Cryptocurrency Volatility Removal via Crypto-Asset Baskets

September 19, 2017

Daniel Rice
drice@greenmangosystems.com

This paper describes a mechanism for using a diversified set of crypto-token assets to create a faster, safer, more flexible, and reliable solution to the bitcoin volatility problem.

1. Background

Bitcoin and other similar cryptocurrencies provide transaction network to send digital cash worldwide. This paper will focus on a Bitcoin solution that will be applicable to many other cryptocurrencies as well.

While Bitcoin, the transaction network, has remained secure and reliable for nearly 10 years, bitcoin, the currency, has exhibited extraordinary price volatility. The 30-day rolling bitcoin price volatility index has often been over 10%.[1] While some bitcoin users may desire exposure to bitcoin price movements, this high level of volatility makes it a poor store of value which negatively impacts its usefulness in many common use cases and hinders its wide adoption.

Example use cases that rely upon continued bitcoin price volatility (not applicable to this solution):

1. High frequency bitcoin trading including futures
2. Speculatively investing in bitcoin as a source of value growth

Example use cases that rely upon bitcoin to maintain a stable store of value (applicable to this solution):

1. Escrow transactions (e.g. wage, real estate) using multi-signature
2. Mobile bitcoin wallets for day-to-day spending
3. Merchant accepting bitcoin as a form of payment
4. Smart Contracts

There are three types of volatility mitigation schemes currently being applied to bitcoin:

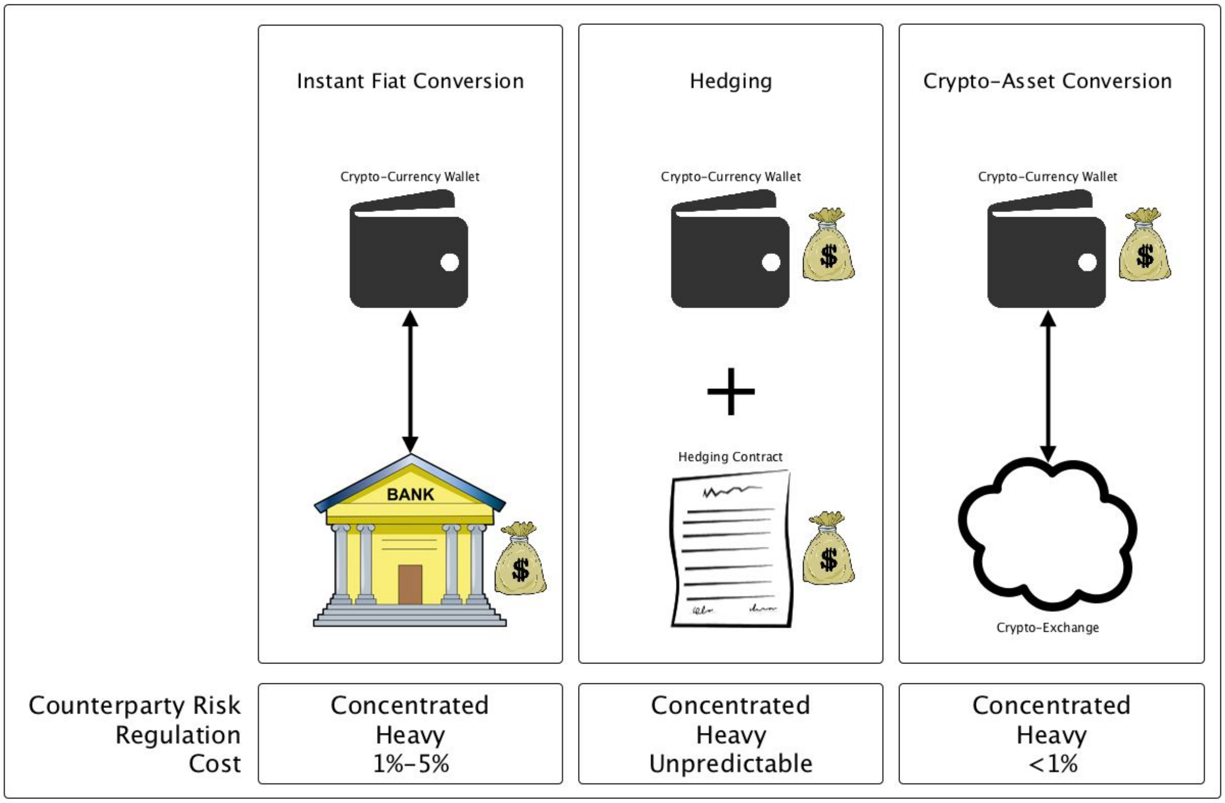
1. Instant Fiat Conversion:
   Solutions such as Uphold, BitPay, and Coinapult convert a client's bitcoin into a currency of their choosing.
2. Hedging:

