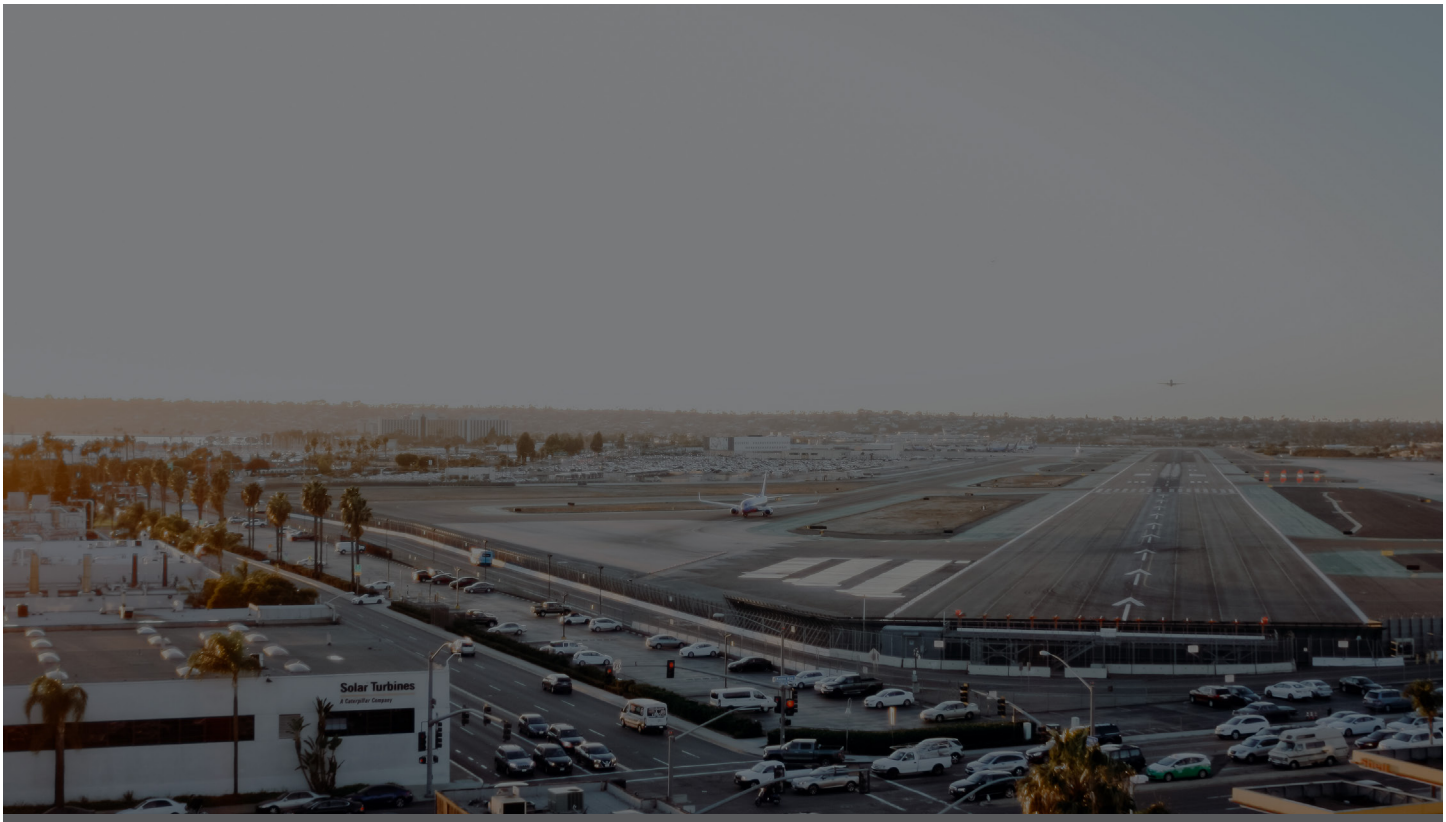


CRYPTOFUSE®

WHITEPAPER

CryptoFuse, Inc.
partnerships@cryptofuse.com
+1 (202) 734-7747
www.CryptoFuse.com

TABLE OF CONTENTS

ABSTRACT

Consumer demand for digital transfers have increased at an exponential rate, and while companies have raced to scale to these demands, one fundamental flaw remains. Without constant internet connection, these systems fail. Current industry-grade point-of-sale systems, as well as supply-chain management platforms are incapable of verifying transactions offline, resulting in an industry-wide Achilles' heel, resulting in millions of dollars of loss each year.

