Commercium Whitepaper

info@commercium.net
commercium.net

COMMERCIUM

Feb 8, 2018

Abstract

Commercium is a dual-chain platform that ensures the most secure and efficient data processing, storage and access. The *Commercium Blockchain Platform* will offer a customized virtual wallet that enables consumers and businesses to easily incorporate blockchain into their financial transactions and any information tracking activities.

The Commercium (i) blockchain or CMM, is an entirely new genesis of the Bitcoin codebase that implements the ZeroCoin protocol, a form of zero-knowledge proofs delivered through RSA accumulator encryption methods. Masternode functionality will be developed no sooner than the one hundred thousandth block, and introduced to offer additional network stability and strength to bolster the distributed ledger. Commercium is possibly the most balanced, secure and private crypto-currency and implementation of distributed ledger technology to-date. The zero-knowledge proof encryption method of the ZeroCoin protocol preserves the integrity of the Commercium blockchain by ensuring auditable supply without sacrificing the ability to mask transaction data, assuring the personal privacy and security of both consumer and business adopters. Intended for simple transactions of value, speed, privacy and security are the roots of the CMM blockchain.

Commercium (ii) or CMMX is slated for development Q3, 2018 as an Ethereum fork and secondary blockchain that will allow users to create, track and manage smart contracts to conduct business and transactions of value with the ability to record additional metadata as needed for managing information, business agreements and relevant data.

Definition of Commercium[1]

plural commercia \-(ē)ə\
Roman law
commerce, traffic : commercial transaction : business intercourse; also : jus commercii

(ALSO: A **commercium** is a traditional academic feast known at universities in most Central and Northern European countries. ... A **commercium** is the more formal form of the tableround, called Kneipe in German. The term is derived from French Commerce and had been used for any sort of noisy event.)

[1] “Commercium.” *Merriam-Webster*, Merriam-Webster, www.merriam-webster.com/dictionary/commercium.

Introduction

The Commercium White Paper was created for information and discussion purposes only. Commercium and the authors of this report do not warrant the accuracy, adequacy or completeness of the information contained within and shall not be liable for any loss or damage resulting from the use of or reliance on any statements or information found in this report. Commercium is an open source, open community platform. The contents of this document are subject to change.

Commercium will consult with professionals in business, banking and financial regulation. This white paper will be submitted to legal and regulatory experts to seek their support in the examination of regulatory requirements and any guidance relating to the development of the platform. Commercium has a mission to contribute blockchain technologies, to the improvement of Domestic and International Commerce and Trade and will always strive to comply with applicable laws and regulations. The white paper is subject to change in accordance with regulatory review and guidance, as well as input from other stakeholders and interested parties.

This white paper describes the functionalities of the Commercium platform and the critical needs it can fulfill; it also provides an overview of blockchain including, distributed ledger technology, cryptocurrencies, and critical gaps in the current blockchain based payments systems, notably with respect to ease of use, accessibility and seamless and borderless transactions of value

Commercium understands the value of cryptocurrency as an alternative payment medium for the purchase of goods and services, whether initiated online or face to face, whether in domestic or international trade, and whether involving simple transactions, commercial contracts or letters of credit. Distributed Ledger Technology not only offers additional layers of security but also data accuracy, completeness, timeliness and permanence, including full supply chain transparency - all critical concerns for individuals, companies and the global economy.

Consumers, entrepreneurs, investors, small and large businesses are looking for better and faster alternatives for commercial transactions including contracts and payments. Commercium is a dual blockchain platform which sets out to solve these issues on a large scale through a customizable wallet interface to conduct transactions of value or create and manage contractual obligations in commerce.

Commercium sets out to explore all aspects of global commerce to raise the bar of expectations for consumers and businesses. We hope to form a solid foundation and present a convenient, public platform to existing companies and startups, who are looking to incorporate distributed ledger technologies into operations.

Table of Contents

Executive Summary

Consumers must become familiar with blockchain and distributed ledger technologies so that organic demand for these tools can drive integration into commerce. Functionalities that enable individuals to pull demand for these services, will prompt corporations and businesses to meet the needs of their customers rather than pushing unusable or complicated platforms. Commercium will work directly with the user base and community members to create intuitive, easy-to-use applications so that consumers can become fluent and confident in the blockchain based tools they use.

Forgoing the typical cryptocurrency business models of price speculation and narrow, profit focus', the Commercium development team is committed to working directly with businesses and regulators to create synergies between conventional models of operation and the streamlining nature of blockchain based transactions of value. As businesses begin to embrace the platform chosen by their customers, Commercium will focus on creating practical and enduring commercial applications of its network and tools.

Commercium is a not-for-profit organization that imposes transparency and will operate under the guidance and governance of a Board of Trustees to ensure that Commercium's consumer focused mission is upheld. Blockchain technologies development is fluid and Commercium will engage governments and regulators around the world as implementations of distributed ledger technologies continue to evolve. Modernizing blockchain and realizing the benefits of technological advancement starts with consumer level accessibility and delivering the tools that meet the demands of corporate and regulatory frameworks.

