ASSET HIGHLIGHT: BITCOIN

Bitcoin has already proven to be a disruptive economic force, a fact that has at least partly driven a substantial increase in price, market-cap and transaction volume of the platform's core token, bitcoin.

In addition to its potential as a platform, Bitcoin has also emerged as an investable crypto-asset.

To properly assess the investment potential of this emerging asset, we need context. In the following document we provide said context via: a quick overview of the platform and its component parts; a discussion about current and future growth drivers; an examination of price, volume and transaction trends; a look at bitcoin as a portfolio tool; and finally a brief overview of some of the largest risks to the platform.

CoinShares Research

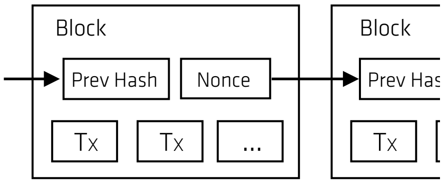
TABLE OF CONTENTS

None of the commentary or analysis contained herein is meant to constitute financial advice. This document is meant to be used as a foundational guide to Bitcoin and its potential. All analysis is meant to provide emerging trends and observations that may offer value in developing your own investment thesis, though past performance is not indicative of future performance. Please consider all risks carefully prior to making any investment, especially in an evolving asset like bitcoin.

VISUAL TABLE OF CONTENTS

pg. 9

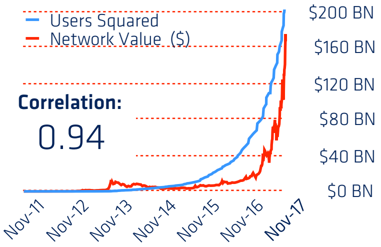
Simplified Block Constituents



To win a block (and the bitcoin reward), a miner must run the information from the previous block through a hashing algorithm, then combine the hash with information from all the valid transactions it intends to include in the next block, plus a number called a nonce, and hash the combined input again. The hash output of these three components combined must equal a number below a certain numerical threshold for the network to accept the block as valid (Fig. 1).

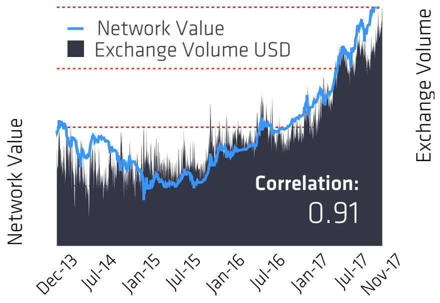
pg. 11

Network Growth vs. Value ($)



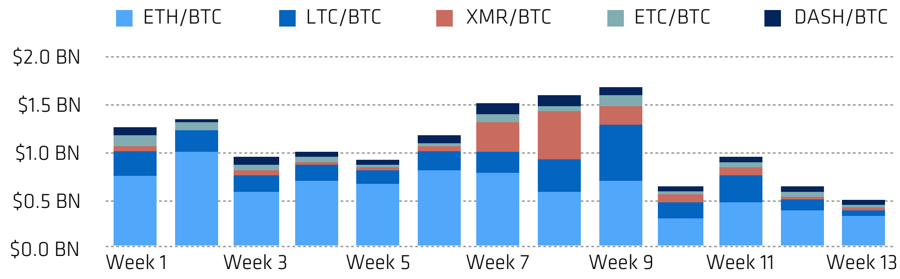
pg. 15

Network Value vs. Exchange Vol. $



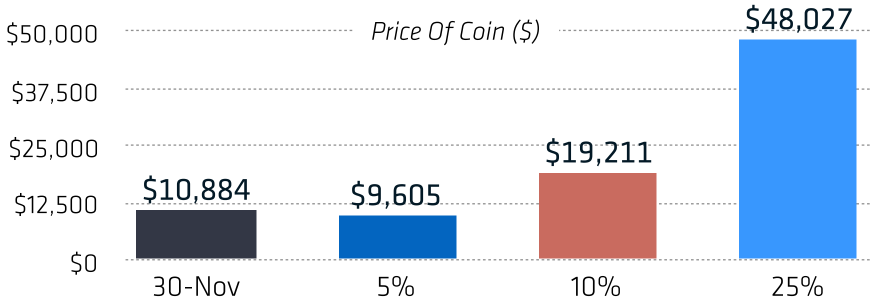
pg. 13

Q3 17 Weekly BTC ($) Volume By Trading Pairs - Top 10 Exchanges by Volume



pg.16

2022 Min. BTC Price Req. to Facilitate 5%, 10% or 25% of Global Stored Value



pg. 17

Bitcoin Annual Returns

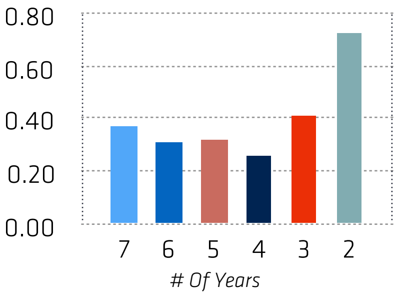
2011	2012	2013
1733%	144%	5474%
2014	2015	2016
-58%	37%	131%

2017 TD	991%

As of: 30-Nov

pg. 18

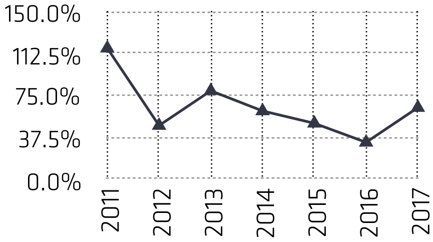
7 - 2 Yr Sharpe Ratio Of Bitcoin



pg. 18

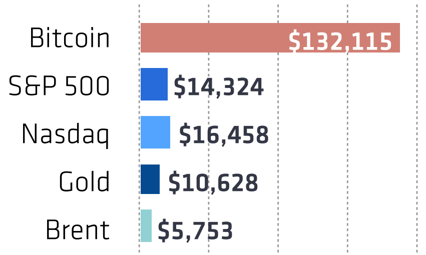
Bitcoin Volatility 2011 - 2017

30-Day Rolling Annualized Standard Deviation of Daily Returns



pg. 17

Performance Of $10K Invest In 2014



WHAT IS NEEDED IS AN ELECTRONIC PAYMENT **SYSTEM BASED ON CRYPTOGRAPHIC PROOF INSTEAD OF TRUST,** ALLOWING ANY TWO WILLING PARTIES TO **TRANSACT DIRECTLY** WITH EACH OTHER **WITHOUT THE NEED FOR A TRUSTED THIRD PARTY**

SATOSHI NAKAMOTO
BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM

BITCOIN BACKGROUND

The first public version of the Bitcoin whitepaper was published 31 October 2008 on the metzdowd.com cryptography mailing list. Its title was *Bitcoin: A Peer-to-Peer Electronic Cash System* [1]. Being but one of a vast multitude of digital money proposals circulating on the mailing list at the time, at first, the paper received only limited attention and enthusiasm from the community.

THE LEGEND

Like many other schools of thought, the creation history of Bitcoin has taken on a certain mythical quality, made possible only through true mastery of cryptography:

Legend has it that Satoshi Nakamoto began working on the Bitcoin protocol in early 2007, during the final phase of the great bull run of the 2000's. Although recent, its entry into the realm of legend stems from the seemingly flawless anonymity techniques employed by Bitcoin's mysterious creator. Even though Nakamoto is on record claiming to be a man born on 5 April 1975, living in Japan [2], and communicated extensively with multiple members of the Bitcoin community, he left no definitive evidence linking himself to any verifiable identity. This has lead to the now common belief that the name is in fact a pseudonym, perhaps even for an entire working group.

At the time, Nakamoto volunteered few if any clues to the public regarding the existence of the Bitcoin project, but retrospective analysis has still enabled a fairly comprehensive event timeline to be reconstructed. The first significant event in Bitcoin's public history is probably the registration of the bitcoin.org domain on 18 August 2008. Around the same time, Satoshi was communicating with known members of the Cypherpunk community on whose inventions Bitcoin partially rests, notably including Wei Dai and Adam Back, inventors of b-money and Hashcash, respectively. None of them admits to knowing Nakamoto's identity. [Continued >>]

The Bitcoin codebase was first released November 9, 2008 on SourceForge.net as an open source project available for contribution by anyone interested and otherwise capable of persuading the community of the utility of their code.

Finally, Bitcoin went live on 3 January 2009. The genesis block included the now famous message "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" [3] as part of its coinbase parameter (more on the coinbase later), as well as the first ever bitcoin transaction: a 50 BTC mining reward sent to the address 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa. Nakamoto's choice of text inclusion has been interpreted in several ways including as a critique of fractional reserve banking and the current monetary system, but what it certainly proves beyond any doubt is that no bitcoins could have possibly existed before 3 January 2009. No pre-mine, no ICO. Over the course of 2009, the popularity of Bitcoin grew substantially and hundreds of nodes were added to the network. In the early days individuals could profitably 'mine' using only standard CPUs with all full nodes also acting as mining nodes. The first mining difficulty increase happened on 30 December 2009, almost exactly one year after Bitcoin first went live.

The second year saw an explosion of value added to the Bitcoin ecosystem. Exchanges were created; the first commercial bitcoin transaction took place (the now infamous 25,000 BTC pair of Papa John's pizzas); a Bitcoin Wiki was written; the first escrow bitcoin trade was conducted; the first portable bitcoin transaction was sent between two Nokia N900 mobile computers; pooled mining was made available; the first bitcoin call option was sold, and the first bitcoin short sale was initiated with a loan of 100 BTC, both facilitated by the newly created #bitcoin-otc trading channel on freenode IRC; and finally, the Bitcoin economy passed US$ 1MM when the bitcoin price touched US$ 0.50 on MtGox.

By 28 January 2011, a quarter of all bitcoins had already been issued. Twelve days later, bitcoin reached parity with the U.S. Dollar on MtGox. Development of the protocol was rapid and many early quirks and bugs had already been resolved. This was also the year of the first alternative coin (altcoin), with Namecoin successfully launching in April 2011.

THE LEGEND (cont.)