CryptoFuse® has solved this issue through our harmonized family of hardware and software solutions, **FuseWare**, which possess the ability to handshake data offline, and update existing ledgers asynchronously when reconnected. The ability to verify data offline is fundamentally new, and opens up a world of possibilities for existing systems.

HISTORY

The internet, as we know it today, is a massively complex system of data transfer that has ushered in a new era of communication. Behind its complexities lie vast networks of information flowing between committed nodes, with computers and smartphones serving as access portals for users to experience the global web. Though it makes up a backbone of daily lives now, it wasn't always this way. Efficient networking and packet transfer systems were designed in recent memory, and the "World Wide Web," as users have grown accustomed to calling it today, was but a handful of research laboratories only decades ago.

Each hurdle to adoption has been solved in turn by some of the brightest minds in science and mathematics, often with funding and oversight from forward-thinking governments and militaries. Each iteration has grown the scale of the internet to levels unthinkable by some even in recent memory. From early "Hello World" tests, to live video, the internet has become one with consumers, furthering our appreciation of technology, and shaping our society.

Though the internet has caught up to the pace of our everyday lives, and even surpassed them in certain cases, it is only as strong as the relays that connect it. Its power cannot expand past its physical limits, and ceases to exist in "dead zones." With a growing amount of users transacting highly sensitive data online, up-time becomes critically important. "offline" transaction models, until now, force users to hope that their transactions are valid, pushing risk factors to all-time highs.

As many major tech companies race to figure out how to expand their functionality online, none have been able to crack the code of real-time, secure, internet-free transactions. This significant challenge has finally been solved, and a new era of internet awaits.

THE CRYPTOFUSE TEAM

Andrew Wayne Couch
Founder & Interim CEO

The invention of **CryptoFuse** begins with founder Andrew Wayne Couch. As a US Army combat veteran with over 11 years of experience inventing, building and scaling companies, Andrew has validated himself to be a proven leader in the emerging tech space. While deployed in Kosovo and Afghanistan, Andrew was trained on encryption and location-based communication systems such as the Blue Force Tracker *FBCB2. This hands-on experience with military-grade technology contributed to the creation of BlockMesh. Following his service, Andrew founded Candy Lab AR, a revolutionary AR platform that used 3D location-based Augmented Reality on top of a proprietary code base coupled with it's own 9-Axis Sensor Fusion Engine. In 2012, Candy Lab AR launched its first of many AR apps (Cachetown). He is a sought after speaker on Augmented Reality, Blockchain, and future technology, and has been featured in Mashable, Adweek, VentureBeat, Forbes, etc and is the recipient of multiple Addy awards. Andrew spearheaded national legislation that made AR more accessible to developers in CandyLab vs. Milwaukee. He is also an alum of the 2015 Blue Startups Accelerator and the 2012 Arch Grants Incubator. **CryptoFuse** is his 3rd tech startup, The first one being yourplates.com which launched in 2007 and sold to Bump.com in 2010 under the name Platester.com.

Continued

The CryptoFuse Team (Continued)

C. “Gunnar” Teague
Chief Technology Officer

Gunnar has been involved with the blockchain community since 2010, building and maintaining over 100 separate mining rigs since that time. He is an established member of the crypto community and has work experience as a security consultant for numerous crypto organizations. Gunnar created a distinct implementation of the SHA-256 in Python and performed research into the other cryptographic algorithms used in Bitcoin. He has most recently worked in a research capacity at Oklahoma State University. His expertise with electrical engineering extends to his time at Sandia National Laboratories and Textron Systems. For that work, he was granted a DOE-L clearance. He has also experimented and built apps using Augmented Reality and Unity, with his most recent app being featured in the Google Play store. Gunnar was instrumental in the invention of the **BlockMesh**, the world’s first asynchronously updating blockchain.

