Microtick Guide

August 2019

Overview

Microtick: Behind the Bits

Blockchain Design
- What Makes Microtick Decentralized?
  - The Role of Validators
- Why Not Ethereum or EOS?
- Microtick as a Cosmos Hub
  - Tendermint Consensus: Understanding the Tradeoffs

Overview

Since the dawn of human commerce, dating back to at least the time of the ancient Egyptians and Mesopotamians, price discovery has played an essential role in bringing buyers and sellers together. This process remains just as crucial in modern times, where price information propagates to interested parties at the speed of light. From stock exchanges to ecommerce marketplaces, the resulting improvements in market efficiencies and reductions in information asymmetries have revolutionized how trade is conducted.

However, the age of instant information has also demonstrated the need for a new type of price discovery mechanism: one which is simultaneously both global (as opposed to being siloed in regional price nexuses) and decentralized (meaning no single party or entity determines these figures.) While most marketplaces and exchanges rely on tried-and-true price discovery methods – for instance, the bid/ask order book – to date, there is no method which is both global *and* decentralized.

The advent of blockchain technology has made this type of mechanism possible. Additionally, this technological development has also led to an entirely new question: *how can information about the real world be channeled into blockchain platforms?* While a multitude of "price oracles" have risen to meet this need, they lack the necessary degree of trustlessness that makes decentralization such a potent force.

"Microtick," herein described, simultaneously addresses both the price discovery and oracle problems. In the process, it empowers three distinct groups – consumers of data, market makers, and traders – with information and abilities previously unavailable. These include:

- Decoupling price discovery from trading
- Eliminating front-running based on colocation with regional prices nexuses
- Providing price discovery for low-liquidity assets (something that isn't readily possible with bid/ask order books, which may have very large spreads)
- Achieving value discovery for nearly any condition that a.) exists in the real-world, and b.) can be expressed as a price
- Speculating on leveraged positions within very short timeframes
- Hedging positions on very short timeframes
- Generating and propagating price data for use in a DApp context

It's not hyperbole to describe Microtick as a truly novel technology; it rests on a foundation of game theory, economic incentivization, and blockchain technology that has not previously been combined in this fashion. Properly implemented, it could represent a meaningful next step in the long history of price discovery: an evolutionary leap forward to address humanity's growing thirst for global, trustless pricing data about *everything*.

This guide provides a comprehensive view of Microtick. We'll explain how it works, describe its blockchain architecture, zero in on crucial design decisions, explore its potential as a sustainable business model and define risks and challenges.

Microtick: Behind the Bits

As described above, Microtick is a new way of achieving price discovery for all manner of assets. It's also a new type of oracle: a way to feed knowledge about real-world conditions into blockchains without users of that data needing to trust a third party.

There are two major differences between Microtick and traditional exchanges:

1.) There is no order book or spread.

Instead, there is only one price that's derived from the interplay between market makers and traders. The term we use for this price is "global consensus."

On traditional order book platforms, market makers sit between the bid and ask and derive profits from the difference. This is not the case with Microtick, where the role of market makers is to provide their own assertions about the price of an asset. The lack of a spread reduces the ability to engage in various price manipulation tactics (such as front-running), and also tends to produce better prices for traders.

2.) Traders can enter leveraged positions on a very short timeframe.