Up until 2011, Satoshi Nakamoto kept in close correspondence with members of the Bitcoin community, regularly communicating with a growing list of code contributors via email and various blog and forum posts. But in the summer of 2011, citing discomfort about Bitcoin's sudden thrust into the international limelight with the Wikileaks scandal, and after receiving a message from volunteer co-developer Gavin Andresen that he would be visiting the CIA headquarters at Langley to give a briefing on Bitcoin, Nakamoto disappeared, never to be heard from again.

TECH & ARCHITECTURE

Bitcoin Core, Governance, BIPs & Forks

The standard Bitcoin reference client is called Bitcoin Core, or the 'Satoshi Client.' It is a full complement of software needed by nodes to run calculations, communicate with other nodes and perform all the tasks required to create and operate the Bitcoin Network. Originally introduced and maintained by Nakamoto himself, control over the Bitcoin repositories have since passed to the Bitcoin community. The first heir to the repository was Gavin Andresen who was handed the reins by Nakamoto before his disappearance in 2011.

> Since Nakamoto left in 2011, the Satoshi Client has seen twelve major upgrades, two name changes, and a moderate cycling of contributing developers. The release name changed to Bitcoin-Qt in 2011 and then to Bitcoin Core in early 2014. Andresen stepped down as lead developer around the same time, and Wladimir van der Laan became his successor, a position he holds to this day.

Bitcoin Core is an open source project open for contribution by anyone willing and able. The upgrade process is standardised under the Bitcoin Improvement Proposal (BIP) framework, introduced by Amir Taaki in 2011. BIPs are published on the Bitcoin repository on GitHub, whereupon they are debated in the community, and either rejected or accepted by developers as a group.

The process of acceptance or rejection utilises a combination of democracy and meritocracy to arrive at consensus. BIP authors must convince the other developers of the utility of their code, and a successful track record of accepted implementations increases the reputation of developers. But even if a BIP is accepted and published within a Bitcoin Core release, it is still entirely up to each individual node whether or not they want to implement the changes. As long as all changes are made backwards compatible, new code implementations will keep the network intact regardless of how many clients choose to run the amended software. Backwards compatible additions are referred to as soft forks, as the upgraded software can co-function with the non-upgraded software.

If, on the other hand, a proposal is made for a code change that is not backwards compatible, the network will fragment should only a subset of clients choose to implement the changes. A non-backwards compatible code change is referred to as a hard fork as the upgraded software cannot co-function with the non-upgraded software. Unlike soft forks, hard forks can result in a network split if only a part of the original network choses to upgrade, creating two incompatible versions that are each smaller than the original network. Hard forks are sometimes necessary and when implementing them it is essential that the changes are non-contentious and that the activation is extremely well coordinated, if the dangers of a network split is to be avoided.

Ultimately, no one can force a Bitcoin node to implement software. It is entirely up to each individual node which software implementation they want to run. Because the fundamental value of Bitcoin stems from its network effect, anyone forcibly attempting to implement hard forks against the will of the network will only achieve their own isolation from the network, thereby losing access to its value, and by extension, access to actual bitcoins. This architecture makes Bitcoin inherently anti-fragile and the network extremely difficult to co-opt.

Technology

Traditional currency relies on a paradigm of multi-level trust in order to function effectively. Central banks must be trusted not to debase their currency. Banks must be trusted to hold our money, make sure nobody tries to send us money they've already spent, and we need their permission and action to transfer it electronically to others. Furthermore, banks are required to hold personal information, safe from thieves and other nefarious actors.

One of the flaws of this model is that trust creates a system of fragility, choke points, single points of failure and corrupting pressures on trusted parties. In the history of banking, almost every single central bank has shown a remarkable willingness to debase their currencies. Traditional banks have a track record over several centuries of violating custodial trust by lending money out in waves of credit bubbles with only fractions left as reserves, leading to regular banking collapses and eradication of deposits. Private information is regularly stolen from centralised repositories, leaving consumers helpless to defend against identity theft and fraudulent transactions.

Bitcoin resolves all of these issues in one single, distributed computer software package, free of charge. Debasement is practically impossible (there is a hypothetical case where debasement could technically be implemented, but only with the express permission of users, more on this later) as the total number of bitcoins allowed by the software is capped at BTC 21MM. No third parties are required, either for holding your funds or for transferring them to another network participant. And lastly, no identities are required as proof of transaction validity. All that is required is a digital proof of bitcoin ownership, whether that proof is tied to an identity or not (it certainly can be) is irrelevant to the network.

Preventing Double-Spending

There is a reason we have not so far seen digital money capable of solving all these problems. The necessity of trusted third parties in digital value transfer systems is a longstanding problem of computer science that has frustrated researchers for decades.

Limiting the supply of a digital asset may sound simple enough in theory, but the ease and low cost of copying electronic digits has made this an exceptionally difficult problem to solve in practice. If value is to be represented as numbers on a computer, what is to stop anyone from copying these numbers repeatedly and spending them over and over? In computer science, this is referred to as the Double-Spending Problem.

The only possible solution so far has been the introduction of a trusted third party to maintain a ledger of all transactions, thereby validating each transaction input as not having been spent more than once. Unfortunately, this places a seemingly irresistible corrupting pressure on these third parties, historically leading to abuse of trusted positions either through negligence or wilful deceit.

Mining

Bitcoin solves the Double-Spending Problem by utilizing a competition-based time stamping service to verify a distributed public transaction ledger known as the blockchain. Instead of all transactions being funnelled through a single point of validation, they are broadcast freely across the entire Bitcoin network, thereby also removing the need to ask for permission when transferring funds.

DEEP DIVE: CHRONOLOGY

In this context it is important to note that when we refer to time stamping, we are not strictly speaking of references to dates and times, but of the relative order in which time stamps are made. In other words, it matters not necessarily at what time 'blocks' are stamped, all that matters is that we can discern with confidence that a certain block came before or after another, thereby knowing with certainty that *[Continued >>]* transactions are not attempting to spend coins which have already been spent at a previous time.

However, time stamping blocks does not by itself guarantee that transactions cannot be double spent. After all, how can we be certain that the network agrees on the current state of the blockchain, and thereby agree on who currently owns what? This is a problem of distributed consensus and a version of this problem is often referred to as the Byzantine Generals' Problem.

DEEP DIVE: BYZANTINE GENERALS' PROBLEM

The Byzantine Generals' Problem roughly boils down to a question of information validity and trust.

Suppose that a group of generals are camped around opposite sides of a besieged city and can only source information about the intentions of their allies through a network of messengers. In order to successfully sack their target, they must attack simultaneously; any uncoordinated attack will result in their own annihilation.

To launch an attack, it is necessary that they be certain that their allies have the same information as themselves such that the plan is executed in unison. But the problem is that they cannot trust that some of the other generals are not in fact traitors. One possible solution is to require a Proof-of-Loyalty to accept messages as true, but proving loyalty is no simple matter.

Bitcoin achieves distributed consensus, thus offering a solution to the Byzantine Generals' Problem by assuming a probabilistic Proof-of-Loyalty through a computer science technique called Proof-of-Work (PoW). The mining group of transaction validators competes for the privilege of time stamping a block full of newly received, valid transactions from the network onto the existing chain of ledger blocks, and is rewarded with freshly minted bitcoins.

Loyalty to the network is incentivized because competing for blocks requires costly investments in highly specialised hardware, electricity and overheads, normally billed in local (fiat) currency, while the reward is paid in bitcoins. This motivates all participants in the mining process to act in the best interest of the network, lest they risk rendering their investment 'worthless' (in local fiat currency terms) by acting in a harmful manner to the network, and therefore the price of bitcoins.

> THE **STEADY ADDITION OF** A CONSTANT AMOUNT OF **NEW COINS** IS **ANALOGOUS TO GOLD MINERS** ***EXPENDING RESOURCES TO ADD GOLD TO CIRCULATION.*** IN OUR CASE, IT IS **CPU TIME AND ELECTRICITY THAT IS EXPENDED**
>
> SATOSHI NAKAMOTO
> *BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM*

TECH & ARCHITECTURE

DEEP DIVE: BLOCKS

To win a block (and the bitcoin reward), a miner must run the information from the previous block through a hashing algorithm, combine the hash with information from all the valid transactions it intends to include into the next block plus a number called a nonce, and hash the combined input again. The hash output of these three components combined must equal a number below a certain numerical threshold for the network to accept the block as valid (Fig. 1).

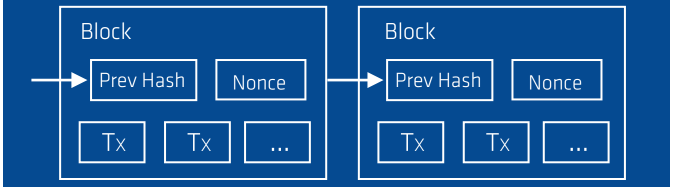


Figure 1. Simplified Block Constituents

Because hashing algorithms are mathematical one-way functions, meaning that the output can be easily computed from the input, but not the other way around, the only way to find a valid hash output is to randomly try new numbers as the nonce until the result is smaller than the required threshold. The process can be likened to a lottery, but one that requires substantial investment in physical infrastructure.

In fact, the cost of mining a bitcoin is rather high and very few individuals are able to profitably mine Bitcoin in today's market. The vast majority of miners are operated in industrial-sized datacentres where economies of scale, cheap access to electricity, and early preferential access to state of the art mining chips are paramount to achieving reasonable margins.

To adjust for computing power joining or leaving the mining network, the threshold, referred to as the difficulty, auto-adjusts every 2016 blocks such that the time it takes to find a new block averages 10 minutes, no matter how many miners are competing to win blocks. This reduces mining returns on existing hardware, forcing a fierce battle for technological improvement and efficiency gains.

Mining enforces a chronological ordering of transactions, ensuring that double spending cannot take place. Because each new valid block requires a hash of the previous block, transaction history cannot be altered without changing the input of the block hash, thereby also altering the block hashes of all subsequent blocks in the chain.

But nodes will only consider the longest chain following their consensus rules as the valid chain, rejecting all others. So in order to rewrite chain history, or publish blocks containing double-spent transactions, attackers must find the new PoW for their fraudulent blocks faster than the rest of the honest network combined. Therefore, so long as a majority of miners are acting in the best interest of the network, an attacker can never hope to outpace the honest miners to double-spend transactions.

