Built by BloqLabs

Version 0.92 (last updated 12.19.2017)

Notes:

(1) This draft Owner's Manual is a work in progress and describes the design and structure of Metronome, a new type of cryptocurrency. Metronome and its underlying technology is still in development and this Owner's Manual will be updated throughout this process to reflect changes throughout the development cycle. While every measure has been taken to ensure the accuracy of the material, Bloq and its partners do not guarantee the accuracy or completeness of the material found in this Owner's Manual.

(2) Potential purchasers of Metronome and participants in the Metronome ecosystem should read this Owner's Manual, including the acknowledgements and disclaimers in Appendix [A], and should carefully consider any risks before making a purchase.

Table of contents

List of Tables and Figures

Motivations

In the development of Metronome, the Metronome authors aspire to take the lessons learned from previous cryptocurrencies and build one whose sole purpose is to be a long-term monetary system. With this in mind, the Metronome authors saw a novel opportunity in:

- Economically engineering something to last
- Bootstrapping decentralized financial products
- Ensuring equal access to token distribution
- Ensuring autonomous, self-governing contracts
- Taking cryptocurrency to the next level… literally

Economically engineering something to last

Some cryptocurrencies' mintage is either static or goes to zero over time – like Bitcoin and Litecoin – raising questions with economists about their long term viability. Other cryptocurrencies' token supply is hand-stitched together in pre-ICO deals that award certain parties a vast amount of supply, resulting in those parties controlling the majority of tokens. Some cryptocurrencies sell out to certain parties in a pre-sale, leaving very little to the general public. Metronome attempts to fix those problems with daily auctions that provide an on-going token supply mintage, ad infinitum. An on-going token supply mintage is theorized to provide sustainability versus other cryptocurrencies whose mintage either is or goes to zero. Metronome was built with longevity in mind.

Bootstrapping decentralized financial products

Bootstrapping decentralized systems into self-sustainability is a new thing, more art than science. Metronome is attempting to break new ground here. All proceeds from Metronome's auctions are sent to two separate smart contracts, which are designed, among other things, to repurchase MTN that owners may want to sell.

Ensuring equal access to token distribution

Cryptocurrency should be more egalitarian. More than just the 1% should have access to the world's next cryptocurrency. Distributing access to the cryptocurrency widely to the public reduces the number of stakeholders with large percentage stakes compared to the entire Metronome economy.

The descending price auction aims to distribute the token at a price purchasers deem fair. Other ICOs' token distribution is hand-engineered and often most is gone in the pre-sale before the public ever gets access.

Autonomous, self-governing contracts

Humans are fallible. Software and math are more predictable decades and further into the future. An algorithm is apolitical, and will not hyper-inflate or manipulate the currency at the discretion of humans. With autonomous, self-governing contracts there are no humans to affect the value of cryptocurrency at the human's discretion.

Taking cryptocurrency to the next level... literally

Every other cryptocurrency is tied to one blockchain network. LTC is only recorded on the Litecoin blockchain. BTC is only recorded on the Bitcoin blockchain. There are risks in being tied to just one railroad: management discord, supply uncertainty, etc. The market does not know that cross-blockchain are even possible, much less a need.

Metronome is the first cryptocurrency that is not tied to one blockchain forevermore. It is the first cryptocurrency that has the potential to be secured by the best blockchain networks, without permanent commitment to any one blockchain. This is a completely new concept, even in the innovative cryptocurrency space.

Executive Summary

Metronome ("Metronome" or "MTN") is a new cryptocurrency, engineered for institutional-level endurance. Metronome incorporates lessons learned from other cryptocurrencies like Bitcoin and Ethereum and is designed to be used for the next 100 years and beyond.

Metronome will be launched to the public with equal opportunity for access. Metronome will have zero founder privileges after launch and features a highly-predictable and reliable token supply.

The Metronome token supply:

- 10,000,000 initial MTN supply
  - 8,000,000 distributed via public descending price auction, as described in more detail below
  - 2,000,000 distributed to founders as founder retention (20%)
    - 25% available for use by authors at end of initial supply auction. Remaining 75% becomes available in 12 equal amounts over 12 calendar quarters
- New MTN minted daily
  - Daily minted MTN distributed via public descending price auction
  - Daily minted volume at the rate that is the greater of (i) 2,880 MTN per day, or (ii) an annual rate equal to 2.0000% of the then-outstanding supply per year

The three core design principles of Metronome are self-governance, reliability, and portability. They make Metronome unique and enduring.

- **Self-Governance**
  - No undue founder influence – governance by contract locked in at launch
  - 100% on-chain, decentralized, autonomous, auditable
  - Not subject to system changes based upon community discord
- **Reliability**
  - Predictable token supply and issuance, ad infinitum
  - Consistent addition of MTN
- **Portability**
  - Ability to import and export MTN across blockchains, exiting the current chain
  - Supports community development of new chain export and import functionalities
  - Enables a migration path to future blockchains as ledger technology matures, acting as key value proposition for the long-term viability of diverse digital currencies

In this document, we propose Metronome as a new cryptocurrency that uniquely satisfies the above criteria as the world's first self-governing, cross-blockchain cryptocurrency. We anticipate that the cryptocurrency and other token communities will devise their own uses for it.

To that end, and in the interest of self-governance, the Metronome authors will have no privileged interest in the Metronome token after the initial auction. Metronome will use a descending price auction for both its initial auction and Daily Supply Lot to give purchasers the opportunity to purchase at the price that they feel is fair.

Background

Blockchain technology

Blockchain is a new type of cryptographically-secure record-keeping technology, that has major implications in the finance sector. It is a distributed and—usually—decentralized ledger accounting for all units in its entire ecosystem. Public and complete ledgers across the entire network need to sync and agree with one another. These are called nodes. Nodes prevent “double spending” of the blockchain units and also validate transactions in blocks on the network.

Blocks are packaged transactional data, the hash of the previous block, a targeted hash, and a number called a nonce. Where nodes validate these blocks, miners write them to the blockchain by attempting to discover a nonce that makes a hash of all the data in the block meet its targeted hash. For their efforts and computational power, they are rewarded with newly-minted units of cryptocurrency.

The “chain” in blockchain refers to the unbroken line of mined blocks that miners write to the decentralized public ledger. Miners must incorporate the data from previous blocks to successfully discover new blocks, making a traceable history to the very beginning of the cryptocurrency.