Blockchain History

Blockchain is a method of linking sets of data called 'blocks' using cryptography to create a continually growing, sequential, permanent record. Each block contains a link or reference to the previous block, transaction data and a timestamp. Blockchain is more permanent and resistant to modification than conventional accounting and data storage methods. Modifying any existing block requires a massive amount of computer power to modify all succeeding blocks in the chain in addition to the encryption process that creates data security as a whole.[2]

Distributed ledgers are blockchains facilitated by peer-to-peer networks that collectively power, validate and process transactions. The permanence of distributed ledger technology versus a private blockchain, results from the scale of the community supporting it, entities known as "miners". In order to modify any part of a blockchain facilitated through a distributed ledger network, collusion of the majority of network participants (miners) is necessary; thereby limiting and even preventing any unauthorized or untraceable data changes.[3,4] Fraud and illicit activity are far less viable in a distributed network that is public and open versus a private blockchain.

Cryptographic Assets Vs. Blockchain

Cryptocurrencies, more aptly termed, cryptographic assets, are a digital medium of exchange that applies cryptography (data encryption), to execute secure transactions of value through a peer to peer network. Founded in 2009, Bitcoin was the first cryptographic asset and grand scale application of distributed ledger technology. Use cases for bitcoin began with trading card games,[5] and online poker[6], but early adopters refer to it as a new form of money. In 2015, Ethereum was introduced as a new way to not only transfer value but also perform contracts.

Cryptographic assets have introduced the ability to independently send and receive value securely and instantly and then to have it recorded to a permanent and immutable ledger. The original cryptographic assets were an experiment that succeeded and proves that processing monies or value, facilitating transactions and recording data through a distributed ledger is very much possible, reliable and secure.[7]

---

[2] vlabvideos. ***Blockchain symposium***, YouTube, 18 Apr. 2016, www.youtube.com/watch?v=ybl5UatYsGI.

[3] Peter Evans-Greenwood, Robert Hillard, Ian Harper, Peter Williams. "Bitcoin, Blockchain & distributed ledgers: Caught between promise and reality", *Deloitte*, 2016, https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-deloitte-technology-bitcoin-blockchain-distributed-ledgers-180416.pdf.

[4] "Financial Times: Crypto currencies are mirroring pre-Crash banking systems." *Financial Times*, www.ft.com/content/9b464912-76ae-11e7-90c0-90a9d1bc9691.

[5] "Mt. Gox." *Wikipedia*, Wikimedia Foundation, 7 Dec. 2017, https://en.wikipedia.org/wiki/Mt._Gox.

[6] Worstall, Tim. "Is Using Bitcoin The Way To Play Online Poker In The US?" *Forbes*, Forbes Magazine, 11 Jan. 2013, www.forbes.com/sites/timworstall/2013/01/05/is-using-bitcoin-the-way-to-play-online-poker-in-the-us/#51551bcf3637.

[7] "John Wolpert talks about the timeline of blockchain." DeveloperWorks TV, 5 June 2017, https://developer.ibm.com/tv/john-wolpert-talks-about-the-timeline-of-blockchain/.

COMMERCIUM

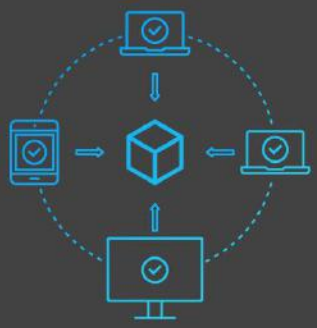
Blockchain Technology - How It Works

A blockchain is a distributed database which is shared and continuously updated by voluntary participants. The blockchain stores a complete history of any transfer of data within the network. It is distributed across many computers and through a process called "mining" some of these computers update the database once a consensus has been reached. Originally defined in the source code for Bitcoin, the blockchain technology has now been used for variety of applications.

Two parties initiate a transaction by agreeing to exchange a unit of value

A unit of value can be any form of data, from funds to securities, to votes, medical records, or ownership.

The requested transaction is combined with other pending transactions to create a block



"Miners" then determine the validity of that block by competing to perform mathematical calculations based on mutually agreed upon ruled to receive a reward

Miners "mine" by rapidly attemping possible solutions to these algorithms. To keep the distribution of rewards predictable, the algorithm increases in difficultly as more people are working on them.

The block is shared across a P2P network of computers, known as nodes, that store the transaction

A peer-to-peer network refers to a system of computers connected directly to one another via the Internet, rather than through a central server.

Once a block is verified, it is added to the blockchain in a permanent, unalterable way

Blockchain entries are assigned a hash function, which contains information from previous blocks. If an attempt to alter a past transaction is made, all following blocks will invalidate this new transaction and it will be rejected.

A hash function is a mathematical operation that processes data of any size and outputs data of a fixed size.

The transaction is complete, and the unit of value is exchanged between the two parties

Multi-Signature Security

Multi-signature is an additional layer of security in processing a transference of value. The total number of signatures required to execute a transaction are predetermined upon creation of a contract or wallet and facilitates an escrow service that requires multi-party approval. Two or more parties are required to agree upon the terms of service and outcome, all signing the transaction to release its values to the intended parties. Multi-Signature Security is a process that ensures delivery of goods upon payment and payment upon delivery of goods while maintaining the opportunity to dispute terms when deliverables are unmet.[8] This is how a letter of credit currently works to secure international sales and purchases. Multi-signature wallets and smart contracts will replace the need for letters of credit.