[1] http://btcvol.info

Bitfinex is an example of services that allows a client to eliminate volatility through various derivative or smart contract solutions.

3. Crypto-Token Assets:
   Tether (USDT), Bitshares (BitUSD) allow you to trade bitcoin for crypto-token assets that attempt to emulate a specific fiat currency or other traditional asset such as gold. The solution described in this paper utilizes crypto-token assets.

Bitcoin Volatility Locking Solutions



	Instant Fiat Conversion	Hedging	Crypto-Asset Conversion
Counterparty Risk	Concentrated	Concentrated	Concentrated
Regulation	Heavy	Heavy	Heavy
Cost	1%-5%	Unpredictable	<1%

1.1 Instant Fiat Conversion

Instant fiat conversion solutions allow merchants to accept bitcoin for payment without any risk of volatility. For a merchant, the experience mimics that of a credit card network. Their customer pays using an electronic payment system, whether bitcoin or credit card, and the merchant receives a fiat payment for the corresponding amount to their bank account.

The drawback of this approach is that the merchant cannot take advantage of the other benefits of bitcoin, such as decentralized instant worldwide payments or multi-signature address protection, because bitcoin is instantly converted back into fiat. Companies developing this type of system are also highly subject to the growing body of bitcoin regulation since it involves taking possession of and transacting fiat currencies on behalf of clients. This approach also requires the use of traditional bank accounts, following tax regulations and in some cases AML/KYC.

1.2 Hedging

Hedging provides a more short term, often contract-based approach to managing bitcoin volatility. The advantage of this method is that it allows a client to continue to hold bitcoin while minimizing the risk of the volatility—one could still take advantage of the technological advantages of bitcoin without the volatility concern. Conversely, hedging approaches are more expensive and have a residual usage cost usually measured as a percentage of the total asset size and the relative market volatility risk. For this reason, hedging is only practical for short and well defined time frames.

1.3 Crypto-Token Assets

Crypto-token assets are a cryptocurrency-based token with issuance controlled by the asset issuer. These monetary devices are an evolution of the Bitcoin protocol made available through extensions such as Mastercoin, Counterparty, and Ripple. Each specific crypto-asset is generally issued by a company on a single extension network of their choosing in the same way that traditional companies issue shares onto an individual stock exchange such as Nasdaq or NYSE. Crypto-token assets can function as a volatility solution for Bitcoin through a rapid exchange of bitcoin for a fiat denominated crypto-asset. As an example, Bitstamp offers a USD-denominated asset on the Ripple network that can be purchased on the open market but can also redeemed 1:1 for USD through Bitstamp.

Crypto-token assets generally have the following benefits in common with bitcoin:

1. Instant worldwide transfer
2. Multi-signature address features
3. Pseudo-anonymity
4. Assets private keys stored locally on your computing device

Crypto-token assets have the following drawbacks in comparison to Bitcoin:

1. Asset value subject to centralized asset issuer solvency
2. Asset value subject to centralized asset issuer reliability

In summary, the advantage of these assets is that they carry some of the benefits of Bitcoin technology. The disadvantage of using a fiat crypto-asset is that each asset’s value is centrally controlled by the issuer. For example, Bitstamp Ripple USD crypto-token assets only hold stable value as long as Bitstamp continues to allow them to be exchanged 1:1 for USD.

