cryptocurrency | digital asset class of the future – bitcoin vs ethereum?

the economist | kraken bitcoin exchange

Ramis Jamali, CFA
Sherwin Li, P. Eng.
Rodrigo Pantoja

Ivey Business School



You have \$1M to invest across two blockchain technologies by buying

bitcoins and ethers – the digital assets or "cryptocurrencies" that power these decentralized computer networks. You cannot touch your investment for the next 5 years. How much of that \$1M do you invest in each? Why?

Cryptocurrency has been a hot topic over the last few years, with hundreds of alternative coins in existence attracting attention from investors. Bitcoin and Ethereum are two prominent platforms, with their respective currencies: bitcoin and ethers, having the largest market cap among cryptocurrencies. To evaluate long-term investment potential, investors need to understand the function cryptocurrencies serve, the underlying technology and their governance structure. We ask the questions: do bitcoin and ethers function as a currency? What are the fundamental technical differences? How does the governance structure benefit one over the other? This paper concludes that cryptocurrencies do not function as money, valuation is driven almost exclusively by speculation and value drivers cannot be determined. Therefore, we conclude that although the underlying technology, blockchain, is revolutionary and provides investment opportunities, the cryptocurrencies bitcoin and ether are speculative in nature are not appropriate as an investment asset class.

Table of Contents

Currency	3
rechnology	
Governance	12
Market Statistics	14
Conclusion	18
References	19

currency

Brief history of currency and our position on cryptocurrency

Commodities

The use of obsidian, grain, rice, and cattle was documented as early as 9000 BCE and is known as commodity money – objects that have value in themselves as well as value in their use as money. Cultures around the world have developed own forms of commodity money through history. For example, commerce within the context of the fur trade in North America during the 18th century saw the use of beaver pelts as a commodity currency. One beaver pelt could be traded for the following: 2 lbs of sugar, 20 fish hooks, 1 gallon of brandy, 1 pair of breeches, etc. Even today commodity money is used in various circumstancess such as cigarettes among prisoners in jail.

Coinage & Representative Money

To provide ease of transportation, coins and later, representative paper money were used. These are currency that can be exchanged for a fixed amount of a valuable commodity, usually gold or silver due to widespread acceptance and perception of value by most cultures. The money is therefore backed by a commodity. For example, in 1715, some states issued tobacco notes which could be converted to a certain amount of tobacco on demand.

Lydian Lion Coin

Speculatively, the first coin in the history of coinage was the Lydian Lion coin, minted by King Alyattes in 600 BC in Lydia (present-day Turkey).



Flowing Hair Dollar

The most expensive coin to date was a 1794 Flowing Hair Dollar, sold for \$10 million dollars at an auction in 2013. The 1794 Flowing Hair Dollar was the first dollar coin minted by the US Mint.



Fiat currency

Fiat, latin for "it shall be", is money that is not backed by a physical commodity. What drives the value of fiat currency is its scarcity and the fundamentals of supply and demand. It is declared by a central authority, a government, to be legal tender. Therefore, another aspect to fiat valuation is its trust by users. If people lost faith in the fiat money, or if the government refused to guarantee its value, the money would be worthless. An example of this hyperinflation is the Zimbabwean dollar. The US dollar has been fiat money since 1971 when President Nixon canceled the convertibility of US dollars to gold. Today, the US dollar is backed by the "full faith and credit" of the US government. Currently most nations utilize fiat currency in their economies.

The functions of money

To assess cryptocurrencies usefulness as money, we look at the three functions of money:

- 1. **Medium of exchange** money facilitates transactions where buyers and sellers can easily agree on the value of the goods or services. Without money, transactions would have to be conducted through a bartering system, which would require a buyer and seller offering goods or services the other wants: the double coincidence of wants.
- 2. **Store of value** refers to the requirement that money must transfer value over time.
- 3. **Unit of account** allows goods and services to be measured in a standardized unit, enabling economic agents to make decisions.



Does Cryptocurrency function as money?

