

WHITEPAPER

# A GUIDE TO THE PRIVATE DIGITAL CURRENCY, 'COG'

Published March 2023



**ROBERT E. FOSTER (FOUNDER)**

**PAUL WOOD (CTO)**

[www.cogfi.org](http://www.cogfi.org)

*“The whole future lies in uncertainty, live immediately”*

*- Seneca*

*N.B. We would like to thank all of our early stage investors for their support and, in advance, we would like to extend our sincere appreciation to all of our future investors/holders/supporters who join us and the rest of the COG community in order to realise and maximise the enormous potential in the Private Digital Currency space.*

# CONTENTS

- 1. INTRODUCTION**
- 2. OUR RAISON D'ÊTRE**
- 3. TECHNOLOGY & TOKENOMICS**
- 4. THREATS TO PRIVACY COINS AS A WHOLE (AND OTHER 'UNREGULATED CRYPTOCURRENCIES')**
- 5. CRYPTOCURRENCY REGULATION AND KEY LEGISLATION**
- 6. THE STORY SO FAR**
- 7. FUTURE DEVELOPMENT (AS OF CURRENT DATE; THIS PUBLISHED VERSION OF THE WHITEPAPER 1.1)**
- 8. CONCLUSION**

## INTRODUCTION

### **What's different: traditional cryptocurrencies vs privacy enabling cryptocurrencies**

When preparing this white paper, we felt it would be most advantageous to go into a level of depth sufficient to suit our intended majority audience, so to speak, rather than produce a whitepaper of hundreds of pages, much of which requiring a very advanced level of mathematical and technological understanding in order to digest; whereas the ultimate aim is really to feel sufficiently informed and, in turn, satisfied that your decision to make an investment in COG has been arrived at based upon the consideration and digestion of a sufficiently sound and broad conceptual basis as compared to any other leading cryptocurrency white paper on the open market (so to speak). To that end, we hope you find the rest of the information within this useful and hopefully join the COG community as another fellow investor and in time become an integral beneficiary of our community too.

### **The future of sending and receiving digital currency, privately and securely, is here.**

Cryptocurrencies store and display their transactions in the blockchain; serving as a publicly available visual ledger. Consequently, the level of privacy or confidentiality of such transactions is extremely low. What does this mean? Well, one problem is that it enables hackers to undertake blockchain analysis from the transaction history available on display,

identify wallets with a desirable amount of cryptocurrency within them and hack those wallets; draining them in their entirety. This particular problem is so significant in fact, that it currently is (at the time of writing) reported to be the highest revenue generating method within the cryptocurrency space!

### **What is a privacy coin? And how are they different from traditional cryptocurrencies?**

A Privacy coin, also known as a *Privacy Enabling Cryptocurrency*, is simply an enhanced version of early stage cryptocurrencies that were developed to enhance the financial privacy of individuals and businesses alike. Each privacy coin typically leverages innovative technological 'mechanisms' that provide privacy, encryption and enhanced security to its users. Examples include using stealth addresses, CT Ring signatures and Zero Knowledge Proofs to obscure the ability of a third party from identifying key information required to compromise the security of the sender or recipient and equally the amounts being transferred (beyond that of a traditional cryptocurrency that doesn't utilise this same privacy enabling technology/methods).

### **Why Privacy (as a utility)?**

Privacy as a concept beyond merely surrounding currency, but in society the world over, can be seen as critical and necessary dating back to as far as when records began. Conceptually speaking, one could argue that the mere wearing of clothing, locks on doors, curtains on windows, internal structuring of the home, religious teachings in marriage and associated boundaries all collectively illustrate the concept (amongst other parameters/ethics) of privacy always permeating society through the ages. Turning to currency, similarly, 'Hawala' is probably the earliest example of the demand for privacy present in currency that still exists today. Legislative evolution which often finds itself playing 'catch up' with technology generally (due to the mechanism of the common law by and large) also demonstrates how at Government/Regulatory level; 'Privacy' is regarded as fundamental. Accordingly, there are countless examples of legislation that has developed to preserve Privacy as technology has evolved. Commonly known examples include: Article 8 of the human Rights Act 1998 & the GDPR Legislation here in England and Wales. With mirroring legislative provision in the US as well as commonwealth jurisdictions including Canada and Australia.

