



crypto

research

.report

**October 2018
Edition IV.**



Smart Contracts

Liechtenstein's Blockchain Strategy

The "Network Effect" as Valuation Methodology

Demelza Kelso Hays

Mark J. Valek



incrementum

We would like to express our profound gratitude to our premium partners for supporting the Crypto Research Report:

Vontobel



www.cryptofunds.li



Contents

Editorial.....	4
In Case You Were Sleeping: Cell Phone Theft Edition	5
A Heist With Perfect Timing	6
Your Phone Could Cost More Than You Think	6
How to Store Bitcoin.....	8
From China to Liechtenstein	9
ETF or No ETF?	11
A Game Changer by the Name of BAKKT	12
The Real World Discovers Bitcoin.....	13
The Final Showdown.....	15
Crypto Concept: Smart Contracts.....	18
Smart Contracts, Decentralized Applications, and Decentralized Autonomous Organizations	19
Smart Contract Theory Applied In Practice	21
Crypto Asset Companies That Use Smart Contracts, DApps, and DAOs	22
When Smart Contracts Are Dumb.....	23
Liechtenstein’s Blockchain Strategy: Prime Minister’s Outlook	30
The Network Effect As a Valuation Methodology	38
The Network Effect.....	39
Metcalfe’s Law Applied to Crypto Assets	40
Network Value to Metcalfe Ratio	41
Network Value to Transaction Ratio.....	44
Network Value/Transaction Value to Growth.....	47
Liechtenstein’s Blockchain Strategy: Insights from the Financial Market Authority	50
Coin Corner: ETH, NEO, ADA, & EOS.....	55
Smart Contract Platforms: Who’s the Smartest in Town?	56
Wrong Dichotomy.....	56
A Non-centralized World Computer.....	57
Why a Programmable Blockchain?	58
Gas – an Essential Component Of Ethereum	58
Can Ethereum Hold Steady?.....	59
Academia Goes Blockchain	60
China Takes on Ethereum.....	62
Differences Are Evident	63
EOS – Ethereum’s Biggest Competitor?	65
Inflation as a Reward	66
Attacking Ethereum.....	67
What About Decentralization?.....	68
A Fight That Is None?	69

Disclaimer:

This publication is for information purposes only and represents neither investment advice, nor an investment analysis or an invitation to buy or sell financial instruments. Specifically, the document does not serve as a substitute for individual investment or other advice. The statements contained in this publication are based on the knowledge as of the time of preparation and are subject to change at any time without further notice.

The authors have exercised the greatest possible care in the selection of the information sources employed, however, they do not accept any responsibility (and neither does Incrementum AG) for the correctness, completeness, or timeliness of the information, respectively the information sources made available, as well as any liabilities or damages, irrespective of their nature, that may result therefrom (including consequential or indirect damages, loss of prospective profits or the accuracy of prepared forecasts).

Editorial

Dear Reader,

Liechtenstein, the home of Incrementum AG and the Crypto Research Report, is the focus of this edition. One highlight of this report is an exclusive interview with Liechtenstein's Prime Minister, Adrian Hasler. Additionally, we cover Liechtenstein's new blockchain law and discuss how this law may impact the global crypto market with a regulator from Liechtenstein's Financial Market Authority. Although taxes on initial coin offerings are lower in other jurisdictions such as Singapore, the Government of Liechtenstein is signaling to investors that the country is open for business. The world's first regulated security token was approved by regulated in September in Liechtenstein.

After our quarterly recap, our **Coin Corner chapter** compares Ethereum, NEO, and the newly released EOS. In the long-term, we doubt that the market can support hundreds of blockchains that have very similar features. Instead, a few distinct blockchains with strong development teams will dominate. Complementary to the Coin Corner chapter, the **Crypto Concept chapter** contains an in-depth analysis of smart contracts, and we discuss why smart contract platforms, such as Etherisc and Polkadot, are making waves in the cryptocurrency market.

Finally, we discuss the "network effect" as potential valuation methodology for crypto tokens. Bitcoin has entered its third bear market that has lasted over six months. The year-to-date return is roughly -50 %, although, the year-over-year return is about +150 %. **However, our network calculations overwhelmingly indicate that the cryptocurrency market is still overbought, and according to this valuation method further corrections could be ahead.**

This edition concludes our first year of publications, and we are excited to embark on our second year of writing the Crypto Research Report. Over the next few months, Airdrops, decentralized exchanges, and atomic swaps will become increasingly relevant for investors and regulators, and our December edition will feature special insights into the legal consequences of these technological advances. Furthermore, we will cover the market sentiment towards the blockchain technology in the Middle East.

Thank you for continuing to read the Crypto Research Report and provide constructive criticism on our analyses. ***As always, the fourth edition of the report will be available for free in German and English on our homepage, CryptoResearch.Report.***

***Demelza Kelso Hays and Mark Valek
Incrementum AG***

In Case You Were Sleeping: Cell Phone Theft Edition



Key Takeaways

- The CBOE plans to launch Ethereum futures, the World Bank has launched the first Bitcoin “Bond”, and NASDAQ will list and trade Bitcoin, Ethereum, and other Cryptos by 2019.
- The Capgemini World Wealth Report shows, more than half of the world’s high net worth individuals (HNWIs) are at least superficially interested in Bitcoin. However, investors still are not able to store cryptocurrencies securely. Coinbase estimates \$ 20 billion will flow into cryptocurrency custodian services this year.
- Cryptocurrency wallets are more secure when two-factor authentication (2FA) is enabled; however, using a phone number for 2FA can make accounts susceptible to hackers. Google Authenticator and Authy are preferred 2FA applications.

Satoshi's vision is very much alive. Nobody wants to miss out on the journey even though it is going to be one hell of a ride.

A Heist With Perfect Timing

Hindsight is an incredible thing. We now know that a Bitcoin investor could have easily sold back in January 2018 when the price was still above \$15,000. We are also cognizant that a Bitcoin investor should have not bought at the high of the last mania in hopes of Bitcoin soaring to \$25,000, \$30,000 or even \$50,000 per Bitcoin.

"It's a fascinating market... a \$400 billion market that nobody owns... we've never seen that before...the industry as a whole could easily go to \$4 trillion, \$40 trillion is definitely possible. It's the ten-year forecast, it's not going to happen overnight."

Dan Morehead,
CEO of Pantera Capital

One thing we do know for sure: once you bought them, you have to be careful how you store digital currencies. Easier said than done – and nobody knows this better than Michael Terpin.

The American entrepreneur and investor has been part of the Bitcoin space for a long time. Since 2013, he has been a part of a group of Angel Investors that invest in young Bitcoin companies. Their name: BitAngels. Back in March 2014, this also led to one of the first digital currency funds. Terpin is now a consultant for Alphabit Fund, one of the biggest hedge funds in the crypto sector.

This is, however, all secondary. Today, Terpin is subject to headline news due to his immense misfortune – and his own legal creativity. In January of this year, he was the victim of a cryptocurrency theft that was the equivalent of \$23 million.¹

Your Phone Could Cost More Than You Think

Terpin became victim to a new type of scam where **an attacker gains access to the SIM card of the cellphone of their victims**. Many websites use the mobile number of their users as a further security measure for more online safety by sending a SMS if there is unusual activity on an account or if certain steps need verification. This is called two-factor authentication (2FA), **which can also be achieved with Google Authenticator and Authy**.

As with almost all security features, 2FA can be misused if hackers are able to gain control over the mobile device. **This method of digital identity theft is also used to illegally gain access to popular social media accounts**. Those are then sold via the Darkweb and traded in Bitcoin. But in Terpin's case, it wasn't his Instagram handle that was compromised. Instead, Bitcoin and other cryptocurrencies were directly stolen from his account.²

—

¹ See "U.S. investor sues AT&T for \$224 million over loss of cryptocurrency," Gertrude Chavez-Dreifuss, *Reuters*, August 15, 2018.

² See "The SIM Hijackers," Lorenzo Franceschi-Bicchierai, *Motherboard*, July 17, 2018.

“...bitcoin could definitely see \$50,000 in 2018...we will probably go through a suffering period of volatility.”

Jeet Singh

How do we know this? From the victim himself. He argues that the fault lies with his mobile provider AT&T, and he wants to go to court. His lawyers have prepared a 69-page paper, which supposedly illustrates the culpability of the network operator. Terpin is suing AT&T for compensation of the stolen \$23.8 million – based on the price at the time the digital currencies were stolen. The day the hack occurred was January 7th, 2018, when a single Bitcoin was worth just over \$17,000.

This was also the day that the Bitcoin price spiked for the last time. During the following four weeks, the price plummeted by more than 60 %. It finally stopped at roughly \$6,000. At the time of writing this report, the price is only merely above this mark. One could almost assume Bitcoin has reached some kind of support at this level. This is at least what investors hope, although a further sell-off could be on the cards. **When a price floor is broken on the downside, it spells trouble for investors because this floor becomes a resistance level on the way back up.** As we suggested in the technical analysis article featured in our [March edition](#), there have been two price rallies since our last report but no new higher highs. **The bear market is still in full swing.**

Figure 1: Year-to-Date Bitcoin Price

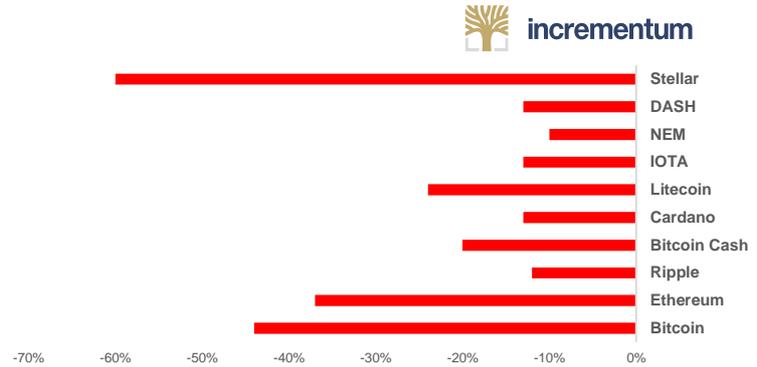


Source: Coinmarketcap.com, Incrementum AG.

Anyhow, Michael Terpin has bigger fish to fry. He is not only suing for the stolen money but also for damages of \$200 million. Should Terpin’s lawsuit be successful, he will not only have found a way to balance out his portfolio against the ups and downs of this volatile market but also how to 10x his money during the bear market. It goes without saying that AT&T refutes any kind of responsibility.

What does this story teach us? Even investors that have been in the sector for years and have accumulated millions are none the wiser when it comes to securing their crypto stash. The details of the heist are not 100 % clear; however, the press coverage leads us to believe that Terpin kept most of his portfolio at an exchange and that one or more of Terpin’s trading accounts were simply wiped out by a hacker. **A further possibility would be that he had saved his private keys insecurely, for example, in his email account or on one of the cloud service providers.** Both insecure options that are not advisable. However, he is not the only one having trouble storing his stash.

Figure 2: Year-To-Date Return of Top 10 Coins



Source: Coinmarketcap.com, Incrementum AG.

How to Store Bitcoin

The question of how to securely store Bitcoin has been around since the emergence of cryptocurrencies. At first glance, it would seem ironic that cryptocurrency users often store their cryptocurrencies with intermediaries such as exchanges and banks because the public blockchain technology was designed to work without banks, registrations, or licenses. It is its own monetary system which insures reliable trade via the Internet.

“No one has ever hacked the bitcoin blockchain, it is the most secure place to put your money and as a stored value it is a great place to be.”

Tim Draper

This was reason enough for technically savvy early adopters to get into Bitcoin. And still we can observe that in extreme circumstances Bitcoin continuously plays its role as a safe haven currency. A look at Venezuela’s current situation of hyperinflation is enough to underline this theory.³ In stark contrast, we can see that Bitcoin remains mainly a speculative asset in the West where price inflation is relatively stable and low, at least for now.

The question of access and storage of digital assets remains largely unanswered. The mainstream investor does not want to bother with private keys or hardware wallets. Cumbersome access and storage also deter institutional players from the sector. **Mature solutions for Bitcoin custodianship are only slowly trickling onto the market.** The investment bank Nomura founded a consortium with the companies Ledger and Global Advisors to come up with a veritable solution. The name: Komainu. Also, three big banks are working on their own solutions: Bank of New York, JP Morgan, and Northern Trust.⁴

A further player is – of course – Coinbase, the emerging Bitcoin giant. Kyle Samani, a partner with the crypto hedge fund Multicoi Capital, is currently testing their custodian service. Bloomberg has even gone as far as to call it a game changer. “There are a lot of investors where custodianship was the final barrier,” Samani said in a phone interview with the news agency. **“Over the next year,**

³ See “Bitcoin Trading in Venezuela is skyrocketing amid 14,000% inflation,” John Detrixhe, Quartz, June 8, 2018.

⁴ See “Regulated Crypto Custody Is (Almost) Here. It’s a Game Changer,” Olga Kharif and Sonali Basak, Bloomberg, June 18, 2018.

the market will come to recognize that custodianship is a solved problem. This will unlock a big wave of capital.”

Coinbase charges a onetime fee of \$100,000 and then a further 0.1 % fee once a month – for a minimum storage of \$10 million. Coinbase calculates that assets of roughly **\$20 billion could flow into custodian services**. The problem is definitely not new. Traditional assets, such as cash, gold bullion, or diamonds also need custodians, which have made a reputation for themselves over the centuries. Cryptocurrencies need to be protected against hackers and in many cases their legal status is not yet defined. Established traditional players such as JP Morgan and Northern Trust are understandably hesitant. They would like to enter the market, but are naturally “extremely cautious”, as a source has told Bloomberg.

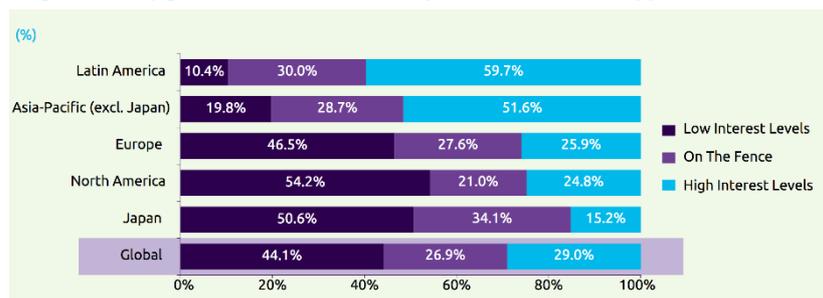
We will of course follow the further development of custodian services for Bitcoin and other cryptos. **Bear markets are the ideal time to improve on the actual infrastructure of the market.** The tentative progress of the custodian sector is a very real reminder of how young this market still is as a whole – and a good indication as to how long it could still take to fully mature.

“In different countries Bitcoin is qualified differently...but to me it’s more than a currency.”

Jeet Singh

A further sign: The boom of 2017 drew in the attention of millionaires to Bitcoin. As the yearly Capgemini World Wealth Report shows, **more than half of the world’s high net worth individuals (HNWIs) are at least superficially interested in Bitcoin**. However only a third feel adequately supported and informed by their wealth managers. What does that tell us? That two thirds of the best wealth managers in the world don’t have a clue about Bitcoin. As their rich clients are starting to complain about this, we guess things will change quickly. That is one main reason Incrementum publishes the Crypto Research Report. We strive to inform investors and also offer cryptocurrency investment solutions such as an AIF-regulated cryptocurrency fund.

Figure 3: Capgemini World Wealth Report – Interest in Crypto Assets



Source: Capgemini World Wealth Report.

From China to Liechtenstein

Back to the question of custodianship: Fidelity, one of the largest US-American finance providers, would like to establish itself in this field. CEO Abigail Johnson can be considered one of the most famous pro-Bitcoin voices the mainstream has to offer. Johnson publicly supported Bitcoin as far back as May 2017. She also does not want to settle on the mere question of storage for Bitcoin. Her goal is easier

access for all mainstream investors. A possible solution: Fidelity could be working on its own crypto exchange.⁵

The race for the next big crypto exchange is totally on. The Swiss stock exchange is working on a crypto trading platform. It supposedly will be one of a kind and is due to start running in early 2019. **“This is the beginning of a new era for capital markets infrastructures. For us it is abundantly clear that much of what is going on in the digital space is here to stay and will define the future of our industry,”** said SIX CEO Jos Dijsselhof.⁶



The Swiss Train Company, SBB, sells Bitcoin and is now advertising Bitcoin on billboards.

The stock exchange in Toronto, Canada has similar plans. As does the stock exchange in Stuttgart, Germany. In Canada, they are working on an app called Bison which allows investors to buy digital assets without paying a fee. A trading platform is also planned. However, the Germans want to take it yet a step further. **They want to make ICOs possible on their platform,** which would make trading new coins instantly possible.⁷

Currently, the market is dominated by Binance. The merely one-year-old exchange has now, after getting a foothold in China and Hong Kong, reached out and set up shop in Malta as well as in Liechtenstein. **A cooperation between the crypto exchange LCX from Liechtenstein should open up a fiat gateway for investors to trade in euros and Swiss francs.** Simultaneously, the government in Liechtenstein is in the processes of passing a law in order to attract crypto companies and ICOs.⁸

The goal is to create a valid alternative to the Crypto Valley in Switzerland. Blockchain companies are checking the legal situation in Malta, Gibraltar, Switzerland and Liechtenstein and in the end choosing to go to Vaduz, says Lawyer and Software Developer, Thomas Nägele.⁹ The so-called Blockchain Act, which is supposedly going to be enforced by mid-2019, is the brainchild of Prime Minister Adrian Hasler.¹⁰ **Within this report, you will also find an extensive interview with the Prime Minister on the topic of Bitcoin, blockchain and cryptocurrencies.**

⁵ See [“Fidelity, a household name in American investing, is plotting a big move into cryptocurrency trading.”](#) Frank Chaparro, *Business Insider*, June 6, 2018.

⁶ See [“A Traditional Stock Exchange Is Also Going to Trade Cryptocurrencies Like Bitcoin,”](#) David Meyer, *Fortune*, July 6, 2018.

⁷ See [“Boerse Stuttgart to develop ICO platform and MTF for cryptocurrency trading,”](#) *Finextra*, August 2, 2018.

⁸ See [“Binance LCX Launches Fiat-to-Crypto Exchange in Liechtenstein,”](#) Ana Alexandre, *Cointelegraph*, August 16, 2018.

⁹ See [“Krypto-Start-ups entscheiden sich selten gegen Liechtenstein,”](#) Pascal Züger, *Cash*, August 13, 2018.

¹⁰ See [“PwC’s Pierre-Edouard Wahl: Blockchain Can Bring Positive Competition to Swiss Banking Space,”](#) Molly Jane Zuckerman, *Cointelegraph*, August 8, 2018.

“We observe a remarkable, globally oriented, and well-educated scene that is very much involved in the advancement of blockchain technology, and we believe that we are only at the beginning of an exciting and long-term development.”

Prime Minister Adrian Hasler

ETF or No ETF?

Which three letters are currently the most important within the Bitcoin sector? Surprisingly it is not FUD (Fear Uncertainty Doubt) but rather ETF (Exchange Traded Funds). Nothing seems to be influencing the price development quite like the question regarding if and when the American SEC will license a Bitcoin ETF. The numerous proposals, which have apparently been put before the commission, have so far only been declined. **In late August, a total of nine ETF applications were all denied.** According to the SEC, the decision itself is not an overall decision regarding Bitcoin; it is, however, an attempt to guard consumers from the unsafe and manipulated crypto market. In plain English: Bitcoin markets are simply not mature enough for the SEC at the moment.¹¹

So why all the hype about a potential Bitcoin ETF? It would most likely create a simple, comfortable, and safe Bitcoin investment opportunity for investors because it would eliminate the storage problem. Trading with gold lends itself as a good comparison at this stage. Anybody wanting to buy precious metals needs a dealer, a safe place to store it and a way to insure it.