Smart Contracts

The enforcement of a negotiation or performance of obligation using a protocol that verifies that the parameters of a contract are met. Smart contracts can be both self-executing and self-enforcing with the intent of offering more security and superior execution than conventional contract law when completing transactions and services.[9] Smart contracts can reduce the time, people and monetary costs associated with performing a contractual obligation.[10] Smart contracts ensure project parameters are met before delivery of goods, services or payment.

---

[8] Davenport, Ben. "What is Multi-Sig, and What Can It Do?" *Coin Center*, 1 Jan. 2015, https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do.

[9] "Smart Contracts." *Investopedia.com*, 18 Apr. 2017, www.investopedia.com/terms/s/smart-contracts.asp.

[10] Dmitry Buterin @dmitry-buterin, et al. "What Are Smart Contracts? A Beginner's Guide to Smart Contracts." *Blockgeeks*, 2016, https://blockgeeks.com/guides/smart-contracts/.

COMMERCIUM

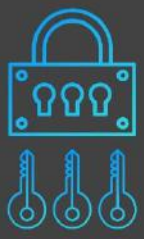
Multi Signature - Explained

In cryptocurrency, a wallet must be signed by a private key in order to verify ownership and approve a transaction. While a wallet's public key is part of a typical lock and key pair with one private key to confirm ownership. MultiSig, short for multi-signature, requires that multiple users or a user with multiple keys to input their private keys in order for access to be granted.

Traditional Transaction

A given public key can only be verified by a single associated private key.

Think of a box with one lock and one key.



Multisig Transaction

A given public key must be verified by multiple private keys in order to validate a transaction.

Think of a box with several different locks.

M-of-N

Refers to a wallet which is associated to "M" amount of keys, and requires "N" amount of keys in order to validate a transaction. A MultiSig wallets typically range from 2-of-2 confirmations, all the way up to 15-of-15, and can adopt any combination in between.

History

Although introduced formally in 2012, The idea of "multisignature" to claim ownership is ancient. Multisig was not popular until 2014 and at the time, these still only accounted for 0.02% of all transactions. Currently, about 10% of all BTC are held in these types of wallets.

What's purpose?

The main implementation is to increase the security of a transaction by minimizing opportunities for theft and dishonesty. In traditional transactions that only require one private key, the device on which the key is stored represents a single point of failure. Requiring multiple keys lessens the threat of theft as the transaction becomes increasingly difficult to compromise with each additional key.

Use Case Examples

Increasing Security

In a 2-of-3 wallet, storing all 3 private keys in different locations minimizes the risk of theft, and still allows you to access the funds should you lose one of the private keys.

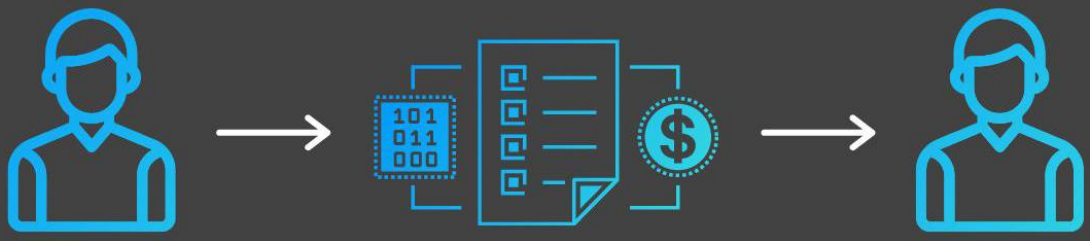
Increasing Trust

In a 3-of-5 wallet, 5 individuals have a private key, so that every transaction must be approved by the majority (3) of key holders.

COMMERCIUM

Smart Contracts - Explained

A Smart Contract represents a layer of code built on top of a blockchain protocol, which details conditions that must be met in order for an exchange to take place. Once these pre-determined conditions are met, the exchange of value is autonomously executed.



Seller

A user sets the conditions upon which the contract will auto-execute.

Buyer

A user meets the pre-determined conditions, triggering an automatic audit and validation of the terms and conditions.

The smart contract is self-executed, and the goods are exchanged once the audit is complete.

The transaction is permanently recorded on the blockchain, and is now public information.

Traditional transactions require middle parties to facilitate their execution. Smart contracts rely on code to adhere to the terms and perform the exchange. The information is then stored on the blockchain and verification of ownership can always quickly be confirmed. This makes the transactions more secure, and indisputable once they have been completed.

Autonomous

Once smart contract created, it is fully self-sufficient and autonomous.

Cost Effective

Removes middle parties, reducing costs associated to operation and administration.

Rapid

Reduces settlement time, resulting in a faster, hassle-free transaction.

Reliable

Offers a higher degree of trust by decreasing the risks of typical transaction.

Transparent

Distributed among nodes, and can be reviewed by both parties.

Permanent

Provides a permanent, verifiable record of contract conditions and transactions.