To summarise the above within this subsection, it is the combination of both the clear consistent historic illustration of a societal commitment to the preservation of privacy coupled with the advancements of technology, that in this current instance and timing with the 'gap' between the rate of evolution in the cryptocurrency space and the preservation of privacy co-existing led to the existence of an 'underserved demand' for privacy.

As a result of this underserved demand for privacy in the cryptocurrency space, COG was born to ultimately service the demand by leveraging the latest technology available (rather than merely any privacy enabling technology) but also investing in regulatory and legislative developments to ensure our existence as we scale considerably upon public launch and over the coming years.

***Weren't cryptocurrencies already private though?***

***Well, no as it happens! Cryptocurrencies on the whole are rather 'Orwellian' - some being more decentralised and/or private than others...***

Thus demonstrated in 1994 when DigiCash performed the first peer-to-peer cryptographic payment over the Internet using cyberbucks.

Then circa 15 years later, 'Bitcoin' was created; the first allegedly decentralised cryptocurrency. Bitcoin also provided an extremely reduced transaction 'cost'. For example, a transaction concerning \$200 would cost circa \$0.0414 via Bitcoin vs a global average cost of \$14.00 to transact \$200 through more conventional and widely used global transactional methods such as via Western Union et al.

However, if we look closer at a cryptocurrency stable coin like Bitcoin, it actually lacks the financial privacy that traditional financial intermediaries/institutions offer. Specifically, if you were to conduct a transaction using Bitcoin, the transaction itself becomes publicly available, potentially traceable, and permanently stored on the Bitcoin network. This includes the

amount of money involved in terms of sent and received and thus held in a digital wallet given you can then analyse the transactions which that particular 'address' has undertaken. As a result of this, many hackers have been able to identify, trace, hack and drain wallets the world over generating such levels of revenue from this activity that it is one of the highest value methods, in terms of monetary value, of theft conducted online today.

The main 'value add' of a privacy enabling cryptocurrency over a 'traditional' or

perhaps better expressed 'standard' non-privacy enabling cryptocurrency is that the former allows for a higher degree of security surrounding the holding of monetary value, the sending and the receipt of cryptocurrency itself. Making your money more secure and safely protected as well as still having the capability to transact globally at high speeds at a fraction of the cost (to the sender or recipient) compared to conventional methods of monetary transfer also.

## TYPES OF PRIVACY COINS

**There are 2 main categories:**

1. 'Privacy by default coins'; and
2. 'Privacy as-an-option' coins.

### **Privacy by default coins**

These coins use privacy enabling technology/methods such as one-time addresses; preventing third parties from identifying the controller of the receiving address. Other methods also include the use of ring signatures. These made it possible to verify that someone from a particular group performed a transaction with a significantly reduced ability to identify a particular sender compared with a traditional stable coin without privacy enabling technology as described previously above.

There is a further privacy enabling technological method/tool described as 'Confidential' or 'Secret' Transactions. Collectively, by implementing the above privacy enabling methods/technology into a cryptocurrency the holders of said currency are afforded significantly greater security compared to 'non-privacy enabling' cryptocurrencies.

### **Privacy as-an-option coins**

These coins are transacted in a way that is visible on a public ledger. However, they allow for holders to benefit from an increased level of privacy in order to conduct privacy-enhanced transactions by essentially optional privacy enhancing features.

## OUR 'RAISON D'ÊTRE'

The Cryptocurrency market as a whole is still in its relative infancy but, whether the market is in its inevitable cycle of Bull or Bear, it is clear that it is continuing to grow year on year.

The demand for privacy in increasingly surveillance-esque states provides a significant opportunity for COG to meet the market demand which is on a clear exponential growth trajectory.

The privacy coin market is already sizable and in clear growth mode. Evidenced by the growth in the number of coins within this sector in recent years and also illustrated by the total market cap size and trading volume growths within this 'vertical'.