In order to determine if cryptocurrencies can be considered currencies, we will assess if it serves the three classical functions of money:

Medium of exchange – at some level cryptocurrencies *can* serve as a medium of exchange, although their acceptance is currently limited. Any two parties can choose to transact in cryptocurrency or through any other medium if they wish. Money is not the only medium of exchange and parties are free to choose what they want as a medium, leafs on trees for example. Bitpay, world's largest bitcoin payment processor, reported 100,000 transactions in 2015. Bitpay has slightly over 50% market share of the bitcoin payment market, if we extrapolate the volume, roughly 200,000 bitcoin transactions were completed in 2015. This clearly indicates that bitcoin serves as a medium of exchange.

Store of value – although some may argue that bitcoin serves as a store of value, this is ill-founded. Bitcoin, a virtual currency, is only as valuable as the market deems it to be and only valuable if it can be converted to a local currency. Bitcoin will not have a value if it cannot be converted to any other currency. In addition, Bitcoin cannot be deposited in a bank, and instead it must be possessed through a system of "digital wallets" that have proved both costly to maintain and vulnerable to hackers.

Unit of account – Cryptocurrencies exhibit very high time series volatility and trade for different prices on different exchanges without a centralized price aggregation mechanism or the possibility of arbitrage. We understand that the volatility and unpredictability of cryptocurrencies' prices undermine their usefulness as units of account.

Based on the above analysis, cryptocurrencies do not serve the traditional functions of a currency.

technology

Technical differences between Bitcoin and Ethereum



Cryptocurrency: An Analogy

Think of the blockchain technology as the construction of a skyscraper. Starting at the floor, you must add blocks onto the previous block. Each block is "connected" to the previous block and references part of the previous block. Similar to how a child inherits DNA from the parents; new blocks reference code from prior blocks, all the way to the "genesis block".

The concept of decentralization and trust can be explained with the skyscraper. A skyscraper, say the Empire State Building, is available for everyone to see. A concrete block on the Empire State Building is true and verifiable because everyone in the world can see it for themselves. To alter a block on the blockchain or skyscraper would have to involve changing the sight and memory of every person who has confirmed that block on the Empire State Building exists, as well as changing all subsequent blocks that reference the block that is being changed. Therefore, data in the blockchain is considered immutable.

Think of each block as a housing for information, or specifically transactions with written code within. Once enough transactions have occurred, a block is created and must be added to the blockchain. The actual process of connecting blocks is done through computational power. To connect a block requires solving a complex mathematical problem akin to guessing the combination on a large combination lock. If any data within the block is changed, the combination password is also changed.

The people who connect the blocks, the bricklayers and construction workers, are called miners. They use powerful computers to connect blocks. Whoever connects the block first, guessing the correct combination, is rewarded with the cryptocurrency: a bitcoin or an ether. The cryptocurrency is therefore a reward for connecting blocks together.

Bitcoin vs Ethereum

Technical differences between the two platforms are a dimension of product differentiation, and represent a source of competitive advantage. Analysis of these technical differences can be used to imply valuation. We analyze various aspects of the underlying technology and ecosystem.

Scripting Language

While bitcoin utilizes a scripting language, Ethereum's language is Turing-This allows for greater complete. complexity in programming and allows for smart contracts code to be written into the transactions. This has widespread appeal in many applications, such as financial services, where smart contracts can be written for regulatory compliance purposes. The ability to write smart contracts into transactions is one of Ethereum's key differentiators and a clear competitive advantage.

Advantage: Ethereum

Mining Technology

Bitcoin mining is primarily performed by specialized **ASIC devices** at speeds of 10 minutes per block using **SHA-256 hashing** whereas Ethereum uses a different algorithm that allows blocks to mined at much faster speeds: one block per 15 seconds. The ethereum algorithm is also designed to be mined by less expensive graphics cards as opposed to ASIC devices. The result is that Ethereum is more scalable.

Advantage: Ethereum

Terminology

Turing Complete

Turing completeness is a concept in which a machine can theoretically solve any computational program given enough time and memory. This is the key that unlocks the ability to write smart contracts.

Smart Contracts

Smart Contracts are programs written in programming code that are run on the blockchain which are attached to transactions. Since the code is written on the blockchain, the code itself is also immutable and censorship-free. The program itself also controls the asset. An example of a smart contract could be "Send x bitcoins from person A to person B on October 12, 2016". A more complex smart contract could be written such that "if person A passes away, verified by external data, transfer x bitcoins to person B, and change the appropriate land title from person A to person B".