Cryptocurrency

A cryptocurrency is a digital currency that uses cryptographic techniques to regulate the addition of new currency supply into the market. Often, its new issuance is a reward for successfully discovering blocks in the above-described mining process. The cryptography also verifies the validity of funds changing hands. Only the private keys held by the transacting users authorizes the transfer of funds between their wallets. Since these transactions are visible on the blockchain (see above) and the use of cryptographic keys ensures that the user intends to send funds and has sufficient funds for a transaction, the need for a third party to transfer and validate the transfer of funds between accounts is reduced. Encryption techniques replace the roles of clearinghouses and other intermediaries. Therefore, cryptocurrencies have the potential to provide greater predictability for monetary supply and issuance over fiat currencies.

Where the fiat currency issuance and supply can be managed extensively by their issuing authorities, cryptocurrencies can only behave as they are engineered to behave. This is why one can predict the monetary supply and mintage rate of a cryptocurrency with greater ease than predicting the monetary supply rate of a fiat currency.

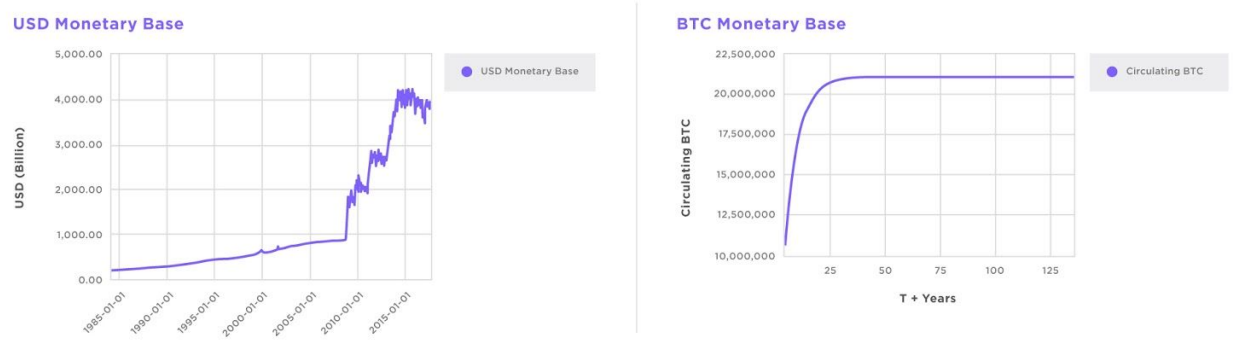

Figure 1: Comparison between USD monetary base and the popular cryptocurrency's, (bitcoin's) token base[1]

Since Bitcoin, other cryptocurrencies—both similar and dissimilar—have been created. These cryptocurrencies collectively make up an active and dynamic market.

Descending price auctions

Currently, most new cryptocurrencies offer their initial disbursements with traditional sales. These sales may include bonuses, early purchaser pricing, and other incentives to encourage purchasers to buy all of their supply. While these incentives can help, they do not guarantee a sell-out and can tend toward asymmetrical public access. If prices start low and increase as the supply drops, institutional investors and other wealthy parties, also known as whales, may have a disproportionate advantage to purchasing the majority of tokens.

Descending price auctions provide interesting opportunities for both initial offerings and continued issuance of cryptocurrencies. With a descending price auction, the price begins at a high initial price. As the auction proceeds, the price is reduced until all units are sold or a pre-set price floor is reached or the auction time limit is reached and the auction ends. Market price discovery is rapid and fair, as each purchaser pays what it thinks is fair at the time of purchase.[2]

[1] Sources: coinmarketcap, coinbase, blockchain.info, Federal Reserve Bank of St Louis
[2] http://onlinelibrary.wiley.com/doi/10.3982/TE502/pdf

Introducing Metronome

Metronome is a new cryptocurrency, engineered for self-governance and longevity, long term-reliability, and maximum portability. Designed for institution-level endurance, Metronome incorporates lessons learned from other cryptocurrencies that came before it, and is designed to be used for the next 100 years and beyond. We believe Metronome is the 1,000 year cryptocurrency.

Self-Governance

- No undue founder influence after launch – autonomously governed by smart contracts
- Resistant to individual or community discord, disagreement or misinterpretation
- Public access to all sale opportunities
- 100% on-chain, decentralized, auditable
- Pricing via descending price auction

Reliability

- Predictable token supply
- New MTN minted daily ad infinitum, at the rate that is the greater of (i) 2,880 MTN per day, or (ii) an annual rate equal to 2.0000% of the then-outstanding supply per year
- Stable, predictable minting of new token supply ad infinitum
- Architected for predictable pricing

Portability

- Cross-blockchain portability allows provable export to, and import from, different contracts or different chains
    - Further protects the cryptocurrency from governance issues and instability
- Community development of new chain export and import functionalities
- Enables a migration path to future blockchains as the ledger technology platform matures

Additional Features

- Payments settled in 15 to 30 seconds
- Mass pay – allowing multiple payments to be sent in one batch
- Subscriptions – allowing for recurring payments between users (see page 24)
- ERC20-[3] and ERC223-compliant[4]

[3] https://theethereum.wiki/w/index.php/ERC20_Token_Standard
[4] https://github.com/ethereum/EIPs/issues/223