Anybody wanting to resell his bullion, needs to physically take it out of the insured safe and find a buyer. This may seem like the most natural thing in the world for true believers who swear on physical investments and hold it long term as a hedge against monetary crisis. But in comparison to the handling of securities, physical storage is rather complicated. Stocks can after all be bought with a couple of clicks on your computer. An ETF takes out the complicated aspect of the process for the consumer (the physical buying and the storage), and in future an ETF could also provide this for Bitcoin. The ETF provider takes over the hard part and the consumer merely presses a button.

According to some professionals, **the bull market in gold and the resulting price bubble following the financial crisis was due to the inauguration of the gold ETF in the year 2004. Many Bitcoin investors hope for the same effect.** The problem is that this ETF is taking its time to get underway and with every decline and postponement of the decision by the US commission board, the price fluctuates severely.¹² To solely base your Bitcoin investment on this decision makes no sense at all in our view. In the long run, there will be one or even an entire array of such investment solutions and the introduction a Bitcoin ETF could only have an ephemeral impact on price.

At the end of 2017, Bitcoin futures were introduced to the market. This was an important step in the right direction. One of the futures providers, the CBOE, is also taking part in the race towards an ETF – and stands a good chance of being among the first to receive authorization. The SEC should treat Bitcoin much like gold or other raw materials, says the CBOE. **When the first ETF will really be approved is yet to be seen and is not**

¹¹ See [“Bitcoin ETFs Aren’t Coming Any Time Soon Thanks to the SEC.”](#) Rachel Evans and Lily Katz, *Bloomberg*, August 23, 2018.

¹² See [“Are Bitcoin ETFs Back on the Table Again?”](#) Crystal Kim, *Barron’s*, March 27, 2018.



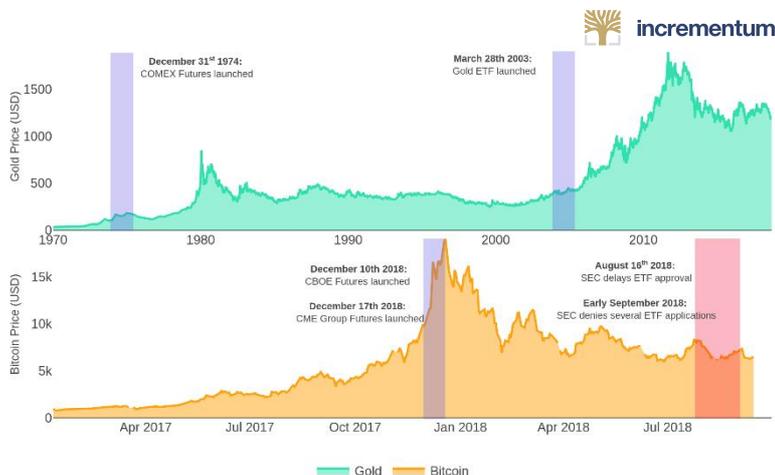
The World Bank launches the world’s first blockchain bond



In partnership with the Commonwealth Bank of Australia, the World Bank used a private Ethereum blockchain to sell a two-year bond worth 110 million Australian dollars (\$79 million) to seven investors.

predictable at the time of writing. It could be weeks, months, or, worst case, even years. It all depends on how quickly the markets develop.

Figure 4: Bitcoin vs. Gold Adoption by Futures & ETFs



Source: Incrementum AG.

As a reaction to the SEC, a couple of young American exchanges have pooled their resources together and created the “Virtual Commodity Association” to work on rules and standards for this young sector. The association is spear-headed by Gemini founders Cameron and Tyler Winklevoss.¹³

A Game Changer by the Name of BAKKT

Some providers do not want to wait on an ETF decision by the SEC. The goal to attract more investors to the sector can also be accomplished via other routes. The most important game changer could possibly come directly from the Intercontinental Exchange (ICE) itself, owner of the New York Stock Exchange.

By November, ICE is planning to set up **a futures contract with physical delivery. This means, “real” Bitcoins will be going over the counter.** The infrastructure of the ICE will be the base of this operation and later a company called Bakkt will take over the crypto plans of the exchange. The Microsoft cloud will be the corner stone for a new crypto trading platform. But the plans do not stop there.¹⁴

“In bringing regulated, connected infrastructure together with institutional and consumer applications for digital assets, we aim to build confidence in the asset class on a global scale,” ICE Chief Executive Jeffrey Sprecher said. He goes on to elaborate on the future: **“Bitcoin could greatly simplify the movement of global money. It has the potential to become the first worldwide currency.”** At this point we are drawn to point out that gold already has this role

“The better the money is at holding its value, the more it incentivizes people to delay consumption and instead dedicate resources for production in the future, leading to capital accumulation and improvement of living standards.”

Saifedeam Ammous

¹³ See [“The Biggest Digital Exchanges Are Teaming Up To Police the Crypto Space.”](#) Matthew Leising, *Bloomberg*, August 20, 2018.

¹⁴ See [“NYSE-owner ICE to form new company for digital assets,”](#) John McCrank and Anna Irrera, *Reuters*, August 3, 2018.

as a global currency for a couple of centuries, but we greatly appreciate Sprecher's enthusiasm towards the innovation of Bitcoin.¹⁵

Sprecher points out that Bitcoin and other cryptocurrencies desperately need a clear set of rules and a reliable infrastructure. We are clearly only at the beginning of this phase.



More and more family offices are looking into the new asset class.

One of the first partners of Bakkt is supposedly going to be Starbucks. **This in short means that customers will in the near future be able to pay for their double shot iced caramel soy-milk Frappuccino with digital money.**

“As the flagship retailer, Starbucks will play a pivotal role in developing practical, trusted and regulated applications for consumers to convert their digital assets into U.S. dollars for use at Starbucks,” Maria Smith, vice president, partnerships and payments for Starbucks, said in a statement.¹⁶

The Real World Discovers Bitcoin

As mentioned before, times of falling prices can be beneficial because they are an impetus for research and innovation to improve the technology. However, positive developments and news do not immediately translate into rising prices. FUD and ETF are not the only acronyms influencing the crypto market. Many paths lead to a wider acceptance of Bitcoin, and the Chartered Financial Analyst (CFA) Institute and International Monetary Fund (IMF) joining the crypto team are likely to help score some points. As mentioned in the previous report with the “Goldman Effect”, we can once again observe the establishment of Bitcoin in “the real world”, or at least on Wall Street.

Thousands of people head to the CFA Institute to undergo excruciating tests in different financial topics in order to call themselves “certified experts”. They now have included questions on crypto markets and Bitcoin into their curriculum. **“We saw the field advancing more quickly than other fields and we also saw it as more durable,”** said Stephen Horan, managing director for general education and curriculum at CFA Institute in Charlottesville, Virginia. “This is not a passing fad.” The CFA seems to be reacting to the rising demand from Asia, where most of crypto trading takes place.¹⁷

¹⁵ See “[Breaking: World’s Biggest Stock Exchange Operator is Launching a Bitcoin Market.](#)” *CNN*, August 3, 2018.

¹⁶ See “[New Starbucks partnership with Microsoft allows customers to pay for Frappuccinos with bitcoin.](#)” Sarah Whitten and Kate Rooney, *CNBC*, August 3, 2018.

¹⁷ See “[‘This Is Not a Passing Fad’: CFA Exam Adds Crypto, Blockchain Topics.](#)” Michael Patterson and Andrea Tan, *Bloomberg*, July 16, 2018.

“Asia dominates cryptos because they’re very used to trading digital assets. South Korea has been trading digital goods related to gaming for two decades. When you move to a purely money based digital currency they understand that culturally, so they get on board quickly.”

Arthur Hayes, BitMEX CEO

In need of more acronyms? How about IMF? The International Monetary Fund is the capital of the international mainstream monetary system. It goes without saying that the IMF originally regarded Bitcoin with a good portion of skepticism, to say the least. However, there has been a slight transition to this first wave of disapproval. Christine Lagarde, the Managing Director of the IMF, has even gone as far as to say that cryptocurrencies have the potential to make the financial system safer. However, she had to balance out her enthusiasm because after all, she is the boss of one of the institutions that Bitcoin is disrupting. As expected of her as a good IMF boss, she did go on to warn against the potentials of a “new vehicle for money laundering and terror financing”. **Overall though, IMF is sending a positive signal for cryptocurrency investors.** Recently, IMF experts went as far as describing a world in which traditional banks, private money and cryptocurrencies all peacefully co-exist.¹⁸

Central banks per se have not yet found a consensus on their stance towards Bitcoin. The Bank of International Settlements (BIS), the central bank of all central banks, has declared itself in opposition to the crypto world. In June, the economists of the BIS published a 26-page report against Bitcoin. Starting with the fact that it is already an environmental disaster and continuing on to state that the promise of the founders will never be met by the current system.¹⁹

The decentralized structure of cryptocurrencies should be seen as a weakness, not as a strength and it is at the end of the day just “too risky” to run a global economy without a center, says the BIS. “Trust can evaporate at any time because of the fragility of the decentralized consensus through which transactions are recorded,” the report concluded. “Not only does this call into question the finality of individual payments, it also means that a cryptocurrency can simply stop functioning, resulting in a complete loss of value.” On top of all this, the BIS claims that Bitcoin could bring the whole Internet to a standstill.

Jay Powell, the head of the US central bank, sees the matter slightly more relaxed. In mid-July he stated in a hearing that the crypto sector is not big enough yet to actually pose a serious threat to the financial system. At that time, the market capitalization was at roughly \$300 billion. By mid-August, it fell by another \$100 billion. The FED has no regulatory power over cryptocurrencies and is also not interested in such an extension of supervision, Powell said.²⁰



Ripple
@Ripple

We're thrilled to announce @BillClinton as keynote speaker for this year's #SwellbyRipple. For more details: bit.ly/Swell2018



Bill Clinton

6:03 PM · 31 Jul 18

1,615 Retweets 3,740 Likes

Ripple and the Clintons seem to have a lot in common. That's why they make such a great partnership.

¹⁸ See “Bitcoin tools could make finance system safer, says IMF boss,” Richard Partington, *The Guardian*, April 16, 2018.

¹⁹ See “Bitcoin Could Break the Internet, Central Bank Overseer Says,” Edward Robinson, *Bloomberg*, June 18, 2018.

²⁰ See “Powell Says Cryptocurrencies Aren't Big Enough to Pose a Threat,” Olga Kharif, *Bloomberg*, July 18, 2018.

“The key thing is that the more [Bitcoin] grows, the more it will deprive governments of the ability to print more money...I think, in the long run, this is going to be a very good thing for everywhere in the world, particularly places in the Middle East.”

Saifedeam Ammous

The Final Showdown

The price of Bitcoin and all other altcoins are on a downwards trend since the beginning of the year. As we can observe, many of the serious contenders are using this time to expand and solidify a new infrastructure. Countries, such as Liechtenstein, are preparing for the next stage of the blockchain revolution. Traditional players such as the IMF, the FED, and the BIS have an eye on Bitcoin and the cryptocurrency market as a whole.

The sector itself is, however, still battling with major maturing issues. A main hindrance is the ICO bubble, which we warned against in our very first report and is still floating around. Jihan Wu, CEO of the mining giant Bitmain, expects this to resolve itself. “I believe ICOs are kind of an unsustainable financial bubble. It will burst eventually. It’s just a matter of time. I believe it’s just one year or two. Either way, it will just disappear.”²¹

Wu believes that in the future, traditional assets in the shape of tokens will be traded freely but not in the form of crowdfunded ICOs. Naturally, he wants to start an IPO on an exchange with his company Bitmain, so he does have his own agenda in mind. In our opinion, he does however have a point. ICOs were the hype of 2017 and especially pushed the price of Ethereum. How far the prices could plummet when the bubble does decide to burst once and for all is too scary to imagine at this point in time. Wu deserves to be heard as he does sometimes know what he is taking about – not something you can say about everyone who is inclined to voice their opinions publicly about Bitcoin and the crypto market these days.

The famous economist Joseph Stiglitz is the source of the lowest price prognosis we could find this time. Back in July, he predicted that countries will fight Bitcoin with a “hammer” and will regulate cryptocurrencies to death. “People in power will move to regulate anonymous transactions. That you can be sure of. **“Bitcoin could easily be worth just \$100 in 10 years.”**²²

We can of course not contradict this statement as (sadly) nobody can look into the future. The specificity of the number does, however, strike us as odd. 10 years ago, there was no such thing as Bitcoin, some investors can even remember a time in which \$100 seemed like an extremely high prognosis. Giving Stiglitz’s statement a positive spin, we would say that considering Bitcoin to still exist in 10 years and still have a monetary value is good enough for us at the moment. From an investors point of view, such forecasts, be it bullish or bearish, are always to be treated with caution.

Entry: Tim Draper. The Billionaire and founder of the venture capital firm Draper Fisher Jurvetson sees a very different, positive future for Bitcoin:

—

²¹ See “[ICOs an Unsustainable Financial Bubble](#)”: Jihan Wu,” *CCN*, August 22, 2018.

²² See “[Bitcoin price warning: BTC will drop to ‘\\$100’ after being ‘regulated into oblivion’](#),” David Dawkins, *Express*, July 9, 2018.

*"I believe cryptocurrencies will overtake fiat currencies in the next five to seven years. I hold a lot of cryptocurrencies and mainly Bitcoin. I am buying more. I feel that crypto and Bitcoin are the future. Fiat is the past. I do still have to hold some fiat currency for everyday transactions today, but I suspect that that will change over the next few years."*²³



Fiat ✓
 @fiat

Why do these "cryptocurrency" people hate us so much? Leave us alone.

8:28 PM · 02 Aug 18

Fiat cars vs. fiat money.

That the crypto world is still prone to hacks and thefts, as just witnessed again with the Ethereum based network Bancor, does not seem to worry Draper in the slightest. Hacks are also part of the traditional banking world. He sees these attacks as an argument for Bitcoin versus altcoins. "The larger the network of wallet holders, miners or stakeholders, the more secure the cryptocurrency. **So, Bitcoin is the most secure.**"²⁴

Draper has a fascinating vision of the future of the finance world. He envisions the following: "I expect that since cryptocurrencies will increase the velocity of money, the current \$86 trillion global market for currency will grow to be about \$140 trillion in the next 10 years, and that growth will be in crypto. In fact, I estimate that fiat currencies will actually decrease in use, and that crypto will become as much as \$100 trillion of that market. I expect Bitcoin to be about 10 % of that market, or \$10 trillion. There is a lot of room to grow there."

And he is right. At the all-time high, when Bitcoin was worth \$20,000 apiece, the whole market was not even worth a trillion. However, many analysts expect to see Bitcoin to land somewhere in the region of \$5,000, \$4,000, or maybe even \$3,000 before we can say the bear market is over.

"Bitcoin is a hedge against the whole world falling apart."

Peter Thiel

In the long run, it will be interesting to see if Stiglitz or Draper turn out to be right. Bitcoin and cryptocurrencies in general have the potential to let Draper's fantastical dreams come true. On that path, however, many, very powerful, traditional financial institutions must still adapt or even fall. We can therefore understand why Stiglitz anticipates strong resistance. To stop Bitcoin as a whole, it would however take a level of international cooperation on a never before seen scale. Satoshi Nakamoto's vision is intact. **Bitcoin has stepped into the ring with fiat. New against old. Online against offline. De-centralized against centralized. And no matter the outcome, it is going to be one hell of a ride.**

²³ See "[Billionaire Investor Bill Draper Explains Why Bitcoin Will Hit \\$250,000 in 2022](#)," Jordan French, *The Street*, July 25, 2018.

²⁴ See "[Another Crypto Fail: Hackers Steal \\$23.5 Million from Token Service Bancor](#)," Jeff John Roberts, *Fortune*, July 9, 2018.

Vontobel

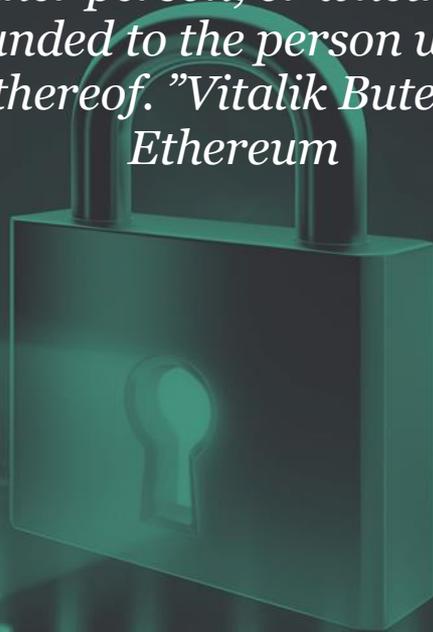
Investment Banking

Driven by the power of possibility



Crypto Concept: Smart Contracts

“A smart contract is a computer program that directly controls some kind of digital asset... The smart contract approach says instead of a legal contract, immediately transfer the digital asset into a program, the program automatically will run code, validate a condition, and determine whether the asset should go to one person or back to the other person, or whether it should be immediately refunded to the person who sent it or some combination thereof.” Vitalik Buterin, Founder of Ethereum



Key Takeaways

- Utility crypto assets such as Ethereum and EOS represent a distinct investment opportunity compared to payment crypto assets such as Bitcoin, Monero, and Litecoin. Nevertheless, utility crypto assets (currently) still are highly correlated (0.8) with payment crypto assets. They displayed a higher beta to payment crypto assets over the past year.
- Utility crypto assets challenge existing business models that rely on intermediaries such as crowdfunding websites like Kickstarter; however, Swiss and US regulators argue that between 95 % and 100 % of them should be legally classified as securities.
- Noteworthy utility crypto assets that are making waves online include Etherisc, PolkaDot, ShareRing, Dfinity, and Cosmos.

“30 years from now, Bitcoin will be the structure to power organizations without leaders.”

Mike Hearn

Smart contracts are dynamic, complex, and incredibly powerful. This technology has the potential to change how business is done because governments and companies can decrease costs, automate contract enforcement, and provide an auditable trail of control. While their long-term potential is unimaginable, they are already disrupting industries such as crowdfunding, law, and insurance. However, smart contracts are made by humans, and therefore, they are not perfect. **Over \$2.4 billion USD have already been lost due to faulty smart contracts.** The future success of utility tokens depends on the ability of developers to build more secure applications that users can trust.

Advantages and Disadvantages of Smart Contracts

Smart contracts have several advantages including:

- 1.) Lower error rate. Instead of trusting humans, smart contracts allow trust to be shifted to mathematics, which should reduce errors stemming from malicious or negligent human management.
- 2.) Automatic implementation of new data and secure storage of historical data.
- 3.) The transparency and auditability of smart contracts also increases the personal responsibility of the humans that manage the smart contract because each transaction with the contract is recorded along with the account that initiated the transaction.
- 4.) By using a smart contract, the parties commit themselves to the rules of the underlying code. In theory, this should reduce the potential for dispute and arbitration costs, as both parties agree to the outcome programmed into the smart contract.

Disadvantages include:

- 1.) Legality of smart contracts is questionable. Since this structure is digital, it can circumvent state licensing requirements. State courts do not have to recognize the rights of investors.
- 2.) Smart contracts are not very flexible. Once a smart contract has been executed on a public blockchain, the contract is vulnerable to hackers. Fixing errors and changing contract terms can be impossible.