Mining versus non-Mining Nodes

In the initial versions of Bitcoin, all nodes were miners and all miners were nodes. Mining was performed using regular CPUs and anyone with a computer had a more or less similar probability of winning a block. Since then, the advent of GPU and later ASIC mining has led to a differentiation of mining and non-mining nodes. Today, all miners are nodes, but not all nodes are miners. Mining has become professionalized, and most mining power is organized in large datacentres.

Transactions & Identity

Unlike traditional financial transactions, Bitcoin transactions require no identity-linked data. Proof of ownership is provided entirely by digital signatures, and these need not be tied to any real-world identities. All that is required for a transaction to be verified as correct by the network is the provision of proof demonstrating that: 1) the address(es) from which one is trying to send funds has a (cumulative) balance large enough to cover the transaction, and 2) the sender has control over these address(es).

The digital signatures used by Bitcoin employ asymmetric cryptography to create yet another class of mathematical one-way functions. Under this system, network participants begin by creating a random 256-bit number (roughly corresponding to a number between 0 and 10^76). This number is referred to as the private key and must be kept strictly secret as whoever controls the private key associated with a Bitcoin address controls the bitcoins.

DEEP DIVE: KEY RELATIONSHIPS

From the private key one can derive a public key using elliptic curve multiplication, a one-way mathematical function. Thus, a private key cannot be derived from a public key. Hashing the public

TECH & ARCHITECTURE

key in turn derives a Bitcoin address, and the same one-way relationship exists between the address and the public key. As a result, it is trivial to prove that an address is derived from a specific public key, but it is probabilistically impossible to derive a public key from an address. Likewise, it is trivial to prove that a public key is derived from a specific private key, but impossible to do the opposite.

Between the private and public keys, there exists a relationship such that one can prove possession of a private key without the need to reveal the key itself. Using 1) an arbitrary message, 2) the private key, and 3) a signing algorithm, the holder of a private key can create a unique digital signature. Then, using the public key and a verification algorithm, anyone can verify whether or not the signed message was created using the private key corresponding to the public key.

In order for a transaction to be valid and the ownership of bitcoins to transfer from one owner to the next, the sender digitally signs a hash of the previous transaction involving their bitcoins and the public key of receiver, adding these to the chain of ownership. The receiver can then easily verify the signatures to assure the validity of the ownership chain.

Curiously, then, no bitcoins actually ever exist as numbers in the blockchain, they are only ever inferred as the difference between transaction inputs and transaction outputs.

Privacy

The relation between the public and private nature of Bitcoin transactions is not dissimilar to that of stock markets, where the "ticker" -containing transaction price and volume information- is public and open for everyone to view, but the identities tied to each transaction are not necessarily known. The size and timestamp of trades can be published without tying them to identities, but privacy is simultaneously not guaranteed: if identities are indeed tied to transactions, tracking of fund movement becomes trivial.

A major difference, however, is that in the stock market, the linkage of identities is necessary for a transaction to be possible, whereas Bitcoin transactions have no such requirement. Identities in stock market transactions do not have to be published, but they must exist and be recorded somewhere to facilitate the transaction. Bitcoin, on the other hand, can be transacted entirely independently of identities: the only requirement is a digital signature, which can exist without identity ties.

What we are left with, then, is the first ever non-forgeable digital bearer instrument.

All that is needed to spend a bitcoin is a private key, and whoever is in possession of the key controls the bitcoins and can spend them at will. If you control your private key, you control your bitcoins. If someone else controls the private keys, someone else controls the bitcoins. It's as simple as that.

UTILITY & GROWTH OPPORTUNITIES

Sound Money

The most innovative property of Bitcoin is its independence of authority and censorship resistance. No entity can coopt the Bitcoin protocol against the wishes of the majority of network participants. It is pure democracy and pure, uncorrupted capitalism condensed into a modular, self-assembling network. The result is the first ever, true digital bearer instrument: beyond the reach of financial powers; beyond the control of governments, benevolent or not; entirely within the democratic control of its users; and free of any requirements of authoritarian questioning or authorisation for transactions; a system with the monetary properties of gold, but the transaction capabilities of the Internet.

This represents the first time in the history of human civilisation where there exists the possibility of implementing digital, ‘sound money.’ Bitcoin as a currency is impossible to debase without the express consent of a majority of the network. A system, not relying on any level of trust whatsoever and whose only assumption is that every participant acts in their own rational self-interest: the very foundation on which modern economic theory already rests.

Most Valuable Use Cases

At present, we hold that there are three main high-level use cases dominating Bitcoin utilization, which comprise its value. The three are, in no specific order of prevalence 1) medium of exchange, 2) store of value, and 3) instrument of speculation. We will discuss its role as a store of value and instrument of speculation later in this section.

WE DEFINE AN **ELECTRONIC COIN AS A CHAIN OF DIGITAL SIGNATURES**. EACH **OWNER TRANSFERS THE COIN** TO THE NEXT **BY DIGITALLY SIGNING A HASH OF THE PREVIOUS TRANSACTION** AND THE PUBLIC KEY OF THE NEXT OWNER AND ADDING THESE TO THE END OF THE COIN.

SATOSHI NAKAMOTO
BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM

UTILITY & GROWTH OPPORTUNITIES

Medium of Exchange

Out of the three main high-level use cases, subsets of more specific uses emerge. Being far too numerous to examine individually within the scope of this paper, we will concentrate on four particularly promising ones emerging from its utility as a medium of exchange: remittance, payments, settlement, and digital currency reserve.

Remittance is perhaps one of the more immediately obvious applications for borderless, permissionless payment protocols. Money can be transmitted anywhere in the world where there is access to electricity and the Internet, with flat fees regardless of amount transferred. A Bitcoin transaction will cost the same whether you are sending BTC 0.01 or BTC 1,000.

No third party is required. There is no need to visit a physical location, no forms to fill in and no reliance on anyone other than yourself properly doing their job for a payment to be sent. There are no opening hours, no bank holidays, and with an appropriate transaction fee, the payment will clear in a matter of hours.

Payments are another rather obvious use case for a "digital payments system." However, the pure utility of using the protocol layer for direct payments carries with it an essential trade-off between scalability and decentralisation, such that under current protocol rules and network architecture, "on-chain" payments at commercial scales are not feasible (more on this later).

This limitation transfers us straight into the realm of the settlements use case. Since it makes little to no economic sense -at least currently- to enter every single transaction into the blockchain, a more suitable role for 'protocol layer transactions' is settlement. If all parties to any aggregation of payments, agree on the final balance, settlement on a permanent, immutable, indisputable ledger represents a much more economically sound alternative to storing every transaction, no matter how small, directly on-chain.

Solutions using the Bitcoin network as an underlying mechanism for clearing or settlement are referred to as Layer 2 (L2) solutions. While there are several centralised payments solutions already available for merchants seeking to accept bitcoin payments, these still suffer from the same legacy issues as trust-based payments, without being able to fully capitalize on the trustless decentralised properties of Bitcoin.

Using an open-source L2 protocol, the Lightning Network as proposed by Joseph Poon and Thaddeus Dryja promises to offer instant payments, low cost, cross-blockchain atomic swaps and scalability to millions of transactions per second. The system works by using smart contracts to send payments between non-trusted nodes, somewhat similarly to package routing across the Internet. Therefore, transactions on a blockchain are only necessary for funding and settling accounts [4].

DEEP DIVE: NETWORK EFFECT

Bitcoin is an example of a system that benefits strongly from network effect: the more users in the network, the higher utility and value. In many ways it is similar to telephone networks or the Internet, where, assuming all nodes are equally connected, the number of connections C in a network of n nodes can be expressed as $C=n(n-1)/2$. For example, if there are 7 telephone users (21 connections) the utility is limited, but if there are 10MM users (50TN connections) the utility is huge. This is a 'positive network effect' and has the capability of creating a positive feedback loop as more users join, adding further value to the network.

Closely related to the principle of connectivity, Metcalfe's Law states that the value of a network grows proportionally to the square of the number of users, or V = N^2, where V represents value and N is the number of users. While it is tough to estimate the total number of Bitcoin users, looking at the growth of individual users on the popular websites blockchain.info and Coinbase can provide interesting insights into the development of the network size (Fig. 2). If we square the sum of the total users across both services and overlay it on a graph of the bitcoin network value since November 2011, we find a correlation of 0.94.

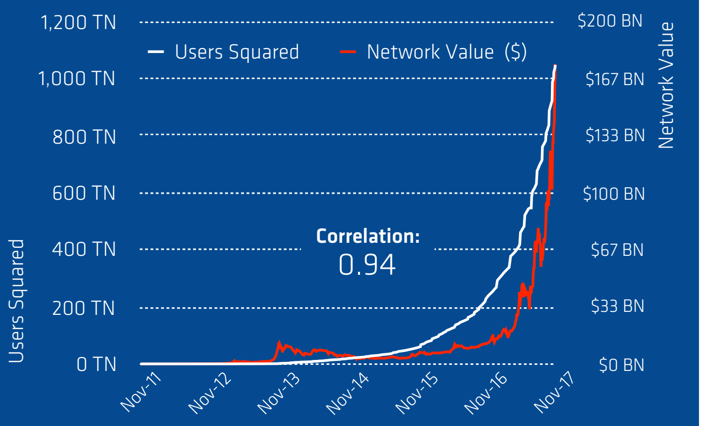


Figure 2. Time Series of the Square Sum of Cumulative Users, Coinbase & blockchain.info vs BTC Network Value

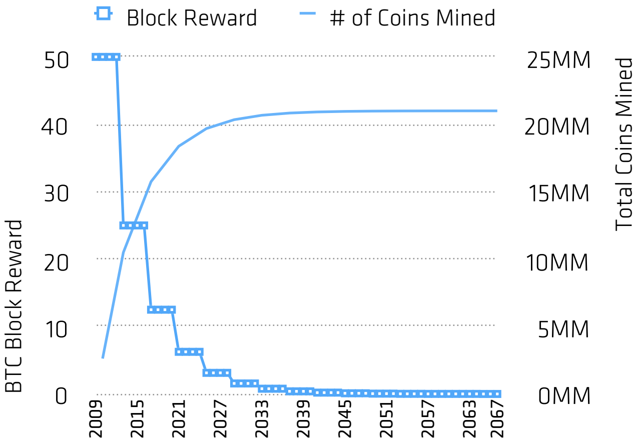
UTILITY & GROWTH OPPORTUNITIES

Store of Value

Bitcoin's similarity to gold is intentional. As touched on in the Technology section, bitcoin issuance is capped with an upper limit of BTC 21MM and no more can ever exist, this is analogous to the finite supply of gold in the earth's crust. The issuance itself is a product of the mining process, another term borrowed from the precious metals industry, with freshly minted bitcoins awarded to miners as a reward for winning blocks.

