traaittCASH Whitepaper

It has been over a decade since the initial launch of Bitcoin in 2008, and in the time since, Bitcoin has failed to fulfill claims of allowing for fully anonymous transactions. In the 7 years since Bitcoin's false promise of anonymity was first broken with the shutdown of the "anonymous" marketplace SilkRoad, we have seen the continued exposure of critical flaws in the Bitcoin protocol. Great strides have been made in research into blockchain technology by both academia and the tech industry, yet Bitcoin and its imitators still offer only weak protection for those who wish to remain anonymous. Other efforts to erode the ability to remain anonymous, such as blockchain scanning technology and 51% attacks, have mostly been addressed with minor hardware upgrades. But for anonymous payments, no cryptographic innovation has been able to successfully tackle larger anonymity requirements, leaving users with the unappealing choices between pseudo-regulated coins or unregulated CryptoNote coins, which in many instances have been nearly useless. traaittCASH, in contrast, offers an efficient PoW algorithm allowing for both CPUs and GPUs to profitably participate in mining. In this whitepaper we attempt to address traaittCASH's potential in an area which crypto-payment systems have repeatedly failed: anonymous transactions. We advocate that traaittCASH has the necessary features needed to facilitate truly private and completely anonymous transactions for users who need it, while still allowing mass adoption through a fun and easy to use interface. We believe that traaittCASH is capable of facilitating completely anonymous transactions while retaining many of the other features that are celebrated in blockchain technology, such as ease of use, transaction speed and UX design.

Introduction

Founded in 2020, traaittCASH is one of many cryptocurrencies that rely on blockchain technology, which is comprised of a network of actors, called nodes, that act as a decentralized system for storing and transmitting information. In contrast to the traditional centralized databases used to store transactions, blockchains are distributed databases, meaning that there is no single governing point of control and nobody with power needs to be trusted in order to use the platform. Blockchain's utility relies on its ability to securely communicate transactions to a decentralized audience and its resistance to censorship, either by other parties or attackers securing the majority of the network's mining power. Cryptocurrencies provide this governance structure itself in the form of currency, and in this way their impact extends far beyond simply providing proof-of-work currency. Today, cryptocurrencies are increasing in popularity, and are in talks as a potential replacement for fiat. While many companies are working to accommodate this growth, for the most part they have carefully designed current technology to avoid allowing truly anonymous transactions by default while leaning on speculation for their value. In this way, the general consensus within these tech companies regarding anonymity in payment systems seems pessimistic at best, specifically for correspondent banking and legacy banking. One of the most widely adopted cryptocurrencies, Bitcoin, even has protections and features built specifically to purposefully break the anonymity of its users. In contrast, cryptocurrencies such as Ethereum and its ICOs purportedly aim to move away from a blockchain that can be censored or controlled by a group with a majority of CPU power. Their supposed answer to this is to build their use cases on platforms, which rely on approval voting and require the user to make a human-readable contribution before authenticating a transaction. With this in mind, we

write this whitepaper to present an alternative, peer to peer, trustless payment system that we believe will allow users to transact in the same invulnerable way that many exchanges and payment providers promise. As a cryptocurrency on the Proof-ofWork (PoW) hash algorithm Chukwa, we believe that traaittCASH is capable of maintaining the imperative characteristics that give cryptocurrencies their value, such as true decentralization and censorship resistance, without sacrificing user anonymity. Explaining all aspects of traaittCASH is beyond the scope of this document and often goes beyond our intention.

Instead, we discuss our primary areas of focus for the future of the traaittCASH protocol in terms of necessity for the development of a currency. We discuss the design considerations and the development of traaittCASHservices.

Related Work

The original creator and founder of the cryptocurrency space was Bitcoin. The original plan for Bitcoin was to provide a decentralized payment method to avoid systems operating under the WHOIS protocol. Since its original white paper titled "Bitcoin : A Peer-to-Peer Electronic Cash System, Satoshi Nakomoto (figure 1), proposed its first release in early 2009. Figure 1: Original Bitcoin white paper Since then, other cryptocurrencies, including explicitly anonymous currencies, began to emerge. One of the first currencies that pursued anonymous transactions as a primary goal was Bytecoin (BCN) (figure 2). Figure 2: Bytecoin: Anonymous Cryptocurrency Bytecoin provided a direct ideological competitor to Bitcoin while also providing similar capabilities. Despite this, it failed to catch on and aside from spurning a myriad of long forgotten forks, Bytecoin fell to the wayside. It wasn’t until the launch of Monero, and the ensuing technological improvements (RingCT, Bulletproofs etc.) that anonymous and fungible cryptocurrencies saw their time in the sun. The technological success of this project has since been overshadowed by its difficulty of use and negative public image. The key concepts of traaittCASH; safe & easy to use Money clearly delineate the progressive direction of traaittCASH vs. Monero and explain why our project was necessary.

XTCASH, building a platform beyond

Creating anonymous and fungible currencies may have obvious theoretical and public appeal on its own, yet we feel those technologies in isolation are only a fraction of traaittCASH’s potential.
Assets are mined every 144 seconds, with a max supply of 88.744.000 XTCASH emitted over the course of approximately 158,3 years.

When XTCASH was first launched in March 2020 we internatlly discussed on integrating a open payment system built on top of XTCASH, currently in beta testing and soon to be production ready.

traaittCASH payments

traaittCASH payments is a payment processing service that is designed to help developers

integrate traaittCASH payments into their existing applications. This service enables merchants to accept traaittCASH instantly while avoiding high transaction fees and waiting periods of settlement consolidation. Through this service merchants can receive traaittCASH payments with zero headache and no specialized workflow

We believe that traaittCASH has the potential to become the future of money and to provide a widely used platform for currency exchange. Thanks to our dedication to limitless scalability, extensions for high flexibility, and near-instant transactions, we are confident that traaittCASH offers a new way forward for decentralized truly anonymous money. As TurtleCoin is a community project, it is impossible to cover the full extent of the software offerings provided by the network.

The core team is dedicated to the continual improvement of traaittCASH.