How Metronome Works

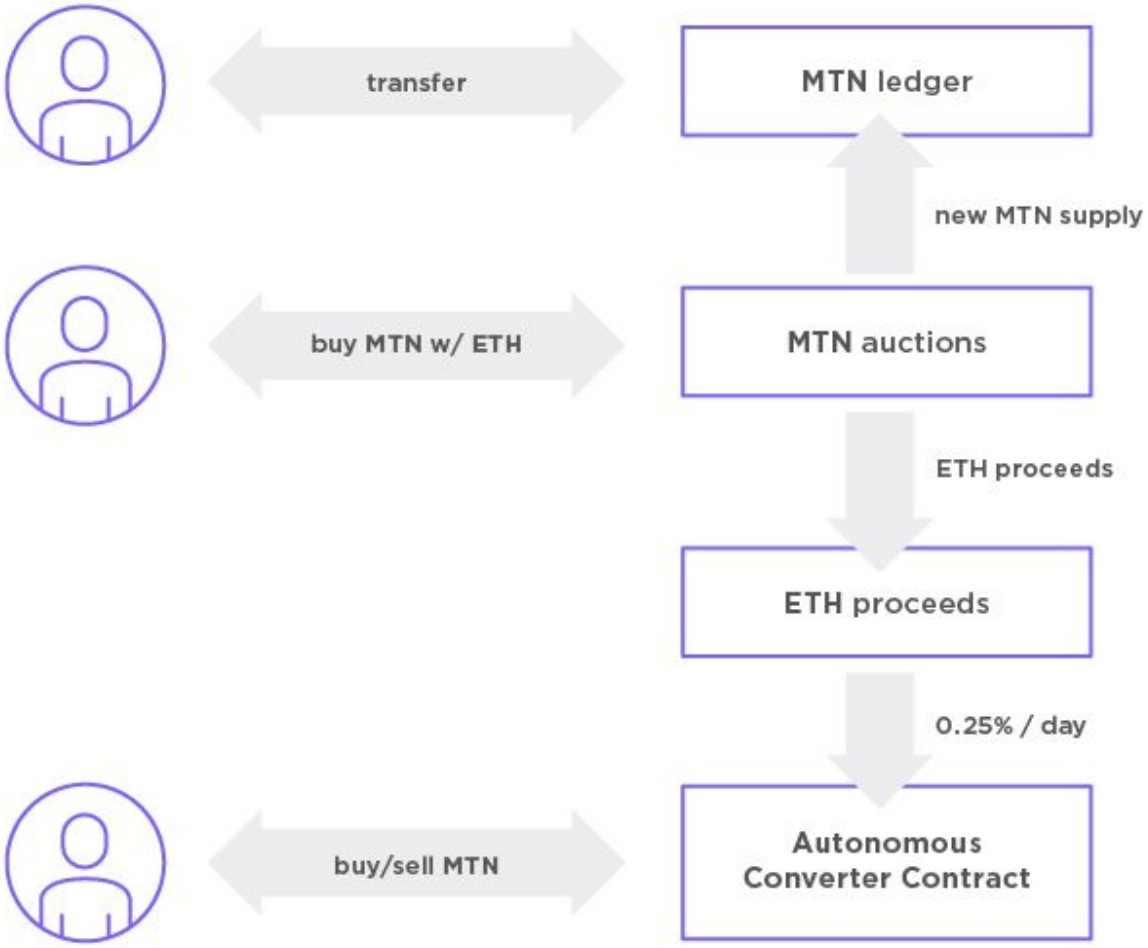

Figure 2: The flow of and interaction between Metronome contracts on the Ethereum blockchain

Launch

The initial Metronome auction and Daily Supply Lot will utilize a descending price auction (DPA), which is different than traditional auctions. In a descending price auction, the price per token starts at a maximum

price. The price slowly decreases until all offered supply is purchased or until the auction time limit is reached and the auction ends. Metronome employs DPAs to establish transparent and predictable pricing.[5]

Buyers purchase tokens in real time with immediate settlement during an auction; there is no need to wait until the end of the auction for tokens to be distributed. For example, some buyers may purchase tokens at 1.5 ETH per token, and immediately use these tokens to purchase goods and services or may sell these tokens via a cryptocurrency exchange or directly with a buyer. If unpurchased token supply remains in the auction after those purchases at 1.5 ETH price point, the auction continues, even as tokens are (in parallel) used or traded in various markets.

Although many supply purchase scenarios are possible, one is worth highlighting: a slow trickle followed by a sudden waterfall. In this scenario, purchasers purchase a small quantity of supply at higher prices. Once the pricing falls below some threshold, the remaining supply might be consumed rapidly.

Phase 1: Initial Supply Auction

- An initial token supply of 10,000,000 tokens is allocated.
- 20% of the initial token supply is retained by founders.
    - 25% available for use by authors at end of initial auction. Remaining 75% becomes available in 12 equal amounts over 12 calendar quarters.
- Descending price auction of 8,000,000 tokens (representing the total initial token supply of 10 million MTN, less the 20% token supply retained by the founders).
- Initial supply auction will last up to 7 days.
- Initial supply auction price is set at 2 ETH per MTN, with a floor price set at 0.0000033 ETH.
- In the initial supply auction, every 60 seconds, MTN auction price decreases by 0.0001984320568 ETH, linearly.
- The auction continues until the entire 8,000,000 token inventory is sold or until the auction ends twenty-four hours after it has begun.
- 100% from initial auction proceeds are stored in the Proceeds Contract

Phase 2: Operational currency

- Every 24 hours, new tokens are added to the Daily Supply Lot following the previous auction's close ad infinitum, at the rate that is the greater of (i) 2,880 MTN per day, or (ii) an annual rate equal to 2.0000% of the then-outstanding supply per year.

[5] Mishra, Debasis, and David C. Parkes. "Multi-Item Vickrey-Dutch Auctions." Games and Economic Behavior, vol. 66, no. 1, 2009, pp. 326–347., doi:10.1016/j.geb.2008.04.007.

- Every 24 hours, an auction is initiated, lasting no more than 24 hours (to avoid auction overlap).
    - Descending price auction of all tokens in the Daily Supply Lot begins at a maximum price of twice the previous auction closing price (*i.e.*, the price of the last token sold if the auction sold out, or the price when the auction timed out).
- Every 60 seconds, auction price decreases to 99% of previous price.
- Auction continues until (i) the entire Daily Supply Lot inventory is sold, or (ii) the end of the twenty-four hour period of the auction, whichever is earlier.
    - If the Daily Supply Lot inventory does not sell out entirely, any remaining MTN will be added to the next day's Daily Supply Lot
- Each purchaser is limited to purchases no more than 1,000 ETH per Daily Supply Lot purchase. However, this limit does not apply to the Initial Supply Auction.
- 100% of Daily Supply Lot proceeds goes to the Proceeds Contract.
- Every 24 hours, 0.25% of the total accumulated balance of the Proceeds Contract is sent to the Autonomous Converter Contract (described below), providing additional options for MTN owners to sell their MTN, if they so desire.

Cross-Blockchain Portability

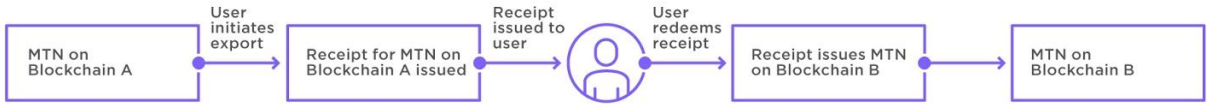

Figure 3: Demonstration of cross-blockchain portability

One of Metronome's unique features is its cross-chain portability, allowing users to move their MTN from one blockchain to another blockchain for any reason. If a user decides to move their MTN, the user must commit to a target blockchain, the destination that will receive the MTN. The user removes their MTN from the token supply on source blockchain A, receiving a "proof of exit" merkle receipt. Then user then provides this receipt to the Metronome contracts on target blockchain B.

The token supply of MTN on blockchain A is reduced, and the token supply on blockchain B is increased through this export/import process. The autonomous Daily Supply Lot is adjusted on a pro-rata basis on both blockchain A and blockchain B, to reflect the new distribution of MTN across blockchains A and B. For example, if 50% of all MTN exist on the blockchain A and 50% of all MTN exist on blockchain B, then the daily auctions on chain A shall mint 1,440 tokens/day, and the daily auctions on chain B shall mint 1,440 tokens/day.