Thus, given the sustained increase in demand for privacy enabling cryptocurrency coins supported by analysis of the growth in trading volume and total market caps, there is a significant opportunity to take advantage of this demand and timing of the market for potential COG investors. We consider that many of the current privacy coins whilst

useful and many containing 'good privacy enabling technology' beyond that of traditional cryptocurrencies, still don't meet the demand of the market to anywhere near the size of the demand nor the specifics within the world of 'privacy' in terms of their application to consumer requirements and investor demand.

To conclude, we aim to offer a privacy coin that utilises privacy enabling technology to afford users with an significantly enhanced level of security and privacy over and above traditional cryptocurrencies, but also to develop DAPPs that will serve to meet the demands of consumers and retail investors alike in terms of their 'usage' of privacy enabling cryptocurrencies in their day to day life. We consider that our focus on both technology and application thereof, together with the frankly underserved demand that currently exists provides us with a significant opportunity to offer a privacy-enabling cryptocurrency that can establish itself as a leading currency within this space. **And this is our 'raison d'être'.**

## TECHNOLOGY & TOKENOMICS

### Technology currently utilised in the Privacy Coin 'space'

#### Stealth Addresses

At its core, a stealth address is simple: it is a one-time address used only for a particular transaction to ensure that the details of the parties involved in the transaction are not disclosed or revealed. Stealth addresses are a way to enhance anonymity for buyers and sellers in a transaction, and there are various ways that stealth addresses can be implemented.

One implementation creates a unique one-time address for each transaction, which makes different transactions to the same recipient unlinkable. This new address can be communicated off-chain, such as through an invoice.

Another implementation shares a key or secret between the two parties that can be used to generate new accounts for each transaction. This key or secret can be extended into a hash chain where each round creates the subsequent public-private key pair, but this comes with the drawback that both parties then have the private key and can spend the tokens.

Solutions on-chain for stealth address hashing can include modifying the public-private key generation process, reusing a public key or signature nonce,

and requiring the seller's address to have a specific prefix.

#### Ring Signatures

First proposed by Ronald Rivest, Adi Shamir, and Yael Tauman in 2001 in their seminal paper, ring signatures have since become an integral part of the cryptocurrency and blockchain space.

In a ring signature, a group of entities each possess their own public/private key pairs. When a member of the group wants to sign a message, they use their own secret key, but the public keys of the other group members. This way, the validity of the group can be verified through its public key, but it's not possible to determine the specific member who signed the message without knowledge of the private keys within the group.

For example, let's say *Rob*, *Maji*, *Dominic*, and *Paul* are in a group, and each have their own public and secret keys. When *Maji* wants to sign a message on behalf of the group, he generates a random value, then uses his own secret key to encrypt each of the random values for the other participants. The message is then encrypted with a symmetric key derived from a hash of the message.

*Maji* then computes the ring signature by applying an encryption function to the random values for each participant. The resulting signature can be verified by checking that the computed ring matches the sent signature.

The process of creating a ring signature involves:

- *Generating encryption with  $k = \text{Hash}(\text{message})$ .*
- *Generating a random value ( $u$ ).*
- *Encrypting  $u$  to get  $v = Ek(u)$ .*
- *For each group member (excluding the signer), calculating  $e = si^{pi} \pmod{Ni}$  and XORing it with  $v$ .*
- *Calculating the signature ( $v = Ek(u)$ ) for the signing party which completes the ring.*

Ring signatures provide a high level of privacy and security for group transactions in the cryptocurrency and blockchain space. By utilising this technology, investors can protect their information and ensure the authenticity of their transactions without revealing their identity.

### Zero Knowledge Proofs

Zero-knowledge proofs are a game-changing innovation in the world of cryptocurrency and blockchain technology. With zero-knowledge proofs, investors can rest assured that their information is secure while they prove the validity of their statements.

At the core of zero-knowledge proofs is the concept of proving a statement's validity without revealing the statement itself. The party proving the claim, known as the "prover," shares information with another party known as a "verifier," who is responsible for ensuring the validity of the claim.