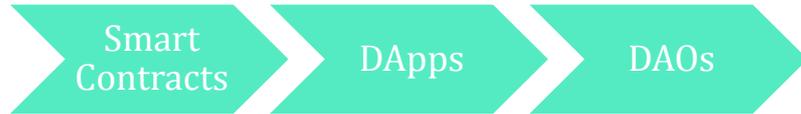
Smart Contracts, Decentralized Applications, and Decentralized Autonomous Organizations

With the rise of cryptocurrencies and blockchains, smart contracts, Decentralized Applications (DApps), and Decentralized Autonomous Organizations (DAOs) are becoming increasingly important technologies that investors should understand. This all began when Nick Szabo coined the term “smart contract” in 1994. To define the term, **a smart contract is a piece of software that represents a set of rules that are automatically executed under pre-determined circumstances.** In other words, **a smart contract is an “if-then” statement that is executed on a distributed peer-to-peer network.**

Since each contract is stored on several computers all around the world, smart contracts do not have a single point of failure. Similar to BitTorrent, not having a single point of failure means that if one computer fails, the whole network does not fail. Nobody has the power to change the smart contract – even the person who made the smart contract. That applies to hackers and governments too!

Smart contracts have the same privileges as cryptocurrency wallets, except they are not controlled by private keys or users. Instead, a smart contract is controlled by the code contained within the smart contract. They can send and receive cryptocurrency, and they can store a balance or have a balance of zero. They can interact with other smart contracts, but users have to pay a small fee to the blockchain network to

interact with the contract because every change needs to be approved and recorded by every computer that maintains the network. This is similar to mining in Bitcoin.



More Resources on Smart Contracts, DAOs, and DApps

In 2014, Vitalik Buterin posted [an article on the Ethereum blog](#) covering how smart contracts work, and how they are distinct from DAOs. Also, a comprehensive [guide to DApps](#) was written by David Johnston in 2014. Finally, a popular YouTuber, [Evan on Tech](#), explains the difference between smart contracts and decentralized applications.

To learn how to program smart contracts, [a free course is available online for beginners](#). The course has 8 sessions dedicated to Ethereum’s smart contract programming language, Solidity.

A DApp is a collection of many smart contracts that are working together to create a product for users. To be a DApp, four criteria must be met. First, the application must be open-source, which means that anyone can download it and look at the underlying code. Second, the application must run on a blockchain or distributed ledger technology, such as a directed acyclic graph. Third, the application must have a token associated with it. This token can be native to the application, such as Augur, or the application can use another cryptocurrency, such as Bitcoin or Ethereum. Finally, the application must use a cryptographic algorithm for confirming changes to the smart contracts that control the DApp.

A DAO is a type of DApp that allows owners to make business decisions by voting electronically and to automate management using smart contracts. DAOs use smart contracts to facilitate digital voting, and to facilitate the voting outcomes. **The goal of a DAO is to reduce managerial overhead and to circumvent regulations particular to geographic regions.**

Essential, a DAO is a company structure for a globally dispersed group of owners. The cryptography and blockchain enables a group of strangers to invest capital together and make financial decisions. Smart contracts enable the company to be run autonomously because they hold the rules of the company and serve as a basis for operation decisions instead of a human. For example, a smart contract could be programmed to distribute dividends to investors once a certain condition is met. If profits are above a certain threshold, the smart contract could automatically send a transaction to shareholder wallets.

Smart Contract Theory Applied In Practice

“There is a lot of intermediaries that end up charging 20–30 % if the concept of decentralization takes off and does well, those fees are going to decline to almost zero.”

Vitalik Buterin

The most popular cryptocurrency that incorporates smart contracts is Ethereum. The founder of Ethereum, Vitalik Buterin, proposed Ethereum in 2013 as a blockchain specifically designed for smart contracts. Ethereum is a worldwide network of computers which enforce, execute, and validate smart contracts. As covered in the previous [Crypto Research Report](#), validation is achieved by a decentralized network of thousands of Ethereum nodes around the world. The centralized nature of the network enables decentralized applications (DApps) to run without downtime, censorship, or third-party interference, which makes the applications immutable or tamper-proof.

In practice, Ethereum can be used to create a decentralized crowdfunding website without intermediaries, such as Kickstarter. Ethereum users can invest in a business idea by sending money to an Ethereum wallet address of a smart contract. If the entrepreneur is unable to raise a certain amount of funding within a certain timeframe, the smart contract can automatically send all of the investors their money back. Instead of paying 10 % to Kickstarter, they only have to pay a 5-cent fee to the Ethereum network to process the transaction to the smart contract. Middleman removed. If company raises \$10 million with Ethereum instead of Kickstarter, they save \$1 million in fees.

Table 1: Correlation of Utility Token and Payment Token Returns

Correlation Matrix	BTC	ETH	XRP	NEM	ETC	LTC	DASH	STRAT	XMR	WAVES	UP	PP
Bitcoin	1											
Ethereum	0.61	1										
XRP	0.36	0.52	1									
NEM	0.34	0.48	0.44	1								
Ethereum Classic	0.52	0.68	0.45	0.44	1							
Litecoin	0.59	0.66	0.42	0.48	0.62	1						
Dash	0.50	0.6	0.38	0.38	0.48	0.52	1					
Stratis	0.55	0.61	0.4	0.44	0.57	0.5	0.49	1				
Monero	0.58	0.62	0.47	0.39	0.57	0.55	0.66	0.57	1			
Waves	0.62	0.66	0.43	0.44	0.52	0.58	0.52	0.71	0.57	1		
Utility Portfolio	0.64	0.82	0.55	0.75	0.78	0.69	0.6	0.83	0.66	0.82	1	
Payment Portfolio	0.74	0.77	0.72	0.53	0.78	0.79	0.79	0.64	0.84	0.69	0.81	1

Source: Coinmarketcap.com, Incrementum AG.

The decentralized nature of Ethereum also allows investors to circumvent regulations that limit how much investors can invest in crowdfunding projects. For example, in the US, non-accredited investors with an annual income or net worth less than \$107,000, are limited to invest a maximum of 5 % of their assets. For those with an annual income or net worth greater than \$107,000, he/she is limited to investing 10 % of the lesser of the two amounts. These rules do not apply to Ethereum and other smart contract platforms such as NEO and EOS.

Blockchains that facilitate smart contracts are often referred to as utility blockchains, and the assets that are associated with them are referred to as utility crypto assets or utility tokens. Table 1 compares the relative return of utility crypto assets to payment crypto assets such as Bitcoin, Monero, and Litecoin. Although a portfolio comprised entirely of payment crypto assets had a higher cumulative return of 227 %, the portfolios are highly correlated with a 0.81 correlation coefficient. **Cryptocurrency investors that bought the top five payment cryptocurrencies in June and sold in January realized a six-month profit of over 1,200 %.**

Figure 5: Historical Return of Utility Crypto Assets vs. Payment



Sources: Incrementum AG.

Crypto Asset Companies That Use Smart Contracts, DApps, and DAOs.

There are already many projects that seek to implement smart contracts via blockchains into the real world. Ethereum is one of the most prominent examples, but a variety of other companies are also harnessing the power of automatic digital contracts, including Cosmos, Dfinity, Etherisc, Polkadot, and ShareRing.

“[A DAO]...is an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do.”

Vitalik Buterin

Table 2: Noteworthy Crypto Assets That Use Smart Contracts, DApps, and DAOs

Crypto Asset	Advantages
Cosmos	Blockchain interoperability with a network of Independent Parallel Blockchains. From the creators of Tendermint, low energy consensus mechanism classical Byzantine Fault Tolerance. Polychain Capital invested in Cosmos.
Dash	Although Dash is not often thought of as a smart contract platform, Dash is a type of DAO because governance is controlled by the masternodes, which allow users to vote on proposals.
Dfinity	Academic team of computer scientists, mathematicians, and economists, founded in Zug with offices in Palo Alto, aims to disrupt technology intermediaries such as Uber, eBay, and Facebook.
Ethereum	Large network of users and developers, largest utility crypto asset by market capitalization
Etherisc	Decentralized insurance – one of the leaders in offering blockchain based insurance products
EOS	Scalable, flexible, usable infrastructure for decentralized applications
Polkadot	Parity Technologies as lead developer, improved anonymity and scalability
ShareRing	P2P Car Sharing, Part of the MOBI initiative, Australian development team
Starcards.my	Similar to Cryptokitties, Starcards allows Ethereum users to collect and trade scarce celebrity digital cards that are stored on the blockchain

Source: Incrementum AG.

A controversial example is the decentralized prediction market named Augur. In late July, [CNN reported](#) on Augur users gambling on whether President Trump would be assassinated by the end of this year. Since Augur is a DApp, no one can stop users from gambling on the probability of criminal and unethical behavior. Even the creators of Augur are unable to stop Augur from existing because the

project is open-source. Not only are the legality of prediction markets questionable, now lives of people will be directly attached to financial gains. If this prediction market does lead to heinous acts be committed, Augur's price will most likely be volatile and downward.

#1 Will France Defeat Belgium in the 2018 FIFA World Cup Semifinals?

Augur predicts **\$17,569.78**
90% Yes at stake

The price for this bet was at \$0.90 per share "that France will win", but once the outcome of the event had been announced, every share was worth \$1. Investors made a safe profit of $0.1/0.9 = 11.1\%$.

Although Augur is enabling people to vote on the probability that Trump, John McCain, or Warren Buffett will survive past the end of this year, most of Augur's prediction markets are based on sports. For example, during the FIFA World Cup, users could vote on the outcome of specific games and earn Ethereum if they voted correctly.

When Smart Contracts Are Dumb

Since 2011, a combined \$2.4 billion has been destroyed, frozen, stolen or otherwise compromised in the crypto asset space due to attacks. The two biggest crypto assets in terms of market capitalized have seen losses of around 1.7 million BTC and 4.54 million ETH over the past seven years. The three biggest mistakes that have occurred in the Ethereum space include the DAO hack, the Parity wallet hack, and the Parity wallet suicides.

The Risk of Trusting Oracles

Smart contracts promise to enforce contracts automatically and remove middle men; however, many applications of smart contracts rely on "oracles" to provide them with information pertaining to the real world. Oracles provide smart contracts with data about the world such as weather forecasts, foreign exchange rates, and election results. Smart contracts automatically execute financial transactions based on the oracle's data; however, oracles can be compromised because they are not decentralized. An oracle can be seen as a counterparty risk, which can result in irrevocable losses of money.

Several solutions have been proposed. Notably, Augur's research on oracles is leading the way. Their model allows Augur users to vote on the truth and to dispute the results of the vote.

Nonetheless, the quest for a secure oracle continues, and the future adoption of smart contracts on public distributed ledgers depends on it.

DAO Hack

The Decentralized Autonomous Organization (DAO) was one of crypto's most highly anticipated projects of all time and a pioneer in the application of the revolutionary capabilities of smart contracts. Some of Ethereum's developers created a spin-off company called Slock.it and created the first DAO using the Ethereum blockchain in April 2016.²⁵ **The DAO application worked like an investment fund, although without the usual investment fund management.** Investors could participate by transferring the Ethereum cryptocurrency, ether, to the fund, which entitled them to voting rights. The investment decisions were supposed to be taken through a joint effort, where every participant could vote on investment proposals. Anyone with a venture project could pitch their idea to the DAO community in hopes of potentially receiving funding from a pool of ether which was controlled by the DAO.²⁶ Once a project was chosen, token holders would receive rewards – much like dividends or interest payments – if the projects turned out to be profitable.

²⁵ See "[Decentralized Autonomous Organization to Automate Governance. Final Draft – Under Review](#)" [white paper], Christoph Jentzsch, 2016.

²⁶ See "[The Story of the DAO—Its History and Consequences.](#)" Samuel Falcon, *The Startup*, December 24, 2017.

The DAO was launched as a smart contract on the Ethereum network in May 2016. At the time, it raised \$162 million worth of ether, making it the biggest crowdfund ever.

Nevertheless, on June 17th, 2016, a hacker perpetrated the DAO network by exploiting a loophole in its software, allowing him to drain funds from the pool of Ethereum tokens owned by the DAO network. 3.6 million ETH tokens were stolen

in the first couple of hours of the attack, amounting to an equivalent value of \$70 million at the time (\$1.2 billion in today's terms). Strangely enough, the hacker stopped draining the DAO for unknown reasons, even though he could have continued to do so.

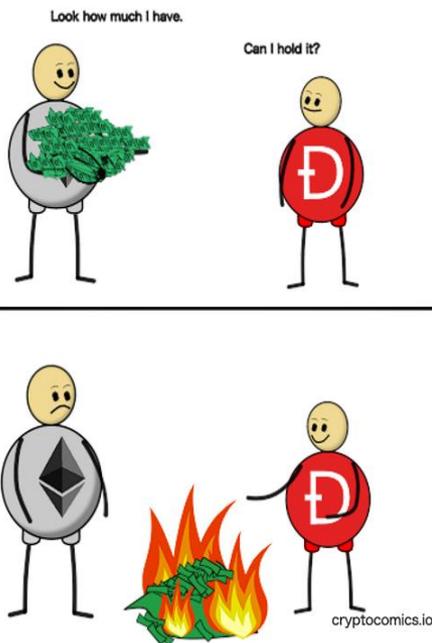
The team and community behind Ethereum were quick in noticing the breach and very soon responded to the situation by presenting multiple proposals on how to deal with the attack. Due to the architecture of the DAO, the drained funds in the form of ether were locked up in a child DAO, another smart contract, which required a 28-day holding period before the attacker could fully withdraw the funds and launder them into circulation. This gave the Ethereum team sufficient time to decide on their course of action.

Vitalik Buterin, the creator of Ethereum, realized the severity of this breach and issued a statement soon afterwards assuring all investor that their funds were safe for the moment. The Ethereum community then decided to render any transaction originating from the attackers account with code hash:

*ox7278do50619a624f84f51987149ddb439cdaadfba5
966f7cfaea7ad44340a4ba*

as invalid, thereby preventing the attacker from withdrawing funds even after the completion of the 28-day holding period.

The hacker later published an open letter to the Ethereum community claiming rightful ownership of the acquired funds. You can see the original letter [here](#). Refunding the investors' ether would have not been possible under the rules of the Ethereum network at that time, posing an existential threat to the network as a whole.



The DAO is to this day the largest crowdfund in history with over \$162 million raised. Less than a month after being launched, the DAO was hacked for \$50 million.

“Just goes to show that any centralized entity will be pushed in that direction, which is why lightning network, atomic swaps and Decentralized Exchanges are the only way to resist surveillance economics.”

Andreas M. Antonopoulos

The solution that the Ethereum foundation came up with was highly controversial.²⁷ They implemented a “hard fork” by releasing a new version of the Ethereum software client that did not include the hacked transactions. They rewinded the Ethereum blockchain in order to remove the hacker’s transactions. The release also included a fix to the bug that the hacker exploited. Not all of the members of the network agreed with the decision of hard forking the chain. Some dissidents left Ethereum entirely and others just continued to use the original Ethereum blockchain, which included the hacker’s transaction. This chain became called Ethereum Classic with ticker symbol ETC.

As with all of the mishappenings described in this article, none of them has arisen due to the fundamental design of the Ethereum network. Instead, the hacks occurred because of design problems in applications that were built on top of Ethereum. The type of attack that destroyed the DAO is known as a reentrancy attack.²⁸ In this attack, the attacker first donated ether to the smart contract (DAO) and then was able to “ask” for the ether back multiple times before the smart contract could update its balance. When the contract fails to update its state (a user’s balance) prior to sending funds, the attacker can continuously call the withdraw function to drain that contract’s funds.²⁹ The code written for the DAO had multiple flaws including the recursive call exploit as well as the fact that the smart contracts sent ETH funds before updating the internal token balance.

Table 3: Notorious Hacks Involving Smart Contracts

Notorious Hacks		
	Year	Amount USD
Misconfigured Ethereum Clients Incident	2018	20,000,000
MyEtherWallet DNS Hack	2018	152,000
Parity Wallet Suicides	2017	160,000,000
Parity Wallet Hack	2017	30,000,000
Veritaseum’s Ether Wallet	2017	8,400,000
DAO Hack	2016	60,000,000
Shapeshift	2016	230,000
King of the Ether Throne	2015	2,000

Source: Incrementum AG.

Parity Wallet Hack

Parity Technologies builds platforms and applications, and it powers large parts of the infrastructure of the public Ethereum network.³⁰ On the July 19th, 2017, an unknown hacker attacked a critical vulnerability in the Parity multisignature wallet on the Ethereum network, looting three massive wallets containing a combined \$31 million worth of ETH in a matter of minutes.³¹ A group of heroic white-hat

²⁷ See “[To fork or not to fork](#),” Jeffrey Wilcke, *Etherum Blog*, July 15, 2016.

²⁸ See “[Smart Contract Attacks \[Part 1\] – 3 Attacks We Should All Learn From The DAO](#),” Pete Humiston, *Hackernoon*, July 5, 2018.

²⁹ You can find a more technical walkthrough [here](#).

³⁰ Learn more about Parity [here](#).

³¹ See “[A hacker stole \\$31M of Ether – how it happened and what it means for Ethereum](#),” Haseeb Qureshi, *Medium*, July 20, 2017.

hackers from the Ethereum community responded by quickly alerting Ethereum users on social media and hacking the remaining wallets before the attacker could. This form of hacking is called white-hat hacking because they hacked for the good cause. If the white hackers had not responded so quickly, the hacker could have hacked over \$180,000,000 worth of Ethereum from vulnerable wallets. Of course, the funds that were stolen by the white-hats were securely redistributed to their respective account holders in the end.

The hacker found a programmer-induced bug in the code that let him re-initialize the Parity multisignature wallet, almost like restoring your iPhone to factory settings. Once having done that, he was free to set himself as the new owner and walk out with everything.

“Bitcoin is not unregulated. It is regulated by algorithm instead of being regulated by government bureaucracies. Un-Corrupted.”

Andreas M. Antonopoulos

Due to the programming model of Ethereum, there is an incentive for programmers to optimize code in order to minimize transaction costs. Every time code is executed on Ethereum, a smart contract, which constitutes a transaction on the network and thus comes with a computation fee, needs to be deployed. An efficient way to reduce costs from the computation fees is to use shared libraries which have already been deployed to the network.

The default settings for the multisignature wallet in Parity had a configuration which did exactly that. It referenced a shared external library, which contained a wallet initialization logic, namely `initWallet()`, which if called could reinitialize the contract the wallet was built upon. It effectively made whoever exploited this flaw the new owner of the wallet. From there, the hacker could simply transfer the funds to any address of his or her choice.



The new Ethereum logo?

However, why did they not just roll back this hack, like they did with the DAO hack? Unfortunately, that was not even an option any more. When the attacker drained the DAO into a child DAO the hacked funds were frozen for a 28-day period before they could be released to the attacker. This prevented any of the stolen funds from going into circulation, which in turn gave the Ethereum community plenty of time to consult the community about how to deal with the attack. In the Parity wallet attack, however, the attacker directly withdrew the funds and could start spending them. Once the stolen ETH was in circulation, it was almost impossible to recover them, much like with a huge sum of counterfeit bills circulating in the economy.