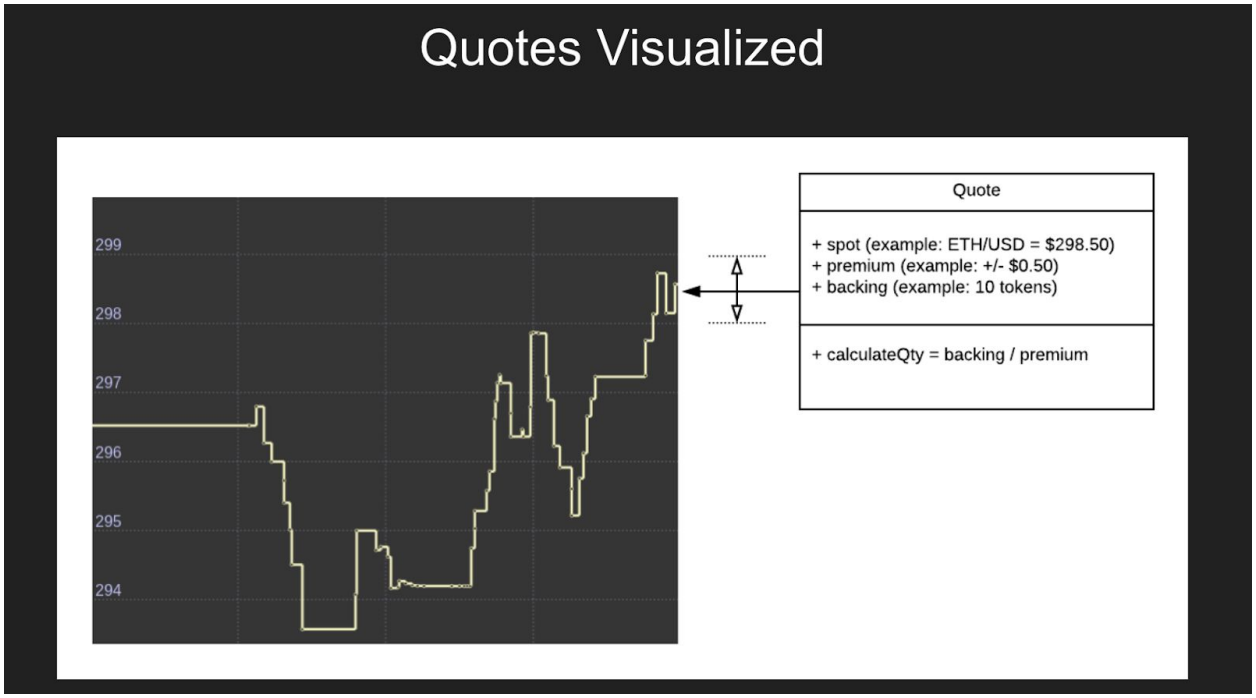
Put and call options have existed for decades. Typically these have monthly timeframes. Part of what makes Mirotick unique is the ability to enter these options for much shorter durations: 12 hours, 1 hour, 15 minutes, and 5 minutes. This granular timeframe is why the platform is called "Microtick." Short-term options offer a new way to profit from even the tiniest of price movements. Leverage for all trades is targeted at 10X, although this multiplier is not set in stone; it can be modified to meet the needs of a particular market.

There are two additional key differences: the duration can begin at the time of the traders' choosing (as opposed to defined expirations), and the options are always at-the-money. This is a contrast to traditional options – for example, MSFT call options, which have a variety of strike prices (out of the money, in the money, and at the money), and monthly expirations.