Inflation is halved approximately every four years. From its initial coinbase (the technical term, not the company) reward of BTC 50 per block, the block reward has since been reduced twice, to BTC 25 in 2012, and then to BTC 12.5 in 2016. Annual bitcoin inflation will still remain above 3.5% until the next halving, projected in 2020, before dropping to less than 1% at the subsequent halving, around 2024 (See Fig. 3). At some point, however, Bitcoin will turn deflationary. Because it is possible to lose private keys or send bitcoins to unspendable addresses, bitcoin issuance will eventually be outpaced by bitcoin losses, ultimately reducing the spendable supply.

fig. 3 Time Series Projection of Bitcoin Block Reward (BTC) Versus Total Coins Mined



Source: CoinShares Research

Limited issuance and predictable inflation schedules are highly desirable qualities for any asset intended as a store of value. When coupled with its unmatched ease of storage, transfer and transaction, it becomes clear that bitcoin is a serious contender to precious metals as a store of value in the digital age. No costly infrastructure is required to own it; it is infinitely divisible (currently set to 8 decimals); it cannot be counterfeited; and the private keys can be stored using materials with any quality of permanence desired, such as metal, crystal or stone.

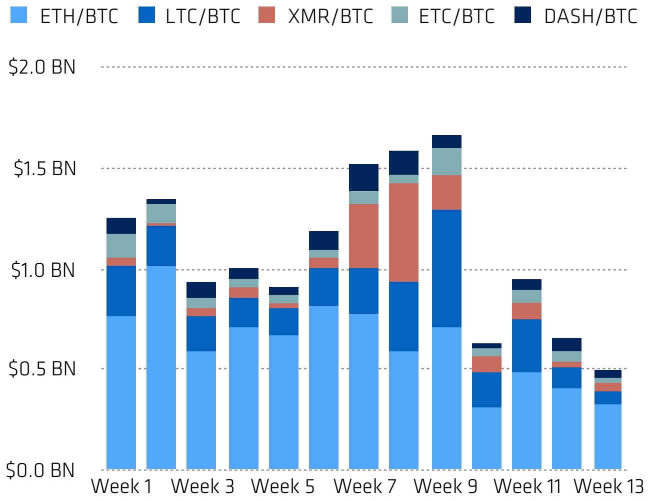
Crypto Reserve Currency

Due to its relatively long history, successful track record, ease of exchange and sizeable liquidity pool, Bitcoin has taken on the role as the major crypto reserve currency.

When Ethereum launched their ICO in 2016, the only accepted method of payment was bitcoins. Many of the largest and most successful ICOs (such as Ethereum, Filecoin and MobileGo) have been priced in both bitcoin and ether. In fact, the vast majority of digital tokens and currencies do not have fiat currency pairs available anywhere, to access them one must either hold bitcoin, ether or more rarely, other major altcoins [5].

Bitcoin currency pairs are extensively traded on crypto exchanges, many of which have an altcoin focus like Bitfinex, Poloniex and Kraken. Weekly trading volumes for BTC pairs on the 10 biggest crypto exchanges averaged more than US$ 1B in Q3 2017 (Fig. 4).

fig. 4 Q3 2017 Weekly BTC ($) Volume By Trading Pairs on Top 10 Exchanges by Volume



Source: cryptowat.ch

The meteoric rise of ICO funding over the course of 2017 saw bitcoin dominance among the top seven cryptocurrencies fall from more than 90% at the beginning of the year to 52% in June, with ether making the largest inroads, peaking at more than 40% in July. But the negative press and heavy-handed government intervention in the ICO space over the course of the autumn has somewhat thawed the altcoin and ICO rally. The current bitcoin dominance percentage is yet again pushing 60% as investors are flowing back into the perceived safety of bitcoin (Fig. 5).

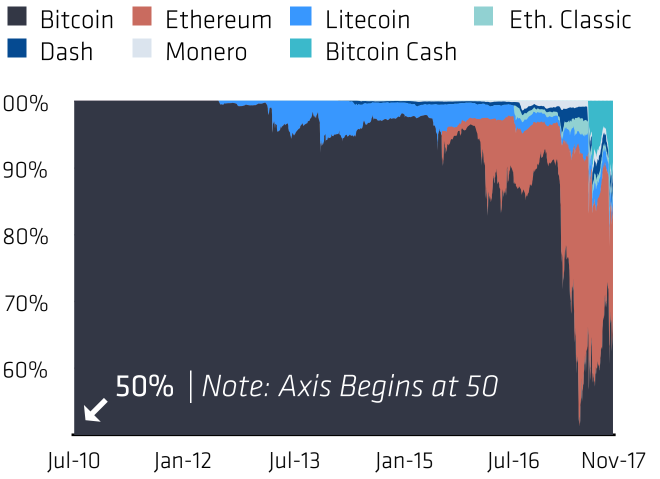
SPECULATIVE VALUE AND RELATIONSHIPS TO WATCH

In this section we have mapped some possible drivers of growth in the utility value of the underlying Bitcoin network. These are nonetheless single components in the aggregate token price and thus affects network value in a non-exhaustive manner. The section bears close resemblance to its sister section in our Ethereum Asset Highlight since many of the relationships highlighted are equally interesting for most cryptocurrencies.

Speculation undoubtedly plays a role in driving the bitcoin price and said speculation does not exist in a vacuum. There are other decentralized tokens with which bitcoin competes on both technical and speculative fronts. One trend to watch when evaluating relative performance is the overall dominance (share of the decentralised token market's outstanding value) of bitcoin among its six closest competitors.

Dominance among decentralised currencies is often measured by percentage of cumulative network value (modeled on conventional market capitalization). Since its first publicly-priced trades, bitcoin has seen its unit value rise from less than ¢1 to a peak of more than $8000. Throughout this period, bitcoin has always been the king of crypto, a position it retains to this day. That being said, over the last few years competing altcoins have slowly eaten away at Bitcoin's dominance, with Ethereum coming within arms length of dethroning bitcoin over the summer of 2017, before retreating throughout the autumn(Figure 5).

fig. 5 Cryptocurrency Dominance as Percentage of Combined Market Cap Since Bitcoin Launch



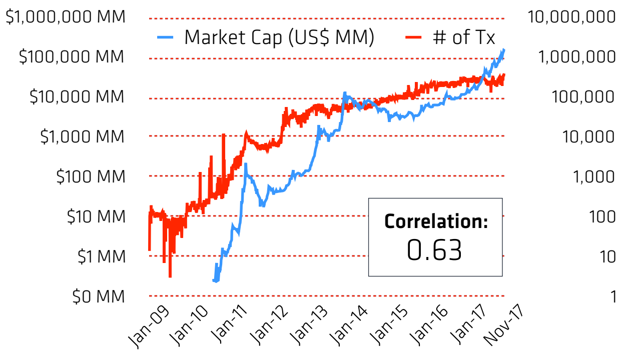
Source: bitinfocharts.com

But more than merely measuring each currency's relative valuation/standing, the long-term dynamics of the dominance curve can illuminate trends in funding patterns between competing protocol technologies. As protocols develop, each addition or reduction of value to the codebase should elicit organic responses in the volume and momentum of funding flows between coins as investors re-weight their holdings based on their belief in the viability of the technologies.

Transaction Volume as an Indicator

As previously mentioned, speculative value in bitcoin is driven by future expectation of utility, weighted (or inflated) by current level of hype in the space. One key indicator many digital asset speculators watch as a relational indicator of both price and network value is the development of daily on-chain transaction volume. We observe a moderate correlation between daily transaction volume and network value (Fig. 6). But there are a few complicating factors potentially reducing the value of this measure.

fig. 6 Daily Bitcoin Transaction Volume (# of Transactions) Versus Network Value



Source: blockchain.info

One is the presence of services like SatoshiDice, the on-chain gambling service. SatoshiDice was introduced in April 2012, after which we observe a massive spike in Bitcoin transactions. Between launch date and when they took their service off-chain in 2013, it is estimated that SatoshiDice transactions represented more than 50% of all on-chain transactions [8].

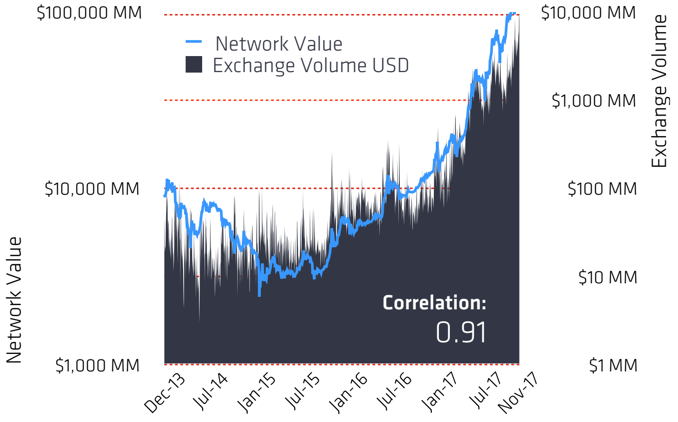
Another issue is the recent bump up against the blocksize limit. Because activation of Segregated Witness, a transaction capacity upgrade, was blocked for months by certain members of the network, while the network simultaneously came under blockchain spam attacks, on-chain transaction capacity began to hit its limit over the spring and summer of 2017. The resulting increase in transaction fees probably had a chilling effect on demand. While the development of a fee market represents pure economical dynamics at work, this is nonetheless a whole new circumstance in the transaction market, making previous trends more difficult to extrapolate.