Parity Wallet Suicides

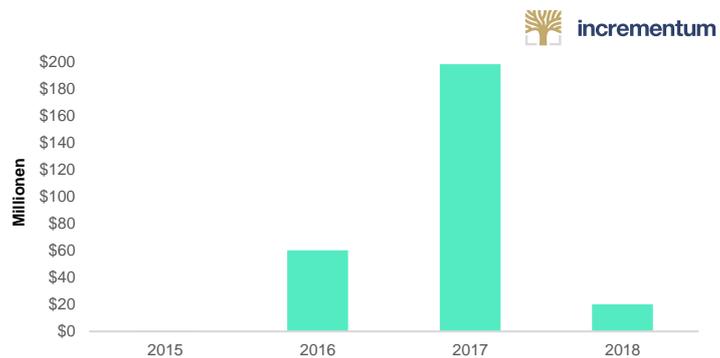
On November 6th, 2017, the Parity multisignature wallet fell prey to yet another attack,³² only this time to one of a much more severe magnitude. A Github user named devops199 wrote a post titled **“anyone can kill your contract”**. Devops199’s post seemed to have good intentions.³³ He wanted to make the Parity

³² See [“Security Alert,” Parity](#), November 8, 2017.

³³ See [“Yes, this kid really just deleted \\$300 MILLION by messing around with Ethereum’s smart contracts,”](#) Thijs Maas, *Hackernoon*, November 8, 2017.

team aware of a vulnerability in the smart contract that powered its multisignature wallets. The security vulnerability allowed any hacker to make him- or herself the “owner” of that contract, thus giving him or her permission to do with the wallet as he or she pleases. Up to this point in time, it still remains unclear what his original intent was, but his following actions were largely met with skepticism: He “accidentally” triggered the “kill switch” of the contract, rendering all Parity multisignature wallets impossible to access. Just minutes after the library was wiped out, devops199 raised another issue following up his “**anyone can kill your contract**” post on Parity’s Github titled “**I accidentally killed it.**”

Figure 6: Loss of Money Due to Ethereum Smart Contracts Per Year



Source: Incrementum AG.

“Bear markets are for builders. The calm, the quiet, the disillusionment... while the fickle and fair-weather peer around with nervous insecurity, the builders become the market’s foundation, preparing the mortar and stone of tomorrow’s towers.”

Erik Voorhees

The scale of this Parity hack compromised a total of 514 k Ethereum tokens, which at the time were valued roughly around \$155 million or 1 % of Ethereum’s total valuation. As a consequence of the hack, no funds can ever be moved out of all Parity multisignature wallets that were deployed after July 20th, 2017 again.

A hard-fork could technically “bail-out” the multisignature wallets that are frozen but that would compromise the foundation of Ethereum’s decentralized, distributed, *immutable*, and tamper-proof ledger. Calls for a hard-fork have largely remained ineffective.

Smart Contracts Represent a Distinctly Different Exposure for Investors Than Bitcoin

Smart contracts have the potential to disrupt industries by cutting out middlemen and bringing together the parties of the contracts directly. They can ensure trust and cut transaction costs. Despite the benefits, *The Economist* criticizes the concept of smart contracts by pointing out the immature state of the industry.³⁴ They further argue that smart contracts are not flexible enough for an economy that needs to respond to ever changing conditions.

At Incrementum, we think that smart contracts are here to stay. From a financial perspective, utility blockchains, such as Ethereum, NEO, and EOS, offer a distinctly different risk-return profile compared to payment blockchains, such as

³⁴ See “[Not-so-clever contracts](#),” Schumpeter, *The Economist*, July 28, 2016.

Bitcoin, Dash, and Monero. Due to the complex nature of smart contracts, utility blockchains are inherently more prone to technology risk. In contrast, since utility tokens do not threaten to disrupt the current monetary system, risk of being outlawed for competing with sovereign currencies is lower when compared to public payment blockchains. However, many regulators are saying that initial coin offerings and utility tokens are violating security law. **Diversifying into both crypto asset classes is prudent for investors that are willing to make the extra effort.**

Notice a pattern?

“This ‘**telephone**’ has too many shortcomings to be seriously considered as a means of communication.”

WILLIAM ORTON, PRESIDENT OF WESTERN UNION, 1876

“There is no reason anyone would want a **computer** in their home.”

KEN OLSON, DIGITAL EQUIPMENT CORPORATION, 1977

“I predict the **Internet** will soon go spectacularly supernova and in 1996 catastrophically collapse.”

ROBERT METCALFE, INVENTOR OF ETHERNET, 1995

“**Bitcoin** should be outlawed, it doesn’t serve any useful social function.”

JOSEPH STIGLITZ, NOBEL LAUREATE, 2018

Being a dreamer **pays off.**



Liechtenstein's Blockchain Strategy: Prime Minister's Outlook

“All these measures we are talking about are meant to maintain Liechtenstein's quality of life for the future and to preserve as well as creating new jobs. This is the main goal we are pursuing in the long run.”

Prime Minister of Liechtenstein Adrian Hasler



Key Takeaways

- Liechtenstein's government has actively embarked a blockchain-friendly strategy.
- Liechtenstein's government is in close contact with the blockchain industry and its financial authority has been building up know-how and resources to stay on top of the blockchain business.
- The Liechtenstein Blockchain Law is being prepared for Parliament and is expected to be enacted by summer of 2019.

For the past two years, the government of Liechtenstein has been crafting a first of its kind law related to the blockchain technology. The law signals to entrepreneurs that Liechtenstein is open for business. Prime Minister Adrian Hasler and Dr. Thomas Dünser from the Ministry of Finance are spearheading the project. This is part of a larger project to “digitalize Liechtenstein” by improving all government services and encouraging innovation in the country.

Some Reputable Names for Crypto Business in Liechtenstein

- 1.) Are you planning an ICO and you need a lawyer? Thomas Nägele at [Nägele Law](#) in Vaduz has gained international reputation for consulting blockchain related businesses.
- 2.) Did you invest in cryptocurrencies and now you feel crunchy about your tax obligations? Matthias Langer at [Actus-AG](#) in Vaduz has published great literature on this topic.
- 3.) Are you a planning a business in Liechtenstein and you need a local trustee to help you get started? Klaus Stark at [Ganten Group](#) has helped many already.
- 4.) Do you need a bank account for your crypto business? [Bank Frick](#), [Alpinum](#), [Bendura](#), and [Union](#) all welcome blockchain entrepreneurs.

Mark Valek: Many thanks Prime Minister Hasler and Dr. Dünser for taking time. We have some questions that we would like to go through so let’s begin!

Liechtenstein has made a name for itself within the crypto industry as a very blockchain-friendly jurisdiction. This has become evident so far from the many ICOs carried out here, by the commitment of the University of Liechtenstein, from regulated crypto funds which were approved here, and now finally also in the imminent adoption of the Blockchain Act.³⁵ What long-term vision for the principality do you see with this blockchain-friendly strategy?

Prime Minister Hasler: *All these measures we are talking about are meant to **maintain Liechtenstein’s quality of life for the future and to preserve as well as create new jobs.** This is the main goal we are pursuing in the long run. Especially with these new technologies, we have found that there is great potential, that it comes with great disruptive power, and that it brings opportunities for*

the small state of Liechtenstein. Our aim is simply to be very open to innovation. We already took up the subject of innovation in the last legislature meeting, and we have already implemented appropriate measures with the Liechtenstein impulse program and want to incentivize the financial sector to innovate, too. The blockchain approach fits perfectly into this strategy, as far as the early recognition of opportunities and taking advantage of them is concerned. Providing legal certainty, which is very important in the financial sector, is always at the top of our list. We have experienced this in recent years in the traditional financial sector as well, and especially with these new technologies, that legal certainty can be created here. These are the main directions.

Mark Valek: Last June, the Blockchain Act was presented with great interest for the first time at the University of Liechtenstein. **This is one of the first comprehensive legislative frameworks worldwide to formulate an expanded set of legal rules for applications of the new blockchain technology.** What are the main cornerstones of this law?

³⁵ See “[Vernehmungslassungsbericht Blockchain-Gesetz](#),” *Ministerium für Präsidiales und Finanzen*, August 29, 2018.



Incrementum Partner Mark Valek with Liechtenstein's Prime Minister Adrian Hasler.

Prime Minister Hasler: *Our aim with this law is to clarify the fundamental questions of the token economy. We have seen very specific areas such as ICOs or cryptocurrencies regulated in other countries. We have chosen to deliberately develop a comprehensive approach to clarify these fundamental questions. **Controlling tokens embodies all kinds of rights on blockchain platforms.** Customer protection is very important for us, so we clearly define all the roles that exist in the token economy and regulate them in order to create legal certainty. A major concern of ours is also the applicability of money laundering laws, due diligence and so on as elementary parts of this new decree that we are planning.*

Mark Valek: Is it known when the blockchain law will come into force?

Prime Minister Hasler: *We are now about to start the consultation process. This is the first phase, then the regulators will have the opportunity to make comments and give feedback. We will then incorporate these comments and submit the relevant legislative proposal to Parliament. **If all goes well, we will probably be able to do this in December.** It is the first time the country is dealing with this bill, and I expect that **we could have the bill in place by summer 2019.***

Mark Valek: Where can interested companies or citizens find out about the law and follow up with questions? Will the law also be available in English?

Prime Minister Hasler: *For the time being, **the consultation is published and can also be downloaded from the [government's homepage](#).**³⁶ However, this will not be in English. **When the law is passed, it will certainly also be translated into English.** We have already translated many laws into English, which are also available on our portal, and I assume that when this law is passed, it will be available in English on the portal as well.*

Mark Valek: What impact do you think the law will have on the domestic banking system?

Prime Minister Hasler: *I expect the Blockchain Act to have a positive impact on our financial center. The law will make it easier for banks and other financial intermediaries to deal with the blockchain. We are already seeing that banks, trustees, and lawyers are very interested in our draft and see great potential for new business models. In the meantime, various companies from the FinTech sector have already settled in Liechtenstein. This radiates to the outside world and leads to other companies taking an interest in our location. We have noticed that a new ecosystem is emerging in Liechtenstein that will certainly continue to grow.*

Mark Valek: You have touched on this somewhat: Are there already companies that have announced their plans to make use of the law?

“Bitcoin was the first engineering solution that allowed for digital payments without having to rely on a trusted third-party intermediary. By being the first digital object that is verifiably scarce, Bitcoin is the first example of digital cash.”

Saifedean Ammous

³⁶ See [“Vernehmlassung zum Blockchain-Gesetz gestartet.”](#) Regierung des Fürstentums Liechtenstein, August 29, 2018.

Prime Minister Hasler: *In recent weeks, we have repeatedly received feedback from companies, and this feedback has been very positive. In Dr. Thomas Dünser we also have a competent contact person in the ministry. He is in close contact with the scene and feels the pulse. This shows that some of these companies are waiting for the law to come into force.*

Mark Valek: Is there something like an association, someone with whom you were in bilateral talks with or was there a central point of contact?

Dr. Dünser: *In drafting the law, we involved a core group of experts from various fields who have already dealt intensively with the blockchain. In addition, I hold relatively frequent discussions with entrepreneurs from the field in order to know the current developments and to recognize the upcoming problems.*

“There is a major revolution taking place that is now allowing for a better currency, one that is more secure, that is decentralized, that is more effective, more useful, it is global, it is open to everyone, it allows people sending money to their families without any big friction, it is a far better currency than fiat currency.”

Tim Draper

Prime Minister Hasler: *It is also exciting in this context that there are already local companies such as law firms, trustees, and also banks that have been intensively involved in this topic for some time. Many of them are in close exchange with Dr. Thomas Dünser and can also bring in input. Thus, a certain scene with both external and Liechtenstein companies has already formed here, and it was a great advantage that one could rely on these resources as well as assessing the know-how in the preparation of such a proposal.*

Mark Valek: Especially with these new technologies, it is important because everyone has to learn somewhere, which we also see as our mission with the [Crypto Research Report](#). Are you in contact with legislators in neighboring countries on the blockchain issue?

Prime Minister Hasler: *We follow very closely what is being done in other states and jurisdictions, which is very interesting for us. We also exchange ideas with international organizations on a regular basis.*

Mark Valek: How do you assess Liechtenstein’s progress as a location for the blockchain industry compared to Switzerland or other international locations?

Prime Minister Hasler: *What we can say for sure is that we have been dealing with the subject of innovation and subsequently also with the subject of the blockchain for several years now and are working hard to optimize the framework conditions in this area. The Blockchain Act is now part of this work, and I think **we are very well positioned given our innovation-friendly government and our financial market supervision, which sees potential in this area. Further, our regulatory laboratory, which is very well equipped to take up the concerns of companies at an early stage, also provides advice and guidance which is quite unique.** These factors coupled with the short distances we have make a great package of Liechtenstein with which we can of course also score accordingly. **Last but not least, our honorary membership is also a great advantage since we also have the EU passport, i. e. market access to Europe.***

“Just like 20 years ago when very few institutions had exposure to hedge funds, it is now time for institutional investors to get off zero allocation to crypto assets.”

Mark W. Yusko

Mark Valek: We want to consider the whole topic from another standpoint: The chairman of the SEC has stated that every ICO he has seen so far resembles a traditional IPO and would therefore be subject to its supervision in the case of the USA. Do you agree with his view?

Prime Minister Hasler: *We take a different view on this subject. There are tokens that are similar to securities and of course they are subject to this legislation – that is clear. However, there are also tokens that often reflect rights of use and, in our view, in Liechtenstein and other European countries, these do not fall under the securities legislation of the financial market regulation.*

Mark Valek: Is the Financial Market Authority in charge of classifying these tokens?

Prime Minister Hasler: *Yes, it is the central authority that classifies them together with the regulatory laboratory and then advises the companies and shows whether it embodies a soft right of use from the point of view of the FMA or it is similar to securities and therefore also subject to financial market regulation.*



Mark Valek, Dr. Thomas Dünser, and Prime Minister Hasler discuss Liechtenstein's Blockchain Law.

Mark Valek: Allow me to bring in another question: I assume that the FMA will inevitably put resources into it. Is there already a specific department there or people who are specifically responsible for that?

Prime Minister Hasler: *A few years ago, the FMA established the Regulatory Laboratory, a cross-divisional organization that dealt with this topic and supported companies. The next step has been taken, and this regulatory laboratory has been further professionalized with supervisory management and equipping it with appropriate human resources.*

Nevertheless, the original areas are still responsible for approvals. This means

*that, as far as a banking licenses, insurance, etc. is concerned, the relevant departments are responsible. But the first point of contact for such businesses is the regulatory laboratory. **There they give feedback if the token falls under the securities law of the financial market regulation or not, and then it goes into the normal process.***

Mark Valek: There's probably a point of contact or a person in charge?

Dr. Dünser: *Yes, there is the head of the Office for Innovation and Regulatory Laboratory for the Financial Centre, Dorothea Rohlfing.*³⁷

Prime Minister Hasler: *The second position of contact is the Ministry of Finance led by Dr. Thomas Dünser, and this is also very important that both the ministry of the government and the FMA have respective contact points on both sides and so that businesses can orient themselves there. We are joining forces so that all the information can be passed on.*

Mark Valek: Which of the local banks and companies are ready to enter the crypto world, or are there interesting projects you have been following?

Prime Minister Hasler: *For obvious reasons, I do not want to mention any special names now, but you can see that the interest of the local banks, but also of lawyers and fiduciaries, is very big. I have noticed in recent months that a great deal of time is being invested there, that appropriate training is being acquired, and specialist skills are being obtained in order to be active in this area as well. It turns out that there are many interesting projects by companies approaching Liechtenstein from outside and are **looking for local business partners to set up their businesses here in Liechtenstein.***

Mark Valek: There are lawyers who specialize in these matters and they are probably the first reference for many foreigners.

Prime Minister Hasler: *Exactly. Some lawyers specialized early on. Some lawyers specialized in these topics at an early stage and are in great demand today. By the way, we also took this expertise into account when drafting the Blockchain Act.*

Mark Valek: Last but not least, are there any other blockchain-friendly measures that are in the pipeline?

Prime Minister Hasler: *We are constantly working on improving the framework conditions and would like to implement this Blockchain Act as a next step. That means discussing it with parliament, adopting it, and then entering it into force. That certainly still needs appropriate resources. Nevertheless, we are constantly in discussions with the market to feel the needs of the community, and to see where further measures are necessary, and we are very much looking forward to implementing further improvements. **But currently there is no concrete project.***

Mark Valek: Wonderful, of course I don't want to take away either of you the chance to make any further comments or suggestions.

Prime Minister Hasler: *I think the questions you have asked were well picked and I think we have given a proper overview of the subject. There's a lot going on right now. Above all, the debate in parliament will be quite exciting. Before that, I*

"People used to use seashells as money. We can't help but think how primitive that was. Today we use paper as money. Eventually people will wonder how we could have been so primitive."

Anthony Pompliano,
Founder & Partner Morgan Creek
Digital Assets

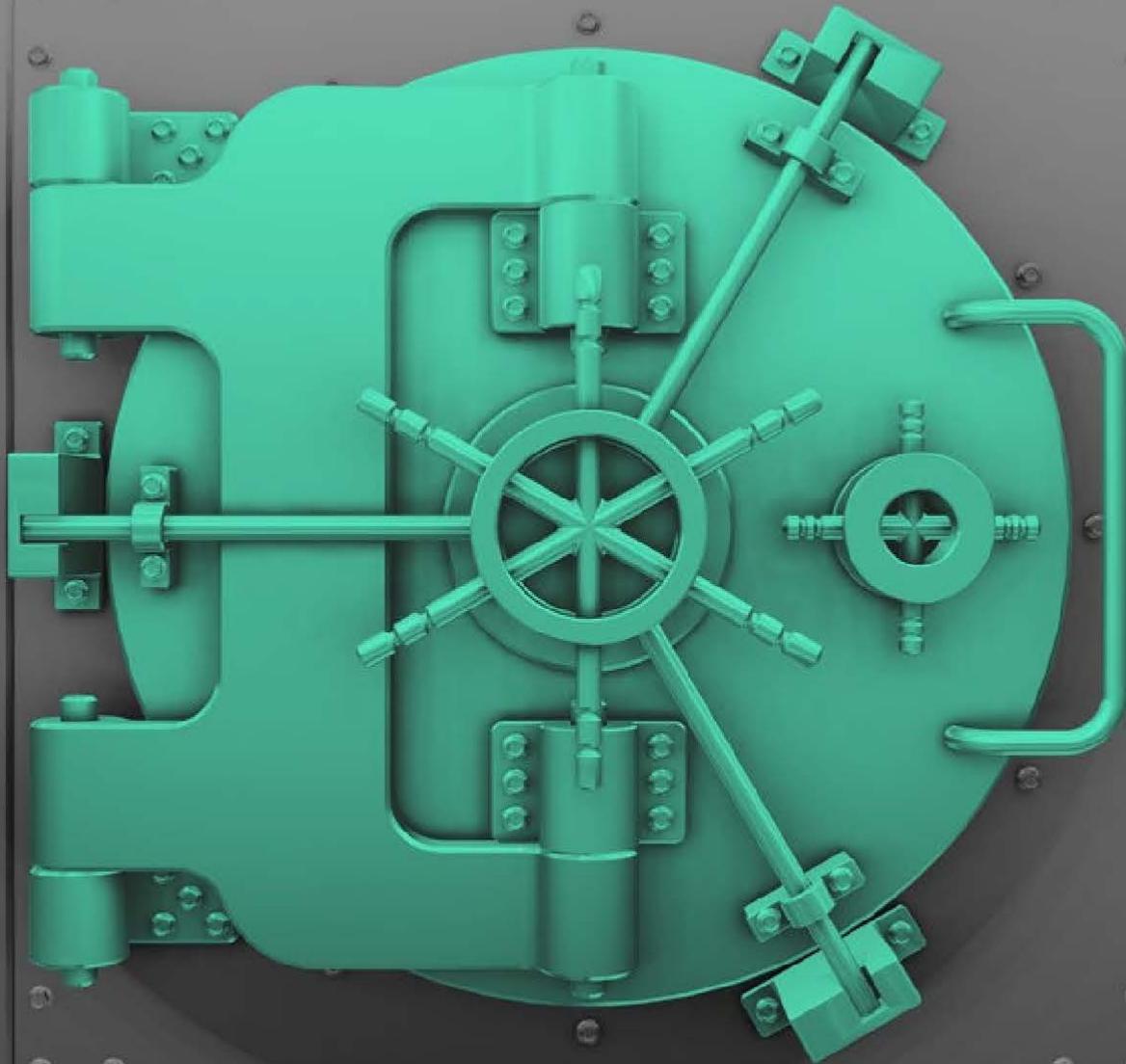
³⁷ See "[Medienmitteilung: Regierungslabor wird verstärkt](#)," Finanzmarktaufsicht Liechtenstein, April 20, 2018.

am already very curious about the consultation that will come out of the comments. Whether this approach which we have chosen will also meet with approval. I assume that, but I am curious about further potential for improvement. In addition, the discussion in parliament will be very exciting and then, in the end, the effects it will have once the law has come into force. We hope that we will get good feedback and that companies in Liechtenstein will find a good location and that many of them will settle here.