Distributed, voluntary consensus governance

The ability to export Metronome from the initial 'genesis' chain launched by its authors, and import to follow-on upgrades released – by its authors or other parties – based on the voluntary consensus of the MTN holder community provides an opportunity for both immutable contracts, and a fair distributed mechanism to upgrade those contracts as the market matures.

If, for example, the market demand greatly exceeds supply, and the real-world price of the original MTN rises beyond what is practical for merchants, some could agree to fork the MTN supply with a new MTN contract on the same or different chains, by exporting funds they control to the new fork. These dynamics have the potential to remove risk from a- priori design of the token supply curves, as new immutable MTN contracts can have upgraded token supply curves for greater commercial use.

Similarly, if market supply starts to exceed demand for a sustained period of time and the price is falling, holders on different MTN forks may agree to "merge" from multiple export sources to a single import destination. By reducing the total economically active supply of MTN through this voluntary consensus mechanism, the token supply is reduced in the event of reduced demand, maintaining stable prices.

How forks and movement to new chains impact the MTN token supply curve and issuance is an open question to the Metronome community. We invite you to participate in defining, implementing, forking, and merging new MTN target contracts of your own, import MTN to new contracts, and see what happens.

Cryptocurrency market context to date

To better understand how Metronome fits into the cryptocurrency world, we need to take a high-level look at the overall landscape.

The landscape

Let's examine several well-known cryptocurrencies, the token supply allocation, issuance schedule, economic resilience and mutability resistance of that schedule.

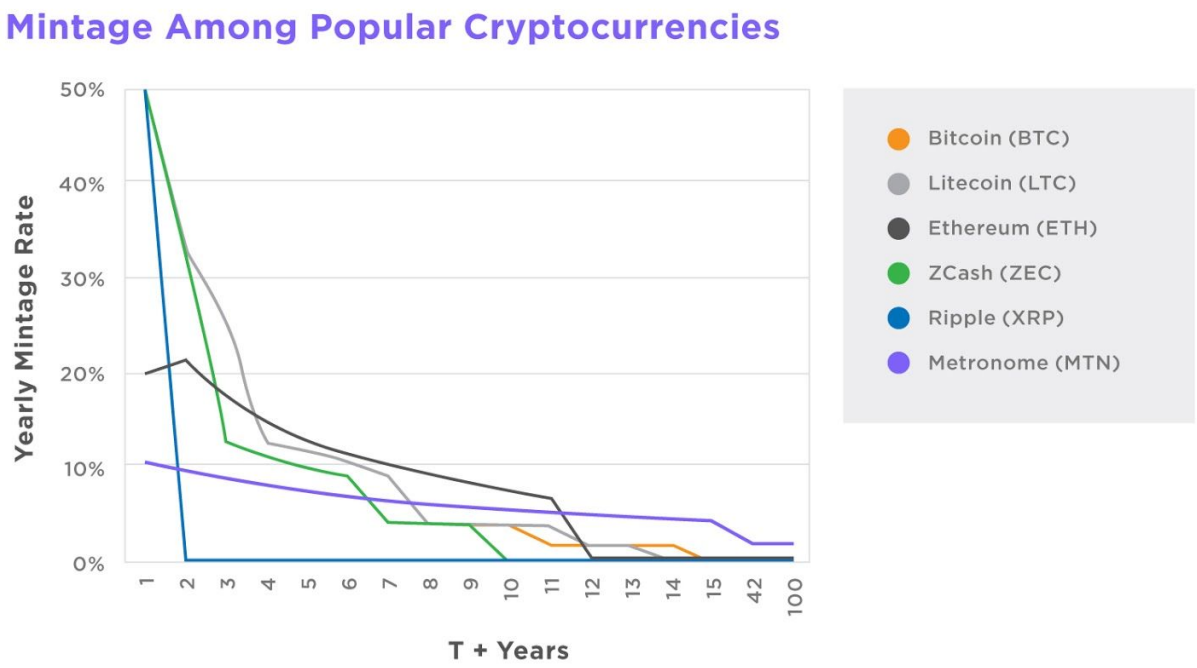

Figure 4: Mintage of popular cryptocurrencies today, note: ETH is a prediction[6]

Bitcoin ("Bitcoin" or "BTC") began on Jan 5, 2009, with public equal access to mining and participation in the ecosystem.[7] New currency supply is added with every block. Block period is targeted at 10 minutes/block every 2,016 blocks. Supply minted is 50 BTC per block, reduced by one-half every four years.

The Bitcoin community ethos places high value on the immutability of Bitcoin's 21 million currency supply limit, and the immutability of the issuance schedule. Once that limit is reached, mining for new BTC stops and transaction fees will, hopefully, provide incentive for miners. It is widely debated within the Bitcoin community whether transaction fees will suffice to keep Bitcoin funded and secure, when supply issuance

[6] Sources: coinmarketcap.com, coinbase, blockchain.info
[7] https://bitcoin.org/bitcoin.pdf

declines to these negligible levels.[8] [9] If Bitcoin were restarted from-scratch today, would its current, absolute deflationary nature be replaced by an enduring mild inflation feature to incent miners to secure the network indefinitely into the future? Perhaps. Low levels of inflation are desirable since it discourages hoarding of resources, *encouraging* investment and – in cryptocurrencies – continuing to secure the blockchain through mining.[10]

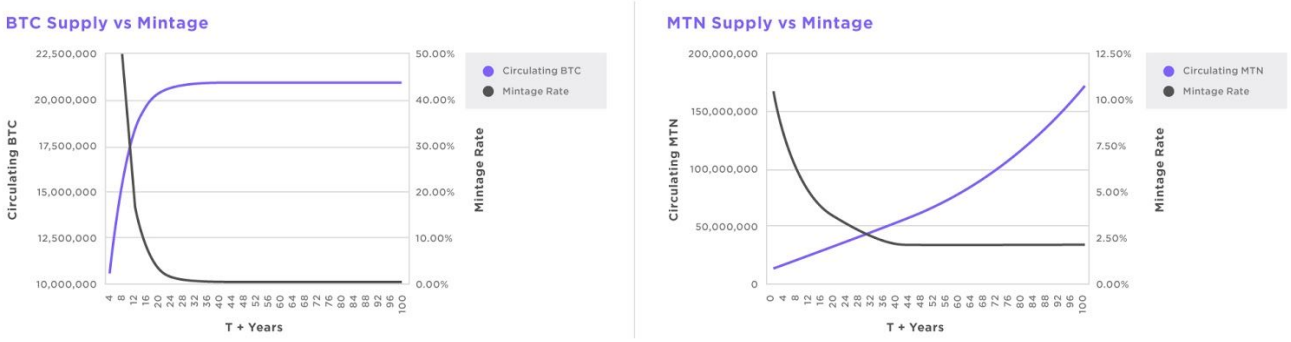

Figure 5: Comparison of Bitcoin and Metronome mintage and circulating supply[11]

The predictability and immutability of the issuance schedule is what users rely on today. Predictability gives market users the ability to plan years, possibly decades into the future. Immutability ensures that the currency supply will not be subject to the whims and frailties of humans. However, Bitcoin has various groups interested in influencing network governance, embroiling the community in contentious forks, uncertainty, and spectacle.