ASIC

ASIC stands for Application Specific Integrated Circuit and is a microchip designed for one specific application, as opposed to general integrated circuits such as common RAM in a computer. In the context of bitcoin mining, ASIC devices are designed to maximize bitcoin mining, quantified by hash rate, while considering electricity costs. An example of an ASIC Bitcoin Miner is the Antminer S9 which retails around \$3000 USD and has a hash rate of 14 TH/s.

SHA-256

Secure Hash Algorithm is essentially a specific method of hashing. Hashing in turn, is the act of using computational power to guess the correct combination required to add the next block onto the block chain. SHA-256 promotes the use of ASIC machines to solve the combinations. Ethereum does not utilize SHA-256 and its algorithm instead enables ordinary graphics cards for computational power.

Blockchain Security

Bitcoin, being in existence since 2009 has a first-mover advantage and has built up considerable mining infrastructure. The current bitcoin hashrate is 1,800,000,000 GH/s compared to Ethereum's 6000 GH/s The result is that it is much costlier to attack Bitcoin's system. Another aspect of security rests in the complexity of the programming. Ethereum's complexity of code creates opportunities for security threats. This has led to the infamous "The DAO attack" of June 18, 2016 where 3.6MM ethers were "stolen". Attacks continue as recently as October 2016.

Advantage: Bitcoin



Community Support Metrics

All alternative coins require constant coding and development activity to progress the ecosystem. Supplementary to development, the ecosystem also requires a supportive community. Public interest is also crucial to gain awareness as a prerequisite to be recognized as a legitimate mainstream currency. Finally, liquidity is important as well. These metrics have been calculated by coingecko.com using parameters such as reddit subscribers, trading volume, code contributors, search engine requests, etc. It is clear that the Bitcoin ecosystem is much more advanced and developed compared to Ethereum. This is not unexpected as Bitcoin has a longer tenure and first mover advantage, whereas Ethereum is still in its nascent stages of development.

Advantage: Bitcoin

Decentralization of Power

Both Bitcoin and Ethereum have concentrated hashrate distribution. The majority of bitcoin mining exists in China, and the majority of bitcoin exists in the control of early miners. Ether's beginnings on the other hand were mostly crowdfunded and pre-mined. Ethereum's hashing algorithm that encourages the use of individual graphics cards instead of group mining using ASIC devices promotes decentralisation. The Ethereum algorithm also rewards uncompleted blocks, known as "Uncle Blocks" which allows individual miners to profit without necessitating participation in a large pool.

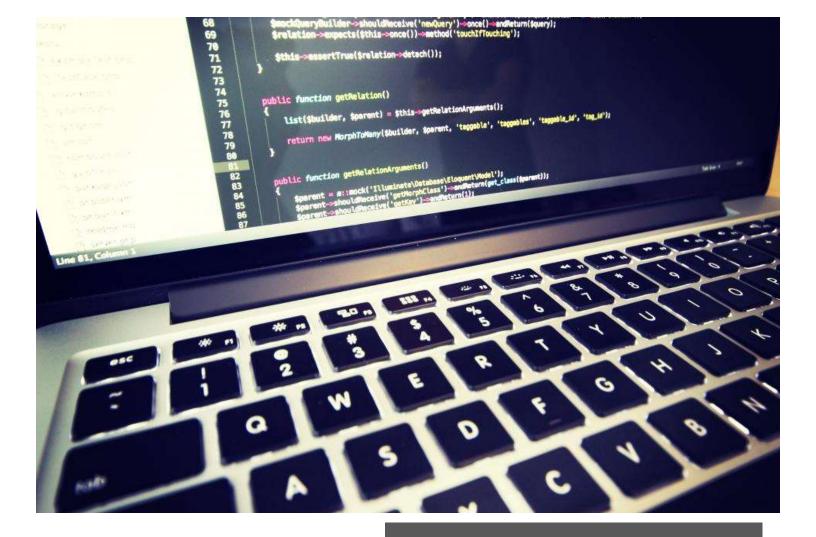
Advantage: in practice: Unknown; in theory: Ethereum

Block Size

Bitcoin has a maximum block size of 1 MB, whereas Ethereum's block size is dynamic and depends on the complexity of contracts being run in the transactions within the blocks. The complexity of each contract is measured in a unit called "gas" and an Ethereum block currently has a maximum size of 1,500,000 Gas. However, the gas limit per block is also variable, and therefore adds another dimension of block size variability. Generally, most Ethereum blocks are under 2 kb in size. The variability in block size enables Ethereum to become more scalable.

