www.Deuscoin.org

Version 1.0.0

September 2017

Prepared by

Deuscoin

Development Team

“BRIDGING THE PAST, PRESENT AND FUTURE OF CRYPTOGRAPHY”

TABLE OF CONTENTS

Definition of DEUS

DEUS: Let us get started by bringing to you the definition of the word DEUS and its history

Deus is Latin for "god" or "deity". ... In Classical Latin, **deus** (feminine: dea) was a general noun referring to a deity, while in technical usage, a divus or diva was a figure who had become divine, such as a divined emperor. In Late Latin, **Deus** came to be used mostly for the Christian God.

KRYPTOS: Means “hidden”

GRAPHEIN: Means “writing”

CRYPTOGRAPHY: The Egyptians used to communicate through messages written in hieroglyph.

THEOS: God

INTRODUCTION

Definition of Cryptography

When we hear the word cryptography, we immediately think of codes, puzzles and secrets. Cryptography has been around for approximately 4000 years and originated in Egypt. The word cryptography comes from these two words: **KRYPTOS** and **GRAPHEIN**. **KRYPTOS** brings the meaning **“hidden”**, while **GRAPHEIN** means **“writing”**.

In ancient Egyptian culture, messages were written in hieroglyphs. Using this method, only the scribes (writers) and recipients knew the codes. This method is actually quite similar to modern cryptography where two keys, PUBLIC and PRIVATE are used to encrypt and cryptographically verify the message.

1. Introduction

The fiat (government-backed cash/currency) in your pockets and clinking change in coins used as monetary media have their own intriguing history to boast. The first recorded monetary system appeared in Mesopotamia around 3000 B.C., where silver and barley were used by Babylonians as universal mediums of exchange and units of account.

The Code of Hammurabi included a set of payment rules by which debts could be settled with either silver or barley. As time goes by, individuals’ status in the public eye was characterised by a monetary measure of their capacity to attain things of significant worth, rather than their capacity to inflict suffering. Money, then, made human settlements less

vulnerable to bloodletting and chaos. As the world became more civilised, we saw the rise of three great ancient cultural centers: Mesopotamia, Greece, and Rome.

Over the course of history, currency has been issued by those in power, be they rulers or democratically elected governments. We can see the stamps of authority of those rulers in power on the currency itself. The connection between unit of account and power runs deep, and the people know it. Just take a look at the bill in your wallet right now or the coin in your pocket. Even today, the stamp is there consistently to remind us.

To highlight an example: The gold and silver alloy coins thought to be the first minted currency --- from the kingdom of Lydia in what is now western Turkey --- notably bore a lion's head insignia. This makes King Alyattes, presumed to be the sovereign behind these coins, likely to be the original author of a millennia-long association between artwork and currency, a practice that has lent these otherwise impractical inanimate objects great power, significance and perceived value.

No currency is minted without artistic finesse. This gesture helps us to differentiate the intrinsic value each currency carries, yet they always retain the symbolism of power. Across the world, dynasties, monarchs and governments have used similar artistic imagery as stamps on coinage. Apart from presenting the coin with authenticity, we also see this as a royal branding, an advertisement of their power in their respective time. So, are units of account and power inseparable?

There was one specific benefit that materialised from the sovereign's capacity to issue money: the creation of seigniorage, which is the ability to profit directly from the issuance of currency. In the modern era, seigniorage exists because of the interest free loan that a government obtains by printing unit of account on comparatively worthless pieces of paper. When currencies were associated with particular weights of precious metals, monarchs exploited this power. Bank credit effectively became money, since it was deemed to be backed by the sovereign. Banks now lend their good names to a borrower as guarantors, and with these instruments became tradable, a bond market is on the rise. This new definition of

money has triumphed... until now.

Bond markets were indeed a financial leap which expanded liquidity in the economy. However, the system is not without risk. Even though entrepreneurship prospects were created, it also gave rise to what we now refer to as 'systemic risk'. This means that if there are losses in one institution, other institutions could be undermined and weakened as well as all who are networked in the financial system. This ripple effect would leave the system vulnerable; therefore, society's trust in this system inevitably weakens.