Litecoin ("Litecoin" of "LTC") is patterned after Bitcoin.[12] Blocks are targeted at 2.5 minutes/block. Supply minted is 50 LTC per block, reduced by one-half every four years. Litecoin is largely a photocopy of Bitcoin, from a currency issuances perspective: The issuance schedule is presumed immutable by most of the community. The new supply issuance declines over time, similar to Bitcoin. Litecoin's governance is similar to Bitcoin, but has some customary deference to the icons in its ecosystem.

Zcash ("Zcash" or "ZEC") behaves similarly. Proof-of-work mining is open to all. Block period is targeted at 2.5 minutes per block. Supply minted is 12.5 ZEC per block, reduced by one-half every four years. As a special case, the first 20,000 blocks have slow-start ramp-up to full 12.5 ZEC emission rate. Instead of a one-time compensation, the development team and support protocol development receive a 10% Founders' Reward of token supply is applied for all blocks up until the first halving, four years from its launch. After that point,

[8] https://bitcointalk.org/index.php?topic=108964.0
[9] Kroll, Joshua A, et al. "The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries." http://www.thebitcoin.fr/wp-content/uploads/2014/01/The-Economics-of-Bitcoin-Mining-or-Bitcoin-in-the-Presence-of-Adversaries.pdf
[10] https://www.brightscope.com/financial-planning/advice/article/8491/Asked-Answered-Zero-Inflation/
[11] Sources: coinmarketcap.com, coinbase, blockchain.info
[12] https://bitcointalk.org/index.php?topic=47417.0

100% of the minted token supply goes to miners.[13] The Zcash Foundation is intended to be the natural locus of voluntary governance of the ecosystem.[14]

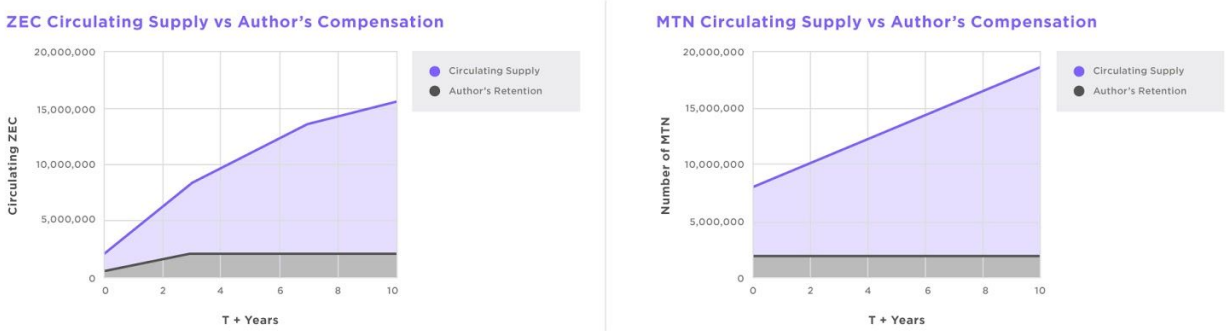

Figure 6: Comparison between ZEC and MTN author's retention vs circulating supply[15]

The Ethereum ("Ethereum" or "ETH") pre-sale raised over 60,000,000 ETH, which were pre-mined into the genesis block.[16] [17] New currency supply – 5 ETH – is added with every block. The new currency supply T+1Y increased 19.8%. T+2Y, 21.2%. T+3Y, 17.4%. Supply increase declines from there. The Ethereum currency issuance schedule is widely communicated to be in flux, and may change as the system evolves.[18] Ethereum is slated to change to proof of stake, which will change its issuance.[19] The issuance is therefore mutable, with the goal of resilience and sustainability. While any changes must be supported by the community and miners, there is still a lot of customary deference to and reliance upon a small founding team.

Ripple ("Ripple" or "XRP") has an available supply of 38 billion XRP.[20] The managing company, Ripple, Inc., has a further 61 billion XRP, of which Ripple Inc has placed 55 billion XRP in escrow.[21] This is centrally managed, with Ripple, Inc. controlling a large portion of the cryptocurrency's ecosystem. Ripple Inc. directly manages the issuance of supply into the market, and XRP is therefore highly mutable. Ripple Inc retains disproportionate governing power.

Metronome takes the lessons learned from these digital currencies and the result is a cryptocurrency designed for institutional-level endurance with issuance, governance, and reliability as the leading principles in its architecture. It is 100% autonomous with zero founder control, making it truly self-governed. Metronome is predictable and mints new MTN at a predictable rate, which makes it stable. It is also able to be imported and exported between blockchains for whatever reason the user sees fit, making it portable.

---

[13] https://z.cash/blog/founders-reward-transfers.html
[14] https://z.cash/blog/funding.html
[15] https://z.cash/blog/founders-reward-transfers.html
[16] https://github.com/ethereum/wiki/wiki/White-Paper
[17] https://blog.ethereum.org/2014/08/08/ether-sale-a-statistical-overview/
[18] https://twitter.com/VitalikButerin/status/879675471532654595
[19] https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
[20] https://coinmarketcap.com/currencies/ripple/
[21] https://ripple.com/insights/ripple-to-place-55-billion-xrp-in-escrow-to-ensure-certainty-into-total-xrp-supply/