SPECULATIVE VALUE AND RELATIONSHIPS TO WATCH

Exchange Volume

We also observe a strong correlation between exchange traded volume (US$) and Bitcoin network value (Fig. 7). However, to elaborate further on the potential trend between daily exchange volume and network value, a deeper analysis is necessary to determine the directionality of any causal relationships. Because exchange volume ($) and network value ($) both contain the bitcoin price as components of their calculation, it may create an inflated sense of covariance between the two.

fig. 7 NETWORK VALUE VS. EXCHANGE VOLUME $$



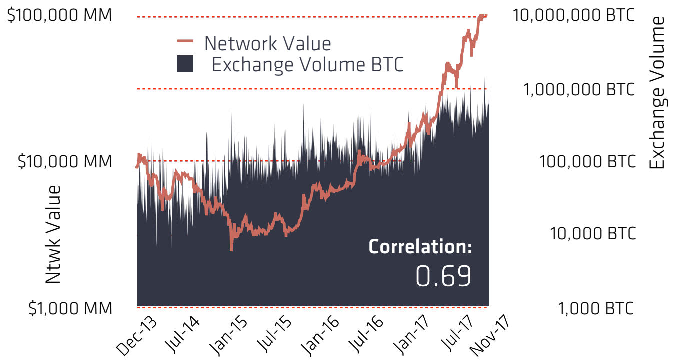
Sources: Coinmarketcap.com, bitinfocharts.com

To standardise the relationship, one can look at bitcoin- denominated trade volumes. These have grown since inception, an impressive statistic given the meteoric rise of the bitcoin price (Fig. 8). Although trade volumes are valuable data points when analysing bitcoin price trends, there are some attributes of various crypto-exchanges that should be noted with caution when looking at available data. There has been, and to a certain degree remains, a tendency for upstart exchanges to offer zero-fee trading in order to attract traders. While this is the complete prerogative of each individual exchange, one consequence of zero-fee trading is that volumes may appear stronger than what could be reasonably expected at more established exchanges where fees are levied.

Our exchange volumes do not include exchanges with a no-fees trading structure.

Please Proceed to Next Column For Fig. 8...

fig. 8 NETWORK VALUE VS. EXCHANGE VOLUME BTC

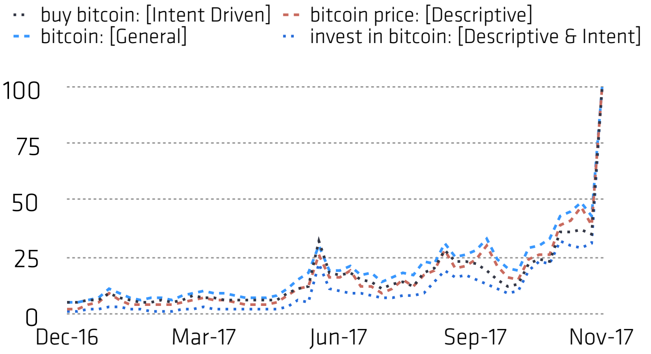


Sources: Coinmarketcap.com, bitinfocharts.com

Search Trends

An additional proxy of perception around bitcoin's use cases can be observed (Fig.9) from recent search trend data comparing the relative popularity of bitcoin related search terms. In this instance, we compare "bitcoin," "bitcoin price," "buy bitcoin," and "invest in bitcoin." These terms are representative of interest, descriptive interest, intent and descriptive intent, respectively.

fig. 9 GOOGLE SEARCH TRENDS FOR BITCOIN TERMS



Sources: Google Search Trends

Of interest are two particular observations: 1) The recent spike (and then relative move toward parity in trend growth rate) of "invest in bitcoin" mid-2017 correlates with the general observation of a new wave of 'investors' (as opposed to early adopters or users) entering the market. This is important because the idea of investing typically includes a time horizon (short, mid or long – term) and thus also indicates a utility of storing value. 2) Prior to mid-2017, the notable relationship to watch was "buy bitcoin" + "bitcoin price." Combined with the dramatic spike in popularity of all terms in the last 2 weeks of November and there is evidence to support the axiom that a rising price is one of the best "marketing tools" for bitcoin adoption.

APPROACHING A VALUATION OF BITCOIN

In this section we will present a simple valuation methodology aimed at giving readers a feel for how future bitcoin value can be modeled. The valuation is in no way meant to be a prediction, or a reflection of current value/price. It is a mental framework for assessing the potential price of bitcoin, if bitcoin's utility as a store of value continues to develop.

Our methodology uses simple market penetration into existing stores of value (in this case, investment gold and high denomination Euro and Dollar bills), and attempts to establish a range of future bitcoin prices given varying penetration levels.

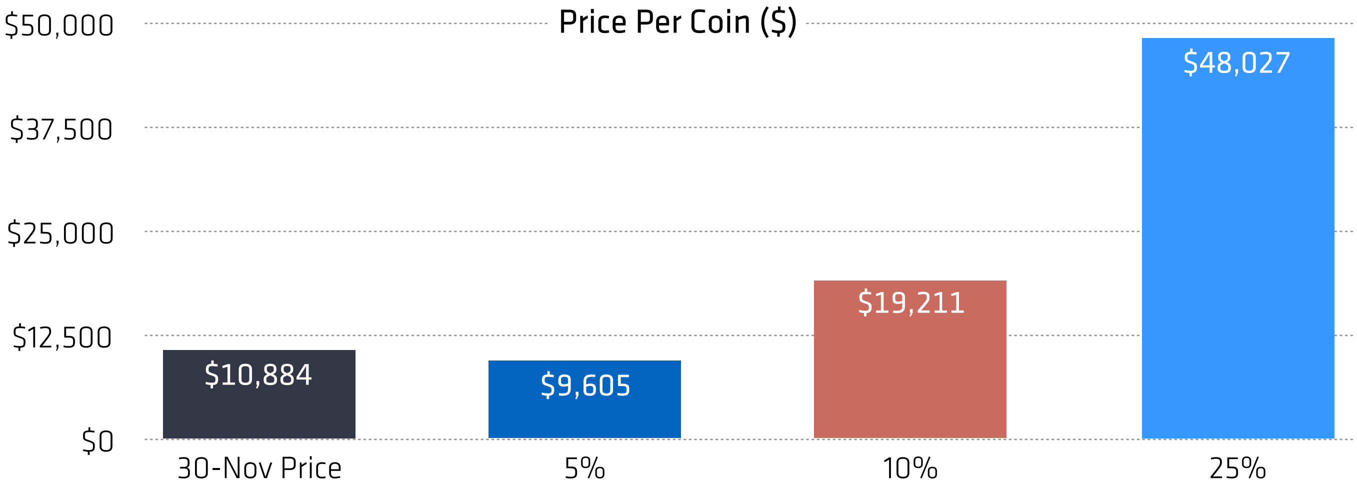
Store of Value

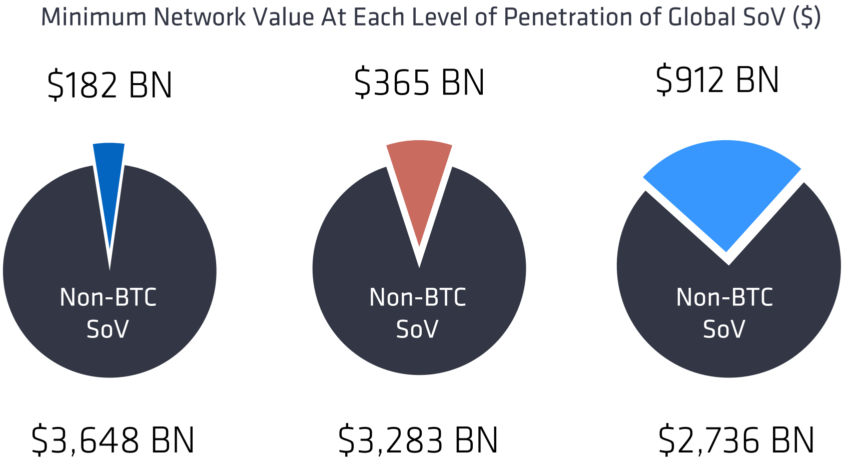
The store of value (SoV) model is relatively simple. Using penetration ranges from 5%-25% and an estimate of 19M bitcoins in circulation (by 2022), we model the necessary size of Bitcoin's asset base in order to compete with investment gold and large denomination Dollar and Euro bills as a store of value.

Here we use Bank of America Merrill Lynch figures as an estimate for global stores of value. Investment gold is estimated at US$ 1.72T, and large denomination bills at US$ 1.50T [7]. Assuming that the value of investment gold will keep up with a conservative 3% global growth rate (IMF estimates 3.7%), and that the cash will need to be inflated by a conservative 2% (IMF estimates 3.3%), we end up with a combined value of US$ 3.65T in 2022.

For penetration levels of 5%, 10% and 25%, the price of a single bitcoin in each scenario would have to be ~US$ 9,600, ~US$ 19,200, and ~US$ 48,000, respectively (Fig. 10).

fig. 10 PROJECTION OF 2022 MINIMUM BTC PRICE REQUIREMENT TO SUPPORT 5%, 10% OR 25% OF GLOBAL SoV





Sources: CoinShares Research, IMF, BAML

HOW TO INTERPRET THE PRICE FIGURES OFFERED BY THIS VALUATION METHOD

These price figures are representative of a "minimum" value imparted to each token as a result of capturing a portion of global SoV. In other words, at each level of penetration, the price point reflects a figure which is but one component of a larger number (total BTC price). Bitcoin can and often does act as more than a store of value, so total price of the token usually comprises at least 3 variables - 1 for capture of SoV, 1 for current speculative value, and 1 for value required to operate as an effective medium of exchange.

ASSET PERFORMANCE & CORRELATIONS

Measuring pure asset returns over the entire lifetime of Bitcoin will return figures that verge on the absurd. Because Bitcoin started its life priced at US$ 0 (even though its cost of creation has always been higher than US$ 0), its return to date is technically infinity, which does not make for good comparison to other assets. If we instead begin in 2011, when decent price signals for bitcoin had been established, we can begin to look at returns in numbers that are at least closer to the orders we are used to.

