BLP ASSET MANAGEMENT

Genesis Block Fund Ltd.

BLP Crypto Assets FIM

BLP Criptoativos FIM

July 2019

Portfolio Manager's comments

Bitcoin dominance started the month at 61.30%, reached a high of 66.58% and ended the month at 65.07%.

We can summarize July with 3 simple words: vol, vol and vol, there was simply a lot of volatility in the markets, reaching 150% realized vol on a 1-month basis, check the skew here. We had eight 24-hour sessions with price swings of $1k plus with the highest one being a $1,548 swing on July16th. It was so volatile that LedgerX derivatives exchange sent out to their customers a survey if there would be demand for them to launch a $100,000 strike BTC option contract (Call & Put) with expiration in December 2020. Can you believe it, the market had a positive response and this Call was trading at $242 bid/$745 offer (still a wide bid/offer but hopefully liquidity will pick up to tighten the spread).

Bitcoin started the month at $10,817 and traded between $9,163 and $12,573 to close at $10,085 down 6.76% for the month. Genesis Block Fund ended down 13.25%. After 5 consecutive months of strong gains, July was our second down month for 2019. After reaching new 2019 highs the market become jittery after tweets from President Trump and comments from US Treasury secretary Steven Mnuchin. It is amazing how far Bitcoin has gotten in order to get the attention of some of the world's most important leaders. Love the re-tweet of Caitlin Long, "The #crypto genie can't be put back in the bottle…". Lawmakers in the US and other countries might try to make it more difficult, but they can't close it down, it is simply not possible as it is a worldwide decentralized system with no owner, headquarter or CEO. Nevertheless, these remarks made players take some profits and stay on the sidelines given the risk of what might come on the Regulation front with the upcoming G7 meetings coming up in late August in France. Another big event of the July was the US Senate Hearings about Libra with some tough opposition. Meltem Demirors from Coinshares also discussed Bitcoin in the US Congress Hearings and it actually seems that Congress drew a fine line between Libra and crypto, listen to a summary of her deposition here, funny that Congressman Davidson asked her about Shitcoins as well. Our small Tezos position was the standout performer up 36% during July while most other Alts got crushed again versus BTC. We reduced some more of our ETH underweight a bit too early and then reduced some more practically at the recent bottom (around 0.021 vs BTC) because when Alts rebound, we would expect ETH to lead the pack on a risk-adjusted basis. A lot of developments on the ETH 2.0 protocol (known as Serenity) are happening with some important improvements coming in the near term.

Fed Chairman Jerome Powell comments on cryptos during the Senate Banking Committee on July 11th also caught the media's attention, below his quote:

> *"I think things like that [the obsolescence of today's reserve currencies] are possible but we really [...] haven't seen widespread adoption. Bitcoin is a good example, almost no one uses it for payments [...] it's a speculative store of value like gold."*

We are glad that Bitcoin was compared to gold by such a prominent figure, hopefully it will someday surpass gold's market cap, currently at approximately $8 trillion vs BTC current $180 billion, that would be approximately 45x from today's prices, no wonder some called it Digital Gold, only time will tell.

We visited a number of companies and exchanges in Silicon Valley and we continue to see great growth, development in the ecosystem, and the products that companies are launching with improved UX. To give a bit of more color on one specific company called FOLD, today they have around 10 retailers (Amazon, Uber, Target, Whole Foods, Starbucks to name a few) accepting BTC as payment via credit using Gift Cards, by year-end they expect to have 500. You may ask why do retailers actually care to be involved in this space and here is the answer, when their customers make purchases with their credit cards the retailers suffer large charge-backs from canceled transactions as well as the hefty fees from the credit cards. When a purchase is made with BTC there is 0% charge back so a huge benefit to the retailer plus they attract a new customer base, the millennials which are active in this space. Also, doing this via LN (Lighting Network) transactions are instantaneous and with virtually 0 fees as well. On July 31st they rolled out rewards on BTC transactions with these retailers giving a further benefit to the end consumer.