Advantage: Ethereum





Mining Technology

Bitcoin mining is primarily performed by specialized **ASIC devices** at speeds of 10 minutes per block using **SHA-256 hashing** whereas Ethereum uses a different algorithm that allows blocks to mined at much faster speeds: one block per 15 seconds. The ethereum algorithm is also designed to be mined by less expensive graphics cards as opposed to ASIC devices. The result is that Ethereum is more scalable.

Advantage: Ethereum

The DAO Attack of June 18, 2016

specific Dao, was a decentralized autonomous organization. Think of a DAO as an investor-directed without capital fund venture management team. Investors gain the right to vote, but no ownership. The DAO became very popular and crowdfunded a total of \$150MM worth of ethers from 11,000 investors through an ICO (initial However, the DAO was coin offering). attacked through a legitimate loophole and drained of approximately \$50MM worth of ethers into a child DAO, which eventually spawned a clone "ether classic" currency, with competing philosophies. The Ethereum community subsequently decided to perform a "hard fork", which conceptually is akin to "rolling back" the transaction and reversing the attack.

Summary of Tech

The underlying Ethereum blockchain technology is a step-change in innovation. Its greatest asset remains its advanced scripting language and hashing algorithm. This allows the Ethereum network greater flexibility and scalability across many applications. We have seen mainstream investment into private Ethereum-based blockchain technology through institutions such as JP Morgan.

The flip side is that Bitcoin has had years of developer support and has progressed in a relatively steady pace with an emphasis on security. The first-mover and network advantage of bitcoin cannot be understated. Currently, bitcoin acts as the defacto reserve currency of cryptocurrencies.

To characterize the two platforms: Bitcoin is a more mature, stable, conservative platform with an emphasis on security. Its primary purpose is the promotion of the bitcoin cryptocurrency. Ethereum is an agile, complex, and relatively untested platform whose purpose is as a platform for applications. The associated ether then, plays more of a supporting role, acting as "fuel" for the platform.

Many within the community have alluded to a complementary coexistence between the two platforms: a proverbial yin yang, and in this regard we agree. Both the security and network of bitcoin and the technology behind Ethereum cannot be written off. Both platforms provide investment opportunities, albeit at different risk profiles.



governance

Cryptocurrency is built on the premises that a decentralized governance model, controlled by the community and all stakeholders, can manage money more efficiently than a centralized organization. What exactly is governance and is it really decentralized for bitcoin and ethereum?

A mechanism for control and change management must exist, even for cryptocurrenies. Without an agreed upon mechanism the cryptocurrency world would be the wild wild west; nobody in charge means everyone is in charge. What will happen if something goes wrong with the technology? Who is responsible for bug fixes? And new features?

Bitcoin and Ethereum have a similar governance model with some important differences impacting long-term investment.

Bitcoin Governance

Bitcoin subscribes to the consensus governance model: all stakeholders have to agree for a change to be implemented. The proponents of this Libertarian model argue that this was the intention of Satoshi Nakamoto, the enigmatic creator of bitcoin. Although at a philosophical level this benevolent paradigm is sound, it presents a predicament from an investment valuation perspective.

A decentralized governance is needed to ensure no single individual or entity can control the currency and take advantage of the system. This was the criticism of central banks and what gave birth to bitcoin. However, a decentralization also means that nobody has unilateral control. So who controls the bitcoin protocol? Bitcoin has a volunteer "core team" of developers who maintain the code and make updates as needed. They don't own bitcoin, but they act as a "control." Anyone can submit changes or suggestions to the community, these changes will be put up for vote and implemented by the core team when consensus is reached. Depending on the scope of the change, implementation time will vary. A simple bug fix or improvement can be implemented quickly; however, a significant policy change will take much longer to be debated, voted on and implemented.

This means innovation and significant improvements within bitcoin will be slow and cumbersome. A polarizing debate within the community revolves around block size. Block size refers to the amount of data and processing time of a batch of transaction to be confirmed; think of this as a stack of paper confirmation slips at a bank. The larger the block size the more power is needed to process them. The issue is that due to growing number of transactions the sizes of these blocks are increasing beyond the set limit, resulting in potential delays and overload on the network. To resolve this issue block sizes can be increased. However, larger block sizes can potentially give more power to large mining pools who can process these larger block sizes faster, resulting in some form of centralization and taking power away from the people. The debate on how to solve this issue has been ongoing for a while within the bitcoin community, and we are no closer to a solution. This tends to be a typical pattern when it comes to significant protocol changes within the bitcoin community.