Mark Valek: Excellent, then I would like to thank Prime Minister Hasler and Dr. Dünser very much for their time and wish them all the best for the future.

Prime Minister Hasler: *Thank you very much, Mr. Valek. Thank you also for your interest and interview.*

Cryptocurrencies. The New Asset Class.



Regulated | Diversified | Liquid

Information about the fund strategy for professional investors (according to MiFID) only.

www.cryptofunds.li

The Network Effect As a Valuation Methodology

“... ether itself will retain a strong and steady value as a cryptofuel, and as a store of value for Ethereum-based security deposits, simply because of the combination of the Ethereum blockchain's network effect (which actually is a platform network effect, as all contracts on the Ethereum blockchain have a common interface and can trivially talk to each other).”

Vitalik Buterin, Founder of Ethereum



Key Takeaways

- Valuation methodologies are key for fundamental analysis, which is a well-known concept in traditional finance. It is now reached the crypto asset world as we see markets slowly maturing.
- We provide a primer on one specific valuation measure, which aims at identifying assets that are over- or underpriced relative to some fundamental measures observed on the respective blockchains and apply this concept for Bitcoin, Litecoin, and Bitcoin Cash.
- While the ratios have their caveats as well, they largely conclude that the bear market might not be over yet and that we could see some further correction when we put current levels in a historical context

A hot topic at conferences in the US is how to value cryptocurrencies.

There are two main models: absolute and relative. Absolute valuation allows investors to calculate a “fair” price for each asset. Then the investor can compare the theoretical “fair” price to the real price that the asset is selling for on the market. If the price on the market is higher than the “fair” price, then the investor receives a sell signal and vice versa. On the stock market, analysts calculate the net present value of future firm revenues or of dividends to arrive at what the stock should be priced at today. In contrast, relative valuation models allow investors to compare several assets. Relative valuation models are often ratios such as the Price-to-Earnings (P/E) ratio which compares the price of an asset to the earnings of a company.³⁸ Cryptocurrency analysts adapted this general valuation framework by computing each crypto asset’s Network Value to Metcalfe (NVM) ratio, Network Value to Transactions (NVT) ratio, and a metric that combines the concepts used in the two prior ratios called Network Value/Transactions to Growth (NVTG) ratio. Higher ratios mean a cryptocurrency is overbought relative to other coins.

In this chapter we develop relative valuation models to help investors compare various cryptocurrencies. **Our calculations suggest that the cryptocurrency market is still overvalued because the market capitalization is not justified by the number of active users or the daily on-chain transaction volume.** We focus our analysis on Bitcoin, Bitcoin Cash, and Litecoin and find that Bitcoin is a better investment than Bitcoin Cash or Litecoin. However, the caveat is that this is only one indicator out of several that one can use for making investment decisions.

The Network Effect

In the 1980s, Robert Metcalfe, an employee at the Xerox Palo Alto Research Center (PARC), devised a novel theory about the value of communication systems.³⁹ The theory later became known as Metcalfe’s Law. His original intent was to describe the purchases and connections of the Ethernet, which was a predecessor to the Internet.

Today, the theory is used to value a network and its users, such as Internet businesses like Facebook and eBay. **Metcalfe’s model proposes a relationship between the value of a network and its size, typically measured in number of users.**⁴⁰ More specifically, he argued that the value of a network is proportional to the square of network nodes (users). For example, assume the social media network Pinterest has n users, **then the utility each user derives from the network is proportional to $(n - 1)$, namely the number of potential connections in the network.** This relationship between utility and users is the so-called **network effect**. If an additional user joins the network, it increases the utility of the others, and assuming that all connections are

Network Value Correlations

Correlations Table		as of 21.09.2018		
	BTC	LTC	BCH	
Metcalfe's Law	0.9653	0.9438	0.8482	

The theory behind Metcalfe’s Law fits extremely well with empirical data, as can be seen from the table above.

³⁸ Fama and French, 1992

³⁹ See “Metcalfe’s Law after 40 Years of Ethernet,” Bob Metcalfe, *Computer*, Vol. 46, No. 12, 2013.

⁴⁰ Ibid.

equally valuable, the total network value should result proportional to $n*(n-1)$, which in turn is asymptotically proportional to n^2 .

Metcalfe's Law Applied to Crypto Assets

Much like online networks, crypto assets are networks of users that are connected in digital space that can interact with other users. **Metcalfe's law means that as more people adopt cryptocurrencies, the more utility each user derives from the network. Ultimately, the result is a proportionately higher network value.**

In an effort to define the role of network effects and understand their consequences in the cryptoeconomic context, Vitalik Buterin outlined the main reasons a large network increases the value of a cryptocurrency.⁴¹

1.) Security effect: systems that are more widely adopted derive their consensus from larger consensus groups, making them more difficult to attack.

2.) Payment system network effect: payment systems that are accepted by more merchants are more attractive to consumers, and payment systems used by more consumers are more attractive to merchants.

3.) Integration network effect: third party platforms will be more willing to integrate with a platform that is widely adopted, and the greater number of these tools will make the platform easier to use.

4.) Size stability effect: currencies with larger market cap tend to be more stable, and more established cryptocurrencies are seen as more likely (and therefore by self-fulfilling prophecy actually are more likely) to remain at non-zero value far into the future.

5.) Market depth effect: larger currencies have higher market depth on exchanges, allowing users to convert larger quantities of funds in and out of that currency without taking a hit on the market price.

6.) Interpersonal single-currency preference effect: users prefer to use the same currency that others are using to avoid interchange fees when making ordinary transactions.

7.) Intrapersonal single-currency preference effect: users that already use a currency for one purpose prefer to use it for other purposes both due to lower cognitive costs and because they can maintain a lower total liquid balance among all cryptocurrencies without paying interchange fees.



John Pfeffer, partner at London-based Pfeffer Capital says Bitcoin will go to \$700,000.

⁴¹ See "On Bitcoin Maximalism, and Currency and Platform Effects," Vitalik Buterin, *Ethereum Blog*, November 19, 2014.

Figure 7: Bitcoin Network Value Compared to Theoretical Metcalfe Network Value



Plotting Bitcoin's Network Value (Market Cap) against the fundamental values suggested by Metcalfe's Law on a log scale visually reveals the strong correlations.

Source: Incrementum AG.

Different types of crypto assets may exhibit different types of network effects as well: a payment token like Bitcoin will probably exhibit a stronger *Interpersonal single-currency preference effect* than a utility token like Ethereum.

Limitations of Network-to-Metcalfe Ratio

While sensibly sound, Metcalfe's law did not go without controversy in the academic community.

For instance, [Andrew Odlyzko](#) et al. raised a valid concern about the model: While Metcalfe's Law suggests that the utility expressed in terms of *potential* connections of users within a network can theoretically approach infinity, there are in fact certain limitations on the usefulness of additional network participants to the individual user after the network has reached a certain size.

Another heavily scrutinized assumption was that each additional user contributes an equal amount of value to the network. It makes sense to argue that for a network of millennial Snapchat users, the addition of further friends entails more utility than if their parents join the network.

Network Value to Metcalfe Ratio

After having gained an understanding of the role of network effects in crypto assets, we can now look at the concrete metrics used to assess their fundamental value suggested by network effects. The first one is applying Metcalfe's Law directly to crypto assets and is called the Network Value to Metcalfe ratio. Its main purpose is to give a sense of how over or undervalued an asset is at the moment.

The more inflated the price is in relation to the utility that network users derive from it, as proxied by the network effect theory, the higher the expected correction towards the theoretical fundamental value implied by the model will be. That said, **the model implies that the price of a crypto asset stands in a direct relation with a fundamental value measured by**

“Metcalfe’s law means that as more people adopt cryptocurrencies, the more utility each user derives from the network. Ultimately, the result is a proportionately higher network value.”

Crypto Research Report

user utility in the long run and that some form of reversion to the mean takes place.⁴²

The Network Value to Metcalfe ratio puts the respective law for describing the network effect in its denominator, while using market capitalization as a proxy for network value in its numerator. The number of network users (n) is approximated by the number of unique addresses that are active on a given day, meaning they are participating in sending or receiving transactions.⁴³ Unique addresses in the Bitcoin ecosystem are payment addresses that have a non-zero balance. While the number of unique addresses is not a perfect measure of the actual number of users on a given day, it generally holds that the more unique addresses are in use the more users the network has and vice versa. Since we are trying to arrive at a long-term fundamental metric, we additionally smooth the daily active user number to a 30-day moving average in order to get rid of stark daily fluctuations related to noise.

The first candidate for our analysis is Bitcoin: Plotting the Network Value of Bitcoin against its seemingly mean-reverting NVM ratio reveals a staggering

Figure 8: Bitcoin Network Value vs. Network Value to Metcalfe Ratio



Source: Coinmetrics; Incrementum AG.

“The Bitcoin market price was sometimes ten times higher than predicted by the Metcalfe model.”

Lidia Bolla, Vision &

relationship. **Large spikes in Bitcoins NVM ratio indicate that the network is being priced excessively high in relation to the number of active users and have historically almost always led to subsequent corrections in its market value.** We can see this quite evidently during the periods of early 2011, mid-2012, early 2013 and late 2017. Remember that the orange trace corresponding to the market value of Bitcoin is depicted on a log scale. We transform all the subsequent historical network values to a logarithmic

⁴² Here we are focusing on the relationship between the network value and an aggregate user metric, aiming at keeping the network effect as general as possible. It would require further research into discerning the individual effects at play to arrive at a complete fundamental measure.

⁴³ For internet companies with strong network effects, the analogous daily active users Daily Active Users (DAU) indicator is one of the most important performance and valuation metrics.

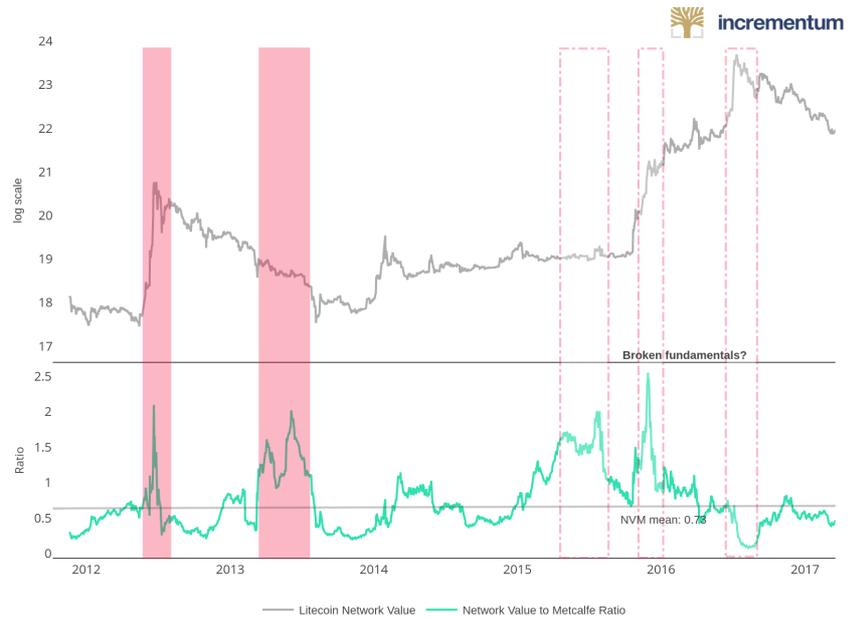
“Crypto assets are networks of users that are connected in digital space that can interact with other users.”

Crypto Research Report

scale for purposes of a more convenient visualization. The y-axis on the chart above represents the log scale on the left and the current value of the NVM multiple on the right.

What we can see is that once NVM moves significantly above its long-term mean (0.21), there are reasons to be concerned about the future near-to middle-term evolution of Bitcoin’s market value. Conversely, an NVM well below its mean has typically meant a good buying opportunity. **The current levels, however, indicate a worrying picture for the state of Bitcoin and strongly suggest a further downwards correction.**

Figure 9: Litecoin Network Value to Metcalfe Ratio



Source: Coinmetrics; Incrementum AG

Figure 10: Bitcoin Cash Network Value to Metcalfe Ratio



Source: Coinmetrics; Incrementum AG.

“First off, you could argue we have had a proper correction in Bitcoin, it has had a 50 percent pull back at one point, which is healthy. But we have still not seen the full effect of the futures contract.”

Kay Van-Peterson, Saxo Bank

Similar patterns, although with less predictive power, arise in the case of Litecoin (LTC) and Bitcoin Cash (BCH). The quality of the latter is further diminished by its short history of data.

For Litecoin, spikes in NVM were mostly followed by corrections in its market value in subsequent periods. However, the most recent “bubble” in late 2017 has in no way been preceded by such a spike. This might be associated with the limitations we pointed out for NVM or with concerns inherent to the Litecoin network, such as the fact that Litecoin development has almost completely stalled, as evident from their Github activity, and Litecoin founder Charlie Lee has sold 100 % of his LTC stake. **Overall, the multiples of BTC & LTC seem to be trading more or less in the same range of 0.01–2, while BCH has inherently exhibited a way more inflated scale, ranging from .90–11.** The current ratios can be found in the following table below. **According to relative valuation, BTC and LTC are overvalued equally compared to their user base, while BCH appears to be grossly overvalued.**

Table 4: Current Levels of Network Value to Metcalfe Ratio

Current Network Value to Metcalfe Multiples		09/21/2018	
	Bitcoin	Litecoin	Bitcoin Cash
Network Value to Metcalfe Ratio	0.33	0.44	5.95

Source: Incrementum AG.

Network Value to Transaction Ratio

Limitations of Network Value to Transaction Ratio

The challenges of filtering out true economic throughput on the blockchain are quite significant and thus compromise the power of the NVT Ratio. For example, there are massive transfers from one exchange to another taking place, which are of no utility to the network whatsoever. Also, one has to be extremely cautious with the measurement of on-chain transaction volume when comparing different blockchain networks, since different protocols imply different ways of accounting for transactions (e.g. Bitcoins UTXO vs. Ethereum’s Account based model) as well as diverse activity on the chains (e.g. transaction volumes on networks with staking rewards such as Dash are inherently inflated compared to, say Bitcoin).

On a further note, there is a concept first introduced by George Soros, called “Reflexivity”: Transaction volumes tend to follow changes in price and vice versa, so the two variables have a “reflexive” relationship, weakening the indicative power of the NVT ratio.

Another valuable relative valuation metric that is related to the Network Value to Metcalfe ratio is the Network Value to Transaction ratio. If we think back to the P/E ratio found in traditional finance, earnings serve as a proxy for the value created for shareholders. If we try to apply this reasoning to crypto assets, we will find that most of them do not have earnings in the traditional sense. However, one can argue that there might be a positive relationship between the utility and consequently fundamental value of a network and the total value of transactions flowing through it. This idea is in line with the interpersonal and intrapersonal network effects discussed in the previous section by Vitalik Buterin.

The most crucial part about the NVT ratio is defining the denominator, namely total transaction value, such that it truly proxies the utility conveyed to users. When looking at transaction volumes in the crypto space, there are currently two main venues where transactions take place: on-chain and off-chain. On-chain transactions refer to activity that occurs directly on the blockchain, while off-chain transactions typically refer to interactions on

remote venues like cryptocurrency exchanges which are not directly documented on the blockchain.

Distinguishing volumes that proxy utility from those that do not is a true challenge in the crypto world and a lot of brainpower is going into that topic.⁴⁴ It is reasonable to assume that on-chain transaction volume is the closest we can get to measuring true economic output on the blockchain, which directly translates to user utility. We proxy the denominator in the NVT ratio with on-chain transaction volume as calculated by the Coinmetrics Team, which publishes their dataset under the name of “adjusted transaction volume estimates”.

Similarly, to NVM, we smooth the daily (on-chain & adjusted) transaction volume figures to a 30-day moving average to ensure that we solely capture a long-term fundamental trend. Using the total market capitalization as a proxy for network value as above, we obtain the following results presented in the figures below:

Figure 11: Bitcoin Network Value to Transaction Value



Source: Coinmetrics; Incrementum AG.

“The Network Value to Metcalfe and Network Value to Transaction ratios are without doubt the most useful relative valuation ratios at the moment.”

Crypto Research Report

For Bitcoin, NVT shows high multiples (between 50–100) indicating a potential overvaluation and low multiples (between 0–30) signaling undervaluation. **It is noteworthy that the current trend of NVT seems to be moving towards levels seen at the peak of the most recent bubble.** This is true not only for BTC but also for LTC, while BCH’s valuation in relation to its transactions volume seems to have stabilized around its long-term mean.

⁴⁴ See [“Introducing our adjusted transaction volume estimates.”](#) Coinmetrics Team, *Coin Metrics*, June 27, 2018.

Figure 12: Litecoin Network Value to Transaction Ratio



Source: Coinmetrics; Incrementum AG.

Figure 13: Bitcoin Cash Network Value to Transaction Ratio



Source: Coinmetrics; Incrementum AG.

“As evident, Bitcoin seems to have the healthiest valuation levels on a relative basis compared to its peers, albeit being quite elevated in an historical comparison.”

Crypto Research Report

Similar to the NVM ratio, the NVT ratio of BTC and LTC are trading in the same range most of the time (20–60), while BCHs multiple is typically above 50 and at some points of its short history touching or overshooting the 100 mark, which might be indicative of an inherent overvaluation of BCH. As already discussed in the case of the NVM ratio, the NVT of LTC does not seem to have followed its historically predictive pattern during the most recent bubble in late 2017. Please refer to our possible explanations for this trend in the previous section.⁴⁵

⁴⁵ See “Re-thinking Network Value to Transactions (NVT) Ratio,” Dmitry Kalichkin, February 4, 2018; “Debunking Market Narratives: Litecoin (LTC) Edition,” Tushar Jain, Multicoin Capital, September 14, 2018.