Interesting announcements/comments:

- Fidelity's crypto arm has officially applied to operate in NY as a trust
- TD-Ameritrade backed ErisX won regulatory approval for a crypto futures product
- Binance will launch a futures trading product that will introduce 20x leverage
- Henry Kravis of KKR & Co. invests in cryptocurrency fund ParaFi Capital
- Docusign will continue to invest and implement blockchain technology
- Fidelity, Deloitte, and Amazon are backing a blockchain accelerator
- Litecoin partnered with the Miami Dolphins football team
- Brazil's Cyrela completes first blcokchain real estate sale
- Goldman Sachs CEO David Solomon said that the bank may look into developing a digital currency
- Dell, Newegg start accepting Bitcoin as payment
- Safeway shoppers can now get Bitcoin back as change at 894 US stores
- 83% of US investors would dip their toes into Bitcoin: New Report

Monthly estimated return

		Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec	YTD	Since Fund Inception
2018	Genesis	-16.0%	-5.2%	-37.4%	57.2%	-20.2%	-20.4%	7.5%	-17.2%	-9.2%	-7.9%	-38.2%	-3.7%	-77.9%	
2019	Genesis	-11.5%	17.5%	7.2%	20.5%	58.6%	12.4%	-13.2%						107.6%	-54.20%
2018	BLP Crypto Assets	-19.2%	-1.8%	-33.7%	61.2%	-14.1%	-17.6%	4.5%	-8.6%	-11.6%	-13.8%	-34.3%	-3.4%	-72.3%	
2019	BLP Crypto Assets	-15.7%	18.4%	10.6%	20.9%	52.8%	8.7%	-14.6%						89.4%	-47.49%
2018	BLP Criptoativos											-7.1%	-0.5%	-7.5%	
2019	BLP Criptoativos	-2.9%	4.1%	2.4%	4.1%	10.2%	1.6%	-2.8%						17.3%	8.46%
2018	BGCI	-15.8%	-10.7%	-43.5%	60.9%	-20.4%	-28.5%	13.7%	-21.7%	-0.2%	-12.2%	-36.8%	-1.7%	-80.9%	
2019	BGCI	-11.8%	15.5%	5.9%	13.4%	58.1%	17.2%	-24.2%						72.0%	-67.55%
2018	CDI	0.58%	0.46%	0.53%	0.52%	0.52%	0.52%	0.54%	0.57%	0.47%	0.54%	0.49%	0.49%	6.42%	
2019	CDI	0.54%	0.49%	0.47%	0.52%	0.54%	0.47%	0.57%						3.66%	10.32%

THE BLOOMBERG GALAXY CRYPTO INDEX (BGCI) ESTIMATED RETURNS STATED ON THE TABLE ABOVE ARE MERELY ECONOMIC REFERENCES AND SHALL NOT BE CONTRUCTED AS A PERFORMANCE TARGET TO BE ACHIEVED BY THE FUNDS NOR A PERFORMANCE PARAMETER APPLICABLE TO THEM (Note that the BGCI only prices during business days at 4pm Eastern time zone, which is different than our marking of 0:00 UTC of the last day of the month).

Tech corner

MimbleWimble

Few ideas within crypto have garnered as much attention as the MimbleWimble proposal. MimbleWimble is a novel protocol that works to improve privacy and scalability for its users. MimbleWimble takes the main architecture of Bitcoin, removes script and adds Confidential Transactions. MimbleWimble was created as an idea for improving scalability and privacy within Bitcoin. Due to the level of modification and tradeoffs involved, it's not currently politically or technologically feasible to include on Bitcoin proper. However, it may be possible to implement as a sidechain in the future. A sidechain is a separate blockchain that utilizes its own consensus, but not its own token. Instead it uses the bitcoin via a two-way peg.