The lack of agility and requirement for consensus makes bitcoin's underlying technology slow and not an attractive investment option in the long-term.

Ethereum Governance

Ethereum is built on a similar philosophy: decentralization and autonomous currency. In many ways Ethereum has a similar governance structure as Bitcoin with a few important differences. The creator and founder is known and there some form of a "corporate structure." Although this is not a management team in the traditional sense, it is more structured than bitcoin is.

Ethereum has chosen a different path when it comes to critical issues. In the past the development team has taken a more unilateral approach to solve critical issues. A recent example is the development teams' response after the DAO attack. After an attack earlier this year 3.6m ethers, the currency of Ethereum, was "stolen," and raised some ethical dilemmas. Ethereum had two options: 1. Leave things as they are or 2. Remove the stolen currency from the blockchain. The developers created a new chain, hard fork, and removed the stolen ether from the blockchain and let the community decide which chain to follow. In simple terms, there are now two different ether chains, the old one is referred to as the ether classic. The classic is the original chain that includes the stolen ethers, while the new chain does not. Ethereum left it up to the community to choose which chain to follow.

Although there was backlash from the community, this model incorporates a "central" control with democratic process. The development team introduces some changes if it deems it necessary and then lets the community decide which will survive. This allows Ethereum to be more responsive and agile compared to bitcoin.

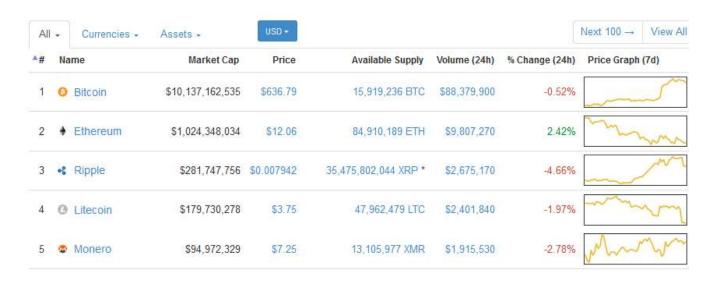
Ethereum's project governance should allow it to be more innovative and outpace bitcoin in technological advancement, making it a more attractive platform.

market statistics

Market Capitalization

According to coinmarketcap.com, at the time of writing, there are currently 645 digital currencies (aka cryptocurrencies) around the world, trading in 2,311 markets or exchanges. **Bitcoin** is the largest digital currency by market capitalization (\$10.1 billion, or 75% of the total market) and daily volume (\$88 million), followed by **Ethereum** (see statistics below):

Crypto-Currency Market Capitalizations



24 Hour Volume Rankings (Currency)



← Back to Top 100

1. Bitcoin (75.43%)

#	Source	Pair	Volume (24h)	Price	Volume (%)
1	E-DINAR	BTC/BRL	\$27,064,100	\$635.97	30.87%
2	Poloniex	ETH/BTC	\$4,383,010	\$636.73	5.00%
3	BitMEX	BTC/USD	\$3,879,130	\$632.32	4.42%
4	DABTC	BTC/CNY	\$2,837,300	\$641.53	3.24%
5	GDAX	BTC/USD	\$2,747,920	\$635.10	3.13%
6	BTC-E	BTC/USD	\$2,720,850	\$633.00	3.10%
7	Kraken	BTC/EUR	\$2,704,680	\$637.29	3.08%
8	Gemini	BTC/USD	\$2,392,380	\$635.44	2.73%
9	Bitfinex	BTC/USD	\$2,332,760	\$637.07	2.66%
10	BTC-X	BTC/EUR	\$2,067,180	\$640.65	2.36%
		View Mo	ore		
Tot	al/Avg		\$87,681,589	\$636.66	

