to our knowledge this is one of the first projects (if not <u>the</u> first project) to propose a form of separate governance for premine. We really want ideas about how best to implement this process (including the RFP) and would welcome your contribution on this front. We'll be opening a channel on Discord labeled

#TransparencyRFP and we would be grateful for your contributions (another great area where interdisciplinary support would be valuable).

3.2 Transparency & waiting period

The maintainers of the premine will be responsible for two things: verify and guarantee transparency and a 30-day waiting period. Transparency means Founder's posting on the Discord channel that we intend to spend *x* XCY on *y* Project paid to person or entity *z*. That's it. All payments processed out of the premine will be made 30 days after posting, a waiting period that will allow discussion, provide opportunity for people to flee and sell if they disagree.Being transparent is generally good governance, and that's what we aim at.

3.3 Payment instructions

The instructions to the key holder will be to release the funds only within compliance to the rules of transparency (posting plans to spend and amount) and the 30 days delay. That's it. We believe this will give visibility into premines use in a way that few (if any) coins offer. We think this process should be "blockchain-ifiable" someday but at this point we're going with human trust.

4. Choice of technology platform

What is the CyprusCoin theory concerning the choice of technology and the future roadmap? In this section of a white paper projects frequently talk about why their technology (which may not have been deployed) is the best and most promising. In our case we'll offer an explanation for why we emphatically chose not to develop any new technology and instead to tap into the TurtleCoin innovation machine. Of course, CyprusCoin will be bringing its own innovations as well but the breadth and scope of the environment is useful for newcomers to understand. The TurtleCoin project is a year old and therefore a relatively newcomer in the space, and is even new to people who have been around for a while.

4.1 Make vs. buy

First, bear with us briefly on another short theoretical detour to share the founder's thinking. It's frequently asked why we chose to implement CryptoNote rather than build something anew. The theory is frequently that CyprusCoin is just another privacy coin, etc; or that we don't have anything new to add. In fact, we agree to some extent; there are several *excellent* privacy coins out there. However, any privacy coin is a mix of technology (*e.g.,* code that protect users) using the coin's unique implementation, and its own policies. The founder of CyprusCoin is very clear on the latter, and it's in this domain(the implementation) that the project aims at gaining user confidence.

The technology is a different thing. The founder made a decision on whether to code anew ("create") a new privacy coin or use something readily available ("buy"). Any firm in the long run will make a *make vs. buy* analysis carefully and set aside their egos when products on the market are just as good, or better, than what you'd make alone.[7]

Despite all the enthusiasm for projects coded anew, it's increasingly becoming a no brainer for any new crypto project to "buy" rather than "create."[8] Why? Because almost all the code in the cryptocurrency space is open sourced, shared on Github, constantly improved and developed by others, so to "buy" actually just requires an investment of resources, not money. If a cryptocurrency wants to abandon the members of the community and start something new, it has to staff up with resources and a plan to build a project that may not be launched for some time (it can take a year or longer to code something anew, recruit the dev team test for vulnerabilities, and launch).

In order to take that on, we would be convinced that either there is a major defect in current privacy coins or that our new innovation would effectively replace the functionality of other technologies. We don't see one or the other as a problem currently. While we may be able to build a technology stack that's more effective than the currently

[7] *See* Michael J. Leiblein, *et. al,* "Do make or buy decisions matter? The infuence of organizational governance on technological performance," *Strategic Management Journal,* Jul 2, 2002 avilable at https://doi.org/10.1002/smj.259

[8] *See* Michael J. Leiblein, *et. al,* "Do make or buy decisions matter? The infuence of organizational governance on technological performance," *Strategic Management Journal,* Jul 2, 2002 avilable at https://doi.org/10.1002/smj.259 (for an overview of the "make vs buy" decision and implications.

available products, we think the better proposition is to "buy" the existing (free) technology, and then invest our "create" efforts in a solid implementation of it coupled with an interdisciplinary approach to secure adoption, usability and long-term anonymity.

4.2 More on TurtleCoin fork decision

As stated above, CyprusCoin is a TurtleCoin fork but gets the coreof the code from CryptoNote (TurtleCoin was forked from Bytecoin which was already an implementation of CryptoNote). Many people haven't had a chance to realize that within the same year that TurtleCoin was launched it has quickly risen to become one of the most innovative, productive projects in the space. TurtleCoin's now prominent place in the Top 100 as a source of innovation was a major part of CyprusCoin's create vs. buy decision.

CyprusCoin will benefit from several innovations that come from TurtleCoin and we also intend to return code to the repositories. For non-engineers, one might think of TurtleCoin, by analogy, as filling a similar innovation-expert-export role as Xerox Parc, Bell Labs or Sun Microsystems did for their industries by offering innovations for others to use. In similar ways TurtleCoin is, in itself, a technology incubator that develops new tools and a platform upon which specific implementations (like CyprusCoin) will be layered.