Network Value/Transaction Value to Growth

The previous two subchapters dealt with the NVM and NVT ratios in great detail, but as we can see from our analyses, the ratios sometimes suggest contradicting findings as far as over or undervaluation of a crypto asset is concerned. Both ratios are without doubt the most useful relative valuation ratios at the moment, however, researchers have noted that a metric combining their insights into one single figure would be desirable. NVT does not factor in the value-added to the network through new users, whereas NVM does not consider the total amount of economic activity that users actually expend on the network as opposed to just owning an address. This is why researchers⁴⁶ are drawing the connection between traditional finance and the crypto world by looking at the second most common relative metric used, namely the Price/Earnings to Growth ratio.

Figure 14: Bitcoin Network Value to Transaction Value to Growth



“Historically, ten days comprise all the performance in any single year of Bitcoin’s price...If you just took out those ten days, Bitcoin’s down 25 percent a year. So as miserable as it feels holding Bitcoin at \$8,000, the move from \$8,000 to \$25,000 will happen in a handful of days.”

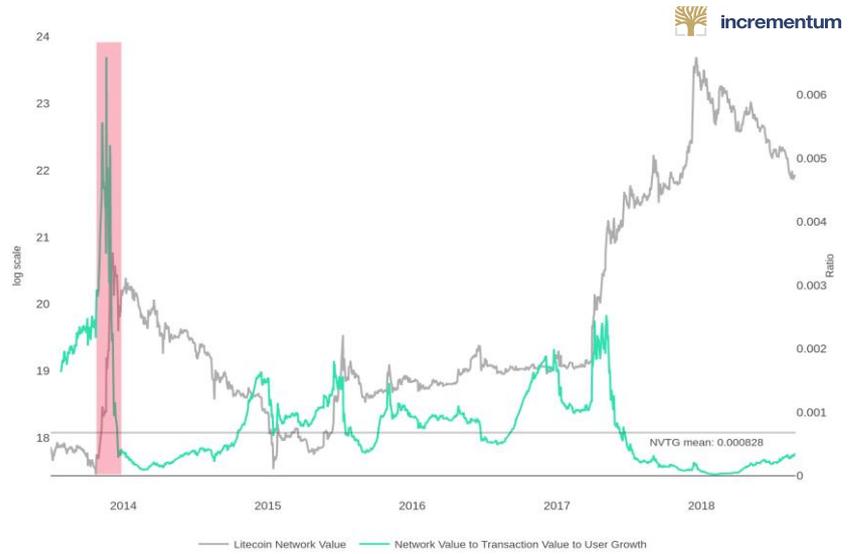
Tom Lee,
Co-founder of Fundstrat

Bitcoins NVTG is approaching its highest levels in two years, which strengthens our conclusion that there might be more pain ahead, unless true economic activity starts to pick up substantially on the BTC Network.

Source: Coinmetrics; Incrementum AG.

⁴⁶ See [“Improvements on the Network Value to Transactions \(NVT\) Ratio & Introducing Network Value/Transactions to Growth \(NVTG\) to Value Crypto,” Vikram Arun, Medium, March 29, 2018.](#)

Figure 15: Litecoin Network Value/Transactions to Growth



Source: Coinmetrics; Incrementum AG.

The PEG ratio is particularly useful in valuing stocks with high growth potential but close to non-existent earnings which would result in a very high P/E ratio and thus an incomplete assessment. If we apply the PEG ratio to crypto, we obtain the Network Value/Transactions to Growth (NVTG) ratio, which aims at factoring in both the economic throughput on a network and the growth of its user base in one single metric. Applying this concept to real networks we obtain the following results shown in Figures 14, 15, and 16.

Figure 16: Bitcoin Cash Network Value/Transactions to Growth



As we argued before already, we think that Bitcoin Cash has started out with very high multiples of NVM and NVT in the first place, which is why the very short sample of data might draw a rather misleading picture. A significant downwards correction as well towards multiples more similar to the ones of BTC given their almost identical final goal may be in the future for BCH.

Source: Coinmetrics; Incrementum AG.

The NVTG metric summarizes the findings we obtained from analyzing NVM and NVT for the three assets separately. **Altogether, the ratios indicate room for further downwards correction towards their respective fundamental value as suggested by user numbers and transaction volumes for Bitcoin and Bitcoin Cash.** As introduced earlier, Litecoin seems to have lost touch with its fundamentals completely, which is why its NVTG ratio appears to be of little predictive value at this stage.

“Bitcoin’s volatility derives from the fact that its supply is utterly inflexible and not responsive to demand changes, because it is programmed to grow at a predetermined rate.”

Saifedeam Ammous

To wrap up, we have summarized the current state according to relative valuation in one table for the selected tokens. As evident, Bitcoin seems to have the healthiest valuation levels on a relative basis compared to its peers, albeit being quite elevated in an historical comparison. Bitcoin Cash has clearly the most exaggerated valuation multiples relative to its user base and transaction volume. We will continue to monitor these ratios very closely in the future and plan to provide regular updates on them.

Table 5: Current Relative Valuation Ratios

Current Multiples	09/21/2018		
	Bitcoin	Litecoin	Bitcoin Cash
Network Value to Metcalfe	0.33	0.44	5.95
Network Value to Transaction	56.6	62.5	65.1
Network Value to Transaction/Growth*	4.6	34.4	84.2

*Here we have multiplied the actual NVTG by a multiple of 10⁵ to make the figures more visually appealing.
 Source: Incrementum AG.

We want to thank Incrementum Analyst Friederich Zapke for contributing to this chapter.



Home of **Cryptocurrency**

TRADE. SEND. STORE.



Visit us on www.bitpanda.com
Made in **Vienna** with ♥ and care

Liechtenstein's Blockchain Strategy: Insights from the Financial Market Authority

“Payment tokens can only be issued to companies with an FMA license, e. g., an electronic money license or a bank license. However, there are certain exceptions that do not require a permit. With securities tokens, it depends on whether the company uses the token to create a financial instrument for investors or to raise debt or equity for the company itself. In the latter case, the enterprise does not require a license from the FMA but should have the so-called prospectus approved.”

Patrick Bont, FMA

Key Takeaways

- Over the past three years, the FMA has received and processed more than 100 inquiries in connection with ICOs. However, only a fraction of them were implemented.
- According to the FMA in Liechtenstein, the planning, preparation, and implementation of an ICO takes between 12 and 18 months, due to the complexity of coin and required permits.

Patrick Bont is a member of the executive board of the Financial Market Authority Liechtenstein, and he is the head of the banking division and the head of the FinTech team at the FMA. For the past three and half years, Mr. Bont has served as lecturer at the University of Liechtenstein's Compliance-Officer Certificate Program. He completed his Master's in Law at the University of St. Gallen. Mr. Bont has written and spoken on the subject of cryptocurrencies, and he is an active member of the Liechtenstein FinTech community.

How to Get in touch with Liechtenstein's FMA

- 1.) Follow Patrick Bont on Twitter [@patrickbont](https://twitter.com/patrickbont)!
- 2.) Attend [the free blockchain meetups](#) in St. Gallen, Switzerland created by Patrick Bont and Beni Bürgli!
- 3.) Meet Mr. Bont in person during one of his speeches like the one at [FinTech.li](https://www.fintech.li)!
- 4.) Stop by the FMA, but call or email them first to arrange an appointment!

Finanzmarktaufsicht Liechtenstein
 Landstrasse 109, Postfach 279
 9490 Vaduz, Liechtenstein
 +423 236 73 73
info@fma-li.li

Mark Valek: An essential aspect of cryptocurrencies and the tokenized economy is the process of so-called initial coin offering (ICOs), i. e. the first issue of crypto tokens. What are the main categories of tokens from a regulatory perspective?

Patrick Bont: *There are numerous approaches to categorize tokens. Discussions are under way among regulators and supervisors as to which approach makes the most sense. The FMA currently assumes three categories: utility token, payment token and securities token. Roughly speaking, one can say that utility tokens entitle to purchase a product or service, payment tokens are to serve as means of payment and securities tokens are quasi-financial instruments. In practice, however, the limits are not quite so easy to draw and there are numerous hybrid forms. From a financial market perspective, payment tokens and securities tokens are particularly relevant.*

Mark Valek: Who carries out the token classification of the ICO in each individual case? Is the classification focused on the legal or technical perspective?

Patrick Bont: *Generally, the token issuer is responsible for clarifying whether its ICO or token falls under financial market law. It is advisable to consult a specialized lawyer. The FMA's FinTech team can of course also be contacted in case of uncertainties. First and foremost, the legal classification is important to us. However, the technical functionalities of a token can give hints to the classification process.*

Mark Valek: Let us assume that a company intends to have an ICO in this country. What does the process look like depending on the token class that is to be issued?

Patrick Bont: *First, the company must decide what it wants to achieve with the ICO. This means that it must assess the ICO economically but also legally and*



Mr. Patrick Bont from the FMA with Incrementum's Mark Valek discussing how to launch an initial coin offering in Liechtenstein.

technically. One also speaks of “ICO economics”. If the decision has been made to issue a “security token” or a “payment token”, the company should submit the corresponding applications to the FMA, preferably with the support of a specialist.



Mark Valek: Does the issuing company require a regulatory license, and if so, which?

Patrick Bont: This in turn depends on the token or the business model of the company and to whom the tokens are offered. “Payment tokens” can only be issued to companies with an FMA license, e. g., an electronic money license or a bank license. However, there are certain exceptions that do not require a permit. With “securities tokens”, it depends on whether the company uses the token to create a financial instrument for investors or to raise debt or equity for the company itself. In the latter case, the enterprise does not require a license from the FMA but

should have the so-called prospectus approved.

Mark Valek: How much time should be scheduled for an ICO?

Patrick Bont: According to our experience, the planning, preparation, and implementation of an ICO takes between 12 and 18 months, depending on the complexity and the required permits.

Mark Valek: What effects will the planned Blockchain Act have on the ICO landscape in Liechtenstein and how will this national law affect international business?

Patrick Bont: It is important to understand that all ICOs currently covered by the financial market law will continue to do so in the future. As an EEA country, Liechtenstein takes over EU financial market regulation and implements and enforces it. The Blockchain Act therefore affects all ICOs that are not covered by the financial market law, i. e. above all utility tokens. The law has the advantage that these ICOs are also subject to certain rules and thus the buyers of the tokens enjoy better protection. However, ICO are only one aspect of the new law.

Mark Valek: How many ICOs have already been reviewed by the FMA or how many are currently under review?

Patrick Bont: Over the past three years, the FMA has received and processed more than 100 inquiries in connection with ICOs. However, only a fraction of them were implemented.

Mark Valek: How does the FMA Liechtenstein prepare itself in terms of resources for the new complexity and increasing requests from companies, particularly with regard to the verification and monitoring of these tokens?

“The regulatory landscape has seen some positive developments in the last six months. Earlier in the year, South Korea highlighted that it was planning to regulate cryptocurrencies and bring them into the open, as opposed to outright banning them. In May, Japan announced that the country is working on cryptocurrency regulation and building a template for ICO and digital currency exchange regulation. Most recently, an SEC official announced that bitcoin and ether are not securities due to the decentralised nature of their networks.”

CoinShares Research

FMA

Finanzmarktaufsicht
Liechtenstein

Patrick Bont: *In June of this year, the FMA set up its own FinTech team. The Regulatory Laboratory/Financial Innovations team deals with questions from companies and entrepreneurs in the field of financial innovation. These are not only start-ups but also banks or other financial intermediaries who want to implement projects. In addition, we at the FMA attach great importance to ensuring that our employees receive further training in these topics so that we can discuss with market participants on an equal footing.*

Mark Valek: Where can a company find out more about any requirements?

Patrick Bont: *I recommend visiting the [FMA website regularly](#). Under the heading “FinTech in Liechtenstein” you will find information on the topic. The FinTech pages are regularly updated and supplemented.*

Coin Corner: ETH, NEO, ADA, & EOS

*“2019’s Trillion Dollar Question: How to merge
Blockchains?”*

Yanislav Malahov, Aeternity



Key Takeaways

- To date, Ethereum is still the largest smart contract blockchain. When it comes to developers, transactions, and DApps, no other platform compares. Of the top 100 tokens by market capitalization, 94 % were built on Ethereum – \$13 billion in capital was generated through Ethereum in this way. Of the top 700 tokens by market capitalization, 87 % are Ethereum tokens. This corresponds to \$15 billion of the \$19 billion collected through the Ethereum platform.
- However, a new cryptocurrency, EOS, has been nicknamed the “Ethereum Killer”. EOS holds the record for the largest ICO ever carried out on Ethereum: \$4 billion. EOS held its Mainnet launch in June this year, switching from an ERC-20 token based on Ethereum to its own blockchain, the EOS blockchain.
- Cardano underperforming: In May, Cardano traded above \$0.37 and ranked as the sixth largest coin on Coinmarketcap listings. It has however been a downhill trend for the coin since then and it trades at \$0.07 today. Investors on Reddit continue to harshly criticize Cardano’s inability to compete with EOS’ low fees and fast confirmation times.

“The main advantage of blockchain technology is supposed to be that it’s more secure, but new technologies are generally hard for people to trust, and this paradox can’t really be avoided.”

Vitalik Buterin

Smart Contract Platforms: Who’s the Smartest in Town?

Grandmother Bitcoin has birthed powerful ecosystems – first and foremost, the Ethereum empire. From July to August in 2014, the Ethereum Foundation launched an Initial Coin Offering to promote its concept to Bitcoin owners. As we already mentioned in our Crypto Concept chapter, the masterminds behind Ethereum were Vitalik Buterin and Mihai Alisie. They realized that a Turin-complete blockchain could enable decentralized applications. Vitalik developed the solidity scripting language to compliment a Turin-complete blockchain. With the technology built, he founded a new crypto asset and after the code had been programmed and \$18 million worth of Bitcoin had been collected in an initial coin offering to advance the project, the first Ethereum block was created on July 30th, 2015.

Wrong Dichotomy

Like Bitcoin, Ethereum attracted a network of users – especially a larger spectrum of software developers. Due to the increasing interest, the Ether price also shot through the ceiling and the rivalry between the two camps increased. Some Bitcoin

supporters – perhaps a little unsettled by the upturn in Ether prices – saw this new crypto asset as a cheap copy of Bitcoin, which was hardly faithful to true crypto values. On the Ethereum side, some exponents were already saying that the programmable blockchain was far superior to Bitcoin and that the former would make the latter obsolete sooner rather than later. To this day, the two camps are fighting each other on internet forums, on Twitter, and at conferences. While Ethereum maximalists are called heretics, Bitcoin maximalists are seen as the fundamentalists of the crypto world.



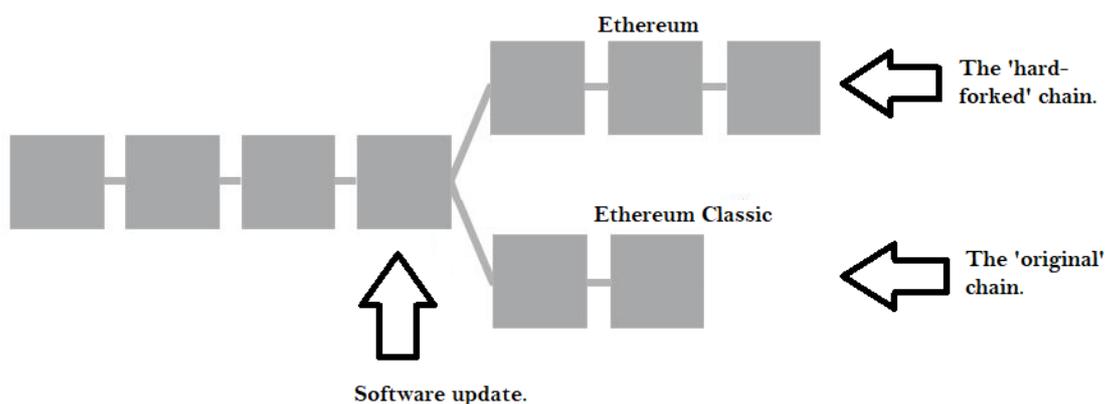
More Adoption > Larger Network > Higher Price of Bitcoin.

This circus around the title “Only True Blockchain” is ultimately nothing but a clownish pseudo battle. Bitcoin and Ethereum are not direct opponents, since they pursue different goals after all. **As an independent store of value, the Bitcoin blockchain must offer the greatest possible security.** This implies that Bitcoin must necessarily be based on a more rudimentary scripting language that limits susceptibility to bugs. The purpose of Ethereum is to resolve this trade-off in exactly the opposite way. Because of the greater experimentation and flexibility in programming capability, greater susceptibility to errors is also accepted at the source code level. **Events mentioned in the Crypto Concept chapter in this edition of the Crypto Research Report, such as the DAO hack and the parity bug are due to programming errors because of solidity’s complexity.** Because the Ethereum approach allows much more in terms of programming, its use case appears much broader, which leads many Ethereum enthusiasts to conclude that Ethereum is the more lucrative project in the long run.

Today, Ethereum is held responsible for the ICO hype during the end of 2017. Quite often the tone is somewhat reproachful: Not only have investors lost a lot of money in this speculative boom, but they have also been led astray by a number of

ICO fraudsters and crypto charlatans. But thanks to Ethereum, anyone can launch their token at low cost without having to worry about setting up a blockchain infrastructure. Ethereum has thus taken crowdfunding to a whole new, global level. **Financing can suddenly be carried out efficiently, quickly and independently via the Internet.**

Figure 17: Hardfork of Ethereum



Source: Hackernoon.

So, while Bitcoin is disrupting the creation of money by central entities such as central banks and commercial banks, Ethereum’s revolutionary power lies in providing a real alternative to the centrally organized capital market. Investment banks have always acted as intermediaries between asset managers and companies or states wishing to issue bonds or shares through an IPO. Before Ethereum, there was no technical way around them. Today there is. The venture capitalist business is currently being turned upside down, which is why it is no longer unusual to find venture capital companies such as Andreessen Horowitz or Union Square Ventures on pre-ICO investor lists. The figureheads of venture capitalists have already had to react to the “Etherealization” of investing – a fate that is likely to hit Wall Street as well.

“The network effect of Bitcoin is powerful and all that matters today is securing ownership of the network, the daily price is just noise.”

Mark W. Yusko

A Non-centralized World Computer

Like Bitcoin, Ethereum is also based on a public blockchain and is therefore ultimately nothing more than a network of tens of thousands of geographically distributed computers, all communicating via the Ethereum protocol. Since Ethereum, in contrast to Bitcoin, can be used to program applications on top of it, the analogy of a world computer applies even better. The Ethereum blockchain functions like a computer. Like a hard disk of a computer, the blockchain stores everything that happens on the Ethereum world computer.

On a programmable blockchain like Ethereum’s, developers can program anything they can program on a local computer. However, the Ethereum world computer differs from an ordinary computer in that it must run according to its programming code and, due to its non-central structure, can only be manipulated at extreme costs. At the same time, such a world computer provides immensely

high robustness. Since the Ethereum blockchain runs on tens of thousands of individual computers, there is redundancy. The Ethereum “hard disk” does not only exist once and in one place only but is distributed all over the world. The downtime risk is therefore diminishingly small.

Why a Programmable Blockchain?

In the context of Ethereum, the term smart contract is frequently used. It was the Ethereum blockchain that first recognized the potential of these “intelligent contracts” and thus popularized the idea. The Bitcoin blockchain already knows a primitive form of smart contracts. In the case of Bitcoin, these are limited to the simple transmission of Bitcoin units. Since Ethereum is a programmable blockchain, the smart contract functions can be extended almost arbitrarily in theory. In addition to the processing of transactions of digital value units, other assets or securities such as bonds, shares, and even physical assets can also be transferred by means of a smart contract. Ultimately, the most diverse contracts that make up our social life today can be converted into computer code, stored in the form of smart contracts on the blockchain and executed by the Ethereum network in a non-centralized manner. This is the vision that is becoming established more and more in the minds of people as Ethereum grows more popular.