Real World Impact Of Blockchain Technologies

Financial institutions and technology firms (Goldman Sachs, Bank of America, IBM, Microsoft, et. al)[11] are in a race to provide blockchain services and technology capable of digitizing and automating “middle man” industries and transaction processing, such as: banking, notaries, clearing houses, and freight forwarders.[12] The speed, accuracy and efficiency with which a blockchain is able to catalogue data, execute transactions and manage contracts makes exploration of the new technology not just potentially lucrative but also a corporate responsibility to stakeholders.[13] Blockchain can increase efficiency adding not just permanence, but trust, cyber security and potentially enormous cost savings.[14]

A highly speculative asset trading market with nearly 2000 cryptocurrencies and assets now exists, similar to FOREX, stocks or commodities exchanges, and yet it remains distinct for its infancy and volatility alone.[15] Each cryptocurrency seeks to, or claims to, apply blockchain and distributed ledger technology in a novel manner, solving some real-world problem or filling some critical niche. In this next-phase of implementing blockchain technologies, we move from theory to practice in managing all kinds of transactions and processes of value that we see in everyday life. Blockchain and distributed ledger technology enable superior `value chain management’ - creating, tracking and exchanging value, as well as collaborative value transparency. However, as the technology has evolved, significant functionality, accessibility and ease of use gaps are emerging.

Adoption Of Cryptographic Assets

Cryptographic assets are not yet truly accessible and face much skepticism with novelty and complexity also obscuring the benefits and possibilities.[16,17,18] In addition, limited wallet capabilities and user interfaces, impractical pricing, volatility and fees are barriers to the speed and scale of adoption in commerce and everyday use. These complications present a litmus test of both technical capability and practical understanding of business and economics.[19]

---

[11] Kharif, Olga. “Big Banks Are Stocking Up on Blockchain Patents.” *Bloomberg.com*, 21 Dec. 2016, www.bloomberg.com/news/articles/2016-12-21/who-owns-blockchain-goldman-bofa-amass-patents-for-coming-wars.

[12] Macheel, Tanaya. “Crypto Colonizing: B of A's Blockchain-Patent Strategy.” *American Banker*, 1 Feb. 2016, www.americanbanker.com/news/crypto-colonizing-b-of-as-blockchain-patent-strategy.

[13] Kelly, Jemima, and Anjuli Davies; “European banks risk lagging Wall Street in blockchain race.” *Reuters*, Thomson Reuters, 19 Oct. 2016, www.reuters.com/article/us-banks-tech-blockchain/european-banks-risk-lagging-wall-street-in-blockchain-race-idUSKCN12J22L.

[14] Long, Monica. “Ripple and XRP Can Cut Banks' Global Settlement Costs Up to 60 Percent.” *Ripple*, 18 Aug. 2016, https://ripple.com/insights/ripple-and-xrp-can-cut-banks-global-settlement-costs-up-to-60-percent/.

[15] “Bitcoin VS Forex.” *Bitcoin News*, 5 Feb. 2016, https://news.bitcoin.com/bitcoin-vs-forex-2/.

[16] “Macquarie Analyst Rejects Jamie Dimon's Bitcoin 'Fraud' Critique.” *CoinDesk*, 28 Sept. 2017, www.coindesk.com/wall-street-analyst-rejects-jamie-dimons-bitcoin-fraud-critique/.

[17] Costelloe, Kevin. “Bitcoin 'Ought to Be Outlawed,' Nobel Prize Winner Stiglitz Says.” *Bloomberg.com*, Bloomberg, 29 Nov. 2017, www.bloomberg.com/news/articles/2017-11-29/bitcoin-ought-to-be-outlawed-nobel-prize-winner-stiglitz-says-jal10hxd.

[18] McCrank, John, et al. “JPMorgan's Dimon says bitcoin 'is a fraud'.” *Reuters*, Thomson Reuters, 13 Sept. 2017, www.reuters.com/article/legal-us-usa-banks-conference-jpmorgan/jpmorgans-dimon-says-bitcoin-is-a-fraud-idUSKCN1BN2PN.

[19] Baird, Nikki. “Blockchain and Retail: Four Opportunities.” *Forbes*, Forbes Magazine, 9 Aug. 2017, www.forbes.com/sites/nikkibaird/2017/08/09/blockchain-and-retail-four-opportunities/#33d2cd7972bf.

Fees

Inordinate transaction fees impede the adoption of cryptographic assets as some business may see increased costs from making the switch. Sending a small sum of money through bitcoin is now so costly that one must use an alternative when working in smaller amounts of money for any kind of transaction of value.[20] In order for cryptographic assets (cryptocurrencies) to be widely adopted as a standard means to conduct business, the fees cannot be so high they impede usability.[21] Converting back to fiat incurs significant additional fees, sometimes in the neighbourhood of 10-15% or individuals must revert to the archaic models of value transactions, which are totally based on trust and contrary to the design of blockchain.

Ease Of Use

Cryptographic asset wallets generally are not user friendly. A simple and secure user interface to buy and sell goods and services, or create and execute smart contracts, is difficult to find. Almost all cryptographic wallets today require some level of technical expertise and programming abilities. The current learning curve of digital assets inhibits mass adoption of blockchain technologies as adopters are typically more technically educated or skilled.[50] Mass adoption requires a simple, secure and effective means to exchange, store, process, send and receive value and execute contracts through one user interface as an individual or business.