Cryptography, while generally trusted, is usually only empirically correct. Most cryptography is not **proven** to be correct. Confidence is gained by lasting a long time without being broken by security researchers. Cryptography relies on assumptions that certain computations are difficult enough that they are practically impossible. Bitcoin depends on the discrete log problem and cryptographic hashing. The beauty of Bitcoin is that it involves only relatively simple cryptographic assumptions that have decades of research. Those primitives being the discrete log problem and cryptographic hashing. If the discrete log problem and hashing assumptions hold, then Bitcoin and MimbleWimble are secure. MimbleWimble combines these relatively simple cryptographic primitives in very sophisticated ways and the result is a system that is quite complex.

Discrete Log Problem

Cryptography is built on the idea that certain operations are easy to compute in one direction, and near impossible to compute in the other direction. The discrete log problem is an important example of this and is one of the most fundamental assumptions. It allows innovations like public key cryptography and signatures to work and be highly efficient.

The discrete log problem comes from discrete mathematics, a branch of math that deals with a limited set of values.

Like Bitcoin, MimbleWimble relies on elliptic curve cryptography (ECC). In ECC, math operations are defined over a range that is the set of points that satisfy a specifically chosen elliptic curve. Points can be added, subtracted and multiplied easily with standard computers. However, division is very difficult, and brute force is the only currently known way. The fact that multiplication is easy, but division is difficult is the property we need to build powerful cryptography. In Bitcoin and MimbleWimble, public keys are derived from private keys. The protocol chooses a point on the elliptic curve and typically labels it H or G, called a generator point. The private key is actually just a whole number chosen at random from a very large set (on the order of 2^{128} or greater). The generator point is multiplied by the chosen scalar to give the public key. The fact that this multiplication is considered extremely difficult to reverse is what allows these systems to operate. Reversing multiplication is also known as taking a logarithm, hence the name discrete log problem.

Cryptographic Hashing

A cryptographic hash function takes an arbitrarily large amount of data called the input and "digests" it into a fixed length string of data called a hash. For a hash function to be a cryptographic hash function, the output must be completely unpredictable and unrelated to the input. A small deviation in the input should result in a completely different hash. This unpredictability is what allows these functions to be secure. Most importantly, it should not be possible for an attacker to find an input that corresponds to a hash from another input. Bitcoin uses the RIPEMD-160 function to generate an address from a public key and SHA-256 for its proof-of-work function. In MimbleWimble, hashing is used to create outputs which in fact are cryptographic commitments. These commitments do not reveal a destination address on the chain but are only spendable when a user has possession of a private key. Both implementations of the MimbleWimble protocol use hashing as the proof-of-work consensus mechanism.

Homomorphic Encryption

Homomorphic encryption is a very cool technique that allows mathematic operations on encrypted numbers. It turns out multiplication is rather hard to get right in a homomorphic encryption scheme. Additively homomorphic meaning that addition and subtraction are preserved over encrypted values. The ability to check whether two separate summations result in equal values turns out to be tremendously powerful. As we'll see, MimbleWimble leans heavily on this additively homomorphic property to continuously verify that the sum of the inputs equals the sum of the outputs without needing to know the values themselves.

Confidential Transactions

Confidential Transactions (CT) uses a Pedersen Commitment scheme which replaces plaintext unspent transaction outputs (UTXOs) values with cryptographic commitments.

UTXOs represent individual piles of unspent money on the Bitcoin blockchain, an alternative approach to account balances. A cryptographic commitment binds the user to a chosen value without revealing what that value is. This means if and when the time comes for the user to reveal the chosen value, they cannot change their mind about the value as only the original value will satisfy the mathematics involved. The cool part is that only recipients of a CT need to learn what the value actually is. Pedersen commitments follow the additive homomorphic property and therefore allow us to check that the sum of the inputs equals the sum of the outputs within a transaction. Transactions can be validated without knowing the amount transacted—a big win for privacy. MimbleWimble uses the CTs scheme for bookkeeping on its blockchain. There are no observable values on MimbleWimble, only cryptographic commitments and range proofs. The homomorphic additive property ensures that the total money supply in the system can be continuously checked without having amounts be visible.