	BTC[22]	LTC[23]	ETH[24]	XRP[25]	ZEC[26]	MTN
Reliability	BTC is famous for its contentious forks and deflationary nature. Token supply and issuance is stable, but finite.	Like BTC, LTC's issuance and token supply is subject to a hard cap, which may threaten chain stability	ETH's issuance and token supply model is in flux. It has forked in the past.	XRP has a stable supply. It is fully governed by Ripple Inc.	Similar to BTC, ZEC is subject to a hard cap which may call into question the security of the chain in the future.	**MTN issuance and supply will remain predictable ad infinitum as defined by its contracts. There is no uncertainty about supply or issuance.**
Self-Governance	BTC is self governed, but has many groups looking to exert undue influence.	LTC is self governed, but customary deference to its icons.	Changes to ETH need community support, but much reliance upon a small team.	XRP is not self governing. Ripple Inc retains sole power of governance over XRP.	The Zcash Foundation is natural locus of voluntary governance.	**MTN is entirely self governed through autonomous contracts.**
Portability	no	no	no	no	no	**yes**
Immutability	strong	strong	Mutable; Will change with PoS	weak	strong	**strong**
Issuance Model	50 BTC per 10 minutes. Decreases by ½ every 4 years.	50 LTC per 2.5 minutes. Decreases by ½ every 4 years.	5 ETH per 15 seconds.	Issued once, by Ripple Inc	12.5 per 2.5 minutes. Decreases by ½ every 4 years.	**Daily MTN auction sales at greater of (i) 2,880 MTN per day, or (ii) an annual rate equal to 2.0000% of the then-outstanding supply per year**
Supply limit	21 million	84 million	unknown	100 billion	21 million	**See Issuance Model above**
Settlement	10 minutes	2.5 minutes	15 seconds	5 seconds	2.5 minutes	**15 seconds**

[22] https://bitcoin.org/bitcoin.pdf
[23] https://bitcointalk.org/index.php?topic=47417.0
[24] https://github.com/ethereum/wiki/wiki/White-Paper
[25] https://ripple.com/insights/ripple-to-place-55-billion-xrp-in-escrow-to-ensure-certainty-into-total-xrp-supply/
[26] http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

time						
Mass Pay feature	yes	yes	no	no	yes	**yes**
Subscription feature	no	no	no	no	no	**yes**

Table 1: Comparison of important attributes between today's cryptocurrencies

Metronome contracts and technical aspects

Four autonomous smart contracts make up Metronome. The general flow is:

1. The first contract is the MTN token and ledger, interacting directly with the blockchain. This is how users settle peer-to- peer transactions, and it can be used as a distributed store of wealth.
2. The token contract is followed by the Auctions contract. A user purchases MTN through the Auctions contract. When a user makes a purchase from the Auctions contract, the contract mints the MTN for the user.
3. The Auctions contract t then sends the proceeds to the third contract, the Proceeds Contract. 100% of the proceeds from the Initial Supply Auction and each Daily Supply Lot are sent from the Auctions contract to the Proceeds contract.
4. Every 24 hours, the Proceeds Contract sends 0.25% of its contents to the fourth contract – the Autonomous Converter Contract – on a daily basis, providing it with available ETH. When a user sends ETH or MTN to the Autonomous Converter Contract, the contract returns MTN or ETH, respectively at the rate determined by the contract.

Since the ratio of tokens in the Autonomous Converter Contract determines their relative value, we expect arbitrage to keep pricing approximately accurate. If the contract has too few MTN (or ETH), that makes it expensive compared to its corresponding pair. A user who believes his or her MTN (or ETH) are not worth that much will tender his or her tokens in exchange for the other token. This can balance the contract's contents, correcting the relative price imbalance.

Metronome Proceeds and Autonomous Converter Contracts

The Proceeds Contract receives the proceeds from the Auctions contract and exports a portion to the Autonomous Converter Contract, providing the Autonomous Converter Contract with ETH supply for purchase and sale. One MTN will be in the Autonomous Converter Contract at the time it is initialized.

In the Initial Supply Auction and every subsequent Daily Supply Lot, 100% of the proceeds will go to the Proceeds Contract. None of the proceeds are ever distributed to Metronome authors. Each day, the Proceeds Contract will forward 0.25% of its total accumulated proceeds to the Autonomous Converter Contract. We expect this can smooth out the variance in daily auction volume, compared to just placing receipts in the Autonomous Converter Contract directly.

When selling ETH to the Autonomous Converter Contract, the amount of Metronome obtainable for a particular amount of ETH in the contract rises. If someone sells Metronome to buy ETH, they will get more ETH back, and if someone wants to use the Autonomous Converter Contract to buy Metronome, they will have to pay more ETH for it.

To the extent that the daily ETH selling in the Autonomous Converter Contract raises MTN value above what the market can support, we believe that arbitrage will capture the excess ETH. However, given that the predictability of Metronome is measured in decades-long timescales, we also expect the market to predict and price in the flow of ETH liquidity into the Autonomous Converter Contract.

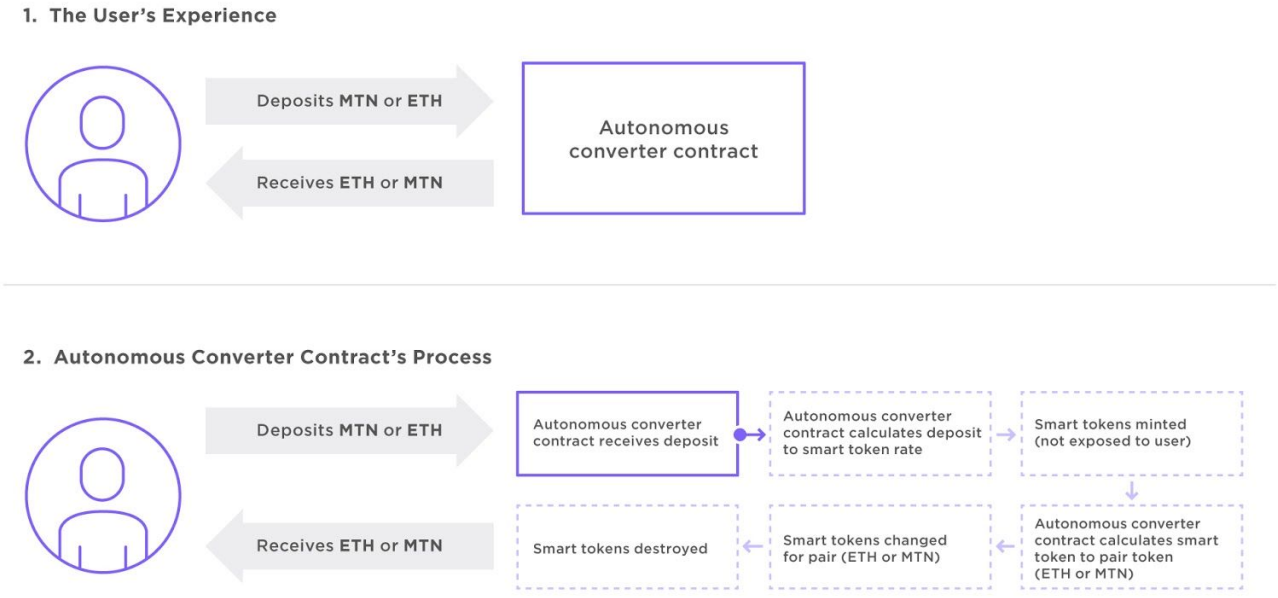

Figure 7: The user's experience interacting with the Autonomous Converter *Contract and the* Autonomous Converter Contract's *back-end process*

