SAFECOIN

THE PURPOSE WHITE PAPER

INTRODUCTION

SafeCoin was born on the premise that a Cryptocurrency and associated coin needs to serve a purpose. The Crypto market is awash with dozens on coins wishing to commercialise and capitalise on the emerging blockchain technology and leverage off the promise of the technology stack's disruptive capabilities, yet; we believe they fail in providing real-world applicability, resolving current problems or serve any potential purpose.

In describing the purpose of SafeCoin, it is worth revisiting the history of coinage and money and as to why they were brought into being, and finally revisiting their purpose.

COINAGE

Precious metals had been widely used for commercial purposes and used as a means of payment, facilitating barters and trade. Typically weighed and cut, the intrinsic value rest in the relative rarity of the metal or material. Practically, this solved the immediate need for trade / barter facilitation by addressing an agreed-upon intermediary store of value and a means of payment in a peer-to-peer exchange of goods or services.

However, dependent on the localised geographies, the rarity would differ vastly with different materials representing differing values due to scarcity and desirability. As trade expanded in civilisations around the Mediterranean and trade routes expanded their reach, this further exacerbated the underlying problem facing a network of markets, their perceived value for the medium of exchange and broad acceptance as a means of payment. This led to the evolution of coinage.

The use of these payment methods and store of value is widely known to have existed in many civilizations globally throughout history, but the use of coinage as we understand it today, can be traced back to Lydia, circa the seventh century. As a concept, coinage is issued by an issuing authority through a minting process and is recognized as a standard across an area by that authority.

COINAGE

In Sardis, the first stamped coins were struck made of a natural occurring alloy called electrum (elektron in Greek) comprised of both silver and gold and a few lesser precious metals. Importantly, the coin weight as well as the ratio of the coin's metallurgical composition was consistency applied in ensuring standardization of value. Coinage was introduced to solve a difficulty within Lydia, its subject territories as well as neighbors, in providing a consistent value for transactions. Quickly, Lydia evolved and was recognized as being at the forefront on retail and trade in the region, in part, due to the facilitation of trade through coinage.

Surrounding territories minted and stamped their own imagery on their coins as a reflection of their area of influence but the relative rarity of electrum and its natural occurrence in Lydia meant that the phenomenon was limited to Lydia and subject territories. It was only in the 6th century that the concept of minting coins in silver and gold respectively, saw the monetary innovation introduced and widespread adoption take place. Quoting from Herodotus a Greek historian (c. 484–c. 425 BC), "So far as we have any knowledge, they (the Lydians) were the first people to introduce the use of gold and silver coins, and the first who sold goods by retail".

COINAGE

The importance of this historic event is that it introduced the first known example of bimetallism; a monetary system wherein the issuing state fixes the relative exchange rate between the gold and silver coins. From these events, ancient civilization monetary systems Daric, Shekel and others were born. Whilst differing currencies were born reflective of their respective issuing state, the resultant premise of their purpose is described below:

Results
Mutually-agreed medium for trade
Store of value
Means of payment for goods or services
Means of payment for taxes and tributes - * (Dependent on governing authorities, specific coins were accepted only)

COINAGE

The stakeholders of this bygone era enjoyed financial independence as they could selectively choose the trade of their choice as they entered into a barter. The trades were private in that there was no mediating financial institution in the peer-to-peer transaction and each individual stored their own hoard providing them the privacy they wished for as well as the coins in itself could not be traced to a history of transactions or other individuals as there was no identities or records of the transactions having taken place, providing anonymity. Anonymity, privacy and independence are all attributes directly enjoyed through the use of coins, a cash-based system of trade.

Cash does not require the disclosure of personal information between both parties involved in a transaction. Governments and financial systems often cite the lack of tracking and auditing as a means of facilitating illegal activities. In this regard, the villainization of the use of cash relentlessly is pursued as an increasing number of countries have imposed caps on cash transactions. Conversely, the limiting of coin or cash based transactions, removes the rights of trading participants or holders of value to the rights of their financial independence, privacy and anonymity.

PRIVACY VS. ANONYMITY

Often these terms are used interchangeably but they differ significantly. A transaction is "anonymous" if no one knows who you are while a transaction is "private" if what you purchased, and for what amount, are unknown. Credit card transactions are not anonymous and they are not private. Your information is fully available to the issuing bank, the merchant, the credit card network, and law enforcement – if subpoenaed. In this regard, the first cryptocurrency, Bitcoin is anonymous but not private. Identities are not revealed in the block chain – but every transaction is visible in the blockchain. A bitcoin user connecting with his personal information to centralized exchanges or using on-line wallets, has now inadvertently given up his right to both privacy and anonymity. As a result, there is little difference in anonymity between using Coinbase and using a bank to transact.