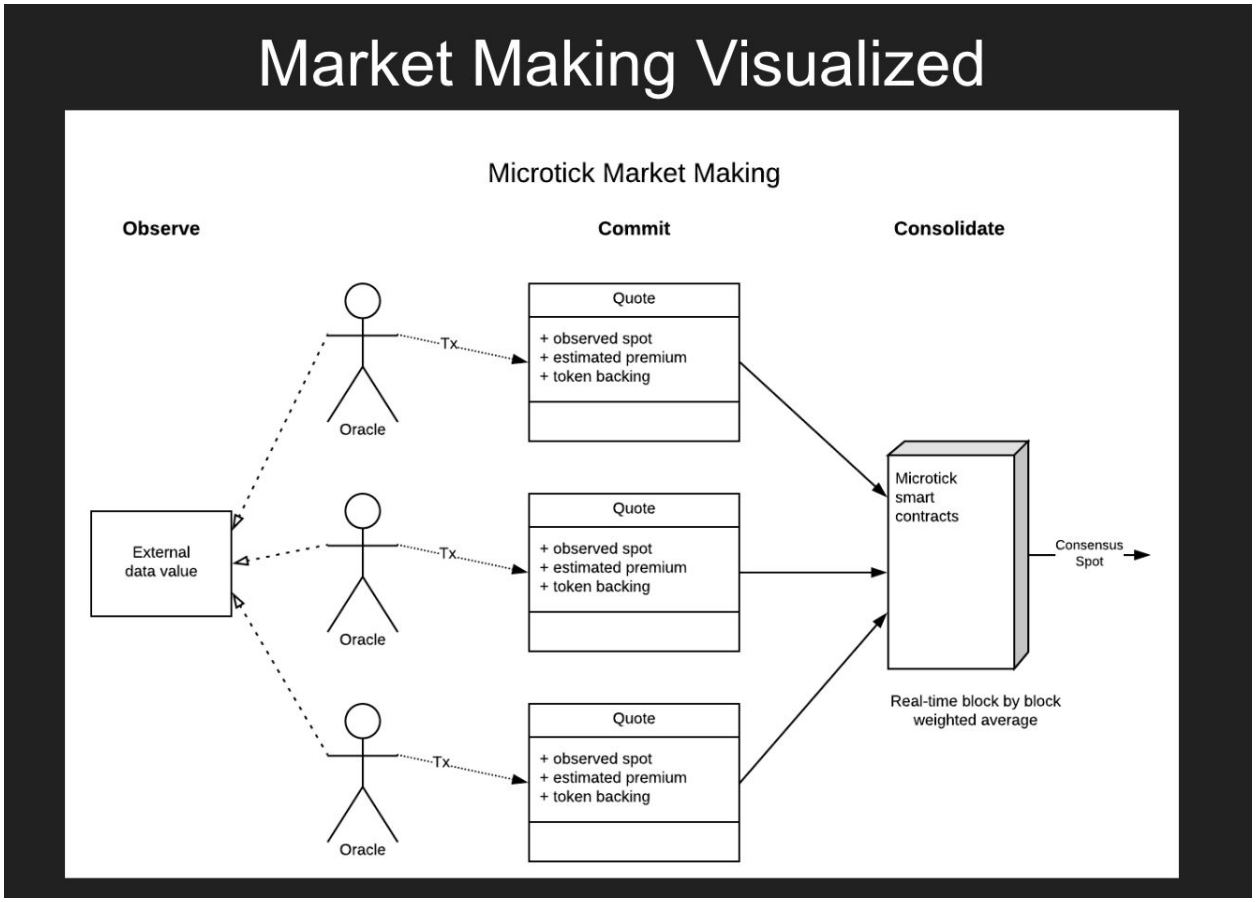
Microtick has two types of actors:

Market Makers: These are the users (or bots) who feed “quotes” into the platform. Market makers are incentivized to provide timely and accurate assertions about an asset’s price. Along with an assertion about what the real-world price is, they also supply “backing” in the form of an on-chain token. This is their skin in the game; if their quote is inaccurate, they stand to lose some or all of this backing through the counterparty market action of honest participants.