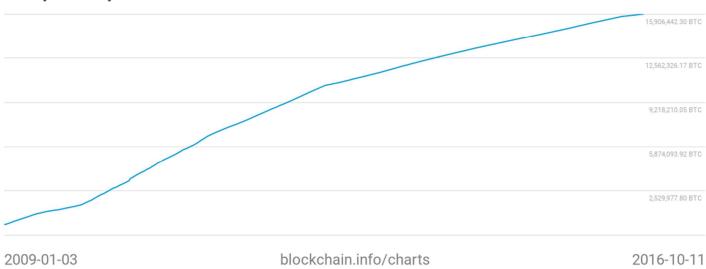
2. Ethereum (8.65%)

#	Source	Pair	Volume (24h)	Price	Volume (%)
1	Poloniex	ETH/BTC	\$4,383,010	\$12.14	43,60%
2	Kraken	ETH/BTC	\$1,123,090	\$12.08	11.17%
3	Kraken	ETH/EUR	\$566,562	\$12.11	5.64%
4	BitMEX	ETH/BTC	\$554,067	\$12.26	5.51%
5	GDAX	ETH/USD	\$480,311	\$12.05	4.78%
6	Bitfinex	ETH/USD	\$479,435	\$12.10	4.77%
7	Kraken	ETH/USD	\$384,881	\$12.03	3.83%
8	YoBit	ETH/BTC	\$274,105	\$12.13	2.73%
9	Coinone	ETH/KRW	\$189,373	\$12.41	1.88%
10	Poloniex	REP/ETH	\$170,762	\$12.13	1.70%
		View Mo	ore		
Tot	al/Avg		\$10,053,060	\$12.13	

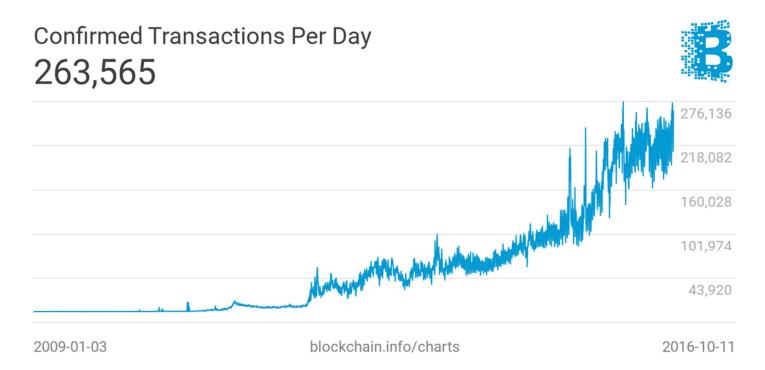
Bitcoins in circulation

15,924,412.50 BTC





The number of bitcoins in circulation is currently growing at an increasingly slower pace, in part because of the emergence of other cryptocurrencies and an increased difficulty in mining, rending mining inaccessible for a typical person.

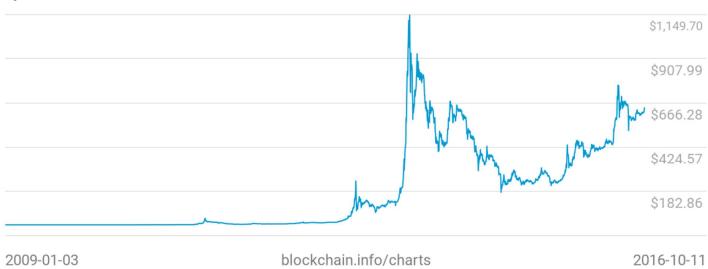


It is important to note that the chart above overstates the use of bitcoins as a medium of exchange because these transactions include situations in which bitcoins are being bought and sold for speculative reasons.

Market Price (USD)

\$639.31

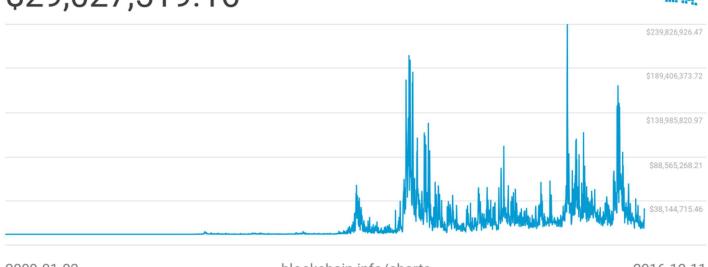




It is important to note that the chart above overstates the use of bitcoins as a medium of exchange because these transactions include situations in which bitcoins are being bought and sold for speculative reasons.