2. A Proposal for Crypto-Asset Baskets

We propose that by diversifying the purchase of crypto-token assets, a client is able to mitigate the counterparty risk concerns associated with using centrally issued crypto-token assets. Beyond Bitstamp, which was mentioned previously, there is a growing list of reputable 1:1 fiat crypto-asset issuers. By diversifying purchases amongst many asset issuers, clients can limit their exposure to any single provider and thus limit their risk of losing asset value due to failure of the underlying issuing entities.

This approach provides the following features:

1. Flexibility
    a. Multi-sig support for escrow transactions
    b. Instant conversion from bitcoin to fiat crypto-token assets
2. Safety
    a. Client holds funds locally in a crypto client wallet. The service cannot initiate a transaction.
    b. Centralized online service does not contain the information required to steal the client's funds
    c. Client's risk is minimized through diversification of assets
3. Recovery
    a. Client can export and exchange assets even if the service is shutdown
    b. Client can restore from a single master key if their client computer or wallet software becomes damaged

2.1 Crypto-Token Asset Selection Criteria

The selection of crypto-token assets utilized in a client wallet crypto-token asset basket will change and grow over time as the available options evolve. For this reason we propose criteria by which we will select these assets manually:

1. The asset is fiat backed 1:1.
2. The asset has consistent liquidity greater than our peak volume.
3. The asset consistently trades within .5% of the corresponding backed fiat price.
4. The issuer is reputable, meaning the entity owners are known and the entity has a good reputation in the industry.

Using this criteria, we have selected the following assets as acceptable:

- Bitstamp Ripple Fiat Assets
- Tether Fiat Assets

We have deemed the following assets unacceptable:

- BitShares USD

- NuBits USNBT

As mentioned previously, we believe that the assets in both of these lists will continue to grow in the coming years, allowing for a marked increase in diversification.