Table 1

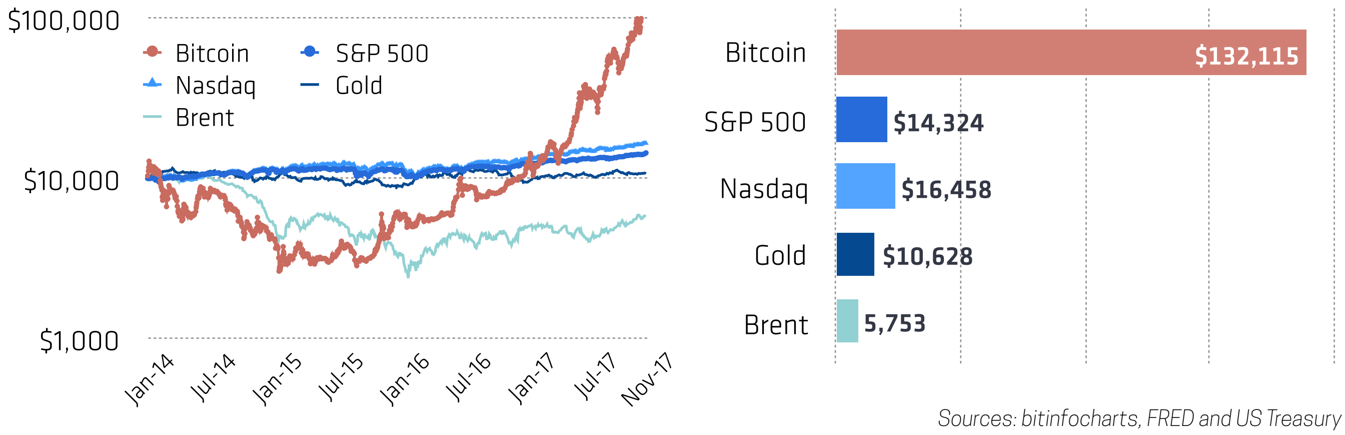
Annual	2011	2012	2013	2014	2015	2016	2017 (YTD)
Returns	1733%	144%	5474%	-58%	37%	131%	991%
Volatility	117%	48%	79%	61%	50%	33%	64%

Sources: blockchain.info, bitinfocharts

Investment case of US$ 10,000

Looking at an investment case of US$ 10,000 investment into our basket of commonly invested assets (S&P 500, Nasdaq Composite, Gold and Brent) at the beginning of 2014, the performance of bitcoin has varied significantly over the period (Fig. 11). From being the worst performing asset until late 2015, bitcoin has raced past every single other asset, and today (Nov. 15), that US$ 10,000 investment would be worth approximately US$ 95,000.

fig. 11 DEVELOPMENT OF US$ 10,000 INVESTED IN COMMON INVESTABLE ASSETS 2014 TO 2017 (YTD)

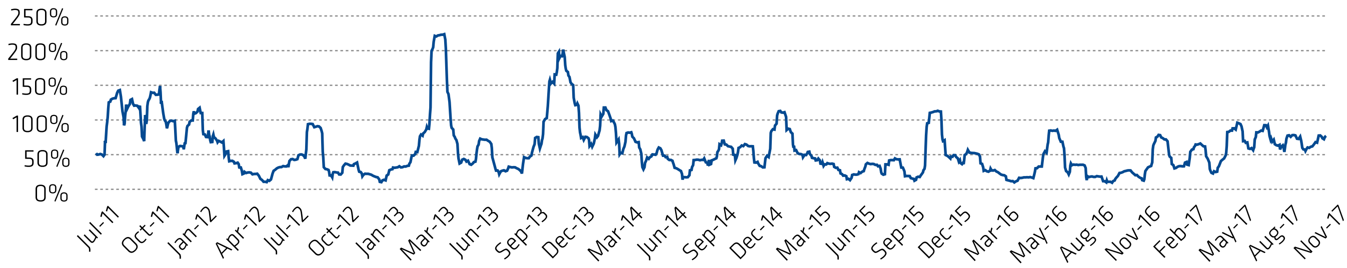


Sources: bitinfocharts, FRED and US Treasury

Volatility

However, in order to access returns on these levels, bitcoin investors must withstand severe volatility. Looking at the annualized volatility of bitcoin (Fig. 12), we can see that although the long-term development is trending down, last year's annualized, average 30-day volatility was still higher than all assets in our comparison basket except Brent (Fig. 13).

fig. 12 BITCOIN VOLATILITY 2011 - 2017 (YEAR-TO-DATE)
(30-DAY ROLLING ANNUALIZED STANDARD DEVIATION OF DAILY RETURNS)

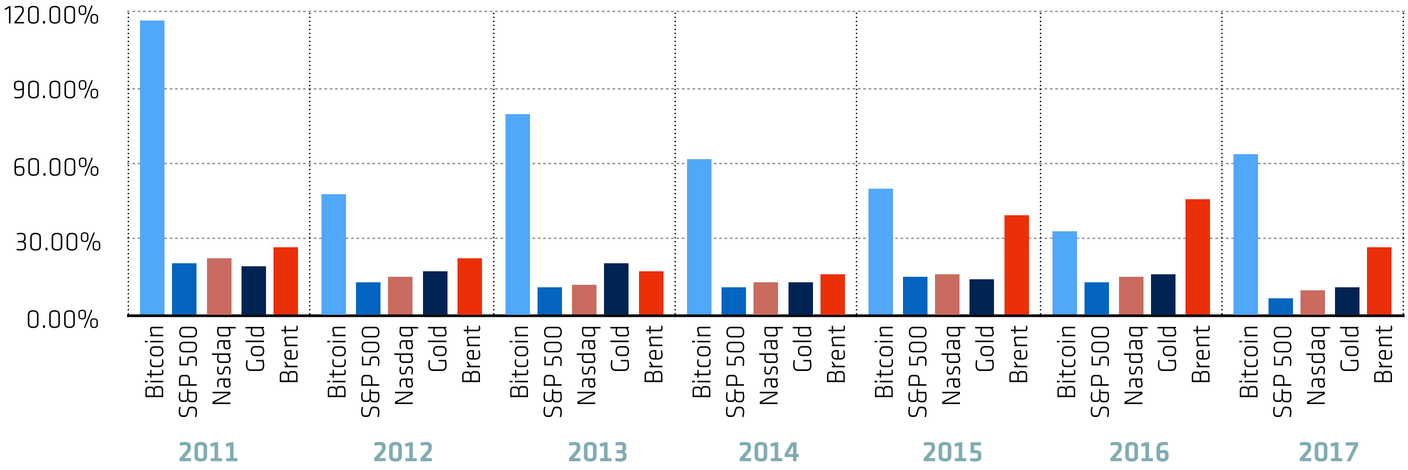


Sources: bitinfocharts

ASSET PERFORMANCE & CORRELATIONS

Furthermore, this year's hefty price action has lead to 2017 year-to-date (YTD) annualized, average 30-day volatility yet again creeping higher than all of our comparable assets (Fig. 13). While we expect bitcoin volatility to dampen over time as the price reaches maturity, bitcoin still behaves like a growth asset requiring substantial risk tolerance on the part of investors.

fig. 13 ANNUAL VOLATILITY 2011- 2017 (YTD) OF BITCOIN & COMMON ASSETS
(1YR AVG OF (ANNUALIZED) TRAILING 30 DAY STANDARD DEVIATION OF DAILY RETURNS)



Sources: bitinfocharts, FRED

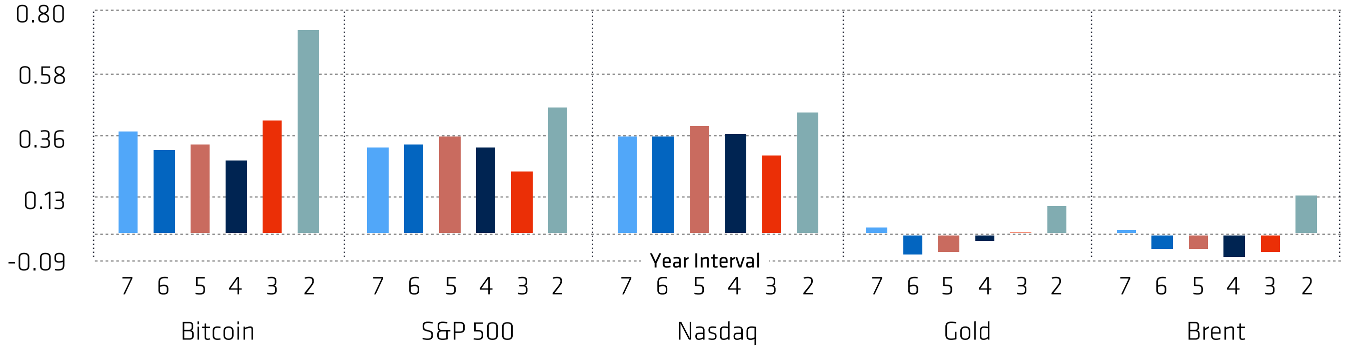
Risk-Adjusted Returns

Neither pure returns nor volatility alone suffice as metrics for prudent portfolio allocation. Because assets are inherently different and incorporate unique risks, returns and volatilities, one must also look to risk-adjusted measures in order to achieve a valuable comparison.

Sharpe Ratios offer one method of comparing returns on the basis of standardised volatility measures. First, pure returns are discounted by a risk-free investment rate, represented by 3-month U.S. Treasury bills. Average excess returns above the risk-free rate are then divided by the price volatility of the asset, represented by the standard deviation of the excess returns. Assets with the highest Sharpe Ratio offer the best compensation to investors for the level of risk they are taking.