conclusion

Although blockchain technology brings innovation and a variety of new applications to many industries, it is clear that the cryptocurrencies based on this technology entail numerous risks:

- 1. The intrinsic value of any cryptocurrency is extremely hard to assess;
- 2. Existing cryptocurrencies are very volatile and this lack of stability might cause investors to experience a permanent loss of capital;
- 3. Digital currency schemes are not (yet) regulated and not closely supervised or overseen by any public authority, and this lack of oversight reduces investor confidence;
- 4. Cryptocurrencies lack transparency, clarity of legal status and certainty of continuity;
- 5. Their functioning is highly dependent on IT, developer and community support;
- 6. Anonymity of the economic agents involved increase counterparty risk and create a market that can be used for illegal activities;

Based on our research and interactions with market participants, we view cryptocurrencies currently behaving more like a speculative investment rather than a conventional currency. At this point, we cannot recommend either Bitcoin, Ethereum or any cryptocurrency as a feasible investment alternative for investors seeking to compound the value of their wealth over time. We have a bias towards the technology of Ethereum, as the platform is scalable and useful to institutions.

The good news is that, as the blockchain technology evolves, creating operational efficiencies in virtually every industry, potentially great investment opportunities are arising in companies surrounding the blockchain ecosystem, such as financial institutions, exchanges, blockchain startups and e-commerce, to name a few. These beneficiaries are tangible cash flow generators that can increase their competitive advantages by adopting this new technology.

We recommend investment in the surrounding ecosystem rather than the cryptocurrency itself, in order to take advantage of the blockchain technology while minimizing exposure to volatility related to the associated cryptocurrency.

bibliography

- 1. Bank, European Central. (2015). *Virtual currency schemes a further analysis*. Frankfurt, Germany: European Central Bank.
- 2. Biegel, O. (n.d.). *What is a bitcoin hash and SHA-256*. Retrieved from YouTube: https://www.youtube.com/watch?v=9mNgeTA13Gc
- 3. Bradshaw, D. (2015). NYU Stern broadens impact of bitcoin expertise. Financial Times.
- 4. BTCManager. (2016, 10 15). *Ethereum continues to be exploited*. Retrieved from BTC Manager: https://btcmanager.com/news/tech/ethereum-continues-to-be-exploited-another-hard-fork/
- 5. Caffyn, G. (2015, August 21). What is the Bitcoin Block Size Debate and Why Does it Matter? Retrieved from Coindesk: http://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/
- 6. Chen, A. B. (n.d.). Bitcoin: Technical Background and Data Analysi. Finance and Economics Discussion Series Divisions of Research & Statistics and Monetary Affairs Federal Reserve Board, Washington, D.C.
- 7. Chris Burniske, A. W. (2016). *Bitcoin: Ringing the Bell for a New Asset Class*. San Francisco: Ark Invest Research.
- 8. Coindesk. (n.d.). *Making Sense of Smart Contracts*. Retrieved from Coindesk: http://www.coindesk.com/making-sense-smart-contracts/
- 9. Diaz, C. D. (2015, December 17). Who controls Ethereum? The relationship between Ethereum and ConsenSys: a mystery that matters. Retrieved from Medium.com: https://medium.com/@celeduc/who-controls-ethereum-94fcb4aa3a50#.xodo2v329
- 10. Hayes, A. (2015). What factors give cryptocurrencies their value: An empirical analysi. New York: The New School for Social Research.
- 11. McGrath, R. (2016, July 21). *Cryptocurrency Governance Processes: A Master Class*. Retrieved from Robert McGrath's Blog: https://robertmcgrath.wordpress.com/2016/07/21/cryptocurrency-governance-processes-a-master-class/
- 12. Nakamoto, S. (n.d.). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org.
- 13. StackExchange. (n.d.). What does it mean that Ethereum is "turing complete". Retrieved from EthereumBeta: http://ethereum.stackexchange.com/questions/2464/what-does-it-mean-that-ethereum-is-turing-complete
- 14. Todd, P. (2016, June 21). *Will The Cryptocurrency Industry Figure Out Governance?* Retrieved from Velocity Blog: http://blog.velocity.technology/cryptocurrency-governance/
- 15. Yermack, D. (2013). *Is Bitcoin a Real Currency?* New York: New York University Stern School of Business.