The ever-growing link of credit relationships meant that businessmen could back their investments. But not every business made a unit of account and not every businessman was good for his debts. After the financial system became interconnected, debt defaults and bankruptcies began to create a 'domino effect' in addition to the inherent risk in debt and credit lending. If a lender began to worry that a large debtor might not meet its payments, that lender might withhold funds from other borrowers, who would then face financing troubles, cultivating bigger concerns. Thus, flimsy public trust could break down. When trust is gone, credit could suddenly dry up, leaving perfectly good debtors unable to make good on their loans, which would in turn make their creditors' finances shaky, further depleting the public pool of trust. This is how the financial crises of the modern era were made. Unit of account had been liberated, but it had also become more dangerous.

So where does all of this leave today's financial systems? Due to financial instability, debates on how to control unit of account and how to define money itself are common and heated.

On one side of the ring we have the believers in gold. The great English philosopher John Locke declared that the gold standard was adopted in the late-seventeenth century. People felt it was necessary to connect their unit of account to a more tangible object in an effort to avoid the public's unit of account from being obliterated by the governments and their banking counterparts. This gave rise to an economic boom with little inflation, and protected the savings of the wealthy. In other words, it was not success for all, as the poor suffered. Monetary constraints and elevated value of the gold triggered many things. People hoarded their money, which caused credit to shut down.

Ultimately, bankruptcies and unemployment ensued. We see financial systems come and go, crisis after crisis. With this, new concepts emerged. Out of adversity, humanity always triumphs in finding a more competent financial system. This new concept focused not on how to constrain the ability of a government to issue currency, but on how to manage banks in their unique role as creators of private, credit-fuelled money. After World War II, governments again professed a longing for a firm monetary anchor and, in particular, a central pole of stability for a distressed international economy. Memories of that period, where inflation drastically eroded the value of the money in people's pockets and then forced them into a painful economic contraction, are still so strong among a certain generation that they feed the appeal of scarce, independent "currencies" such as gold and, as we shall see, Crypto-Currency.

This history lesson of money begs a simple challenge: How to design a system that most effectively facilitates the exchange of goods and services and generates prosperity while preventing the institutions that manage that system from abusing the trust that comes with their responsibility as financial stewards.
"Deuscoin represents a viable solution to this challenge"
In appreciation of the phrase above, the first step is for Deuscoin to be accepted widely as a viable unit of account, and to become trusted as a means of expanding exchange and prosperity.

One familiar benchmark says that for a currency to become viable it must function as a medium of exchange, a unit of account, and a store of value. For example, US Dollars can be used to buy almost anything worldwide. They are also used to measure the value of pretty much anything. In fact, many believe that their savings will be protected over time if they are denominated in dollars.

Crypto-Currency is now used as a medium of exchange by various people for many transactions, but few use it as a unit of account. A seller that accepts Crypto-Currency invariably list their products' prices in the national currency of the country in which they are based. As for a store of value, the speculators who've bought Crypto-Currency in the hope of

future gains certainly believe it has this feature, but for most people its volatility precludes it. Crypto-Currency price in dollars soared 8,500 percent in the first eleven months of 2013, but then lost two-thirds of its value in the following six months. Who would put their life savings in that kind of market experiment?

“Deuscoin offers a remarkable capacity to facilitate low-cost, near-instant transfers of value anywhere in the world. Deuscoin’s early adopters have employed strategies based on lessons learned from the history of money.”
At first, the early adopters of Deuscoin faced a challenge, which was to build a bigger community around Crypto-Currency. It started out with as little as two members, steadily growing. With motivation fueled by the desire for progress, the expansion of Deuscoin represents a new opportunity to transform how we buy, sell, and store value.