Cut Through

As just mentioned, MimbleWimble collapses all transactions within a block into a single block-wide transaction. The structure and transaction boundaries are removed. If a transaction is spending a very fresh (unconfirmed) input, then it is possible to completely remove the intermediary outputs without affecting the validity of the chain.

To conclude

The MimbleWimble protocol combines the above into a specification for a blockchain suitable for simple payments. It uses a modified version of CTs so that the balances are stored as cryptographic commitments rather than publicly visible amounts. Transaction structure is removed within each block, and the blocks are validated as a whole. Interestingly, the system does away with addresses, and instead outputs are actually commitments that can only be spent by people with knowledge of a particular parameter used to create the commitment. This parameter is known as a blinding factor and was originally included in CTs purely for privacy. In a clever modification, MimbleWimble uses the blinding factor as the private key that authorizes the spending of an output. These blinding factors are now fundamental to authentication and must not be shared.

MimbleWimble is a stripped down blockchain protocol suitable for simple payments. Since it removes addresses, senders and receivers must cooperate via a secure and private medium to create transactions before broadcasting a transaction to the network. This is significantly different from address-based systems where it is easy to receive money while offline and without a private communication channel.

Privacy

Amounts are obscured and it is difficult for third parties to decipher what is happening without extensive outside knowledge. The consolidation of transactions within a block helps privacy as well. However, if a spy node receives transactions individually, they can begin to compile a forensics database that associates inputs with outputs, possibly linking them to IP addresses. This information could later be used to possibly deanonymize parts of the chain later with learned information. Both implementations of MimbleWimble utilize a proposal called Dandelion a network routing proposal originally created for Bitcoin that creates plausible deniability. It passes transactions around via several hops and, in MimbleWimble, later aggregates them randomly before they are sent to miners for inclusion into a block. This will make it much harder for spy nodes to learn about what's happening. Transactions reliably obscures the amounts, but the transaction graph is only hidden as well as the user can find simultaneous transactions to combine theirs with.

Scalability

MimbleWimble does not feature significant improvements in tx/s over existing cryptocurrencies. CTs offers privacy benefits but requires significant resources. Combining individual transactions at the block level removes a small amount of bandwidth overhead. The biggest benefit is for new nodes joining the network. Recall that the chain is validated by continuously checking whether the total input and output sides of the equation balance. Because of this, it is possible to prune matching inputs and outputs and still check that the chain validates. This means that when new nodes want to join the network, they may be able to download just the relevant subset of historical inputs and outputs. Existing nodes are also able to reclaim a bit of disk space.

Grin vs Beam

Grin and Beam are two separate implementations of the MimbleWimble protocol. Beam is structured as a product of a company, while Grin is an open source community effort. Both projects have chosen a similar block time. The other main difference between the projects lies in their monetary policy. Some Grin supporters believe that its true purpose is to be a Bitcoin testnet. Beam has a hardcoded supply cap and a team incentivized with Beam tokens, so they have made choices more appropriate for an increasing token value.

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
Website	www.blpcrypto.com.br/en/

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
Administrator	Planner
Auditor	UHY Bendoraytes & Cia
Legal Counsel	Freitas Leite
Contact	contato@blpcrypto.com.br
Website	www.blpcrypto.com.br

BLP Criptoativos FIM – Investimento no Exterior Characteristics

Minimum Investment	R$1,000
Subscription	Monthly until the 27th day of the month
Redemption	Monthly with pre-notice before the 20th day of the month
Administration fee	1.50% p.a.
Performance fee	20% over CDI with High Water Mark
Administrator	Brasil Plural
Distributor	Genial Investimentos and Órama
Auditor	UHY Bendoraytes & Cia
Legal Counsel	Freitas Leite
Contact	contato@blpcrypto.com.br
Website	www.blpcrypto.com.br

IMPORTANT DISCLUSURE AND DISCLAIMER

THIS LETTER IS INTENDED ONLY FOR THE USE OF THE RECIPIENTS HEREOF, AND CONTAISN 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.

ANBIMA

A presente Instituição aderiu ao Código ANBIMA de Regulação e Melhores Práticas para os Fundos de Investimento.