First introduced in 1985 in the paper "*The knowledge complexity of interactive proof systems*", zero-knowledge proofs have since become a widely recognized and trusted method for securely sharing information without revealing its contents.

With zero-knowledge proofs, one party can prove the truth of a statement to

another party, without revealing any information beyond the fact that the statement is indeed true. This powerful tool has seen continual improvement and is now being used in a variety of real-world applications, solidifying its place as a crucial component of the cryptocurrency and blockchain landscape.

### ZK-SNARKs

ZK-SNARK stands for *Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*, and it is one of the leading forms of Zero Knowledge Proofs used in cutting-edge blockchain technology. It has the following properties:

- *Zero-knowledge:* The verifier can check the validity of a statement without learning any additional information about it, apart from whether it's true or false.
- *Succinct:* The zero-knowledge proof is smaller than the secret information being proven, and can be verified quickly.
- *Non-interactive:* Unlike interactive proofs, the proof process only involves a single interaction between the prover and verifier.
- *Argument:* The proof meets the "soundness" requirement, making cheating highly unlikely.
- *(Of) Knowledge:* The zero-knowledge proof can only be constructed with access to the secret information (witness), and it is difficult or impossible for a prover without the witness to create a valid proof.

This method of Zero Knowledge Proof requires users to trust the participants involved in the generation of parameters, but it also enables the creation of proving protocols that can function without a fully trusted setup.

### **Crypto Mixers**

A crypto mixer is a service that mixes the cryptocurrencies of various users to conceal their source and ownership. This provides a level of privacy that is otherwise difficult to achieve in transparent public blockchains such as *Bitcoin* and EVM-compatible blockchains such as *Ethereum*, *Polygon*, *BNB Chain*, *Avalanche*, *Fantom* and more.

### **How a Crypto Mixer works**

A crypto mixer pools and shuffles the cryptocurrencies deposited by multiple users, and then transfers the funds to new addresses under each user's control, after deducting a small fee. To increase privacy, some mixers schedule withdrawals in random amounts and intervals, while others attempt to hide the fact that a mixer is even being used by adjusting transaction fees and withdrawal address types.

### **Types of Mixers**

There are mainly three categories of crypto mixers: Centralised Custodial Mixers,

CoinJoins, and Smart Contract Mixers.

*Centralised Custodial Mixers:* These early mixers, established as early as 2011, temporarily take control of users' funds and are operated by a single entity. They pose additional privacy risks and are often targeted by law enforcement agencies as unregistered money services businesses.

*CoinJoins:* This type of mixer is integrated into privacy wallets and combines users' coins in a single transaction with those of other users. CoinJoins are non-custodial, meaning they never hold users' funds.

*Smart Contract Mixers:* These mixers are also non-custodial but work differently from CoinJoins as the functionality of the mixer is hosted in a smart contract on a compatible blockchain, usually EVM-compatible blockchains such as Ethereum, Polygon, BNB Chain, Avalanche and so on. On supported chains, the user sends their funds to an on-chain smart contract which functions as a mixer. In return, the user receives a cryptographic note as proof of deposit. They can then withdraw the funds to a new address at any time by sending the note to the mixer, where the cryptocurrencies are shuffled. Smart contract mixers often collaborate with service providers known as 'relayers' to pay the gas fees on mixer withdrawal transactions, ensuring the user can withdraw their funds with no transaction history or connections to other services.

## **THREATS TO CRYPTOCURRENCY, PRIVACY COINS AS A WHOLE AND OTHER 'UNREGULATED CRYPTOCURRENCIES'**

Ultimately, whatever the business it is important to explore not only 'Strengths and Weaknesses', 'Opportunities' but crucially also 'Threats'. This enables us to maximise the opportunities ahead and also ensure that the growth of COG is not only maximised but also crucially 'sustained'.

As demonstrated by the Tokenomics of COG in terms of the Total Supply and the release of additional coins over the next 4 years (together with our commitment and investment in legal expertise/advice surrounding regulation coming into the cryptocurrency sector as a whole); the COG project has a clear long term 'purpose' and is clearly distinct from the vast array of 'altcoins' many of which are widely documented as being scams via 'rug pulls' and such like.

