

Portfolio Manager's comments

It has been a grueling 11 months since we launched our crypto funds and we wished we could have done better for our investors. Bitcoin is quite used to 80% plus drawdowns (see table below) but with a medium/long term view our Investment thesis has not changed at all. We want to share this [Forbes](#) article that mimics our rationale, but we will need patience for the market to turn around. I strongly recommend you to watch [The End of the Beginning](#) presentation from Benedict Evans, Partner at Andreessen Horowitz's fund.

BITCOIN CRASHES
BITCOIN IS A GAME OF ACCUMULATION.

11/20/2018

DATE	HIGH	LOW	% DECREASE	# OF MONTHS TO NEW ATH	# OF YEARS TO NEW ATH
12/17/17 TO ???	\$19,900	\$4,035	-80%	???	???
11/29/13 TO 08/15/15	\$1,140	\$150	-87%	18 MONTHS	1.5 YEARS
04/10/13 TO 04/12/13	\$260	\$45	-83%	7 MONTHS	.60 YEARS
06/11/11 TO 11/21/11	\$35	\$2	-94%	19 MONTHS	1.6 YEARS

Bitcoin dominance remained on a tight range during November, started the month at 53.90%, reached a high of 54.47% and ended the month at 53.50%.

The first week of the month BCH had a pump in expectation of the new hard fork on November 15th. The heated fight between BCH ABC and BCH SV caused a big selloff in the market breaking the old support of BTC around the \$6,000 level which forced the market to test new lows for the year. The initial result post fork was negative, meaning that the sum of the 2 new coins was less than the original BCH. Towards the end of the month the sum of the 2 new coins recuperated to similar levels prior to the pump of the fork.

Volatility, which was coming down month after month, picked up after the important \$6,000 support, which we wrote in October, broke down. The [DOJ investigation](#) on Tether (which we also mentioned a few times in the past investment letters) added further fuel to the fire.

Bitcoins started the month at \$6,317 and traded between \$6,552 and \$3,585 to close the month at \$4,017, down 36.41% for the month, worst monthly drop in the last 7 years. Genesis Block Fund ended down 38.12% while BLP Crypto Assets FIM ended down 34.52%. We swapped a small position in FUN tokens into [WAX](#) tokens. WAX is a decentralized

exchange for virtual assets and one of the most active blockchains according to [Block'tivity](#). XRP suffered less than the other large coins, which hurt our relative position during the month.

At the last week of the month, SEC's Chairman Jay Clayton participated on the Consensus Invest conference in New York and made some [comments](#) on the crypto space. If you have time, listen to the [fireside chat](#) between Nassim Nicholas Taleb and Naval Ravikant at the Blockcon event.

Interesting announcements/comments:

- [Morgan Stanley](#) report says crypto is now an Institutional Asset Class
- [Amazon](#) has launched a new service for building blockchains.
- [AWS](#) teams up with Ethereum marketplace.
- [Fidelity's CEO](#), Abigail Johnson gives a rare interview.
- [Silvergate Bank](#), the main crypto bank files for an IPO.
- [ICE's Bakkt](#) delays Bitcoin futures launch from December to January.
- [Overstock's CEO](#) bets on blockchain and predicts a [cryptocurrency "Revolution"](#).
- [Ohio](#) starts accepting Bitcoin for tax bills.
- New York awards first-ever [BitLicense](#) to Bitcoin ATM Company.
- You can now send and receive Litecoin on [Facebook Messenger](#).
- How can we increase [voter turnout](#)? Bitcoin may be the answer.
- [Eric Schmidt, ex-Google CEO](#), said Ethereum has huge potential.
- [BBVA](#) puts \$150mm syndicated loan on the Ethereum Blockchain.
- [KPMG](#) issues lengthy report on Institutionalization of Cryptoassets.

Monthly estimated return

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec	YTD 2018	Since Inception
Genesis	-16.00%	-5.17%	-37.38%	57.20%	-20.19%	-20.59%	7.50%	-17.21%	-9.20%	-7.90%	-38.12%		-77.08%	-77.08%
BLP Crypto	-19.19%	-1.78%	-33.74%	61.16%	-14.11%	-17.57%	4.50%	-8.56%	-11.63%	-13.85%	-34.52%		-71.42%	-71.42%
Bitcoin	-27.80%	1.73%	-32.93%	32.51%	-18.90%	-14.55%	21.49%	-9.55%	-5.85%	-4.65%	-36.41%		-71.62%	
TOP10	-21.20%	-12.40%	-41.64%	53.12%	-20.90%	-19.41%	8.70%	-17.59%	-2.89%	-9.23%	-36.50%		-80.28%	
CDI	0.58%	0.46%	0.53%	0.52%	0.52%	0.52%	0.54%	0.57%	0.47%	0.54%	0.47%		5.87%	

THE BITCOIN AND TOP10 ESTIMATED RETURNS STATED ON THE TABLE ABOVE ARE MERELY ECONOMIC REFERENCES AND SHALL NOT BE CONSTRUCTED AS A PERFORMANCE TARGET TO BE ACHIEVED BY THE FUNDS NOR A PERFORMANCE PARAMETER APPLICABLE TO THEM.