2. Deuscoin Core Technology

The Problem with Proof-of-Work Based Blockchains
Bitcoin relies on mining (Proof-of-Work) to secure its network and validate transactions. Users who mine are rewarded with Bitcoin, thus providing them with an incentive to secure the network by giving a reward for each block mined. But this system is not without a catch. Because the reward for mining decreases and the price of electricity increases over time, a “computational arms race” has begun, in which companies worldwide compete, building more powerful hardware, in order to gain an advantage over others and increase the chances of receiving block rewards. After the last bitcoin is created in 2024, miners will no longer receive any block rewards. Bitcoin will become more and more scarce in the years following. Meanwhile, miners could sell huge amounts of bitcoin with relatively low fees since they control the network, while demanding higher fees for transactions from the public. If this sounds familiar, it's because this is the same system being used today by corporations, and their executives who receive huge salaries and pay a very small percentage of taxes relative to the average working family.

Bitcoin mining is simply not for everyone. Typically, only those who can afford to risk huge

amounts of capital are in the mining process, and control of the Bitcoin network is in their hands.

Despite a number of problems, innovation has turned crypto-currency into a decentralised network in which anyone can participate. 'Altcoins' are a group of coins that build on concepts introduced by scientists and engineers, including the infamous Satoshi Nakomoto. These alternatives to Bitcoin solve a number of problems, and the future looks promising. However, each of these projects comes with a unique set of challenges, and many of them have failed, been hacked, or turned out to be scams. Therefore, Bitcoin is still the most powerful and secure network in the world today.

What exactly is Deuscoin?

Deuscoin is a peer-to-peer, decentralised, digital Crypto-Currency based on Bitcoin. It is a payment network without a single point of control or issuing authority. It depends on cryptography and peer-to-peer networking to validate balances and transactions. Deuscoin uses pre-mined proof-of-work (PoW) technology.

Bitcoin mining will be completed around the year 2024, at which time, all of the Bitcoins which will ever be mined will exist in a bitcoin wallet. Therefore in this sense, Bitcoin and Deuscoin are very similar even though Deuscoin is pre-mined.

Why Premined PoW Makes Deuscoin a Superior Alternative:

Deuscoin is not Bitcoin. In fact, Deuscoin can and should be a better Crypto-Currency.

Deuscoin was designed by developers of deus and skilled software architects. Deuscoin uses Premined PoW solely as a way to distribute coins more fairly, and more competitively as opposed to an Initial Public Offering (IPO) or Initial Coin Offering (ICO), while employing the tested and proven network security of Bitcoin.

A pre-mine exists when a community allocates a certain amount of currency credit to a particular address before releasing the source code to the open community. This is often done based on the reasoning that they need to pay for certain features such as listing on exchanges and development of core features such as block explorers.

In order to maintain the security of the network, miners must still exist, even in a premined PoW cryptocurrency such as Deuscoin. Instead of a block reward, miners receive only transaction fees for blocks that are mined by their systems. After 2024 when the last Bitcoin is mined, Deuscoin and Bitcoin will be no different in terms of mining. Mining a premined cryptocurrency such as Deuscoin allows people to secure the network in the same way as Bitcoin's network is secured, but maintaining centralized control of coin supply, instead of allowing miners to control the coin supply, which has led to the "digital arms race" and high transaction fees that currently plague the Bitcoin network.

Premining and centralized control of supply of coins in circulation, while still maintaining a maximum total supply, is an energy efficient solution; the entire network can be sustained on low-powered hardware, and there is little incentive to add more mining power to the network. Equal and fair participation is important because it allows Deuscoin to remain as decentralised as possible, without turning over control to a handful of powerful mining corporations. Deuscoin is not only for the privileged. There is no need to buy specialized hardware or spend exorbitant amounts to mine Deuscoin.

Attacking the Deuscoin network is in theory as difficult as attacking the Bitcoin network, and a successful attack is supposed to be far less damaging, as the number of coins in circulation can be increased to counter-act an attack. In practice, attempting to buy enough Deuscoin to gain control of the network would drive the price up to exorbitant levels, making it counter-productive for attackers. Thus, the network is secure.
Another major benefit in a premined PoW system is that the owners of the network assets (Deuscoin holders) are also the ones who control the network. This is a contrast to crypto-currency where there is a disassociation between those who control the network (miners) and those who own its assets (crypto-currency holders). Deuscoin is transparent and keeps these interests aligned. The main strengths of Deuscoin are sustainability, increased security (particularly against the “51% attack”), and its economic properties, which allow it to function as a long-term store of value, or “backbone” currency.