WHY BITCOIN AND MANY CRYPTOS FAIL

Bitcoin is the first digital currency to achieve widespread adoption. It rose to prominence due to the fact that unlike traditional e-cash schemes it requires no trusted parties. In modern times, financial transactions are "agreed to" through a mediator bank that decides on the fate of the transaction. In contrast, Bitcoin leverages a distributed ledger known as the block chain to store transactions made between users. Because the blockchain is massively replicated by mutually-distrustful peers, the information it contains is public. Bitcoin removes the necessity for a central authorizing financial agency and replaces it with a tamper-proof distributed peer-accepted model. However, it fails to offer even a modicum of the privacy provided by traditional payment systems, let alone the robust privacy of anonymous e-cash schemes.

WHY BITCOIN AND MANY CRYPTOS FAIL

Increasingly it is accepted that it is possible to surface the identity of crypto currency owners by using information in the block chain itself, such as the structure of the transaction graph as well as the value and dates of transactions. With this understanding that Bitcoin is not anonymous in itself, different methods and techniques have been utilized for those with sufficient motivation to obfuscate their transaction history with the help of mixes or tumblers.

A mixer allows users to entrust a set of coins to a pool operated by a central party and then, after some interval, retrieve different coins (with the same total value) from the pool. Mixers suffer from the following limitations:

THE MIX CAN TRACE COINS

THE MIX MAY STEAL COINS

THE DELAY TO RECLAIM COINS MUST BE LARGE TO ALLOW ENOUGH COINS TO BE MIXED IN

Given the limited utility of some crypto coins, these risks may be acceptable to some users.

WHY BITCOIN AND MANY CRYPTOS FAIL

We believe that legitimate users wishing to keep their spending habits private from others, do not wish to spend additional effort ensuring their own privacy. Further, many others may not even be aware that their privacy is typically compromised.

The crypto community should be offered a different option and remain SAFE. People using SAFECoin are offered instant, risk-free transacting and privacy, guaranteeing the shielding of their data and their transactions from publicly accessible means as was the case with the advent of money described earlier. SAFECoin ensures that anonymous transactions guarantee the market value of a coin is independent of its history, thus ensuring legitimate users' coins remain fungible.

SAFECOIN | ORIGINS

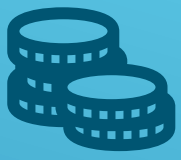
MANY CRYPTOCURRENCIES PRECEDING SAFECOIN HAVE PIONEERED INNOVATIONS THAT HAVE YIELDED NETWORK ARCHITECTURE, DISTRIBUTED LEDGERS AND CONSENSUS MECHANISMS FOR STORAGE, TRANSMISSION AND SECURITY. SAFECOIN HAS SELECTED THE BEST OF THESE INNOVATIONS IN ESTABLISHING SAFECOINS TECHNOLOGY STACK AND PLATFORM, ENSURING WE EVOLVE FROM ESTABLISHED DEVELOPMENT EFFORTS AND INNOVATE FURTHER IN ENSURING SAFECOINS LONGTERM VIABILITY.

THE SAFECOIN TEAM THANKS AND ACKNOWLEDGES THE FOUNDATIONAL PROJECTS: BITCOIN, DASH, KOMODO, SUPERNET, ZENCASH AND ZCASH AND FURTHERS THESE COMMUNITY-DRIVEN CRYPTO-CURRENY PROJECTS BY ENSURING THAT SAFECOIN INNOVATIONS ADD TO THE GLOBAL COMMUNITY POOL OF KNOWLEDGE BY REMAINING OWNED BY THE PUBLIC DOMAIN, A SHARED SATOSHI VISION.

WHY SAFECOIN?

No ICO, No unfair distribution, no cash-grabs

No Mining Tax, Treasury, no dev fees and No Node Tax



A Transparent and published small Pre-Mine for Bounties, Airdrops, marketing and initial coin listing on an exchange

Community Voting and Funding rounds for additional listings

On-going Focus on the communities privacy and anonymity rights, whilst building value

Safety Isn't Expensive; It's Priceless

SAFECOIN | PRIVACY EVOLVED

ZK-SNARK

SHIELDED TRANSACTIONS IN ZCASH CAN BE FULLY ENCRYPTED ON THE BLOCKCHAIN, YET STILL BE VERIFIED AS VALID UNDER THE NETWORK'S CONSENSUS RULES BY USING ZK-SNARK PROOFS.