Continued

BLOCKMESH & OFFLINE BLOCKCHAIN

There are two primary issues with an offline blockchain. First is the issue of synchronization: how do you prevent wasted work and energy as you attempt to reconcile the chain and bring it back online? Second is the issue of double spending: how do you verify that the transaction has not already been spent to another party without the ability to see the entire blockchain at once? And how do you prevent someone from trying to double-spend if they put the double spend online first?

The first question is solved in software, rather than relying on a traditional blockchain protocol, **CryptoFuse** solutions will use a '**BlockMesh**' for the public record structure. This way when multiple independent offline **BlockMesh** are reconciled, instead of conflicting with each other and wasting resources they instead combine together and strengthen each other. Due to this model, **CryptoFuse** devices can be used both offline and online at the same time since a **BlockMesh** chain can be updated asynchronously, unlike a standard blockchain.

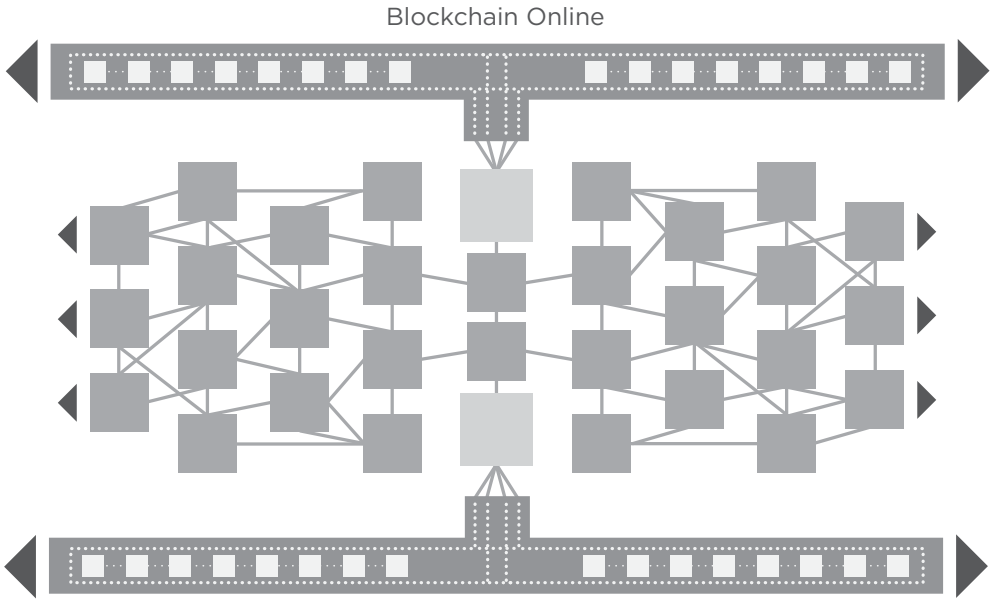
When offline, **Fuse** takes advantage of the day-to-day interactions of their users to create a high-latency mesh network and keep users' devices synced and up to date without having to actually bring them online. Each new block created, either offline or online, connects to multiple previous blocks, which naturally tie together and strengthen the **BlockMesh**, which would otherwise branch infinitely and become useless. Utilizing both a software **BlockMesh** and physical mesh network allows **CryptoFuse** devices to operate in spaces otherwise impossible for legacy devices.

Continued

BlockMesh and Offline Blockchain (Continued)

The second question: While **CryptoFuse** devices are online, traditional methods are to prevent double spends. When offline, these devices uses our proprietary operating systems to prevent and detect when a malicious party attempts a double spend. Each device will fully synchronize with the other before transacting, and the transaction is immediately added to the **BlockMesh** using a modified Proof-of-Work (PoW). This and various other methods are used to prevent double spends as well as identify non-official hardware. In short, it is through the predictability of hardware rather than software which is used to provide security offline.