Tech corner

51% Attacks explained:

Just mentioning them makes crypto traders freakout, and with good reason. A successful 51% attack against a cryptocurrency would, at best, take a big chunk out of that cryptocurrency's price. And, at worst, could destroy the cryptocurrency altogether.

Put simply, a 51% attack could occur when a malicious actor (or group of actors) controls

more than half the mining or hashing power on a blockchain. A 51% attack, also known as a “double-spend attack”, allows the attacker to rewrite history on a blockchain. In practical terms, it means the attacker can spend that particular cryptocurrency twice.

As an attacker, one would buy something with bitcoin, then initiate a 51% attack to create a new version of the blockchain – one that doesn’t include my transaction. Sounds pretty scary when you put it like that. That said, it is rather difficult to actually pull off a 51% attack on an established network. Bitcoin has never been hit by a 51% attack. Most large cryptocurrencies are safe, software bugs notwithstanding. Some smaller protocols have been attacked. If you can pull one off, you only become a time traveler. You do not have the ability to break the rules of the network, steal cryptocurrency from others, or create new currency out of thin air.

To understand more, let’s go over how we might perform a 51% attack (hypothetically, of course). To initiate a 51% attack, we need to “fork” the blockchain, which means splitting it in two. Then we need to convince the network that our malicious forked blockchain is the real one. But there is a problem: Cryptocurrencies need to have a way of knowing which blockchain is the ‘real’ one. Working this out is very simple – the longest one wins. By going with the longest blockchain on the network, the network can always be sure that the current blockchain is what the majority of the mining power wants. The longest blockchain being the *real* one has some other benefits too. For example, cryptocurrencies are often community driven. If the community does not like a particular update, miners won’t switch to the new software. If miners don’t switch to the new software, the old chain continues and remains the *real* blockchain for the network.

Essentially, to perform a 51% attack, we need to keep our fork secret. We can keep our fork either secret to one computer, or let it go between the nodes we control. Once we have our fork, we need to keep it up to date with the rest of the network. Essentially we create a mirror image of the original blockchain. You can think of our secret blockchain as a reset button. Once we have it, we can do something on the live blockchain and not copy it into our secret one. Then, we can mine a bit harder on our secret blockchain and have it be a little longer than the real one. That’s why we need 51% of the hashing power on the network. Nodes in a cryptocurrency network always follow the longest chain, as it usually indicates what the network at large wants to do. Once we release our secret blockchain to the network, all the nodes grab it and see it as the *real* one, as it is the longest. And once our blockchain is the *real* one, whatever we did before is undone. Often the thing undone in 51% attacks is a transaction. We can pay for something and then switch out the old blockchain with our secret one where the cryptocurrency is instead transferred to a different address. This is referred to as a double spend. The network will reject the original transaction, as it will occur after the new transaction from the perspective of the new blockchain.

The attack does not give us the power to do whatever we want. We must still follow the rules on the network. If we don’t follow the rules, our new blockchain is rejected by the network, and the attack fails. The requirement to following rules makes for an interesting combination of what we can and can’t do during the attack.

An Attacker can:

Cause double spends

Collect block rewards and cause other miners to have invalid blocks

Stop transactions for a time, or remove confirmations from being added to the blockchain

An Attacker can not:

Steal cryptocurrency from others

Create cryptocurrency out of nothing

Completely stop a transaction from occurring

Genesis Block Fund Ltd. Characteristics

Minimum Investment	\$100,000
Subscription	Monthly
Redemption	Monthly with 15 days pre-notice
Administration fee	2% p.a.
Performance fee	20% over 6M Libor with High Water Mark
Administrator	MG Stover
Auditor	Cohen & Co
Legal Counsel	Walkers Global and Freitas Leite
Contact	genesis.block@blpasset.com.br