Coin Mixer

KOMODO JUMBLR COIN MIXING

TOR

TOR NETWORK ANONYMOUS COMMUNICATION

E2E TOR

ENHANCED END-TO-END TOR DEEPONION INTEGRATION FOR IMPROVED CONNECTION AND TRAFFIC

OBFS4

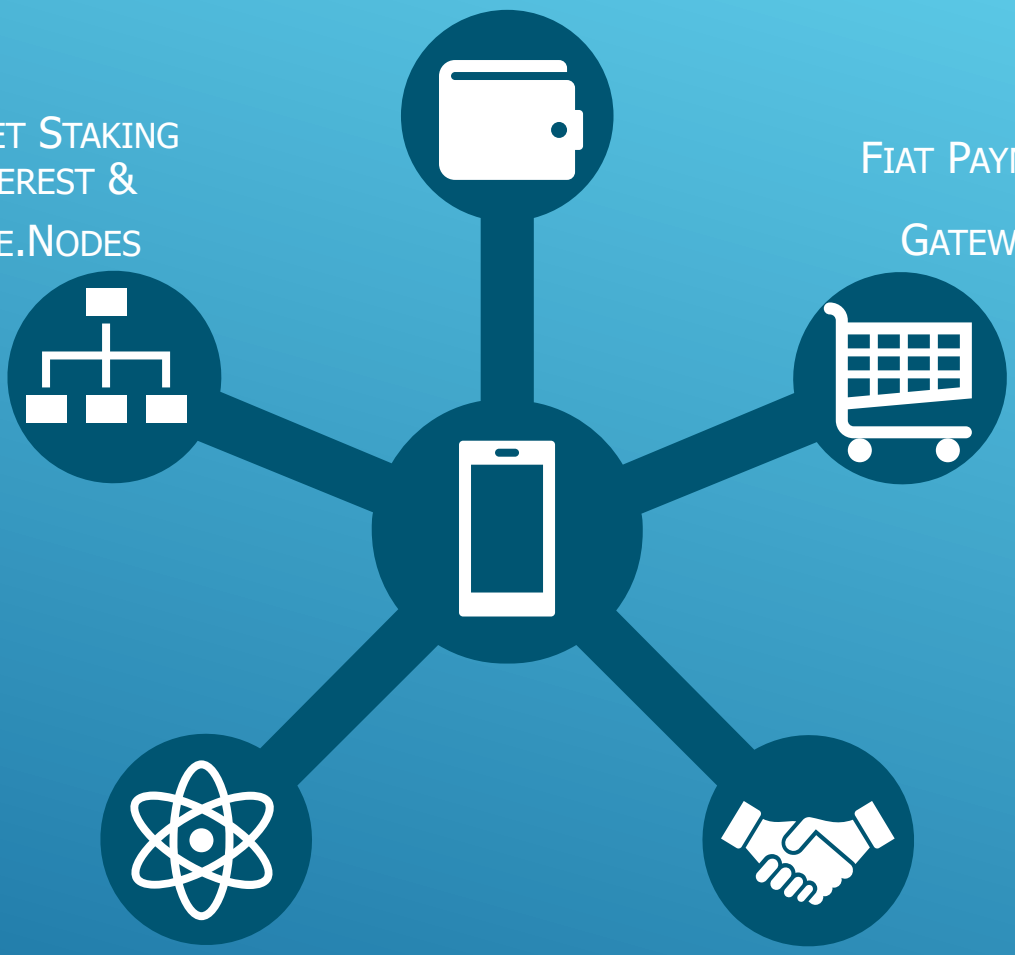
OBFS4 IS OBFUSCATING OR ENCRYPTING THE DATA BETWEEN THE USER AND THE TOR NODE, MAKING IT IMPOSSIBLE ANALYZE THE PACKETS AND DETECTING THAT THE TOR IS USED

SAFECOIN | TRADE EVOLVED

GUI WALLET

WALLET STAKING INTEREST & SAFE.NODES

FIAT PAYMENT GATEWAY



CROSS-COIN ATOMIC SWOPS

FAIR.EXCHANGE DECENTRALISED EXCHANGE

SAFECOIN | SPECIFICATIONS AT LAUNCH

Component	Details
Hash Algorithm	Equihash
Consensus	PoW
Privacy	ZK-SNARKS + Jumblr
Nodes	SafeNodes
Block Time	60 Seconds
Total Supply	36 Million
Block Reward	128 Coins Halving (90 Days)
Wallet PoS Interest	5% Yearly Cumulative
Pre-mine	3 Million

WWW.SAFECOIN.ORG