Bitcoin is one of the most volatile major investment assets. Even so, when applying the Sharpe Ratio to bitcoin and a basket of commonly investable assets, bitcoin has outperformed all competitors 3 out of the last seven intervals, including the most recent two. During the last two years, it has compensated investors nearly 7 times more than gold, 5 times more than brent and 1.5 times more than the S&P 500 and Nasdaq (Fig. 14) relative to the level of risk assumed.

fig. 14 (7-2YR) SHARPE RATIOS - MONTHLY RETURNS (VS. 3-M US TREASURY BILL) OF COMMON ASSETS



Sources: bitinfocharts, FRED, US Treasury, CoinShares Research

ASSET PERFORMANCE & CORRELATIONS

Returns Compared to Common Assets

One of the most exciting attributes of the cryptocurrency space is highlighted in Table 1 (pg.17): where assets with similar returns (and risks) have largely been unavailable to anyone outside the venture capital industry, the open nature of crypto-markets has made high- risk/ high-return assets accessible to a much wider public. The 3-month returns in Table 2 makes the risk/reward relationship of the crypto-space compared with more 'traditional' assets abundantly clear.

Table No.2 Quarterly Returns of Bitcoin and Other Common Assets

	Bitcoin	S&P 500	Nasdaq	Gold	Brent
Q4 2015	**79.6%**	6.2%	8.2%	-5.3%	-22.9%
Q1 2016	-4.0%	0.8%	-2.7%	**16.7%**	0.4%
Q2 2016	**56.8%**	1.3%	-1.5%	8.8%	31.9%
Q3 2016	-10.3%	3.1%	**9.2%**	-1.3%	1.2%
Q4 2016	**55.8%**	3.3%	1.3%	-13.4%	13.9%
Q1 2017	8.9%	5.5%	**9.8%**	8.6%	-5.0%
Q2 2017	**132.0%**	2.6%	3.9%	-0.2%	-9.8%
Q3 2017	**75.3%**	4%	5.8%	3.3%	21.1%

Sources: bitinfocharts, FRED

Correlations of Returns per Asset

Extending the discussion on comparative returns, Table 3 below shows the correlations between the daily returns of bitcoin since 2015 against the same set of assets as in Table 2 above, using Pearson's Correlation Coefficient.

The inclusion of uncorrelated assets into a diversified asset portfolio generally serves to lower its overall volatility. Thus, large movements in single assets only affect the overall portfolio value in a dampened manner as the probability of all assets moving together is low. Conversely, if all portfolio components move in unison there is an increased propensity for the entire portfolio value to follow the movement of single assets and greatly diminishing diversification benefits.

The daily returns correlation between Bitcoin and traditional investment metrics such as the S&P 500, Nasdaq, Brent Crude and Investment Gold indexes is nearly zero. Its closest correlated traditional investment is gold, with a Pearson's Correlation Coefficient of 0.06. This property makes bitcoin uniquely useful as a portfolio-balancing tool for investors seeking diversified exposure to multiple assets.

Table No.3 Correlations of Daily Returns

	Bitcoin	S&P 500	Nasdaq	Gold	Brent
Bitcoin		-0.022	-0.028	0.062	-0.011
S&P 500	-0.022		0.942	-0.179	0.295
Nasdaq	-0.028	0.942		-0.171	0.213
Gold	0.062	-0.179	-0.171		-0.032
Brent	-0.011	0.295	0.213	-0.032	

Sources: bitinfocharts, FRED

RISKS

Major risks to Bitcoin can be roughly classified into two general categories: Technological risk, and attack vulnerability, with certain cases of overlap. Here we will outline the most pressing risks, as we see them, with the express caveat that we cannot possibly cover every conceivable one.

Block Reward Tapering

Mining rewards have two current constituents: the block reward and transaction fees. Some time around the year 2140, the block reward will round to zero, ending the fresh issuance of bitcoins. However, because of the shape of the issuance curve (see Fig. 2), more than three quarters of all bitcoins have already been issued, and by the end of 2036, this figure is expected to be 99%.

At current bitcoin prices the cumulative annual block reward is worth more than US$7B. The total value of the block reward plus transaction fees is what makes an attack on block consensus prohibitively costly, preventing certain malicious behavior in the consensus layer. For these types of attacks to remain unreasonably expensive to execute, either total transaction fees must grow to replace the block reward, or the bitcoin price must rise in an inversely proportional manner to the block reward, or the more likely scenario, there must be a combination of both.

For a dependable fee market to develop, there must be a balance between transaction throughput and transaction fees. Any economist will swiftly point out that equilibrium will arise between transaction costs and transaction throughput, determined by transaction supply and transaction demand.

But for a price to exist the quantity of a good cannot be unlimited, and so there must at all times exist some restriction on the availability of block space (this, in return, causes other potential issues which we will cover further in the next section).

Finding the correct balance between restricting block space and allowing sufficient throughput to cover demand is not a trivial matter and no commonly accepted solution has yet been offered. Unless a reliable stream of transaction fees can be expected to cover mining costs Bitcoin's consensus security model risks collapsing with potentially devastating consequences for investors.

Scaling

Bitcoin scaling is a highly complex problem that cannot be sufficiently covered in the scope of this paper. We will endeavor to give a surface-level overview of the problems that has received the most publicity, but would like to stress that the matter is much more complicated than it first appears. For a more thorough treatment of Bitcoin scaling we can refer you to the Bitcoin Wiki [9] and the Bitcoin Core Capacity Increase FAQ [10], and we recommend a detailed investigation of their listed sources.

Under the current protocol, Bitcoin transactions are limited to approximately 5 per second [10], depending on the size and type of the transactions. Bitcoin has a blocksize limit of 1 megabyte, assigned by Nakamoto as a spam-reduction measure in 2010 to reduce blockchain bloat.

As we briefly mentioned in the Technology section, under the current protocol there is an essential tradeoff between on-chain transaction capacity and decentralization. There are two reasons for this, but both relate to the cost of operating Bitcoin nodes, affecting the number of network participants who could afford running a full node.

The first reason is cost of storage: All full Bitcoin nodes must keep a full copy of the blockchain in order to verify transaction history back to the genesis block. If every single transaction of a payments network on the scale of Visa (on the order of 5,000 per second [11]) were to be recorded in the blockchain, it would grow by more than a hundred gigabytes per day [9], making it unrealistically expensive for most people to run a node.

The second reason is slightly more complex and results from bandwidth limitations: In our Ethereum Asset Highlight we briefly touched on the concept of stale or orphaned blocks. A stale block is a valid block found by a miner that reaches the network too late because another miner has successfully propagated a different valid block to the network. Unlike the Ethereum protocol which rewards stale blocks as Uncles, stale blocks in Bitcoin are simply disregarded by the other nodes.

If we assume an average Bitcoin transaction size of 500 bytes and a peak transaction demand of 5,000 per second, each 10 minute block would need to contain approximately 500 megabytes of data [9]. Acknowledging that not all locations currently have access to high-speed Internet connections, transmitting such a large block reliably to the entire network could take several minutes.

This would greatly increase the chances that another miner finds a valid block and successfully propagates it, before your own block is sufficiently propagated, risking that it becomes stale. Such an effect has a particularly centralising pressure on mining as co-

RISKS

located miners would benefit greatly from reduced transmission times between each other.

Additionally, as we mention in the previous section, the supply of a good must be limited for a price to exist. This creates a friction between increasing block space for scaling purposes and limiting it for the sake of securing sufficient fees to cover future mining rewards. The balance between the two is perhaps one of the most hotly debated topics in the Bitcoin community and one that largely remains unsolved from a community consensus standpoint.

It is important to realise that scaling bitcoin by multiple orders of magnitude is not impossible; it just simply cannot be done under the current protocol structure. However, the immaturity of the current software and the need for significant upgrades to the protocol in order for Bitcoin to compete as a value transfer network on a global scale represents a notable risk to investors.

Harmful Legal or Regulatory Action

Although Bitcoin, like any other distributed network, cannot effectively be shut down without finding and disabling every single network participant, it is still vulnerable to damage dealt to it by powerful state actors. Damage of this kind cannot realistically kill the network, but it can certainly inflict severe monetary loss on network participants and deal powerful blows to adoption and use.

While, for example, outlawing the software is entirely unenforceable, it would almost certainly drive participants off the network for fear of government repercussions, causing negative price pressures. Overly burdensome regulation can have much of the same effect.

With the exception of a handful of smaller undemocratic countries, state-level responses to Bitcoin have thus far been measured and reasonable. Most governments have chosen to observe its growth and development, more or less leaving it alone so as to not stifle innovation. This is a very reasonable response to a system, whose total network value has until recently been lower than most Fortune 500 companies, however, we cannot assume this cautious approach will continue as Bitcoin's network value begins to approach the M1 value of established world currencies.

Running a Full Node is Costly and Technically Challenging for Most Users

Unlike mining nodes, regular full nodes are not directly compensated for their services by the network. Running a full node is in the rational self-interest of bitcoin holders as it is the only way users can be certain that none of the protocol rules have been broken by other participants without relying on someone else's trusted information.

However, operating a node comes with a very real cost and normally requires separately dedicated hardware on the part of the user. Although there is specialized lower-cost hardware coming to market it is still expensive enough that only a subset of all users can be reasonably expected to have a separate computer running Bitcoin Core. There are less hardware intensive ways of running a full node, but these solutions, while not immensely technically challenging, are still sufficiently difficult to put off most users.

Competition & Technological Obsolescence

Since the first altcoins began emerging a few years after Bitcoin's invention there has been a Cambrian explosion of new coins and tokens in the cryptocurrency space. Altcoins now number in the thousands, and with the rapid proliferation of ERC-20 tokens, this trend has only accelerated. There is a chance that one of the alternative coins could replace bitcoin as the major juggernaut in the crypto asset space.

Hostile State-Level Adversaries

State-Level actors could chose to covertly attempt to harm the Bitcoin network. It is not difficult to imagine how branches of government stakeholders in the current financial system could come to view Bitcoin as a threat and choose to take aggressive action.

Such an effort, especially one not overtly giving away their hostile intent, is likely to be directed at the community itself. Because Bitcoin's architecture is robust in the face of outside attacks, the most effective assaults might have to come from within. The classical method for such strategies is to foment internal hostility within the community, creating factions, which will expend considerable time and energy on infighting while leaving the overall network fragmented and more vulnerable to separate harm.