BLP Crypto Assets FIM – Investimento no Exterior Characteristics

Minimum Investment	R\$100,000
Subscription	Monthly
Redemption	Monthly with 15 days pre-notice
Administration fee	2% p.a.
Performance fee	20% over CDI with High Water Mark (<i>come cotas</i>)
Administrator	Planner
Auditor	Crowe Horwath
Legal Counsel	Freitas Leite
Contact	contato@blpcrypto.com.br
Website	www.blpcrypto.com.br

IMPORTANT DISCLOSURE AND DISCLAIMER

THIS LETTER IS INTENDED ONLY FOR THE USE OF THE RECIPIENTS HEREOF, AND CONTAINS CONFIDENTIAL INFORMATION. THIS LETTER MAY NOT BE REPRODUCED, DISTRIBUTED OR PUBLISHED BY ANY SUCH RECIPIENT HEREOF FOR ANY PURPOSE, WITHOUT PRIOR WRITTEN AUTHORIZATION OF BLP GESTORA DE RECURSOS LTDA.

THIS LETTER IS FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED TO PROVIDE SPECIFIC INVESTMENT ADVICE FOR YOU AND SHOULD NOT BE RELIED UPON FOR THAT PURPOSE. YOU SHOULD NOT ACT OR RELY ON ANY INFORMATION PROVIDED HEREIN WITHOUT SEEKING THE ADVICE OF A PROFESSIONAL.

NO INFORMATION PROVIDED IN THIS DOCUMENT CONSTITUTES A SOLICITATION, OFFER OR RECOMMENDATION TO BUY OR SELL SHARES OF ANY INVESTMENT FUND TO BE MANAGED OR SPONSORED BY BLP GESTORA DE RECURSOS LTDA. OR ITS AFFILIATES NOR SHOULD IT BE CONSTRUED AS SUCH IN ANY JURISDICTION WHERE SUCH A SOLICITATION, OFFER OR RECOMMENDATION WOULD BE ILLEGAL.

THIS LETTER MAY CONTAIN ASSUMPTIONS, ESTIMATES, ILLUSTRATIONS AND INDICATIVE VALUES (THE "INFORMATION") WHICH MAY BE AMENDED AT ANYTIME THEREBY IMPACTING ON THE OUTCOME OF THE PRESENTED BUSINESS. ALTHOUGH COLLECTED FROM RELIABLE AND SELECTED SOURCES, BLP GESTORA DE RECURSOS LTDA. DOES NOT ENSURE THE ACCURACY, UPDATING, PRECISION, ADEQUACY OR VERACITY OF THE INFORMATION PROVIDED HEREIN. NO REPRESENTATION IS MADE THAT ANY TRANSACTION CAN BE AFFECTED AT THE VALUES PROVIDED HEREIN AND NEITHER BLP GESTORA DE RECURSOS LTDA. NOR ANY OF ITS DIRECTORS, OFFICERS OR EMPLOYEES ACCEPTS ANY LIABILITY WHATSOEVER FOR ANY DIRECT OR CONSEQUENTIAL LOSS ARISING FROM ANY USE OF ANY INFORMATION CONTAINED HEREIN.

THE PAST IS NOT A GUARANTEE FOR FUTURE PERFORMANCE. ANY PERFORMANCE FIGURES PRESENTED HEREIN ARE GROSS OF TAXES.

INVESTMENT FUNDS PERFORMANCE IS NOT GUARANTEED BY FUND ADMINISTRATORS OR FUND MANAGERS, BY *FUNDO GARANTIDOR DE CRÉDITO* – FGC OR BY ANY CAPITAL PROTECTION MECHANISM.

THE FUNDS REFERRED HEREIN HAVE LESS THAN TWELVE (12) MONTHS OF OPERATION. AN ANALYSIS OF AT LEAST 12 (TWELVE) MONTHS IS RECOMMENDED WHEN EVALUATING INVESTMENT FUNDS' PERFORMANCE.

INVESTORS MUST NOTE THAT AN INVESTMENT IN ANY INVESTMENT FUND TO BE MANAGED OR SPONSORED BY BLP GESTORA DE RECURSOS LTDA. WILL BE SUBJECT TO RISKS. THE VALUE OF INVESTMENTS MAY FALL AS WELL AS RISE AND INVESTORS MAY NOT GET BACK THE AMOUNTS INVESTED.

BEFORE MAKING AN INVESTMENT DECISION, PLEASE READ THE RELEVANT OFFERING DOCUMENTS, THE FUNDS' BYLAWS AND OTHER OFFERING MATERIALS IN THEIR ENTIRETY.