Limitations Of Cryptocurrencies

The adoption of blockchain and distributed ledger technologies is prohibitive due to costs and fees associated with available options and currently no service, tool, or business exists to provide a simple yet secure user interface that resolves issues of practicality and functionality. Commercium (CMM & CMMX) seeks to eliminate this gap by providing the optionality and usability of two independent blockchains (dual-chain) delivered through a customizable wallet application with consumers front of mind.

Today, participation requires subject matter expertise that goes beyond traditional business, finance and trading realms to ensure the successful integration of cryptographic tools and distributed ledger technologies. Removing the expert level barrier to entry will ensure that blockchain technology and cryptocurrencies can become a common and standard means to conduct business with as an alternative medium for value transactions.[22,23]

---

[20] Shin, Laura. “Will This Battle For The Soul Of Bitcoin Destroy It?” *Forbes*, Forbes Magazine, 25 Oct. 2017, www.forbes.com/sites/laurashin/2017/10/23/will-this-battle-for-the-soul-of-bitcoin-destroy-it/#2f128fc3d3c0

[21] Ver, Roger, @rogerkver. “Full blocks cause high fees and unreliable confirmations which destroy usability. Usability drives adoption. Adoption drives price. #BitcoinCash.” *Twitter*, 13 Nov. 2017, 07:16, https://twitter.com/rogerkver/status/930091962597699584.

[22] Baird, Nikki. “Blockchain and Retail: Four Opportunities.” *Forbes*, Forbes Magazine, 9 Aug. 2017, www.forbes.com/sites/nikkibaird/2017/08/09/blockchain-and-retail-four-opportunities/#33d2cd7972bf.

[23] Young,Joseph. “McAfee: Bitcoin is too complex for the average individual.” *NEWSBTC*, 2 Jan. 2016, www.newsbtc.com/2016/01/02/mcafee-bitcoin-is-too-complex-for-the-average-individual/.

Technological advancement has always been revolutionary, but true adoption and benefit to humanity comes from functionalities that drive ease of use and accessibility. Computers, originally workstations, were adopted by the masses when a simple interface was developed and no longer required coding expertise (the first Apple and IBM personal computers). The internet was a massive leap forward, but the desktop browser, how we interface, drove its adoption. E-trading in capital markets was introduced in the 90s and delivered autonomy and cost savings to retail investors. Technological advancement leads to accessibility, expands reach, and drives productivity. It creates independence.

The Commercium Platform

Commercium is a dual-chain platform that focuses on functionality and ease of use and consists of the creation of two utility chains that can be used in commerce and a way to execute value transactions and business agreements, privately and securely. The priority of the platform is to create an easy to use set of tools, in an application that will be known as the Commercium Wallet. Cryptographic assets and blockchains have the ability to create or improve societal efficiencies by streamlining the way value is transacted and recorded - eliminating the need for third party facilitators. The Commercium platform accomplishes this by leveraging a custom wallet and network infrastructure designed to integrate distributed ledger technology into one seamless experience for consumers and business adopters.

The Commercium blockchains will be delivered through a public distributed ledger network where individuals (miners), may contribute hashing power (computing power) through a process known as ‘mining’ in exchange for block rewards. This method uses what is called a ‘Proof of Work’ algorithm (PoW), verifying the legitimacy of transactions and writing data to the blockchain, while simultaneously incentivizing miners and unlocking total supply of CMM. Adopters benefit from the additional data security, speed and accuracy offered by a distributed ledger network through immutable and permanent records making it superior to a private blockchain. The Commercium Platform serves as a medium to conduct commerce on a consumer to business level as well as execute contracts and agreements in a business to business capacity.

Global and unrestricted, blockchain and distributed ledger technologies renew the strength and possibilities of open source development. Individuals from all over the world have come together and contributed their knowledge and expertise to blockchain development while simultaneously raising awareness of systemic and sociological issues that span nations. While it is not a solution to every problem the world faces, distributed ledger technology is now being applied in very novel manners across various industries and facets of society. As we set out to trailblaze in the industry, Commercium will contribute to the open source development of blockchain technologies through platforms that will allow businesses and individuals to integrate distributed ledger technologies, further accelerating the rate of innovation, adoption, and the real benefits of cost, time and efficiency savings.

Commercium I (one)

Commercium will be developed in two stages. Stage I (one) will consist of the creation of CMM (Commercium I), its blockchain, and a user friendly wallet interface. The wallet will facilitate peer-to-peer transactions and is a secure place to store value. The wallet will be available for Windows, Linux, macOSX and mobile devices.

The Commercium development team and community will create tools, applications and foster use cases and the adoption of the platform by consumers and business for integration into

mobile/online gaming, e-commerce, local business, face-to-face transactions, and more. The team will seek to list CMM on multiple cryptographic asset exchanges (where practical and safe for adopters) to increase accessibility and price stability through market forces.