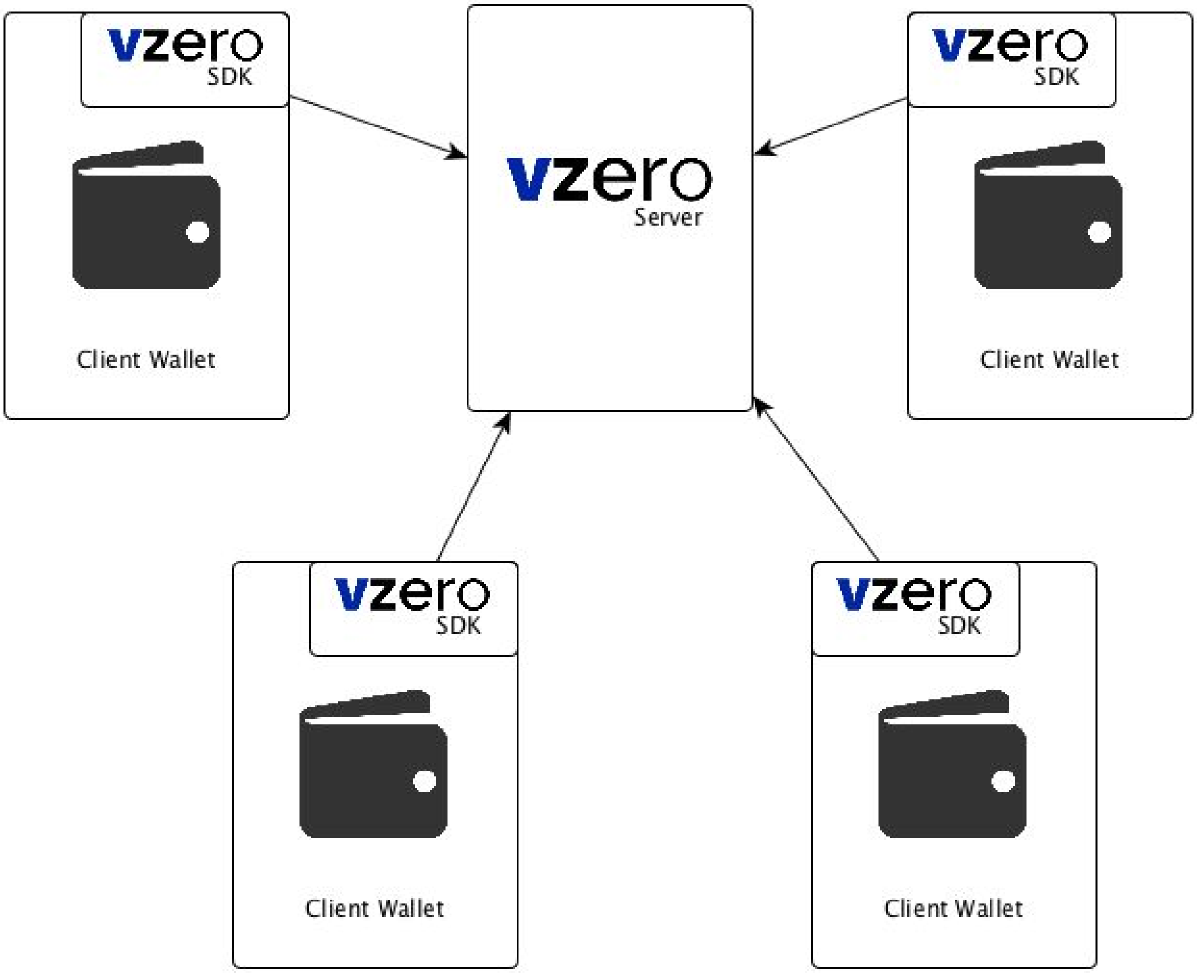
3. vzero System Architecture

vzero is a concept for a system architecture. The system is comprised of a client integrated SDK as well as a server component. The SDK is open source and designed to be a trusted component for a client that eases integration of vzero into their existing architecture. The SDK code limits counterparty risk by treating the vzero server as an untrusted party. For this reason a client's private keys are never transmitted to the vzero server. Furthermore, the SDK can independently run its own approval process such as querying third party exchanges to verify that the vzero server is providing a reasonable exchange rate before accepting a transaction. In a similar manner, other clients on the network are treated as untrusted parties as well. Much like the architecture of the Bitcoin network itself, anyone is free to write their own SDK implementation, but most clients will opt to use an existing implementation since it cuts down on the development and testing involved in using the network.

vzero's SDK communicates directly with the vzero server. The vzero server creates an order book to facilitate trades, but never takes control of any assets directly. The exchange of assets happens in a trustless fashion between the parties. The specific details of the trustless exchange are not covered in this document, but for reference can be implemented in a similar manner to those used by CoinShuffle[2], or Lightning Network atomic swaps.