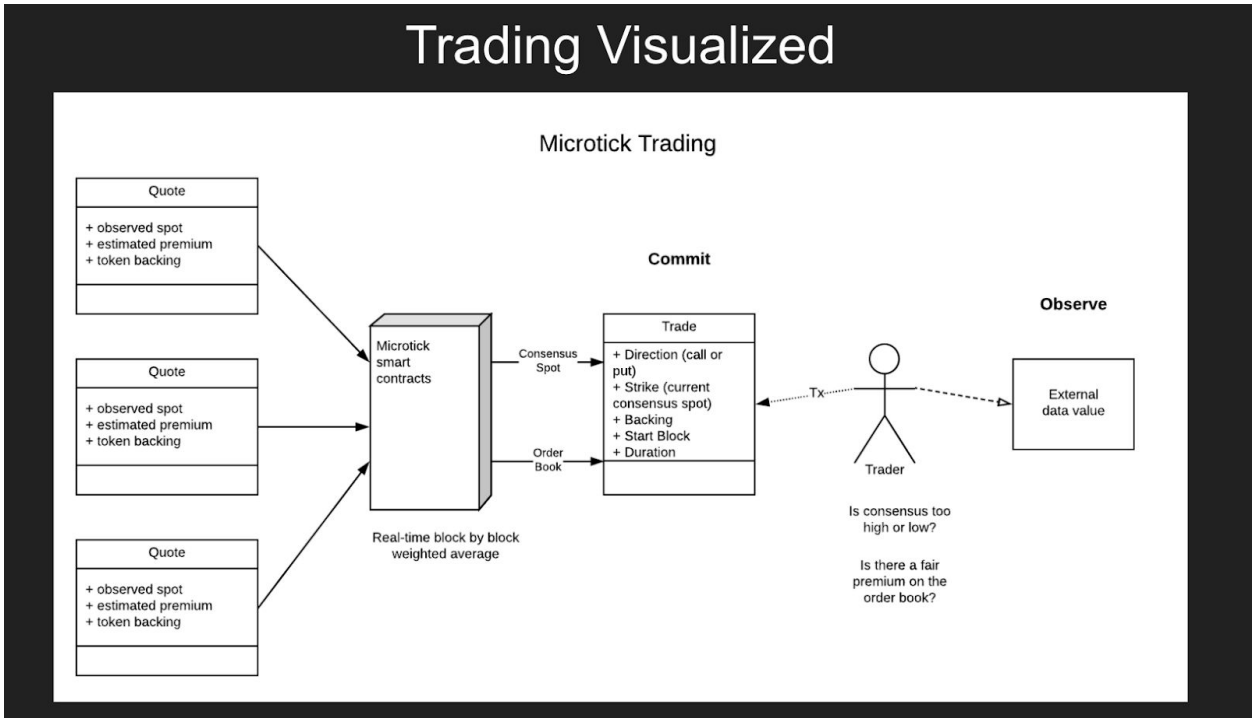
Market maker quotes are constructed as follows:



The aggregate quotes provided by multiple market makers create the “consensus spot price,” as shown here:



Traders: These actors play the role of counterparty. They observe what the market makers are saying about the current price, and trade based on those observations. Traders can buy Call options (when they expect the price to rise), and Put options (when they expect the price to fall). These are currently configured as European-style options; traders must hold on to the position until expiration, as opposed to having the ability to sell them before expiration, as is the case with American-style options.



Microtick's ability to produce accurate, difficult-to-manipulate price information stems from the interplay between traders and market makers. When a market maker submits a quote that deviates from prevailing conditions, traders can profit from this inaccuracy by buying a Put or Call. Crucially, this trade will move the price, helping to correct the inaccurate spot price.

Let's clarify with a simple concrete example. A more rigorous explanation of this self-correcting feedback mechanism will be provided in a subsequent version of this Guide, and in the upcoming white paper.

Imagine ETH is trading at $300 on all the major exchanges. In this case, a rational and non-malicious market maker would likely provide a quote at $300, with a premium to factor in any expected volatility. On the other hand, a malicious actor (for example, an entity who stood to benefit from manipulating Microtick's price data), might assert that ETH is in fact at $295.

In this case, a trader could quickly purchase a Call option, knowing that the price will quickly move upward.. Additionally, honest market makers would be providing correct quotes. The actions of traders and market makers would cause the price to correct to its "accurate" level – and in the process, the malicious actor would lose their backing. Thus, market makers have a disincentive to assert the wrong price.

(Important note: this dynamic only functions if there are multiple market makers.)

Blockchain Design

The mechanics described in the prior section apply to Microtick as a discrete, self-contained module, without any regard to blockchain architecture. The economic incentives and feedback mechanisms created by the interplay between market makers and traders are designed to produce a single consensus price which is difficult to manipulate – even without the decentralization inherent in properly-implemented blockchains.

But while Microtick could hypothetically exist as an off-chain piece of software, its positioning as a decentralized application in a blockchain environment presents two crucial benefits:

- Increased trustlessness, immutability, decentralization, and censorship-resistance
- Relatively frictionless and transparent transmission of price data to other DApps

What Makes Microtick Decentralized?

As described previously, Microtick has the potential to give anyone the power to make a price assertion (plus a premium to reflect expected volatility) over a given time duration. The system calculates the consensus price as the weighted average from the various

price assertions made by multiple Market Makers. The fact that *anyone* can be a Market Maker makes the price more decentralized and difficult to manipulate.