CMM

CMM will function as a payment medium, and is intended for simple, real-time consumer-to-business (C2B) and business-to-business (B2B) transactions of goods, services and value. CMM is an entirely new genesis of the stalwart bitcoin codebase and applies the ZeroCoin protocol, standard RSA encryption methods, and zero knowledge proofs. This codebase offers speed and privacy in transactions of value. The ZeroCoin protocol itself ensures that supply is fully auditable and prevents counterfeiting. Furthermore, as whole, this method protects individual and business adopters from nefarious actors by not just simply camouflaging their transaction data, but masking it all together. Outside of authorized entities, this protocol prevents the use of topology and heuristic methods to identify wallet owners as is currently possible with many of the available cryptocurrency platforms such as Bitcoin.[24]

Masternode functionality is slated for development no sooner than the one hundred thousandth (100,000th) block. Masternodes will bolster the strength and stability of the distributed ledger network. The Commercium blockchain is the most highly functional, secure and private iteration of distributed ledger technologies to-date and its development team is dedicated to continuous improvement and contribution to blockchain technologies that enable consumer level adoption and application every day and in commerce.

Ease Of Use

A wallet is an application where owners can store CMM and CMMX off of exchanges in a private location in a unique and personal address generated by the wallet to use the Commercium Platform as a medium to send and receive value. The Commercium Wallet application will be developed for the consumer with functionalities that address essential income and reporting, seamless transactions of value and intuitive contract creation among many other planned developments. Changing the experience and potential application of blockchain technologies for everyday users by delivering a simple and seamless application is a directive of the Commercium development team.

Commercium Wallet

Over the course of Commercium development, tools for keeping records, to manage projects, to manage supply chains, process transactions and create smart contracts will be created. The wallet will facilitate the exchange between CMM and CMMX. Alternative cryptographic assets and currencies may be added as their functionality and importance is realized in the evolution of

[24] Miers, Ian, et al. “Zerocoin: Anonymous Distributed E-Cash from Bitcoin.” http://zerocoin.org/media/pdf/ZerocoinOakland.pdf , 2013.

blockchain technologies as an alternate payment medium. An easy pay system for the mobile device users will be created, exploring methods such as: swiping phones or creating a temporary and secure connection between peers. Commercium simplifies the user experience providing a one stop portal to use Commercium blockchains in commerce and business activities.

Commercium II (two)

Commercium (ii), CMMX, will begin development as the primary, CMM blockchain, is adopted and will be created alongside the various wallet functionalities designed to integrate this secondary CMMX blockchain. While CMM is the principle blockchain, CMMX will be focused on the needs of businesses and provide a means and medium to facilitate and execute smart contracts, agreements and create, store and track data for business-to-business operations.

Dual-Chain

Two separate blockchains will enhance user efficiency and limit bottlenecks where an overload of both simple transactions as well as contract execution can grind a single network to a halt. A dual-chain platform creates separation between transferences of value and executing contract or managing more complex data. Dual-Chain enables a more seamless experience for adopters, limiting the waiting times during periods of high network traffic. Dual chain can provide the utmost security and enable deeper levels of security with more efficient data processing.

CMMX

CMMX is an Ethereum codebase that’s principle application will be in integrating smart contracts to the Commercium Wallet. The CMMX supply will be unlimited to meet the demands of businesses allowing for the creation of new assets as needed. By working with regulators and lawmakers, the Commercium development team eventually seeks to make CMMX a tool and service for converting to and from local fiat currency for its additional data capture ability.

Security And Privacy Of Users

Security and privacy are tandem issues. The CMM codebase protects users by totally anonymizing transaction data to protect user privacy, in and of itself offering a level of personal security to consumers and businesses. As Commercium is committed to protecting a user’s privacy the development team will continuously explore, create and implement tools, resources and applications and plugins that increase user security and privacy without sacrificing usability of the platform. However, the directive of Commercium is to work within legal and regulatory financial frameworks and methods to discourage or prevent use of the platform for nefarious activities will be explored and developed, such as: logging single transactions greater than ten thousand dollars, addresses that transact over one million dollars per month, caps on transaction size or the requirement to use CMMX contracts to input additional metadata for larger transactions.

Commercium Fund

The Commercium Fund is designed to support a self-sustaining open source platform. Upon initiation of the primary CMM blockchain, a onetime sponsors endowment of ten million units of CMM will be deposited into a wallet owned by Commercium with controls in place to ensure the funds are not misappropriated. The Commercium Fund is intended to meet the obligations of maintaining the infrastructure and rewarding developers of the Commercium Platform and blockchains, as explained below. Donations to the Commercium Fund will also be accepted and help to enhance the product offering that the Commercium team actively develops for consumers and business users.

For funds from the Commercium Fund to be released for Commercium development and/or special projects, until further notice the founders will be required to reach majority consensus approving these initiatives. All internal and external proposals from contributors to Commercium will require a contract that outlines the specifications, goals and deliverables. Projects that do not benefit or further develop Commercium, driving to its core values of simplicity, security, accessibility, seamless integration and open source development, will be rejected.

As Commercium will be an international, not for profit organization and open source platform, transparency is essential to building trust with adopters, regulators and lawmakers. Quarterly, Commercium will ensure that its finances are made public for any interested parties to review. In addition, a Board of Trustees will be formed to ensure that the directives and core values of Commercium are upheld.