[2] http://crypsys.mmci.uni-saarland.de/projects/CoinShuffle/coinshuffle.pdf

Architecture Overview



3.1 Exchanging Bitcoin and Crypto-Token Assets from the Client Perspective

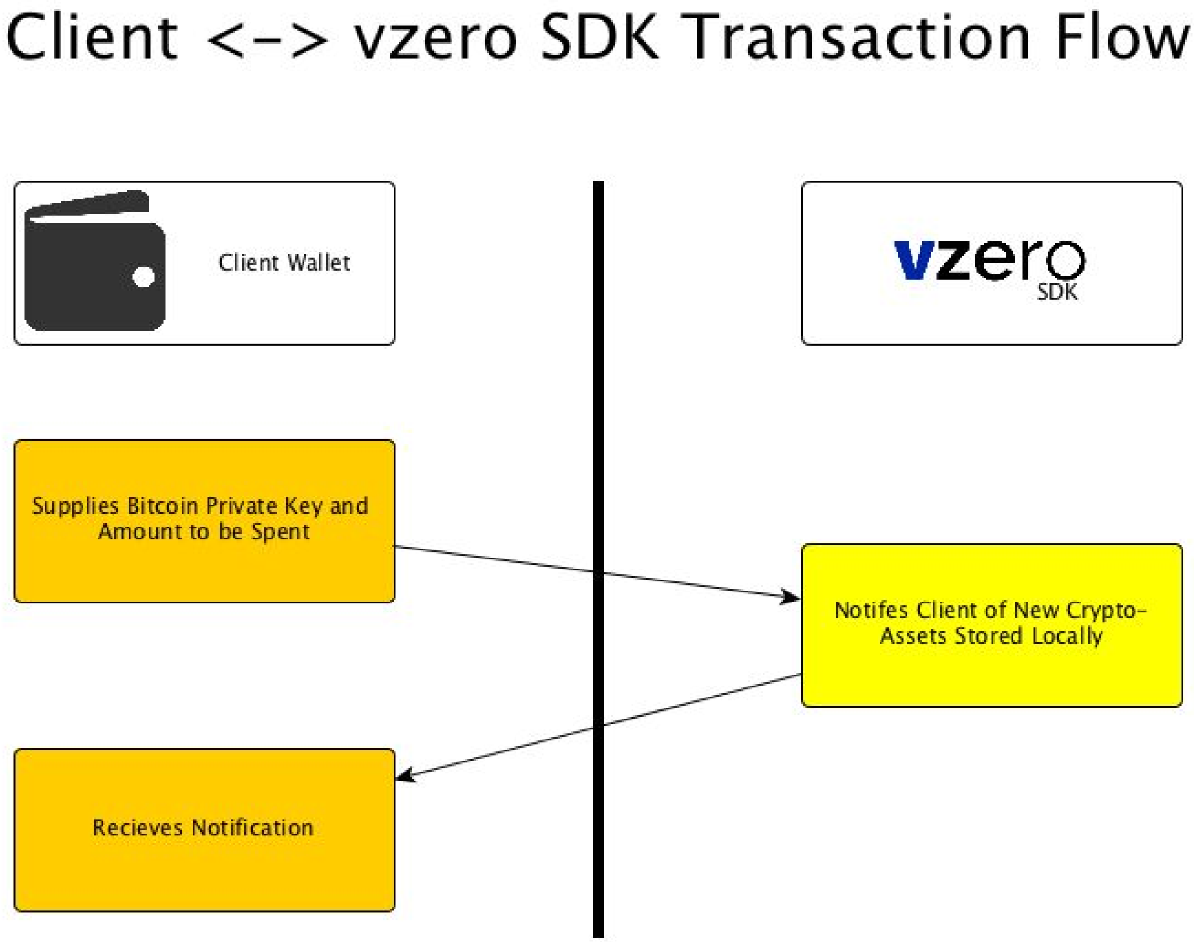
In this section, we detail a simple example of how client applications can exchange bitcoins for crypto-token assets through a market order using the vzero SDK.

The client initiates an exchange by taking the following action:

- Supplies the SDK with private key associated with a bitcoin address and the amount of bitcoins to be spent from the given address

vzero SDK ends the transaction by:

- Notifying the client of the new crypto-token assets stored locally


Client <-> vzero SDK Transaction Flow
Client Wallet
vzero
SDK
Supplies Bitcoin Private Key and Amount to be Spent
Notifes Client of New Crypto-Assets Stored Locally
Recieves Notification

This example demonstrates the simplicity of using the SDK. The SDK takes a number of additional steps on behalf of the user to complete the process. These steps include:

- Buy/Sell order submittal
- Fair price verification
- Asset packaging for local storage
- Crypto-currency address creation
- Contract verification and gatekeeping