3. Deuscoin Core Features and Specifications

Deuscoin is a 100% proof of work PRE-Mined crypto currency based on Bitcoin core technology. Since the technical specifications of Bitcoin core are well-known and available on the internet, they are not discussed herein. However, a basic explanation is given.

a) Deuscoin Supply

The total supply of Deuscoin is 100 Million coins (plus 5000), divisible to eight decimal places. All coins were issued immediately after the creation of the genesis block (the first block in the Deuscoin blockchain), leaving the genesis account with an initial balance of 100 Million Deuscoin.

b) Network Nodes

A node on the Deuscoin network is any device that is contributing transaction or block data to the network. Any device running the Deuscoin software is seen as a node. This does not include mobile phones who are running only a wallet and not the deuscoin-core software.

Nodes can be subdivided into two types: hallmarked and normal. A hallmarked node is simply a node that is tagged with an encrypted token derived from an account's private key; this token can be decoded to reveal a specific Deuscoin account address and balance that are associated with a node. The act of placing a hallmark on a node adds a level of accountability and trust, so hallmarked nodes are more trusted than non-hallmarked nodes on the network. The larger the balance of an account tied to a hallmarked node, the more trust is given to that node. While an attacker might wish to hallmark a node in order to gain trust worthiness within the network and then use that trust for malicious purposes, the barrier to entry (cost of Deuscoin required to build adequate trust) discourages such abuse.

Each node on the Deuscoin network has the ability to process and broadcast both transactions and block information. Blocks are validated as they are received from other nodes, and in cases where block validation fails, nodes may be "blacklisted" temporarily to prevent the propagation of invalid block data.

Each node features built-in DDOS (Distributed Denial of Services) defence mechanisms which rate-limit the number of network requests from any peer.

c) Blocks

As in other Crypto-Currency, the ledger of Deuscoin transactions is built and stored in a linked series of blocks, known as a blockchain. This ledger provides a permanent record of transactions that have taken place, and also establishes the order in which transactions have occurred. A copy of the blockchain is kept on every node in the Deuscoin network, and every account that is unlocked on a node (by supplying that account's private key) has the ability to generate blocks, as long as at least one incoming transaction to the account has been confirmed.

<u>All blocks contain the following parameters:</u>

• A block version, block height value, and block identifier
• A block timestamp, expressed in seconds since the genesis block
• The ID and hash of the previous block
• The number of transactions stored in the block
• The total amount of Deuscoin represented by transactions and fees in the block
• Transaction data for all transactions included in the block.
• The payload length of the block, and the hash value of the block payload
• The block's generation signature
• A signature for the entire block
• The base target value and cumulative difficulty for the block

Agile Architecture

The earliest Crypto-Currencies were mainly architected as payment systems. Deuscoin recognises that decentralised blockchains can enable a broad range of applications and services, but not on what those services should be or how they should be built. By design, Deuscoin excludes any unnecessary complexity in its core. Only the most successful components of its predecessors remain intact. As a result, Deuscoin functions like a low-level, foundational protocol: it defines the interfaces and operations required to operate a lightweight blockchain, a decentralised communication system, and a rapid transaction processing framework, allowing higher-order components to build on those features.

The core deuscoin software does not support any form of scripting language. By providing a

set of basic, flexible transaction types that can quickly and easily be processed, Deuscoin creates a foundation that does not limit the ways in which those transaction types can be used, and does not create significant overhead for using them. This flexibility is further amplified by Deuscoin low resource and energy requirements, and its highly readable, highly organised object-oriented source code.

Basic Payments

In any Crypto-Currency, the most basic feature is the ability to transmit tokens from one account to another. This is Deuscoin's most fundamental transaction type, and it allows for basic payment functionality.

Multisignature Payments

Deuscoin's simplest smart contract allows multiple parties to 'sign' and approve payments in a simple, configurable consensus-driven voting system. For example, if 2 out of 3 users sign a transaction, then it will be sent automatically. If more than 1 rejects the contract, the money is freed up to be spent elsewhere. Any number of parties can be included in such a payment, for example, 10 out of 10 could be required to sign a transaction, or 30 out of 100 signers.