Cryptomiso.com tracks the logs of projects that check open-source code into Github and other open repositories, where TurtleCoin ranks #66 of all cryptocurrencies in its overall number of check-ins to GitHub. A check-in is essentially the deposit of new code to be shared with the community, and it's a good milestone to demonstrate execution on plan, innovation, and ability to scale.

TurtleCoin stands out among peers that are privately funded, owned or run by private companies, and that have been around for much longer. TurtleCoin is coming up fast on several brand-name projects, unlike TurtleCoin, that were funded by the private sector or by private ICO raises:

#60, Ethereum (ETH). Founded in 2013 (w/ICO to fund development)
#63, Quantum Resistant Ledger (QRL). Founded in 2016 (w/ICO to fund dev)
#65, Siacoin (SIA). Founded in 2014 (private company Nebulous, Inc. funds development)
➢ ***#66, TurtleCoin (TRTL). Founded in 2017. No premine. No ICO. No paid devs.***
#73 BitcoinCash (BCH). Founded in 2017. Premine + family ties with BTC.
#73 Zcash. Founded in 2017. (Funded by private company "Zcash Electric Coin Company")
#112 Ravencoin. Founded in 2017. (No premine but subsidized developers from Overstock)

As can be seen above, not only is TurtleCoin one of the innovation leaders among all cryptocurrencies, there is also no other community like it in terms of the innovation that's being produced. For these reasons, we believe that TurtleCoin is an ideal platform for our project and will continue to be a source of innovation (and an opportunity for us to give back) for many years to come.

4.3 CryptoNote

We chose CryptoNote technology ("CN") as the basis for XCY because CN is widely regarded as the most secure and scalable privacy code available, and because it addresses the core needs of offshore business people and XCY users. At the core of privacy issues for offshore businesspeople is traceability and linkability of transactions. XCY accomplishes this with CN technology in the following implementation.

4.4 Unlinkable transactions

XCY users have a single address, like Bitcoin, but with the addition of a one-time destination key. The combination provides the untraceability that Bitcoin cannot provide. With Bitcoin, all transactions that take place between the network's participants are public, this is one of the matters the original writers of the CryptoNote code addressed with six criteria for "ideal electronic cash" proposed by T. Okamoto and K Ohata.[9] As to untraceability, the CryptoNote authors developed technology (that CyprusCoin now uses):

> The destination of each CryptoNote output (by default) is a public key, derived from recipient's address and sender's random data. The main advantage against Bitcoin is that every destination key is unique by default (unless the sender uses the same data for each of his transactions to the same recipient). Hence, there is no such issue as "address reuse" by design and no observer can determine if any transactions were sent to a specific address or link two addresses together.[10]

The core of this constitutes the CN addressing methodology which can include payment IDs and other mechanisms to obfuscate payments.

4.5 One-time ring signatures

In addition to the use of unlinkable payment addresses, XCY offers one-time ring signatures to allow "unconditional unlinkability." This allows "mixing" transactions to occur with other public keys, making it very difficult to identify who the sender is.

4.6 Proof-of-Work plan and mining specifications

We have an emission factor of the coin set at 18 which means fast emission of our coin. This has been done to have emission process completed in a reasonable time and thereafter focus more on additional products and improvements than circulation and coin price.

4.6.1 Policy on algo changes and ASIC resistance

We are ASIC resistant and committed to miner decentralization. We're implementing a "follow the leader" policy for our core technology adoption and unless there is a compelling reason to do differently, we intend to do the same in our choice of mining algorithm. As of the time of publication, TurtleCoin is planning a fork. We'll follow those details and intend to do the same.

Recall that we have taken a somewhat different view of the role of miner: they are much more critical to a project in the early days, but can quickly turn the mentality of a project into one where the end goal is some mining objective. We want to collaborate closely and convert our mining partners into ambassadors for the use-cases for the coin; ultimately, we don't want to get lost as another mining project. Additionally, as noted below, the project is facing a mining challenge because of the quick emission and we are looking to the community to find the best solution.