4. Instant Atomic Crypto-Currency Exchange and Double-Spends

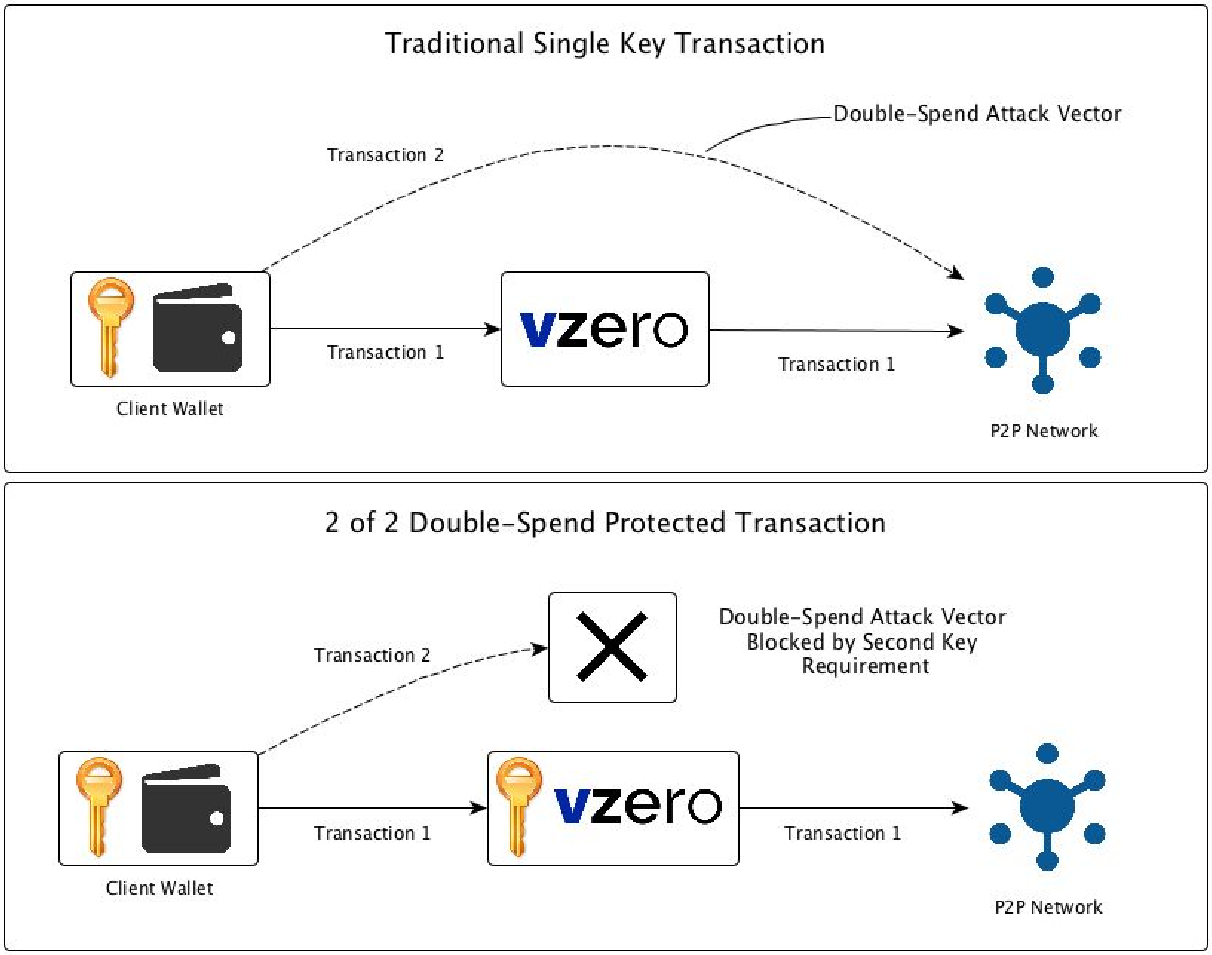
Instant transactions are a necessary and important feature for this service. A new Bitcoin block is added to the blockchain about every 10 minutes. Full transaction confirmation takes an hour on average.[3] This service must process transactions in less than one second to be competitive

[3] http://bitcoin.org/bitcoin.pdf

with existing payment methods such as credit cards, but this puts the service at risk of double spend attacks since transactions need much more than one second to confirm. There are 3 main ways for a vzero service provider to remove double-spending risk in transactions:

1. Know the customers, so that they can be held liable for any double-spends they create
2. Use 2 of 2 multi-signature addresses with the client holding one key and vzero or another trusted third party such as GreenAddress.it[4] holding the other. This approach allows for both parties to verify and approve each transaction.

Using 2 of 2 Muti-Signature to Block Double-Spends



3. CheckSequenceVerify Payment Channel Atomic Swaps[5]

[4] https://greenaddress.it/en/faq/

[5] https://bitcoinmagazine.com/articles/atomic-swaps-how-the-lightning-network-extends-to-altcoins-1484157052/

Payment Channel Atomic Swaps are the most logical solution for their speed, and lack of transaction counterparty risk of any kind.

5. Other Applications of Crypto-Asset Baskets

While this document focuses on locking crypto-token assets to a specific fiat currency, the same asset-basket approach and transaction system can be used for a number of different purposes such as:

- Multi-fiat currency diversified crypto-asset baskets
- Altcoin investment diversification