The **BlockMesh** protocol in its current form utilizes a modified Proof-of-Work (POW) consensus mechanism. Our team has plans to move to a new, proprietary consensus mechanism, known for these purposes as Proof-of-Interaction (POI).



PROOF-OF-INTERACTION (POI)

Proof of interaction: In order to reach consensus, a **BlockMesh** with offline tx's cannot use traditional methods, since it requires a single node to be aware of the entire network state at once.

In order to address this, **CryptoFuse** has invented a new consensus model, known here as Proof-of- Interaction (POI).

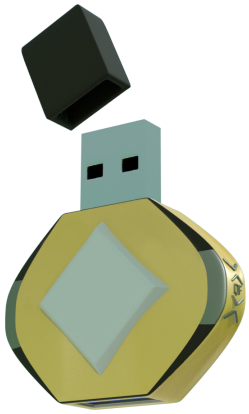
POI allows each **Fuse** device to mine its own tx's, and rewards them at a scaled rate related to how much offline transactional data it contributes to the online network.

THE FUSEWARE™ FAMILY OF SOLUTIONS

The FuseWare™ family of solutions includes both hardware and software systems. This is currently comprised of the Fuse, FusePro™, FuseAPI™, and FuseGo™ (mobile app).

These products can work harmoniously, or separate, to complete their stated objectives.

FUSE



What is the device?
Allows the user to securely transmit transactional data offline through use of digital representative containers.

Stores a small portion of the **BlockMesh** and offline transactions to be shared with other **Fuse** devices. **Fuse** needs to be paired to a user's mobile device in order to work.

Comes with proprietary hardware security (small screen, numpad for pin) which prevents a compromised phone from transacting without your permission. **Fuse** needs to be in range of bluetooth in order to transact.

How it integrates/interacts with other FuseWare devices?
Do you need other **FuseWare** devices to be operational? No, a user only needs **FuseGo** (mobile app) to interface.

Can it sync small amounts of the **BlockMesh** with other **FuseWare** devices? Yes, it is inherently capable of interfacing with other **FuseWare** products.

Can it sync much larger, or all of the **BlockMesh** when online? Yes, it can do a full refresh that will update the online ledger to its most recent state.

Use cases:
The **Fuse**, when paired with a mobile phone via the **FuseGo** app, is intended to work for supply chain tracking, identity/2FA, and consumer financial transactions.

The **Fuse** can also accommodate cryptocurrency transactions, when approved cryptocurrencies are transferred to proprietary **CryptoFuse** digital containers.

FUSEPRØ™

What is the device?
Allows users to securely transfer transactional data offline or online.

Stores a large portion of the BlockMesh and offline transactions to be shared with other **FuseWare** devices.

Does not require an additional app or mobile phone and in future iterations will accept traditional payment methods, such as credit cards.

Possesses the capability to upload other FuseWare device data to the **BlockMesh**, when online.

How it integrates/interacts with other FuseWare devices?
Do you need other **FuseWare** devices to function? No, the **FusePRO** can function autonomously.

Can it sync part, or all of the **BlockMesh** with other **FuseWare** devices? Yes, and it can, in turn, upload that device's transactional data to the **BlockMesh**.

Why would a user choose a **FusePRO** over another **FuseWare** device? The **FusePRO** comes native with a vastly expanded device memory storage, allowing it to complete its tasks offline for longer duration, and ensuring the longevity of the device. The **FusePRO** will also allow for QR codes to be utilized, making it a perfect unit for supply chain situations.

Continued

FUSEPRØ™

Use cases

When unloading a truck to a warehouse or signing for cargo off of ships, trains and planes a user may not have the best online connection or no connection at all when signing for the cargo or product. With the **Cryptofuse** technology a Supply Chain user can use the onboard camera on **FusePRO** with its extra memory and is able to scan and log transactions all day long, once the user has an online connection the online ledger will update due to the fact the authorized handshake took place previously with information on date, time and other various records.