“The most encouraging thing about crypto is the amount of sheer opposition.”

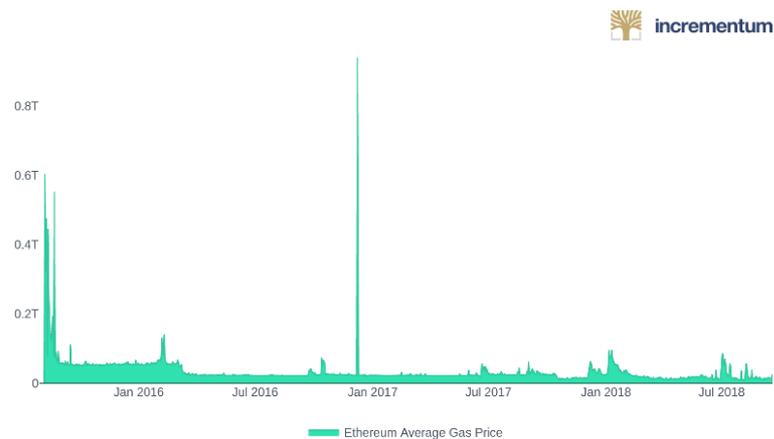
Alex Otsu

The elegance of a smart contract lies in the fact that it is a digital contract that executes itself according to predefined parameters. In other words, if the contract conditions are fulfilled, the contract is executed according to its content. A comparison with a vending machine helps here. One feeds the vending machine with money and receives the selected goods in return. There is no need for a third party to deliver the goods. The theory behind a smart contract works in a similar way: When you pay a smart contract, you receive the corresponding goods, a transfer certificate, a driver’s license or something else. In addition, **the smart contract not only defines the rules and sanctions relating to the agreement, it also enforces them itself.**

Gas – an Essential Component Of Ethereum

Ethereum clients are the individual computers that make up the Ethereum network, and execute the programming code defined in a smart contract. Since Ethereum is Turing-complete – a term from computer science – the computers of the Ethereum network are capable of executing code of any complexity. At the same time, Turing-completeness also means that a smart contract or its programming code would be executed endlessly by the Ethereum clients. Such an endless loop would render the Ethereum blockchain non-functional, since the execution of a single smart contract would consume the resources of all the computers participating in the Ethereum network.

Figure 18: Ethereum Average Gas Price



Source: Incrementum AG.

“The average user should pick up Bitcoin to experience the future of money. To gain a glimpse into an exciting technology. To learn about how money could be in the future and also become aware of how limited money and banks are today.”

Andreas M. Antonopoulos

As a solution, Vitalik Buterin integrated a mechanism into Ethereum that enables the Ethereum clients to determine the execution length of each smart contract in order to prevent endless loops. The keyword here: Gas. Each execution of a smart contract costs a certain amount of gas. But this is just a form of expression. Behind every gas price that has to be paid for the execution of a smart contract is a certain amount of ether, the cryptocurrency of the Ethereum blockchain. How much ether it costs, or in other words, how high the respective gas price is, depends on the current utilization of the Ethereum network. **Not all smart contracts cost the same gas price. Depending on the complexity, the amount of ether to be paid is smaller or larger.**

In principle, the gas from Ethereum can be compared to the gasoline of a vehicle. Just as petrol makes a vehicle run, gas ensures that a smart contract is executed. Just as a car comes to a standstill when the fuel tank is empty, the Ethereum gas also defines an upper limit for the execution of smart contracts and thus prevents endless loops.

The recipients of ether paid via the gas price are the Ethereum clients who are responsible for the execution of smart contracts. Each smart contract costs a minimum execution price. However, if a higher price is offered, the chances of processing and execution are greater, as Ethereum clients are usually controlled by miners who earn wages by chasing the most lucrative offers.

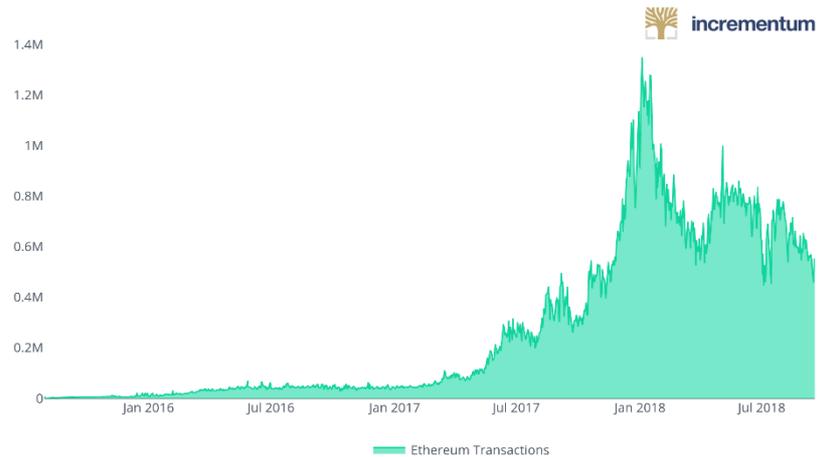
Can Ethereum Hold Steady?

Whoever buys Ether invests in the first decentralized world computer. As such, Ethereum aims to become the backbone of a future decentralized internet. Should the Ethereum network ever reach this important position, Ether will be the “crypto-fuel” to power the entire Ethereum machinery. Just as the oil age made the Rockefeller family and others rich, Ether owners could one day become the new “oil barons” due to the crypto revolution.

Ethereum is now (only) three years old. Since the first Ethereum block was created on July 30th, 2015, the blockchain has become the second largest crypto asset in

terms of market capitalization and already has over 250,000 developers today. To date, approximately 1,800 DApps have been registered. Ethereum is also undoubtedly the most successful blockchain-based crowdfunding platform. Of the top 100 tokens by market capitalization, 94 % were originally built on Ethereum – \$13 billion in capital was generated through Ethereum in this way. Of the top 700 tokens by market capitalization, 87 % are Ethereum tokens. This corresponds to \$15 billion of the \$19 billion collected through the Ethereum platform.

Figure 19: Ethereum Transaction Volume



Source: Incrementum AG, Etherscan.

“We believe that the current situation of Bitcoin is comparable to the early days of the internet. Back in the ‘90s it required a lot of patience to download a single song, while nowadays we are streaming movies in HD quality.”

Lidia Bolla, Vision &

This growth and the resulting dominance have led to the emergence of other smart contract platform projects. Although Ethereum has experienced a meteoric rise, **to handle decentralized services and applications on scale that make it a viable alternative to traditional centralized solutions, effective scalability is required. The Ethereum community has recognized this and is working on it – but it has not yet made a significant breakthrough.**

This is where many alternative smart-contract platforms see their chance to outsmart Ethereum. If they succeed in scaling sooner and better, not only the old world but also the new world should be able to build its applications on one of these alternative smart contract platforms.

Academia Goes Blockchain

Most smart contract projects try to outpace Ethereum with speed. Such as Cardano, a project that is also described as the “Japanese Ethereum” in the crypto community because it was launched in Japan and is said to have had around 95 % of all ICO investors coming from the land of the rising sun.

“Bitcoin: a digital currency with limited and known supply, no borders, and no central group controlling it. US Dollar: a digital currency with unlimited and unknown supply, border restrictions, and controlled by a banking cabal.”

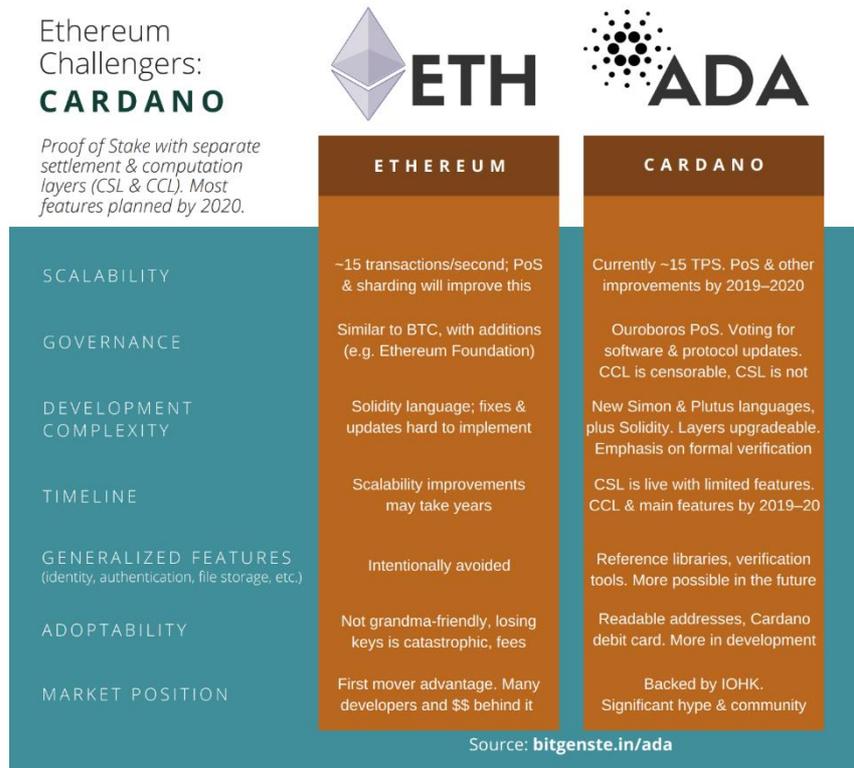
Erik Voorhees

Cardano does not focus on speed. On the contrary, the focus is on accuracy and correctness. Cardano was founded by Charles Hoskinson, who worked for Ethereum and BitShares. The fact that Hoskinson is a mathematician clearly mirrors Cardano’s path forward. No other smart contract project is more academically influenced and geared towards mathematical correctness. For the developers behind Cardano, the technical evaluation of the code is the most important thing. It is their intention to subject Cardano protocols to a peer review system and, if possible, to validate any program code with formal verification. A program code can be seen as formally verified once it is mathematically proven that it is correct for all inputs. Although formal verification does not (yet) prove that a code does what it is supposed to do, it does prove that certain errors can be excluded for sure. This kind of formal verification is a new area, and although other projects are increasingly oriented towards it, Cardano wants to be the leader when it comes to formal verification.

Although Cardano already runs on its own main net, many of the features and characteristics of this smart contract platform are still under development. **For an outsider, there is little secure information available at the moment.** Already today it seems to be clear though: While with many other projects the accounting of value transactions and the execution of smart contract commands are one and the same, with Cardano, these processes are separated into two different “layers”. There is the “settlement layer” for value transfer and the “computational layer” for the application of smart contracts. **Cardano hopes that this split will enable it to better reconcile key aspects such as scalability, privacy, regulatory issues, and compliance.** The two different layers are also based on two different programming languages. One language is specific and limited but less prone to bugs and other unforeseen programming errors, while the other is more flexible. Depending on the application, one or the other programming language can be used, which is why Cardano offers a certain choice here.

Only time can tell whether this careful way of peer reviewing and formal verification will lead to success in the incredibly fast-moving crypto world. After all Cardano’s peer-reviewing appraisal method also has its exquisite critics. Their argument: Academic peer review processes do not always provide certainty and are therefore often not worth the effort. Nevertheless, at Cardano, people just want to do philosophically, mathematically, and technically clean work. Consequently, their project could provide the crypto world with some interesting approaches regarding smart contract platforms going forward.

Figure 20: Ethereum vs. Cardano



Source: Bitgenste.

China Takes on Ethereum

“Bitcoin is at the same stage as the Internet in 1992–1993. At that time, it took UNIX command-line skills to send email. No way near ready for mainstream adoption.”

Andreas M. Antonopoulos

Another project, which wants to establish a platform for a future internet comes out of China. Formerly known as Antshares, the project changed its name to NEO in June 2017 and immediately caused a sensation among crypto investors. But soon the question arose among them: Can a blockchain project from China even be successful when the Chinese government took a firm stand against Bitcoin and ICOs in 2017?

With China and its iron measures, it is always complicated. If you look closely, you will see that China has not generally opposed blockchain technology; after all, in its five-year plan, China’s central bank has taken a stance for exploring the possibilities of blockchain technology. It is just that the Chinese government is solely interested in blockchain projects that are predictable and thus controllable. And this is exactly where NEO seems to be entering the picture, probably for good reason and quite intentionally.

It is the declared goal of those responsible behind NEO to focus on speed and regulatory compliance. With NEO, blockchain technology can be used to digitalize assets of all kinds and to automate administration and trade in order to create structures for a smart economy. **A digital identity solution seems to be indispensable for this, which is why the NEO Council – the body for the promotion of the NEO ecosystem – already supports a GDPR-compliant digital identity solution with PikcioChain.** If a blockchain platform is based on pseudo or even anonymity, it is of little interest for a

government – especially one like China – as well as for companies, since regulatory requirements can hardly be fulfilled this way.

At the same time, NEO is also focusing on solutions for the development of privacy and data protection. Through its partnership with OnChain, a company that promotes blockchain projects, NEO wants to enable companies to protect personal data. Founded by Da HongFei and Erik Zhang, who have also created NEO, OnChain is working with governments and corporations to create public and private blockchains that will eventually connect to the NEO ecosystem through OnChain’s decentralized network architecture (DNA).

Like Ethereum and other smart contract projects, NEO already has an open source community for developers and programmers called City of Zion. NEO also has an ICO platform that will allow payment solutions, distributed trading exchanges, and more.

The consensus mechanism of NEO is called Delegated Byzantine Fault Tolerance or dBTF. **Behind this term lies a governance model known to us from the traditional world: that of a representative democracy.** The NEO token

holders appoint delegates, so-called accountants, who ensure consensus and thus maintain the network. There are a total of seven accountants. Compared to Ethereum, the number of nodes validating the network is much smaller. In addition, the NEO accountants still have digital identities and real names – so they are visible to everyone, while the network nodes at Ethereum are anonymous. The fact that the accountants at NEO are known certainly makes sense with regard to the goals of this project. **In order to meet the regulatory requirements, the blockchain project must have this degree of transparency.**

The delegated accountant model can prevent transactions from having to be validated by all nodes in the network. This way, NEO can handle a higher number of transactions than Ethereum. In addition, NEO transactions are final. This means: Forks, i.e. splitting the blockchain into several chains, are impossible. If the accountants reach a consensus of 66 %, the transaction is not only included in the blockchain but is final and cannot be made obsolete by a fork. One more difference between Ethereum and NEO concerns the programming languages for the development of smart contracts. Ethereum requires Solidity – a programming language specially developed for Ethereum. NEO, on the other hand, supports many of the most popular programming languages. Therein, NEO sees the advantage of enabling traditional developers to program on the NEO blockchain without having to learn a new programming language.

Differences Are Evident

Of particular interest is the fact that NEO, like Ethereum, knows gas. While Ethereum also uses the ether token as gas, NEO has a separate gas token in addition to the NEO token.



The ICO market in Q2 2018 accounted for 45 % and 31 % of the traditional IPO market and venture capital market, respectively, despite regulatory uncertainty and volatility.

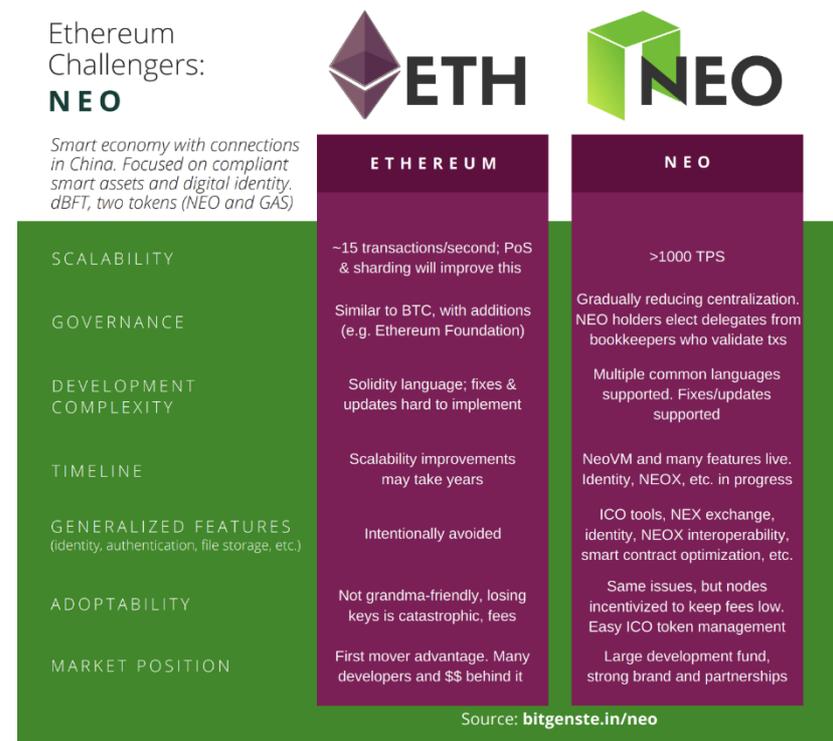
The NEO token makes it possible to be a “shareholder” in the NEO platform. As already mentioned, NEO token holders are entitled to appoint the accountants. The share-character of the NEO token is strengthened by the fact that the token is not divisible.



The GAS token, on the other hand, is used to pay for all operations such as transactions in the NEO network and thus functions as a sort of crypto fuel. Payment in the form of GAS tokens is made to accountants, but also to all NEO token holders. A personal NEO wallet is required to collect the GAS tokens.

This decoupling of NEO and GAS is particularly interesting because accounts do have the tendency to keep transaction fees low. The reason is the following: High transaction fees, which only benefit accountants, prevent operations from being carried out on the NEO blockchain. The fewer operations, the less reward NEO token holders receive. This leads them to vote for accountants, who in turn keep transaction fees low.

Figure 21: Ethereum vs. Neo



Source: Bitgenste.

These are the features that make NEO an interesting smart contract platform. From a macro point of view, however, **this platform differs from Ethereum in one fundamental aspect: NEO has apparently placed itself in the service of the Chinese government.** Consequently, NEO is by its very nature a planned and top-down orchestrated undertaking, which seems to have been driven primarily by the NEO Council in the interest of the Chinese officials. From NEO’s point of view, this strategy has an intact chance of success. Anyone who manages

to get popular in China itself and serves a market of 1.4 billion people can already book his project as a success.



Novogratz predicted that Bitcoin's lowest price in this bear market occurred on September 13th, 2018 at \$6,350. Unfortunately, Bitcoin was not able to stay above that limit and dropped past his lower bound prediction to \$6,200 on September 19th, 2018.

And even if one or more smart contract platforms were to establish themselves in the West, this would not mean the end of NEO. Tech giants from the USA such as Facebook or Amazon provide a good example: Although their dominance in the world outside of East Asia is growing, they have virtually no chance against the domestic platforms in China. **Why should this be any different in the area of smart contract platforms?**

Ethereum might also experience some influence by interest groups such as Consensys or the Ethereum Enterprise Alliance, its ecosystem nevertheless tries to generally uphold the philosophy of organic growth. In this sense, Ethereum is more of a platform emerging out of a spontaneous order. Because of these different intentions, the two projects are difficult to compare. While NEO strives for an advanced future that is adapted to the existing actors and circumstances,

Ethereum is working on a new future to which the current companies and states will have to orient themselves someday.