Attacks like these constitute a substantial risk to investors as the potential success of attacks could cause meaningful damage to confidence in the protocol, conceivably resulting in negative price pressures as investors leave the network.

Brand Theft

Due to the open source nature of the Bitcoin protocol, no single entity owns the Bitcoin trademark, or the underlying software used by the protocol.

RISKS

This leaves the network open to attempted brand theft by altcoins using (minimally altered) copies of the Bitcoin protocol, with the hope of misleading unwitting users into using their altcoins while believing they are using Bitcoin.

The Bitcoin network is resilient to brand theft as well, but attacks like these could be very damaging to public trust, potentially causing market instability. While the open source nature of the project makes intellectual theft an absurdity, loss of public support could still cause losses to investors through negative market action.

Even though hard forked altcoins are incompatible with the Bitcoin network (Bitcoin nodes will reject their blocks and ban the nodes from their peers), nothing can prevent members of the altcoin communities from still referring to their tokens as “Bitcoin,"risking confusion among uninformed users. It is therefore important that investors remain knowledgeable about the product they are purchasing in order to avoid being sold altcoins marketed as bitcoins.

Additional Risks

This discussion simply presents the larger risks to the future utility of the network as we currently see them. It is not meant to be exhaustive, and should not be considered as such. As with any investment opportunity it is important to perform proper diligence and know the risks of the market you are investing in, prior to investment.

SUMMARY

The invention of Bitcoin marks a paradigm shift in the evolution of money. Unforgeable digital bearer instruments have never before been possible within the realm of computer science and the utilization of cryptographic techniques to achieve such properties represent a revolution in the development of digital assets.

For the first time in history humanity is now equipped with provably sound money that is purely democratic in nature and decentralised across the entire Internet. Debasement is no longer possible and monetary power can yet again rest with the users of money, not with a centralised issuer.

Cryptocurrency as an asset class is unlike all others. It combines the monetary properties of gold with the communication properties of the Internet: it is scarce and expensive to create, but can be securely transferred globally in a matter of minutes with no third party permission required.

As an investment, bitcoin has produced stellar returns. An investment of US$ 10,000 at the start of 2014 would have returned approximately US$ 95,000 if it had been held until mid November 2017. Although it still experiences large volatility, its risk-adjusted returns are superior to all other global commonly invested assets. Furthermore, it is entirely uncorrelated to all other non-cryptocurrency assets, making it an excellent addition to a diversified portfolio.

The risks, however, are substantial. This is uncharted monetary and technological territory and Bitcoin could well fail. Regulation may stifle growth, government intervention may make investors uneasy and there may exist technological risks which are currently unknown. As with all investments, conduct your own thorough research on the asset before investing capital. We hope this paper has helped guide your research efforts in the right direction.

GLOSSARY

Cryptocurrency	A cryptographically secured, decentralized, digital bearer asset with a democratically
Bitcoin	Upper case Bitcoin refers to the telecommunications protocol and network
bitcoin	Lower case bitcoin refers to the native currency running on the Bitcoin protocol
Protocol	A set of instructions dictating a common structure of communication between separate parties
Network	A web of interconnected nodes communicating with each other using the same compatible protocol
Nodes	The single unit components of a network
Blockchain	One of the central data structures in Bitcoin, containing all blocks ever mined
Blocks	Modular data structures containing valid Bitcoin transactions, a reference to the previous block, and a proof-of-work
Proof-of-work	A solution to a computationally expensive task, probabilistically proving that the presenter of the proof has expended computational effort in creating it
Miners	Nodes tasked, through competitive computational work, with compiling Bitcoin transactions into blocks and time stamping these onto the blockchain
Mining	Mining refers to the competitive task of expending computational work in order to win the privilege of time stamping blocks onto the blockchain (which is rewarded by the Coinbase transaction) and the act of adding a new valid block to the blockchain
Coinbase	The first transaction in a block where the block miner can create new bitcoins from nothing and send them to themselves as a reward for mining the block
Backwards Compatibility	A change in software that allows interoperability with the previous version of the software
Soft Fork	A change in software that is backwards compatible
Hard Fork	A change in software that is not backwards compatible

CITATIONS

[1] https://bitcoin.org/en/bitcoin-paper

[2] http://p2pfoundation.ning.com/profile/SatoshiNakamoto

[3] https://en.bitcoin.it/wiki/Coinbase

[4] https://lightning.network/

[5] https://coinmarketcap.com/

[6] https://en.bitcoin.it/wiki/Controlled_supply

[7] BAML: Exchanging Views Bitcoin, Ethereum, Ripple – valuing cryptocurrencies, Sep. 8, 2017

[8] https://bitcointalk.org/index.php?topic=80312.1580

[9] https://en.bitcoin.it/wiki/Scalability

[10] https://bitcoin.org/en/bitcoin-core/capacity-increases-faq

[11] https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf

Certification concerning research analysts

The research analyst(s) denoted by an “AC” on the cover of this report certifies (or, where multiple research analysts are primarily responsible for this report, the research analyst denoted by an “AC” on the cover or within the document individually certifies, with respect to each security or issuer that the research analyst covers in this research) that:

(1) all of the views expressed in this report accurately reflect his or her personal views about any and all of the subject securities or issuers; and

(2) no part of any of the research analyst's compensation was, is, or will be directly or indirectly related to the specific recommendations or views expressed by the research analyst(s) in this report.

IMPORTANT DISCLAIMER:

CoinShares (UK) Limited is part of a group of companies (the "CoinShares Group") which includes XBT Provider AB (Publ), the issuer of four series of Certificates listed on Nasdaq Stockholm: COINXBT:SS and COINXBE:SS, which are both referenced to Bitcoin, and COINETH:SS and COINETHE:SS, which are referenced to Ethereum. Members of the CoinShares Group are committed to strong standards of service and corporate governance and are proud of the CoinShares Group's reputation and standing within the world of crypto-currencies and other digital assets. However, CoinShares (UK) Limited, which is the issuer of this document, is not a regulated financial advisor (and does not hold itself out as such) and is not authorised or regulated by the Financial Conduct Authority.

Crypto-currencies can be extremely volatile and subject to rapid fluctuations in price, positively or negatively. Investment in one or more crypto-currencies may not be suitable for even a relatively experienced and affluent investor. Each potential investor must make their own informed decision in connection with any such investment (after having sought independent financial advice thereon). Past performance is not necessarily a guide to future performance. Any estimates of future performance contained herein are based on assumptions that may not be realised.

This research document is not intended for the use of retail investors. (Accordingly, should a retail investor obtain a copy of this report they should not base an investment decision upon the content of this document and are strongly recommended to seek independent financial advice upon any investment which they are contemplating).

The material contained or referred to herein:

- is not (and is not intended to be) an offer to buy or sell (or a solicitation of an offer to buy or sell), crypto-currency, nor does it Constitute investment, legal, tax or other advice; and
- has been obtained, derived or is otherwise based upon sources which are believed to be reliable.

However, no guarantee can be (or is) provided in relation to the accuracy or completeness of the same. To the extent permissible at law, CoinShares (UK) Limited does not accept:

- any liability arising from the use, misuse or non-use of the material contained or referred to herein; or
- responsibility for any financial loss incurred as a result of a decision to invest in one or more crypto-currencies.

Please also note that no member of the CoinShares Group is under an obligation to disclose or otherwise take into account the contents of this document if or when advising customers or dealing with investments on their customers' behalf.

Material contained in this report satisfies the regulatory provisions concerning independent investment research as required under MiFID. Information concerning conflicts of interest, and the management thereof by the CoinShares' Group, is contained in the CoinShares Group's 'Policy for Managing Conflicts of Interests regarding Investment Research.' It should be noted that certain members of the Global Advisors' group of companies, of which the CoinShares Group is a division thereof, do, from time to time, act as a market-maker or adviser in relation to crypto-currencies for individuals and/or entities mentioned in this document (and may be represented on the board or other governing body of such entities). Additionally, such members of the Global Advisors' group do, from time to time, act as a principal trader in the crypto-currencies referred to in this report and may hold those (and other) crypto-currencies. Employees of the Global Advisors' group (including the CoinShares Group), or individuals and entities connected thereto, may also from time to time hold one or more of the crypto-currencies mentioned in this document.

The views and sentiments of the CoinShares Group, expressed or which are reflected in this document, are subject to change from time to time and without notice. The CoinShares Group may (and does intend), from to time, to prepare and issue other reports. These further reports may be inconsistent with, and reach different conclusions to, the information contained or referred to herein. Please note that members of the CoinShares Group are under no obligation to ensure that such other reports are brought to the attention of any recipient of this report.

Additional notice to U.S. Persons: This document is not appropriate for any person (natural, corporate or otherwise) who is a US Person as defined under Regulation S of the United States' Securities Act of 1933, as amended (which such definition includes, for the avoidance of doubt, any US resident, corporation, company, partnership or other entity established under the laws of the United States). Accordingly, this document should not be distributed to, used or relied upon by any US Person.

Additional notice to UK residents: Although not intended to be, this document and the communication of it may contain material that is interpreted as a 'financial promotion' for purposes of the United Kingdom's Financial Services and Markets Act 2000 ("FSMA"). The contents of this document and any communication of it have not been approved by any person for the purposes of Section 21 of FSMA. Accordingly, this document and the communication of it is issued only to, or directed at persons in the United Kingdom who are reasonably believed to be: (i) Investment Professionals within the meaning of Article 19 of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 ("FPO"); (ii) Certified High Net-Worth Individuals within the meaning of Article 48 of the FPO; (iii) High Net-Worth companies, unincorporated associations etc. within the meaning of Article 49 of the FPO; (iv) Sophisticated Investors within the meaning of Article 50 of the FPO; (v) Self-certified Sophisticated Investors within the meaning of Article 50(A) of the FPO; and (vi) Associations of High Net-Worth or Sophisticated Investors with the meaning of Article 51 of the FPO.

THE NETWORK IS **ROBUST IN ITS UNSTRUCTURED SIMPLICITY.** NODES WORK ALL AT ONCE *WITH LITTLE COORDINATION.*

SATOSHI NAKAMOTO
BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM

CS