Business financial transactions

The **FusePRO** is perfect for businesses that currently use Square or similar point of sale systems For the same price the merchant can take debit and credits cards when connected online, get rewards for being part of the network as well as take offline crypto payments without the worry of double spending.

FUSEAPI™

What is the product
Allows access and browsing to the **BlockMesh** and the blocks.

Allows custom software to interface with the p2p network.

Allows custom data to be added to the blocks (smart contracts) *example of custom data.

FuseAPI™ will allow any native app to work with the **Cryptofuse** technology. By updating a native app with **FuseAPI** the developers application will be able to transact with other **Cryptofuse** devices that has an offline or online connection.

Use cases:
Merchant solutions, existing payment processing systems.

STEP BY STEP OF AN OFFLINE TRANSACTION

Step through of an offline transaction process between two parties: (It should be noted that like in the other cryptos it's possible to send data without two parties concurrently present)

Senario
You're on a road trip with a friend and you want to contribute to the gas fund but have no cash. However, there's no sell service so you can't Venmo him. But hey! You and your friend have shiny new **Fuse** you want to try out!

If you want to transmit something of value, the **Fuse** device must be loaded with it beforehand like a debit card this, however, is not necessary for the transmission of logistics data.

The user then inputs the data they want to add to the container in the **FuseGo** app.

The **FuseGo** app then transmits this data to the **Fuse**, which both the user and the **Fuse** verify before the Fuse signs the message.

Once the message is signed the **Fuse** returns it to the **FuseGo** app.

Key point
By keeping the blockmesh, private keys, and signing process on the **Fuse** it keeps the user honest even in financial transactions. By allowing the user to visually verify each transaction signe dit prevents malicious software on the phone from compromising the system.

The signed message is then transmitted from one phone to the other, where it is then relayed to the the 2nd party's **Fuse** to be verified once again. Note that the signed message is stored on both Fuse's either of them can later connect to an online node to share it with the rest of the network.

FUSEGO™

FuseGO™ is the proprietary app of the **FuseWare** line. **FuseGO** connects to the **Fuse** device to provide the online capability that the device itself lacks.

FuseGO is a management app allowing for the **Fuse**, or connected device to interface with the online **BlockMesh**.

The technology and process comes from **FuseAPI**, with the exception that the **FuseGO** IOS and Android app is owned by **CryptoFuse**. It serves as the first operational app using the FuseAPI, and showcases development potential to others looking to include **FuseWare** solutions in their architecture.

CONCLUSION

Within the past few years, the world has witnessed exponential growth in digital transfers, yet one fundamental flaw in the system has resulted in failure of transaction verification, and the unnecessary loss of many millions of dollars – **continuous internet connection**. Current industry-grade PoS systems, as well as supply-chain management platforms **DO NOT** have the ability to authenticate transactions **offline**. Until Now!

CryptoFuse had recognized this significant global issue, and solved it. Our **FuseWare** family of solutions perform – offline ultra-secure data transfers, and online asyncronous ledger reconciliation – opening the potential for existing systems, and the increase to your bottom-line.

Secure. Internet-free. Transfers.

DEFINITIONS

Blockchain
A peer-to-peer linked digital ledger in which data can be added and stored in a distributed manner using cryptography.

ByteChain
As ByteBlocks are opened from the Micro Miners, a ByteChain begins. This is similar to a blockchain, except the ByteChain is designed to work both offline and online.

ByteDrop
A functionality similar to an AirDrop, but designed explicitly for crypto containers, using a device called a Fuse.

Closed Protocol - A state when ByteBase is the only exchange for its ALTBytes (formerly known as ALTCoins).

Micro Mining
The process by which transactions are verified and added to the online public ledger, known as the ByteChain.

Open Protocol
The ByteBase Exchange when it is connected to other Exchanges.

Smart Contracts
A computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties.

Supply Line Data
Supply data that normally would require an internet connection can now be encrypted and work offline and reconsilited when an internet connection is available.