EOS – Ethereum’s Biggest Competitor?

“Bitcoin, having no counterparty risk and no reliance on any third-party, is uniquely suited to play the same role that gold played in the gold standard. It is a neutral money for an international system that does not give anyone country the ‘exorbitant privilege’ of issuing the global reserve currency.”

Saifedeam Ammous

In doing justice to the drama of the crypto world, some of these smart contract counterparty platforms bear the name “Ethereum-killer”. Probably the most prominent of these projects is EOS, also called “Ethereum on Steroids” by some. While Ethereum is an established blockchain project with a fully functional platform, EOS is still in its infancy. Following the largest ICO ever carried out on Ethereum, which raised a record \$4 billion, EOS held its Mainnet launch in June this year, switching from an ERC-20 token based on Ethereum to its own blockchain, the EOS blockchain.

Although EOS ultimately also enables the programming of smart contracts, there are some important differences. For example, Ethereum smart contracts are developed using JavaScript/Solidity. Smart contracts on the EOS blockchain, on the other hand, must be written in C++. Since this programming language is not as common and user-friendly, some programmers see this as an entry threshold that could put EOS at a disadvantage compared with other smart contract platforms. At the same time, EOS is supposed to feature the implementation of C/C++ libraries in the future, which would considerably expand the possibilities for developers.

Unlike Ethereum, EOS’s consensus mechanism is based on the so-called Delegated Proof of Stake or DPoS for short. This type of consensus finding was invented by EOS founder Dan Larimer. **As with NEO, DPoS entitles every EOS token holder to choose validators in a voting process. Analogous to the motto “one person, one vote” the voting process follows: one token, one vote.**

This also means that those who have more EOS tokens have a greater influence on the voting result.

The validators are called EOS block producers because they produce the EOS blocks in mutual agreement and check their correctness in order to maintain the

functionality of the blockchain. In total, EOS token holders will have to elect 21 block producers who are effectively capable of managing the blockchain and keeping the network secure and functional. They are rewarded for their work with new EOS tokens. If a block producer does not do its job well and, for example, validates invalid transactions, his status as a block producer can be revoked. The reconciliations are carried out approximately every two minutes. In principle, it is therefore possible to change validators every few minutes. In addition to the 21 active block producers, there are about one hundred other block producers in standby mode. If a block producer is deselected for whatever reason, one is being elected out of the reserve.

The idea of the EOS founders behind this structure is as follows: Because the task of actually processing and validating the transactions is delegated to only 21 block producers, the basic protocol and, thus, the actual blockchain itself should be able to be scaled to enable millions of transactions per second. In reality, the EOS project has so far completed a maximum of 3,097 transactions per second successfully. In an objective comparison, EOS has performed significantly better than Ethereum, even though the actual goal of millions of transactions has hardly been achieved. But EOS is not only capable of processing a larger number of transactions per second – the transaction speed is also higher. After just one second, the blockchain reaches finality via a newly added block.

Inflation as a Reward

Interestingly, no transaction fees are envisaged to make EOS work as they are regarded to be more of an obstacle by the EOS founders. In this context, they often refer to an example concerning Facebook: Facebook servers process over 50,000 likes per second and ultimately each of these likes represents a transaction. **If one had to pay a transaction fee each time on a blockchain-based social media platform, this would be detrimental to the customer experience.** While at Ethereum, the miners who validate transactions and add them to the blockchain are paid for this service through transaction fees, the validators within the EOS system are not remunerated with transaction fees for their verification work. To be fair, it has to be said: Ethereum is also working on second- or third-layer scaling solutions to mitigate the problems described above.

But how are the EOS block producers remunerated instead? They receive newly created EOS tokens through the EOS protocol. Each year, five percent more EOS tokens are produced. In concrete terms, this means that the EOS token stock is inflated by five percent a year. Of these five percent, the block producers each receive one percent as a reward for validating the transactions. The remaining four percent will be placed in a separate pool, from which proposals for improving and



Pomp
@APompliano

Folgen

Unpopular opinion: Institutions will come under pressure in next 5 years if they have 0% exposure to Bitcoin & digital assets. As fiduciaries, they need to invest capital in the best risk-adjusted opportunities.

Digital assets historically provide best returns per unit of risk.

Tweet übersetzen

09:57 · 16. Sep. 2018

199 Retweets 791 „Gefällt mir“-Angaben

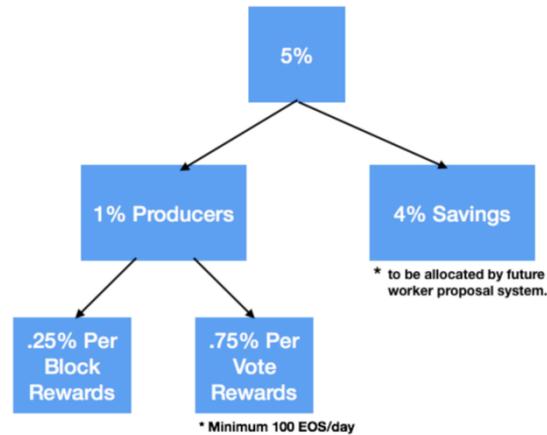


44 199 791

In a scenario-weighted analysis, if 8 % of the world's current investment in store of value assets was invested in Bitcoin, Bitcoin's price would be \$65,000 per coin over the next eight years.

further developing the EOS blockchain will be financed. EOS also aims to ensure that block producers cannot share their earnings with those from whom they receive their votes. This way, “buying of votes” should be prevented.

Figure 22: Distribution Of “EOS Inflation”



Source: Medium @bensig.

“From a cryptoeconomic point of view, transaction fees not only serve to provide incentives but also prevent malicious players from spamming the blockchain network with an unnecessarily large number of transactions.”

Crypto Research Report

From a cryptoeconomic point of view, transaction fees not only serve to provide incentives but also prevent malicious players from spamming the blockchain network with an unnecessarily large number of transactions. EOS, on the other hand, prevents such spam attacks by making blockchain bandwidth usage dependent on the number of EOS tokens. Anyone who owns one percent of all tokens is entitled to one percent of the entire bandwidth of the network. In order to increase the chances of a targeted network overload, the attacker must increase his possession of EOS tokens, which causes ever-increasing costs. Spam attacks are therefore not ruled out, but they are economically expensive.

Anyone who wants to develop a DApp (decentralized application) on Ethereum will, as it were, make use of the computing power of the Ethereum miners and pay for it with ether gas. EOS, on the other hand, is based on an ownership model: If you hold one-thousandth of the EOS network, you also have one-thousandth of the computing power combined on EOS Blockchain. This ownership model enables DApp developers to realistically estimate their hosting costs at any time.

Attacking Ethereum

EOS is also committed to revolutionizing the concept of crowdfunding once again. Today, the Ethereum platform can be used to collect funds directly via an ICO – also known as a token sale. One issues a token and in return receives Ether, Bitcoin, or other cryptocurrencies. It is inevitable that fraudsters, swindlers, and charlatans will also receive financial resources this way. It is the hope of EOS sympathizers that crypto projects will migrate away from Ethereum in the longer term and switch to EOS for crowdfunding. This was the case, for example, with Everipedia, a for-profit competitor of Wikipedia.

“2018 is also proving to be a record-breaking year for ICO funding, with total funding raised in the last 6 months already surpassing the total of 2017.”

Smith and Crown

The EOS ecosystem knows no ICOs or Token Sales, only the Airdrop. If a project wants to finance itself via the EOS blockchain, its EOS-based tokens are passed on to the EOS community free of charge via Airdrop. After the tokens of the project have been distributed via Airdrop, the market determines the value of the tokens according to the law of supply and demand. The team behind the project can then sell a percentage of its own tokens to raise money for the project.

However, it seems somewhat unclear how a token distributed over an Airdrop without capital can gain value in the first place and thus be accepted by the market.

At best, the venture capital fund created within the EOS ecosystem should come into play here. Behind this fund is the company Block.one, which conducted the ICO for the EOS token in 2017. The venture capital fund is intended to make strategic investments in various projects based on the EOS Blockchain. It is only natural that this venture capital fund should be used to invest in promising projects that also want to carry out an Airdrop via the EOS blockchain. Of course, the question then arises as to how strongly Block.one influences crowdfunding on EOS. After all, a certain pre-selection takes place through the venture capital fund, which is not the case with Ethereum. **The tradeoff is between allowing fraud on Ethereum or censoring innovation on EOS.**

What About Decentralization?

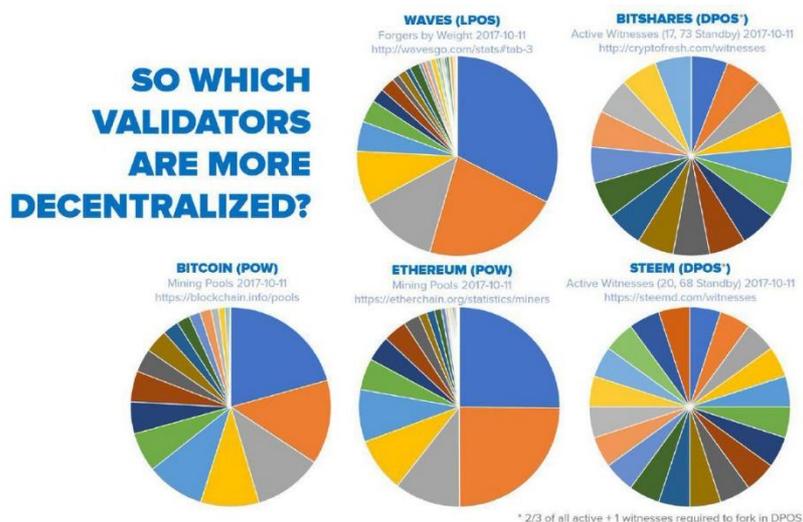
The decisive question crypto investors are asking themselves today: Who will prevail in the long term? Ethereum or EOS? Are there any clues? Investors, for example, are focusing on the most prominent people behind the two projects: The battle between Ethereum and EOS has thus also turned into a battle between Vitalik Buterin and Dan Larimer. Some Ethereum supporters refer to Buterin's allegedly astronomically high intelligence quotient, which would make him an even greater genius than Larimer. The opposite side meanwhile refers to the crypto projects BitShares and Steemit, which both originated from Larimer and would lead him to triumph. In the end, these comparisons are interesting, but they have little relevance for the future of the two smart contract projects.

More revealing are project-specific debates that were initiated by Vitalik Buterin and Dan Larimer, among others. In the theoretical debate, the question of decentralization ranks at the top of the list. In the case of the EOS blockchain, it is ultimately a comparatively small number of nodes that maintain the network. In a world like that of crypto, which is committed to the decentralization of social structures, a blockchain concept with only 21 block producers naturally arouses suspicion. Is EOS decentralized enough or do the 21 block producers not rather remind us of a cartel or an oligarchy? **Many honest crypto experts still consider it technically impossible to escape the blockchain trilemma, according to which there are inherent trade-offs between security, scalability, and decentralization, at the level of the basic protocol.**

On the EOS side, there are some exponents for whom decentralization is not an absolute value. Since decentralization is always associated with mathematical and economic costs, compromises must be made in this respect in order to achieve the

goal of mass scaling DApps. In their view, EOS is just as decentralized as the scaling intention requires. The fact that there are just 21 block producers can be traced back to Larimer’s previous experience with his other DPoS systems BitShares and Steemit. This number is therefore not engraved in stone or better written in code. In the light of new findings, it could also be changed, according to their arguments.

Figure 23: Decentralization of Different Validators



Source: Steemit @adamantine.

“Bitcoin has come down below its 200-day moving average, and that is important because the currency has been going up at 170 % percent per annum for six years...It’s come off 65 percent since its highs, and if you put 100 bucks in each of the four times it’s touched its 200-day moving average, you’d have a 285 percent return...it’s a screaming buy right now.”

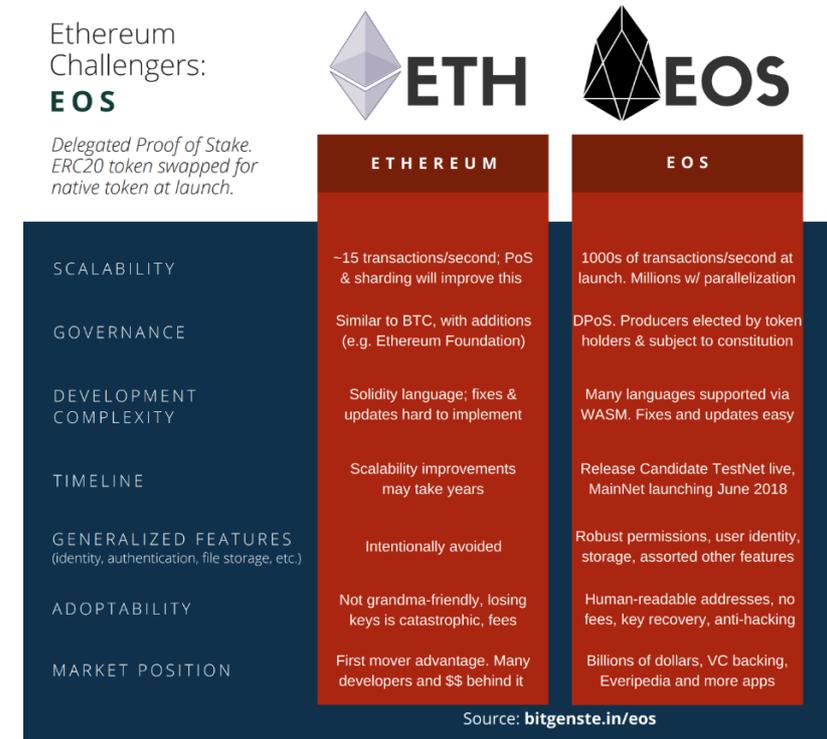
Dan Morehead, CEO of Pantera Capital

Other advocates of EOS do not consider the EOS blockchain to be less decentralized than Ethereum at all. **They point out, for example, that at Ethereum three parties account for more than 50 % of total hashing power.** If these three actors were to play together, the Ethereum blockchain could be successfully attacked and transactions could be spent twice. They also argue that Larimer’s earlier projects BitShares and Steemit have shown that DPoS systems are more decentralized than than proof of work used by Ethereum and Bitcoin because proof of work has an inherent tendency towards centralization due to economies of scale. Interestingly, it seems as if the EOS community generally consists more of people who prefer a certain amount of leeway to exert influence instead of a total inability to supervise. One can read the argument again and again that it can be considered sensible for “democratically” elected block producers to be able to intervene in the interest of the EOS community during emergencies such as a hack or bug.

A Fight That Is None?

Ethereum, EOS or another smart contract platform? The discussions about who will win the race are likely to continue for some time. Ethereum has by far the most developers, has many influential companies thanks to the Enterprise Ethereum Alliance, and is still by far the most widely used crowdfunding platform. EOS has become accustomed to its own blockchain by now and unites three of the most renowned crypto investors behind it, Mike Novogratz, Peter Thiel and Jihan Wu.

Figure 24: Ethereum vs. EOS



Source: Bitgenste.

“The biggest change the SEC needs to implement is to partner directly with cryptocurrency engineers to develop a new kind of regulation.”

Bryan Bishop, Bitcoin Core Developer

However, this fight is based on the assumption that only one smart contract platform is optimal. Most likely there is enough room for more than one winner because different applications require different blockchain infrastructures. The battle for supremacy among these platforms is reminiscent of the tug-of-war between the various operating systems in the early years of the computer and internet age. Just as several operating systems exist today with Mac, Windows, and Linux, no single winner is likely to emerge this time either. DApps can even run on multiple smart contract platforms simultaneously. Bancor, a blockchain protocol for the creation of smart tokens, for example, has already announced that it will use EOS as a foundation alongside Ethereum.

About Us

The Team



Mark Valek

Portfolio Management & Research



Demelza Hays

Research & Portfolio Management



Cristian Ababii

Research



Friederich Zapke

Research

The Report

As a sister report to the internationally acclaimed [In Gold We Trust report](#), the Crypto Research Report brings the same quality and rigor to understanding the cryptocurrency market. The Crypto Research Report is a report produced by Incrementum AG.

The Company

Incrementum AG is an owner-managed and fully licensed asset manager & wealth manager based in the Principality of Liechtenstein.

What makes us stand out in the asset management space? We evaluate all our investments not only from a global economic perspective but also by taking into account global monetary dynamics. This analysis produces what we consider a truly holistic view of the state of financial markets. We believe our profound understanding of monetary history, out-of-the-box reasoning and prudent research allows our clients to prosper in this challenging market environment.



Advisors

In order to provide accurate information on the most important and recent updates in the crypto space, a diverse team of thought-leaders, academics, and finance experts form our board of advisors. The mission of our board is to stimulate discussion on the most pressing risks and opportunities in the cryptocurrency market. Our advisors come from different countries, different education paths, and different careers. However, they all have one trait in common: their avid interest in the blockchain technology and cryptocurrencies. To stay up-to-date, the advisory board meets on a regular basis to discuss current affairs and the next quarter's outlook. All meeting minutes are posted as a transcript and released for free on our website at www.CryptoResearch.Report. Our board members include:

Max Tertinegg

Max Tertinegg is the CEO and co-founder of Coinfinity in Graz. Since 2014, Mr. Tertinegg has worked with merchants, investors, and regulators in Austria to build a cryptocurrency community. Currently, he is working on cryptocurrency storage solutions that are affordable and easy to use.



Oliver Völkel

Based in Vienna, Oliver Völkel is a partner at StadlerVölkel Attorneys at Law. He assists corporations and banks in all stages of capital market issuings and private placements (national and international). His focus is on new means of financing vehicles (initial coin offerings, initial token offerings) and drafting and negotiation of cross-border facility agreements and security-documentation, also in connection with cryptocurrencies and tokens. Mr. Völkel also advises on other cryptocurrency related banking matters, regulatory matters, capital markets regulation, general corporate, and corporate criminal matters.



Stefan Wieler

Stefan Wieler, CFA, CAIA, is the vice president of research and corporate sales at Goldmoney. For the past two years, Mr. Wieler has been the head of research at BBL commodities, which is an energy-focused hedge fund that trades WTI, Brent, RBOB, HO, Gasoil, and Natural Gas. Previously, he was a senior oil analyst for Goldman Sachs.



We sincerely want to thank the following friends for their outstanding support:

Our knowledgeable advisors including Max Tertinegg, Oliver Völkel, and Stefan Wieler, the generous authors who contributed to this report including Nikolaus Jilch, and Pascal Hügli. We are also grateful to the newest member of the Incrementum team, Cristian Ababii

Contact:

Incrementum AG
Im alten Riet 102
9494 – Schaan/Liechtenstein
www.incrementum.li
<http://www.cryptoresearch.report>
Email: crypto@incrementum.li

Disclaimer:

This publication is for information purposes only, and represents neither investment advice, nor an investment analysis or an invitation to buy or sell financial instruments. Specifically, the document does not serve as a substitute for individual investment or other advice. The statements contained in this publication are based on the knowledge as of the time of preparation and are subject to change at any time without further notice. The authors have exercised the greatest possible care in the selection of the information sources employed, however, they do not accept any responsibility (and neither does Incrementum AG) for the correctness, completeness or timeliness of the information, respectively the information sources, made available, as well as any liabilities or damages, irrespective of their nature, that may result there from (including consequential or indirect damages, loss of prospective profits or the accuracy of prepared forecasts).

Copyright: 2018 Incrementum AG. All rights reserved.