The two main 'threats' are simply:

1. Regulation within the cryptocurrency sector as a whole; and
2. Increasing competition within the Privacy Coin sector space.

We have invested heavily in our analysis of existing competitors within this space during our development and have also invested considerably in seeking legal expertise/advice from leading specialist lawyers within both the cryptocurrency space but crucially additionally, within the financial regulatory sector as a whole. From the outset. Furthermore, this will remain an integral focus at the heart of the project over the coming years to ensure the sustainability of the coin and enabling us to maximise the success of the COG project for our investors too.

To conclude, whilst the cryptocurrency sector will experience increased regulatory impact over the coming years (which will inevitably also apply to privacy coins) the reality is it will serve to provide clear opportunities for those 'projects' (coins) that remain at the forefront of any regulations and also will provide for increased confidence in the cryptocurrency space for investors as 'scam coins' and other unscrupulous projects will find it increasingly difficult to 'exist'. This will in turn sustain the continued rapid growth of the sector as a whole however it is nevertheless important to ensure that we continually keep on top of any regulatory obligations so as to protect and preserve our success.

## CRYPTOCURRENCY REGULATION AND KEY LEGISLATION

Along with technology, this is a key focal point for COG. It is absolutely no secret that Regulation at Governmental and Legislative level is a case of when and not if in the cryptocurrency space. More accurately, it has actually been in existence for years already; simply laws surrounding Fraud, Anti-Money laundering regulatory obligations and FCA (or jurisdictional equivalent) obligations already govern this space. We've all seen the impact of this taking place in respect of numerous sentencing of 'rug pull' misdemeanours the world over, also litigious ongoing examples at the time of writing include the SEC v XRP case illustrating the application of the HOWEY Test and we're currently (again at the time of writing) witnessing the unfolding of the SBF litigation which will likely set an array of precedents within this space.

What we are seeing without doubt, is that legislative provisions, regulations and commentary direct from governments and Regulators are clearly indicating that cryptocurrency is here to stay as is privacy. Simply, for all the right reasons, it is a case of getting rid of the scams, guarding against future scams, money laundering wt al. Which is the focus rather than outright universal banning of an entirety of currency simply because it utilises cryptographic technology.

This extends to privacy enabling technology too which whilst the laws and regulations in this space are still embryonic in nature at the time of writing the general consensus is promising to say the least. Providing currencies operate within the

legislative provisions/frameworks of those referred to above.

We have included a summary of some of the additional legislative provisions relevant below. Please note this is a fast evolving 'space' currently either ongoing litigation and the development and implementation of Government led regulation. Thus, this section is merely a commentary and is only in relation to the information available at the time of writing in respect of the English and Welsh jurisdiction. Please thus bear this in mind if you are resident outside of this jurisdiction when digesting the contents of this whitepaper. The focus of which is to provide a summary of our privacy enabling cryptocurrency: COG in its entirety. Not, to be treated as a comprehensive summary of privacy and cryptographic law.

Accordingly, two key examples of privacy preserving legislation below:

1. Human Rights Act 1998 - the right to private life
2. GDPR legislation

### **On the horizon:**

Even some of the publicly available rhetoric from government and regulatory level discussions (in the UK and beyond) to date surrounding the above have proven to illustrate the recognition/acknowledgement of privacy as a vital concept in currency. Specifically, Governmental discussions here in

the UK have revealed their plans within CBDC's to retain/incorporate a privacy capability up to a certain limit for transactions and spending. Seemingly on an 'opt-in' basis. Notwithstanding the aforementioned, there is a clear unequivocal indication at both the legislative level universally and specifically to currency itself that 'privacy' as a concept is valued immensely highly and accordingly is sought to be preserved constitutionally across a number of significantly influential economies. This is directly relevant to 'COG' as we continue to invest and keep a close eye on the legislation and regulatory obligations that evolve and become incorporated over the

coming years. Clearly, privacy as a concept whilst desired evidently as far back as the 8th century (Hawala) is still to the current day regarded at Government level as a key part of society that is here to stay; and within currency itself.