4.6.2 Current coin & mining specifications

Algorithm:	CryptoNight Lite v.1
Block time:	60 seconds
Difficulty:	Retargets each block
Decimal Point:	6
Mining:	PoW, ASIC-resistant
Emission Factor:	18 (Fairly Fast Emission)
Premine:	760.000 (2%) (see governance plan below)
Total:	38 Million XCY

4.7 Plan for four-year mining cycle (i.e., XCY's open conundrum)

Our plan for a four-year total mining cycle has the advantage of getting the coins in circulation as quickly as possible so as to provide maximum opportunity for deployment and use while reducing speculation involved with

[9] Tatsuaki Okamoto and Kazuo Ohta, "Universal electronic cash" in CRYPTO, pages 324–337, 1991.
[10] Id.

different mining techniques, technologies and uses. We believe that this is the right plan in spite of the fact that there is no consensus yet among technologists or economists as to how to secure and incentivize a blockchain that does not have coins to be rewarded to PoW miners (and our emission rate will hit that point at year 4).

Our open conundrum is that there are no viable models yet for sustaining a PoW blockchain network, once there are no coins anymore to be minted. There are lots of theories and a few tests, but no model that's clearly superior to another. We don't pretend to own the magic formula for that and we've heard the concerns about investing in a project that's mined for four years with a plan (just theoretical) for a year 5. A fork may be required, and other alternatives may need to be studied, such as a Proof of Stake model. The backstop options are a transaction-fee-only based network which has been proposed in other cases.[11] Look for progress on this and an anticipated decision by the end of 2019.

5. CyprusCoin Labs

Yes! We are working on innovations. We introduce the projects here:

5.1 Offshore Plus

Via the Offshore Plus program there will be a marketplace where offshore related freelancers and sellers of various kinds can sell their goods in exchange for XCY (merchants may accept other currencies that meet certain privacy criteria). Although we'll describe this project in other materials, we want to point out that CyprusCoin is being developed as part of a non-exclusive ecosystem that we believe will add value to the privacy coin niche overall.

5.2 XCY Card

Wouldn't it be great if there were a strategic alliances to allow for consumer-based fiat cards with untraceable invoices that are settled in XCY? That's one of our key visions. We'll be testing plans, technology and working with partners starting in 1Q19.

6. Miner liquidity (exchanges)

At the early stages of a coin, before any new functionality, services or products are made available, the valuation of the project is a matter of pure speculation. With a fast-emission coin like ours, one of the most important things we can do is provide fora for liquidity for miners. A total of forty percent (40%) of the total mineable XCY will be on the market by October 18, 2019 (within one year of launch).

We recognize our role in helping to find and to provide some quality vetting of exchanges. However, we believe firmly in the principle of trust nobody and constantly verifies. That being said, we have worked very closely with each of these exchanges and we believe that they are safe and secure. We vouch for no exchange, however, and thus please do your own research or ask other Cypriots on Discord about their view.

In our view, exchanges during the first year or two of our project server primarily the users on the left side of Moore's Technology Adoption Curve (miners, enthusiasts, and probably you, if you're reading this)

6.1 Current listings

As of the publication of this White Paper, XCY is currently listed on three exchanges:

P2pb2b, https://p2pb2b.io (requires KYC for withdrawals)
FirstCryptoBank, https://fcryptobank.com
Raisex, https://raisex.io

[11] We will propose thought papers later with options.

6.2 Future exchange plans

We may add up to one more exchange by 2Q19, but we do not anticipate a push for more exchange listings until there is sufficient market demand for it. Our premine is intended for development efforts, not exchange payments (although such things are possible). In the first two years of a coin, more exchanges is not better.

7. Conclusion

We hope that you will come and join our project. Whether you join us as a miner, a user, or as an online contributor, we will welcome in the best way!

8. Real-world partners

CyprusCoin will need many real-world partners in order to succeed in its virtual mission to "cross the chasm" to legitimize, facilitate and enable real-world offshore transactions. Our mining pools our important partners to us. As always, please use them, be kind, don't trust them, don't trust anyone. On that basis we hope to be friends for a very long time:

Mining Pool 1:	https://cyprus.cncoin.cf
Mining Pool 2:	https://xcy.cnpool.vip
Mining Pool 3:	http://cnpool.cc/xcy
Mining Pool 4:	https://xcy.cnpools.space/

9. Links for more information

Website:	http://cypruscoin.club
ANN Thread:	https://bitcointalk.org/index.php?topic=5053829
Twitter:	https://twitter.com/CyprusCoin
Discord:	https://discord.gg/Qkj34PS *(main place for community interaction)*
Telegram:	https://t.me/CyprusCoin
Reddit:	https://www.reddit.com/r/CyprusCoin
YouTube:	https://www.youtube.com/channel/UCYpIEHmcEYXcugPb97v4-qQ

Github:	https://github.com/CyprusCoinClub/CyprusCoin
Zed (Win):	http://cypruscoin.club/Cyprus.zip
Paper Wallet:	https://watt3r.github.io/paper-cyprus
Web Wallet:	https://xcywallet.com

Block Explorer:	http://explorer.mycypruscoin.com

10. Frequently Asked Questions

We get lots of questions from the community and we want to keep them coming.