Economic prediction

While the Autonomous Converter Contract seeks to approach a market-determined price, the auction contract has a fixed pricing schedule each day. Consequently:

- When the auction's token price is higher than the Autonomous Converter Contract's, buyers would be expected to be less likely to buy tokens from the auction. They would be better off buying the cheaper tokens from the Autonomous Converter Contract.
- When the auction's token price is lower than the Autonomous Converter Contract's, anyone can make arbitrage profits by buying at auction and selling the tokens to the Autonomous Converter Contract. This would arbitrage out any ETH imbalance in the Autonomous Converter Contract. However, since everyone wants to do this, the auction would be expected to sell out before the price discrepancy becomes significant.

In sum, buyers in the auction would be expected to attempt to buy tokens at auction at a price very close to the current price in the Autonomous Converter Contract, and each day's later buyers will be able to profit

from its earlier buyers, essentially getting paid for the risk that they will not be able to buy at all in the auction.

Once the daily auction sells out, excess demand could be met by trades on the Autonomous Converter Contract, possibly increasing the token price. We expect that each auction would sell out, because the descending price will eventually decay below market price.

The math

When the user transacts with the Autonomous Converter Contract, there is always price slippage, since users are throwing off the ratio between token supplies. Formulas determine all the prices, such that whether the user makes lots of tiny purchases or one big purchase, everything comes out the same.[27]

There are two formulas: one calculates how many smart tokens a user gets for MTN or ETH, the other determines how much MTN or ETH a user gets for smart tokens. Smart tokens are never exposed to the user.

Building accurate and efficient "elementary functions" is a serious engineering task. New implementations are necessary since Ethereum has only 256-bit integers.

By restricting the Autonomous Converter Contract to two cryptocurrencies – MTN and ETH – at reserve ratio 0.5, the math is simplified and only a square root is needed, which is simple to implement and reasonably efficient to run.

The math is as follows:

R = Reserve Token Balance

S = Smart Token Supply

F = Constant Reserve Ratio

T = Smart tokens received in exchange for reserve tokens E

E = Reserve tokens received in exchange for smart tokens T

The original formulas are:[28]

$$T = S((1 + \frac{E}{R})^{F} - 1)$$

$$E = R(1 - (1 - \frac{T}{S})^{\frac{1}{F}})$$

In our case, because F is set to 0.5, the formula can make do with fixed-point multiplication, division, and square root:

$$T = S(\sqrt{1 + \frac{E}{R}}) - 1)$$

$$E = R(1 - (1 - \frac{T}{S})^{2})$$

A worked example

[27] https://drive.google.com/file/d/0B3HPNP-GDn7aRkVaV3dkVl9NS2M/view
[28] https://www.bancor.network/static/bancor_protocol_whitepaper_en.pdf

Let's say the Autonomous Converter Contract has 1000 ETH and 2000 MTN, and there are 10000 smart tokens. The Autonomous Converter Contract's price for MTN is 0.50 ETH. A user believes this is on the high side and wishes to trade 100 MTN for ETH. At the current nominal price this would return 50 ETH, but actually the user will get less due to price slippage.

Step one: Trade 100 MTN for smart tokens.

$$T = S(\sqrt{1 + \frac{E}{R}} - 1)$$

$$T = 10000(\sqrt{1 + \frac{100}{2000}} - 1) = 10000(\sqrt{1.05} - 1) = 10000(1.0247 - 1) = 10000(0.0247) = 247$$

The user receives 247 newly-minted smart tokens. The total supply of smart tokens is now 10247. The total supply of MTN held in the Autonomous Converter Contract is now 2100.

Step two: Convert 247 smart tokens for ETH, this is fulfilled automatically by the contract, the user is never exposed to the smart tokens.

Assume that 1000 ETH so is the reserve supply for the formula:

$$E = R(1 - (1 - \frac{T}{S})^2)$$

$$E = 1000(1 - (1 - \frac{247}{10247})^2) = 1000(1 - (1 - 0.0241)^2) = 1000(1 - .976^2) = 1000(1 - 0.953) = 1000(0.047) = 47$$

The user receives 47 ETH for their 100 MTN.

The contract now contains 953 ETH and 2100 MTN, or 0.45 ETH per MTN. By selling some MTN, the user has lowered the price of MTN in the Autonomous Converter Contract compared to ETH. He or she receives ETH approximately midway between the initial price and final price.

The 247 smart tokens are destroyed when they are traded in, lowering the smart token supply back to 10000.

Transaction ordering mitigation

The user can predict the outcome of his or her trade, provided no other transactions are executed ahead of the user's. There is no way to guarantee this; in fact, other parties could see his or her transaction in transit, and issue their own transaction ordering. Miners in particular could do this very effectively.

To mitigate against transaction ordering, we require the user to specify a minimum return. If he or she does not get at least that much back from their trade, his or her transaction rolls back; he or she pays only a small transaction fee to cover the computational cost of executing the transaction.

Token Supply Economics

Theory

- Predictability of supply enables market participants to accurately gauge supply 12 months, 5 years, 50 years into the future
- Pricing is determined via descending price auction

Supply

- Initial supply: 10,000,000 tokens, via descending price auction
- Supply after initial supply: an annual supply that is the greater of (i) 2,880 MTN per day, or (ii) 2.0000% of the then-outstanding supply per year
- Auction settles in near-real-time
    - Can sell available tokens immediately after purchase
        - No need to wait until end of auction to transfer
    - Economists say this gets the best price for the auction, since everyone pays their price limit[29]

Supply schedule

Time	Circulating MTN	Mintage Rate	Daily Mintage
T + 1 year	11,051,200	10.512%	2,880
T + 2 years	12,102,400	9.512%	2,880
T + 3 years	13,153,600	8.686%	2,880
T + 5 years	15,258,880	7.399%	2,880
T + 10 years	20,517,760	5.400%	2,880
T + 50 years	63,499,700	2.000%	3,411
T + 70 years	942,382,561	2.000%	5,070

Table 2: Supply Schedule

[29] http://onlinelibrary.wiley.com/doi/10.3982/TE502/pdf

Autonomous Proceeds Provider

- Consists of the Metronome Proceeds Contract and the Autonomous Converter Contracts
- 100% of Initial Supply Auction and Daily Supply Lot proceeds are sent to the Proceeds Contract.
- The Proceeds Contract sends 0.25% of its daily balance to the Autonomous Converter Contract, providing it with MTN supply (see Figure 2).
- Users can change their MTN for ETH and vice versa through the Autonomous Converter Contract (see Figure 7).