Rishi Sunak, at the time of writing the UK Prime Minister, has expressed a desire to make the UK a leading global crypto hub which has been widely documented. Accordingly, there has been a clear illustrative example of awareness at government level of the distinction between scams and legitimate cryptocurrency and digital currency (such as CBDC's).

## THE STORY SO FAR

### COG initial launch on Polygon

The COG ecosystem will start with the launch of the COG token as a store of value currency on the Polygon blockchain. Launching on Polygon provides a number of advantages including:

- The ability to leverage a trusted and reliable blockchain;
- Incredibly low gas fees; and
- A user base that is already well aligned with many of the ambitions shared by the COG team.

These factors are just a few reasons for why the Polygon blockchain is the ideal starting point for the COG token. In addition to the above, by launching the COG token on the Polygon blockchain initially, the COG ecosystem will be able to capitalise on:

- Polygon's existing user base;
- Network effects; and
- Market liquidity.

This gives COG instant market reach on launch, and will provide a stable and trusted foundation for the COG token to provide value and growth to its early adopters, while making the onboarding process for users familiar with

EVM-compatible chains and DeFi simple and practical.

Looking forward, for COG to truly realise its vision of providing privacy on the blockchain, its goals extend further than the COG token and its native dApps on Polygon. The eventual launch of COGchain as a standalone blockchain will bring a new level of private technological advancement to the COG ecosystem. COGchain will be built from the ground up with privacy-enabling and privacy-enhancing features and protocols integrated into its structure and code, delivering an unprecedented level of privacy and security. COGmail, COG Gaming and COGsino will be rewritten and upgraded for the launch of COGchain, leveraging features built into COGchain that are otherwise impossible or impractical on EVM-compatible chains. When COGchain launches, COG's existing users will benefit from easy, fast, and private bridging of their COG tokens from the Polygon blockchain to COGchain.

By initially focusing on creating a secure and stable store of value for the token, the COG team can establish a solid base for further developments in the ecosystem, such as private sending of COG, COGmail, COG Gaming, and

COGsino, all of which will be developed to run natively on Polygon before the move to COGchain. This phased approach allows the team to carefully consider, architect and implement the

privacy-enhancing and privacy-enabling features that are integral to the success of the COG ecosystem, with guidance and input from the COG community as it emerges.

## FUTURE DEVELOPMENT

(AS OF CURRENT DATE; THIS PUBLISHED VERSION OF THE WHITEPAPER 1.1)

### Development of key dApps on COG to address the rapidly growing demand surrounding the 'use' of privacy-enabling cryptocurrency:

#### **COGsend: Anonymous 'sending and receiving' of cryptocurrency.**

Through COGsend, users have the ability to send and receive cryptocurrencies anonymously through the use of COG's proprietary smart contracts, with a small fee paid in COG to facilitate the maintenance and ongoing development of the service. COG's proprietary technology allows for the obfuscation of transaction origins and destinations, providing users with a high level of privacy and security when conducting cryptocurrency transactions. COGsend employs a unique combination of EVM-compatible smart contract technology, zero-knowledge proofs, cryptographic notes and randomised transaction scheduling to make it incredibly difficult for any interested party to trace the movement of funds. This makes COGsend an ideal choice for individuals and organisations who prioritise confidentiality and privacy in their financial transactions. The eventual launch of COGchain will offer additional security to COGsend, with features built natively into COGchain that would be

otherwise impossible or impractical on EVM-compatible chains.

#### **COGpay: Anonymous and secure spending of cryptocurrency**

COGpay is a digital card service that prioritises privacy and security. The COGpay digital card enables users to make purchases online or in physical stores while keeping their identity and spending activities private and obscured. The digital card is topped up with funds via COGsend and integrates with the COG privacy-focused ecosystem, allowing users to make transactions with confidence that the source of the funds will remain confidential.