Decentralization And Governance

Decentralization is a contentious subject and productivity is not possible without still having an administrative function to continue to drive the platform forward while maintaining transparency and open source development. Furthermore, it is our belief that the concept of decentralization is generally misunderstood and doesn’t pertain so much to the governances or possible corporate hierarchy of an organization, but instead, decentralization is the manner in which a blockchain is run as a peer-to-peer, distributed ledger network, versus privately.

Commercium will advance with the participation of community members who work with the administration to continuously improve the dual-chain platform and its offerings. In 2018 Commercium will begin recruitment for the development team, seeking applications from individuals of all disciplines - programming, finance, law, business, media and marketing - to accelerate platform development. The platform will continuously evolve to meet the demands of its international user base and keep up with the changing technology and regulatory landscape.

Use Cases And Practical Application

Fostering and supporting practical use cases is paramount to the Commercium mission. The community will explore, develop and execute viable means to apply the Commercium Platform for everyday use. Entertainment, gaming, peer to peer transactions, and basic commerce activities will be developed by members of the Commercium community using the open source codebases.

Gaming

- Engage developers with a way to reward their users for participating in their platform.

Entertainment

- Engage entertainment and attraction businesses, such as arcades, festivals, restaurants and venues offering a new means for customers to enjoy their products and services.

Transactions and trade

- Commercium will target local businesses and consumers, offering new methods for payment and settlement of transactions in exchange for goods and services.

E-Commerce

- Plugins will be developed allowing online shops to offer Commercium as a method of payment.

Private messaging

- CMM is a genesis of the ZeroCoin Protocol and an inherently privacy-based asset. Instant messaging will be explored using the Wallet interface.

CMM may not be able to achieve the above listed use cases. CMM may wish to pursue other opportunities and applications of the platform. The possible use cases listed above are intended as an example and may not be fully implemented in the future.

Regulation

The regulatory landscape is continuously evolving and different around the world. Of late, some governments have shown strong opposition to cryptocurrencies and assets, while others simply want to impose consumer and investor protections, better define the new industry and ensure that taxes owed are actually being paid while reducing or eliminating criminal activity.[25,26] Regulation and guidance from lawmakers will take some time to be realized and applied, but given the attitude of world leading nations, this road block will be removed over time and to the benefit of the cryptocurrencies, assets, blockchain technologies and their adopters.

Commercium hopes to work with regulators and lawmakers wherever possible to help guide a seamless transition and the adoption of blockchain technologies as vehicles for the transference of value by consumers and businesses around the world. In order to begin facilitating this, the Commercium Wallet application will focus on immediately offering a simple record keeping tool that will output the information necessary for consumers and businesses to meet their essential income reporting needs.

---

[25] Sharp;, Alastair. “Canada regulators say most crypto currency offerings need oversight.” *Reuters*, Thomson Reuters, 24 Aug. 2017, www.reuters.com/article/us-canada-regulation-digital/canada-regulators-say-most-crypto-currency-offerings-need-oversight-idUSKCN1B42CA.

[26] “SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities.” *SEC.GOV*, Securities and Exchange Commission, 25 July 2017, www.sec.gov/news/press-release/2017-131.

Conclusion

Commercium is the first not for profit organization and open source development platform that focuses on consumer level adoption. Ease of use, privacy and security will drive accessibility, evolution, and adoption of blockchain technologies and new payment mediums by everyday people. Eliminating the misconceptions and learning curves that bar entry into the space is the objective of the Commercium Platform. The development team is dedicated to creating an all-encompassing, secure, “push of a button” software platform that integrates CMM and CMMX blockchains to facilitate commerce, execute business agreements and value transactions. Commercium strives to contribute to blockchain technology and the next wave of implementation.

Historically, technological advancement resulted in rapid progress in the fields of science, medicine, law, economics, infrastructure and wealth distribution. For example, E-trading was introduced to the masses in the early 1990’s and brokers, firms and fees were reduced or removed from the process of investing in capital markets. Retail investors were able to independently manage equity holding, retirement funds and save massive amounts of money from fees that were cost prohibitive to potential investors. E-Trading made capital markets accessible and efficient. It increased the rate at which money was able to enter and exit markets, reduced fees, increased liquidity, forced transparency and caused fairer pricing (tightening the spread of an assets value).[27]

This simple advancement and application of Internet technology - provided via a ‘digital interface’- changed the investment world with real-time, accurate and independent investing. Blockchain and distributed ledger technologies are the next technological revolution and the Commercium Platform will provide a new gateway that creates the same accessibility for individuals that e-trading, the personal computer and the internet browser did in the 1990’s.

Distributed ledger technology will create unity in commerce, increases profits, savings and efficiencies and is superior to private blockchains. Commercium brings functionality and ease of use to the masses.

[27] E-trading - https://en.wikipedia.org/wiki/Electronic_trading

Technical Specifications

CMM - Primary Blockchain (B2C & C2C)	CMMX - Secondary Blockchain (B2B)
Algorithm: Equihash ZeroCoin Protocol Block Time: 30 Seconds. Block Reward: 32 Maximum Supply: 210,000,000 (Two-hundred and ten million).	Algorithm: Ethash Fork: Ethereum Block Time: TBD Block Reward: TBD Maximum Supply: Unlimited

Roadmap

February 8th, 2018 marks the initiation of the CMM blockchain. Through simplicity and accessibility, The Commercium development team seeks to remove the steep learning curves and barriers to entry that have stalled mass adoption of blockchain and distributed ledger technologies. Each division of Commercium will simultaneously work to accomplish the platforms Roadmap.