API Reference

Metronome Core

Token API

The token API used to query and transfer MTN tokens is the familiar ERC20 token standard.[30] Metronome also incorporates desirable aspects of the ERC223 standard,[31] along with some custom ERC2-related functions.

Standard ERC20

const name	Metronome
const symbol	MTN
const decimals	8
function totalSupply	ERC20-compliant; refer to ERC20 standard.
function balanceOf	ERC20-compliant; refer to ERC20 standard.
function transfer	ERC20-compliant; refer to ERC20 standard.
function transferFrom	ERC20-compliant; refer to ERC20 standard.
function approve	ERC20-compliant; refer to ERC20 standard.
function allowance	ERC20-compliant; refer to ERC20 standard.
event Transfer	ERC20-compliant; refer to ERC20 standard.
event Approval	ERC20-compliant; refer to ERC20 standard.

ERC223

transfer(address _to, uint _value, string _fallback, bytes _data) returns (bool ok)	_fallback is the name of the function being called. _data is the encoded parameters for that function
function onTokenReceived(address _from, uint _value, bytes _data) returns (bool)	This is the function that ERC223 tokens are expected to call, when transferring to the contract; it's the equivalent of the fallback function.

[30] https://theethereum.wiki/w/index.php/ERC20_Token_Standard
[31] https://github.com/ethereum/EIPs/issues/223

Custom ERC20-related functions

Function approveMore(address _spender, uint _value) returns (bool)approveLess(address _spender, uint _value) returns (bool)	These are safer versions of approve. They are not standard, but can be used by users who want to avoid the chance of a well-known race attack against the standard version when updating values.
Function multiTransfer(uint[] bits)	Allows multiple transfers in a single transaction. Each uint in the bits array represents a transfer; the leftmost 160 bits are the address, and 96 bits to the right are the amount.

Merkles

These functions are not intended for manual use, but there is some thought that they could be the foundation for interesting UI features.

Function setRoot(bytes32 root)	Sets the merkle root associated with msg.sender
Function rootsMatch(address a, address b) constant returns (bool)	Returns true if the two addresses have matching roots.

Subscriptions

These functions are part of a unique Metronome feature: subscriptions on the blockchain. Users are able to facilitate relationships and recurring payments between other users and institutions via subscriptions. The user subscribes by authorizing them to withdraw a weekly payment. The authorized group or individual then is able to move the payment from the user's account to any account they see fit. The user is able to cancel subscriptions if and when necessary.

This addresses an issue that other cryptocurrencies have struggled with in the past. Paying for subscribership based material is either not possible or onerous with many popular cryptocurrencies. The Metronome subscription feature fixes that.

function subscribe(uint _startTime, uint _payPerWeek, address _recipient)	Subscribe to someone, i.e. authorize them to withdraw weekly payment _startTime is when the subscription will start _payPerWeek is the tokens payable per week including decimals _recipient is who gets to withdraw the tokens

function cancelSubscription(address _recipient)	Cancel the subscription _recipient is who are you unsubscribing from
function getSubscription(address _subscriber, address _subscribedTo)	Get subscription info _subscriber pays _subscribedTo is recipient of subscription startTime is when the subscription started payPerWeek is how much can recipient withdraw each week lastWithdrawTime is when the recipient last withdrew
function subWithdraw(address _from)	Withdraw funds from someone who has subscribed to you, returns success _from is your subscriber
function multiSubWithdraw(uint[] bits)	Withdraw funds from a bunch of subscribers at once. Each uint in bits holds just an address.

Auction API

Function () payable	Standard fallback function; send ETH, receive MTN tokens immediately
function whatWouldPurchaseDo(uint _eth, uint _t) constant returns (uint weiPerToken, uint tokens, uint refund, uint numMinutes)	Tells the user what the results would be, of a purchase at time _t _eth is the amount of ETH to be sent _t is the timestamp of the prospective auction purchase weiPerToken is the resulting price tokens is the number of tokens that would be returned refund is the ETH refund the user would get (if exceeding daily limit) numMinutes is the number of minutes between this prospective purchase and last one

Metronome Autonomous Converter Contract

Autonomous Converter **Contract API**

changeEthToMtn(minReturn) payable returns (uint mtnAmount)	Change ETH to MTN. Throw if the returned MTN would be less than minReturn Return the amount of MTN
changeMtnToEth(amount, minReturn) returns (uint ethAmount)	Change MTN to ETH. Throw if the returned ETH would be less than minReturn Return the amount of ETH
ifChangeEthToMtn(uint _ethAmount) constant returns (uint _mtnAmount)	Return how much MTN the user would get for the given _ethAmount.
ifChangeMtnToEth(uint _mtnAmount) constant returns (uint ethAmount)	Return how much ETH the user would get for the given _mtnAmount

Glossary of Contract Terms

- **Autonomous Converter Contract** The smart contract, allowing people to trade MTN with ETH or ETH to MTN.
- **Autonomous Proceeds Provider** The Metronome Proceeds Contract and Autonomous Converter Contract.

- **Constants** Holds a few common constants like DECIMALS.
- **Daily Supply Lot** The descending price auction that adds newly minted MTN into the ecosystem daily.
- **EVM** Stands for Ethereum Virtual Machine.[32]
- **Fixed_Math** Implements fixed-point arithmetic, including add, subtract, multiply, divide, square, square root. Will include overflow protections. For binary functions it assumes that both inputs have the same number of decimal places.
- **Formula** Implements the core Bancor-style formula, using the fixed math functions. Formula is stateless, all the variables are passed in as parameters.
- **Metronome** The main auctions contract.
- **Migrations** Part of Truffle's migrations capability.
- **ReserveToken** Implements MTN. Gives the Autonomous Converter Contract the right to move tokens around (in response to trading events).
- **Proceeds Contract** Accepts ETH from Metronome, forwards 0.25% of its balance to the Autonomous Converter Contract every 24 hours.
- **Smart Token** The token issued by Autonomous Converter Contract that acts as an intermediary when changing between MTN and ETH (and vice versa) via the Autonomous Converter Contract. This process is automated and is not exposed to the user.
- **Token** The MTN token purchased by purchasers.

[32] http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

APPENDIX A

[Coming Soon]