The COGpay digital card will provide a high level of security, with features such as two-factor authentication and SMS notifications for transactions. In addition, the card will have no physical form, eliminating the risk of loss or theft. The user's COG funds will be held in a secure, decentralised wallet, protected by state-of-the-art encryption.

Overall, COGpay is an innovative solution for privacy-conscious individuals who want to spend their COG anonymously and securely. By integrating

with the COG ecosystem, it provides a seamless and secure payment solution that can be used with confidence.

### **COGsino: A Privacy-Focused Blockchain-Based Casino**

Introducing COGsino, a new blockchain-based casino that promises to provide players with maximum privacy and security for their funds. As part of the COG ecosystem, which utilises the fast and secure Polygon blockchain, COGsino leverages the latest privacy technologies to hide the origin of player funds, ensuring total confidentiality for all transactions.

COGsino will operate on the Polygon blockchain, which allows for fast and secure transactions. When a player deposits funds from their crypto wallet into their COGsino account, the journey those funds take is obscured using advanced zero-knowledge proof technology, which enables COGsino to validate the integrity of these transactions without knowing any other information about it. This results in a high level of privacy, as the only knowledge that COGsino has of the transaction is whether it is true or false, and the funds themselves are moved in a way that is difficult to trace.

COGsino's privacy-focused approach sets it apart from other online casinos, on-chain and off-chain alike, which lack the security measures necessary to protect the privacy of their players. With COGsino, players can enjoy the

excitement of online gambling in a secure and private manner.

The casino games offered by COGsino will include popular favourites such as blackjack, roulette, and baccarat. Additionally, COGsino will offer a variety of slot machine games, including classic slots, video slots, and progressive jackpot slots. For players who enjoy the thrill of poker, COGsino will offer a variety of poker games including Texas Hold'em, Omaha, and Seven-Card Stud. The casino will also offer games such as craps and sic bo, which are popular among players who enjoy dice-based games.

COGsino will also offer live games, allowing players to experience the excitement of a real-life casino from the comfort of their own home. With live dealers, players can interact with real dealers and enjoy games such as blackjack, roulette, and baccarat in real-time.

In addition to standard casino games, COGsino will also offer sports betting and virtual sports betting, allowing players to place bets on their favourite sports teams and events in a safe, secure and private way, made possible only by COGsino and the COG ecosystem.

With a wide range of games, COGsino is sure to have something for everyone, whether you're a seasoned gambler or a casual player. The use of cutting-edge privacy technologies, combined with the fast and efficient Polygon blockchain, will ensure that players have a secure and enjoyable gaming experience at COGsino.

## COG Gaming

COG Gaming will be a blockchain-based gaming service that aims to provide a secure and private gaming experience for players. As part of the COG ecosystem, which uses the Polygon blockchain, COG Gaming leverages the latest privacy technologies to hide the origin of the player's funds, ensuring that their transactions are protected from prying eyes.

The games offered by COG Gaming are designed to be simple, addictive, and entertaining, with a focus on fun high score games in the vein of popular Flash and mobile games. Players can expect to find games such as puzzle games, arcade games, and casual games that can be played quickly and easily.

One of the key features of COG Gaming is the potential for players to win prizes in popular cryptocurrencies, including the COG token, Polygon, and USDC. This adds an extra layer of excitement and motivation for players, as they compete for real-world rewards in addition to high scores and bragging rights.

Whether you're looking for a quick distraction during your break or a more in-depth gaming experience, COG Gaming has something for everyone. With its focus on privacy and blockchain technology, it offers a secure and transparent platform for gaming and rewards.

## COGmail - Senderless Messaging by COG

COGmail is a secure messaging platform within the COG ecosystem that leverages the power of zero knowledge proofs on the Polygon blockchain to enable users to send messages and data anonymously. This ensures that the sender's identity remains private and untraceable, making it a perfect solution for users who require the highest level of privacy in their communications, while also leveraging blockchain technology to ensure the authenticity of said communications.