Short Term

Administrative

- Incorporated as an International, not-for-profit, blockchain platform.
- Form a Board of Trustees.
- Work with Regulators, lawmakers and organizations to bring blockchain technologies to the mainstream.
- Recruit developers of all disciplines to advance the platform and product offerings.
- Continuously increase accessibility of the Commercium Blockchain Platform.
- Develop and engage with users and Community Supporters through educational materials, activities and events

Technologies

- Create web plugins and tools for integration in business and ecommerce for usability.
- Work with mining pool operators in a non-financial capacity to develop and maintain network infrastructure and accessibility.
- Develop easy to use wallet functionalities to enable everyday consumers and business.
    - Essential income & turnover reporting tools
    - Address book
    - Addresses (CMM/CMMX)
    - Smart Contracts
    - Multi-sig Escrow

    - Recurring Payments
    - Off Chain Transaction Alternative
    - Web Plugins and APIs for e-commerce

- Actively plan and develop the secondary, CMMX blockchain, providing smart contract and data capture functionalities for business to business commerce activities.
- Deploy CMM and CMMX dual-chain interoperability through the Commercium Wallet.

Together the divisions of Commercium will actively develop business initiatives, use cases and foster adoption, while simultaneously working with regulators and lawmakers taking the platform into its next five years of development.

Long Term

- **Continue to work with legal and regulatory bodies to drive mainstream adopt of blockchain and distributed ledger technologies.**

- **Encourage and support adoption of the Commercium Blockchain Platform use cases by businesses and entrepreneurs.**

- **Continued focus on Wallet development and business to business features through the CMMX blockchain.**

- **Accessibility of Commercium Blockchain Technologies through strategic partnerships and regulatory guidance.**

Glossary

Currency - a medium of exchange for goods or services within an economy.
Commodity - a marketable item produced to satisfy wants or needs.
Asset - represents a value of ownership that can be converted into cash.
Securities - interchangeable or negotiable financial instrument that holds some type of monetary value.
Capital markets - Markets for buying and selling equity and debt instruments.
Fiat - Currency which value is determined by government and free market.
Fee - represents an amount beyond the initial cost estimates, and reflects factors such as processing.
Volatility - the velocity at which the price of a given asset, security, commodity fluctuates and can denote risk.
Clearing - activities from the time a commitment is made for a transaction until it is settled.
Regulatory body - A government institution intended to protect consumers, prevent fraud and illicit activities.
Cryptocurrency, cryptographic asset - digital assets designed to facilitate transactions, monetary or otherwise, seek to solve a problem and provide another option to store and use value.
Blockchain - A series of records known as blocks are recorded in a chain where each additional record is dependent on the previous.
Distributed ledger technology - A blockchain supported over a vast decentralized network where there is no central server, body or node which it operates from.

Forward Looking Statement

The information contained herein is: (i) provided by the principal founders of the organization/entity and (ii) publicly available from directories, publications and websites, as mentioned in the body and the endnotes where possible or appropriate. In some cases, non-publicly available information was used, including independent research, studies or paid services from individuals and organizations. While the information set forth herein is deemed by the organization/entity to be accurate, the organization/entity shall not be held liable for the accuracy of or any omissions from this white paper, or for any other written or oral communication transmitted to recipients and any other party in the course of its evaluation of transactions involving the organization/entity.

Any person or entity seeking to make an investment in the organization/entity or the assets/technology should not rely on the information set forth in the plan as complete. In addition, the analyses contained herein do not claim to be appraisals of the assets, or the valuation of any entity. The organization/entity makes no guarantees regarding any benefits received from investment, nor the legal, tax or accounting effects of any transaction; and this white paper does not constitute an offer to sell, or a solicitation of an offer to buy securities.

In furnishing the white paper, the organization/entity undertakes no obligation to provide recipients of the white paper with access to any additional information or to update this white paper or to correct any inaccuracies that may be contained herein. There exists substantial information with respect to the organization/entity and its future prospects, and there are a substantial number of risks associated with an investment in the assets/technology, which are not set forth in the plan.

Furthermore, the potential fulfillment of ‘forward looking statements’ contained in the plan are subject to change due to unexpected events, market shifts, or circumstances that cannot be known at this time. Forward looking statements are based on expectations, estimates and projections at the time the statements were made that involve a number of economic, business, and numerous risks and uncertainties which could cause actual results or events to differ materially from those presently anticipated. Forward looking statements in the plan may be identified through the use of words such as, but not exclusively to: “expects,” “will,” “anticipates,” “estimates,” “believes,” or statements indicating certain actions “may,” “could,” “explore,” or “might” occur. Such estimates and projections are subject to significant uncertainties beyond the control of the organization/entity. Although such projections are believed to be realistic, no representations are made as to their ultimate attainability.