Q: I've read the whitepaper and the founder of XCY all throughout remains anonymous, but everything else is specifically detailed, why is that?

A: Yes, this is in fact one of the main reasons for the white paper, to capture the mission and spirit of the project in as much specifics as possible but not attach specific personalities to it. Because of your question, we have added some additional information in the body of the white paper to describe the rationale further for anonymity.

Q: If you're anonymous, why should we trust you?
A: You should not trust us-- nor should you trust any developer, any coin, any project. We are setting up CyprusCoin so that it can continue even without the lead dev; the work is in progress but watch for this.

Q: Is this a project about hiding money in Cyprus?
A: No it's not actually a project about "hiding money" at all. Providing an anonymous, untraceable unlinkable payment system providesvalue for investors but also for human rights activists, journalists and others that do not yet have (but one day will) instant access to global sources for payments.

Q: What are the qualifications of the founder?
A: The CyprusCoin founder completed a PhD in computer engineering (some time ago) and helped develop e-commerce initiatives from early growth days of online advertising and sales. The CyprusCoin founder can wear the dev hat (and did most of the work to launch the coin alone) but is more of a CEO/generalist and as mining progresses, intends to focus on usability cases. On some level the "founder" has also become a collective voice within the community.

Q: Who are the supporting developers and what are their qualifications?
A: There are several additional developers for CyprusCoin. This project is open source, the developers that are involved publish their code in the open for all to see. As this is a privacy focused coin and project the identities and thus qualifications of developers might not always be transparent. However, their code is all that really matters at the end of the day. There is a built in forcing factor to push the project forward, the project goes well, the developer goes well.

Q: The rate of 18 is fast for a coin, what will happen in four years when it's all mined?
A: In actuality in 4 years it's 99% mined, and that makes a difference because the remainder can be used as micropayments. However, yes, the coin is mostly mined within 4 years (44% in the first year). We intend to address this but we don't want to make the mistake of getting stuck into a decision that we don't need to make yet. There are several projects underway that test different options and we'll revisit this and decide by end of 2019.

Transparency & Premine

Q: How much is the premine and who has the keys?
A: Premine is 760,000 XCY (2% of total). Founder currently has the keys but will initiate process to hand them to another trusted party.

Q: Why give the keys to people if that requires trust--I thought Blockchain was trustless?
A: Agreed. There's no AI app yet but would do it if available.

Q: Why such a simple thing, why no contracts or other evidence?
A: Because we're not the government, your business, etc. We want to share high-level what we're doing but this isn't the place for contracts, deliverables, or lawyers. We'll post it, if you believe us, great, if you don't we understand.

Q: Can the community veto a choice to spend on one thing or the other?
A: No, it's not really a veto, because we want to retain the right to drive the vision. However, we're opening this up because we recognize that people have voices and opinions, so please bring them.

Q: Why the 30-day wait? Why not one day, one week, one year, etc?
A: One of the main issues with premines is the exit scam --- the founder just disappears one day and cashes out the pot. Even with a transparency on the wallet, it's possible for a founder to take the money out overnight. If the timer is set,

e.g., 30 days, then other holders who disagree with a decision to spend premine will have 30 days to liquidate their investment before the premine spend in question occurs.

Q: Do you know who will be submitting for the RFP?
A: No we do not, although we hope that some law firms, accounting firms and other real-world "trust" entities will offer services.

Q: What if no company offers services or one that nobody trusts?
A: We recognize this risk and note it's even more complicated because we're asking a company to take it on as a percentage of the coin's value, but the coin has very little value today. We'll cross that bridge if it gets there.

Q: Can we move it to AI, don't we trust computers, logic and blockchain more than people?
A: We'd love to do an AI or trustless solution of some kind but there's nothing off-the-shelf that could meaningfully be deployed, that's why we're going old school.

FAQ for Mining

Q: Is this a miner-focused coin?
A: Yes, we do care about miners -- that's one of the reasons we chose a very miner-friendly fast-emission coin. However, our long term focus is on usability and making XCY work, not mining. We think this focus is going to help bring value to the miners in ways that many "mine & speculate" coins do not. For this reason, mining interest will be strong at first but will be replaced quickly by user participation.

Q: What is Emission Factor 18?
A: It's the four-year emission plan, with the first 40% of the coins mined after Year 1. The best tutorials on the emission curve are on CryptoNote's website, at https://cryptonotestarter.org/tools.html

Q: What about the rumors about ASICs on CN lite?
A: We've decided to take a "follow the leader" approach with our technology and at this point in our development TurtleCoin is the leader. We'll do a close follow to their response to any change in the algo scene.

* * *