Senderless messaging via COGmail has many important and valuable use cases, including:

- **Whistleblowers:** People who have sensitive information to share, but are concerned about retaliation, can use COGmail to communicate with journalists, human rights organisations, or government agencies, while keeping their identity hidden.
- **Activists and protesters:** In countries where speaking out against the government or participating in demonstrations is met with severe consequences, COGmail allows individuals to share information about their activities and movements without fear of being identified and persecuted.
- **Business professionals:** In industries where the protection of

- confidential information is critical, COGmail provides a secure and private channel for employees to communicate with each other, share sensitive data, and collaborate on projects.
- Healthcare providers: Healthcare providers who handle sensitive patient information can use COGmail to communicate with their colleagues, share health records, and exchange ideas without risking the exposure of their patients' data.

These are just a few examples of the many situations where COGmail can provide a crucial layer of protection and privacy for its users. Whether it's for personal, professional, or political reasons, COGmail is a powerful tool that gives its users the ability to communicate freely and securely.

## **COGchain - The Private Blockchain by COG**

COGchain is a necessary step in the COG ecosystem's journey towards creating a privacy-focused blockchain for its users, and this is where COG's efforts are leading towards in its roadmap. As a standalone blockchain, users on COGchain will benefit from native privacy-enabling and privacy-enhancing features, built directly into COGchain's code, to give users greater control over the disclosure of their data and transactions.

The transition from a token on the Polygon blockchain to its own standalone blockchain will bring about significant improvements to privacy and security for users. COGchain will allow users to carry out secure and private transactions, with the added benefit of fast and efficient processing times. Privacy is not native to any EVM-compatible blockchain - COGchain will address that by creating a blockchain with network and security protocols that put privacy first. COG users on Polygon will be able to bridge their tokens from Polygon to

COGchain quickly, and of course, privately. All dApps created in the COG Polygon ecosystem will be ported to COGchain over time, with most COG dApps on COGchain requiring less code than their Polygon equivalent as the privacy technologies required will be available natively on-chain and can be safely referenced instead of being included in now-redundant smart contract code.

As a privacy-focused blockchain, COGchain has the potential to be used in a variety of industries where privacy and security are of utmost importance, such as finance, healthcare, and even political activism. The ability to send and receive information and funds without having to reveal one's identity could be life-saving in some cases, such as in regions with oppressive regimes or where political activists face persecution.

COGchain's launch as a standalone blockchain is an important step towards creating a more private and secure online world for its users, and the COG ecosystem's commitment to privacy is reflected in this exciting development.

## CONCLUSION

It is well documented that irrespective of the markets being in their inevitable Bull or Bear cycles; the market of cryptocurrency as a whole is growing rapidly year on year. Specifically, the privacy market within the cryptocurrency sector is growing rapidly and is still at a very early stage as far as the potential growth is concerned.

To illustrate, the market cap of the Privacy coin sector is \$4.8B representing 0.48% of the total cryptocurrency market cap. The Privacy Coins Sector saw \$485.3M in trading volume over the last 24 hours. Privacy coins utilise cryptographic technologies to protect the privacy of their users. Thus providing a mechanism to enable users of cryptocurrency to truly return to the heart of one of the original purposes and significant advantages of cryptocurrency.

COG will thus offer an opportunity for investors (at the time of writing) to be involved at an early stage in a project which has 'privacy' enabling technology development at its very core and to join a rapidly growing community

that will afford investors with unrivalled transparency and insight within our journey; not seen by the majority of many crypto projects. Our additional commitment and investment into seeking continual legal expertise from specialist leading lawyers in the cryptocurrency and financial regulatory 'arena' will also provide investors with peace of mind as we grow whilst embracing the regulatory impacts that other cryptocurrencies will undoubtedly overlook. Thus providing sustainability and protection in our ability to continue to operate in a market that for good reason is going to become exposed to increasing regulation in the coming years.

What is certain is, the use of digital currency is increasing rapidly the world over, the demand for privacy in an increasing 'surveillance state' is higher than ever and continuing to rise. COG offers the opportunity (through privacy enabling technologies coupled with investing in regulatory expertise) to investors to benefit from the opportunity to meet the rapidly growing demand for privacy enabling digital currency.

**We look forward to you joining us on the journey ahead.**