Any trader can hedge in either the up or down direction (from the consensus price) over the same time duration, based on their perception of a.) where price is likely to head, b.) expected volatility over the given duration, and c.) the "adjusted premium" offered by the decentralized code that runs on the blockchain. Validators (described in further detail below) play a crucial role in the decentralization of said code.

The Role of Validators

Microtick will also be positioned within a new type of blockchain architecture where the security of said blockchain would depend on a decentralized set of Microtick validators. Anyone could validate on this blockchain.

Validators process the changes produced by the decentralized code and ensure it can't be modified. These actors would play a key role in maintaining the decentralization of Microtick. In contrast to running on servers controlled by us, Microtick code would be verified by validators who are not affiliated with the company. Properly implemented, this eliminates the possibility that we could single-handedly modify the outcome of Microtick trades and prices. In fact, no single actor could modify the outcome. This plays a crucial role in protecting the platform from manipulation.

This paradigm mirrors how decentralized code functions on the Ethereum platform; in that case, a "global computer" featuring thousands of distributed nodes runs and verifies the code, making it highly decentralized and difficult to manipulate. A set of distributed validators can play a similar role, checking that the code is executing properly and processing blocks, but without having the ability to censor or modify transactions.

With a system of validators, Microtick could arguably be highly decentralized both at the platform level (as described earlier), and at the code-verification level.

Why Not Ethereum or EOS?

Microtick itself is blockchain-agnostic; hypothetically, it could be supported by various platforms. While Ethereum, EOS, and Cosmos were all considered for the DApp, the first two have characteristics that make them less-than-ideal choices.

Ethereum – The standard-bearer for decentralized applications is not currently able to handle the high transaction throughput generated by Microtick. In fact, we estimate that even one marginally successful market - say, ETH/BTC - would effectively "cryptokitties" the network. Even if overhead were available, the sheer number of on-chain transactions (priced in gas) would impose significant costs on all Microtick participants.

Another challenge is finality. While Ethereum's blocktime is much faster than Bitcoin's, it shares its probabalic finality with its proof-of-work cousin. In practice, this means a transaction isn't effectively finalized until at least a few minutes have elapsed. This is not well-suited for Microtick.

We vetted various layer-2 Ethereum scaling solutions, such as Plasma and Starkware, in recent months. While these offer superior transactional throughput, they have a combination of undesirable UX trade-offs that make them a poor fit for Microtick. (One promising solution – a validator-based chain called SKALE – may offer a better fit down the road.) Additionally, once IBC is in production, we may be able to bring Microtick data to the Ethereum chain.

Layer-1 scaling, or "ETH 2.0" may someday offer a promising platform for Microtick; both transactional throughput and finality ought to be vastly improved. But with a

full-scale rollout of ETH 2.0 likely two years away, it's not a reasonable option in the near-term.

EOS – On the surface, EOS seems to offer a good environment for Microtick; its zero-fee transactions, fast blocktimes (1-2 seconds), and high transactional overhead are all desirable characteristics. However, we believe the consensus mechanism behind EOS is overly centralized.

Specifically, the delegated-proof-of-stake (DPOS) mechanism, featuring 21 nodes vying to produce blocks, is not sufficiently Byztantine Fault Tolerant. In its short life, there have already been examples of cartel formation amongst the 21 block producers. One can expect that incentives to attack the network will increase if/when more values accrues to it. Additionally, there have been multiple instances of EOS accounts being changed retroactively. This lack of immutability – and concomitant confusion about what constitutes "finality" – run contrary to our goals for positioning Microtick as a maximally-decentralized application.

Microtick as a Cosmos Hub

Cosmos offers a much more promising foundation for Microtick. Specifically, it provides scaling benefits by allowing each DApp to have its own "zone," or blockchain. Meanwhile, its use of Tendermint provides a consensus mechanism that – properly implemented – *should* be sufficiently decentralized. As an added benefit, Cosmos' *raison d'etre* is to interoperate with other blockchains. This could facilitate a more frictionless sharing of price oracle data – for example, with Ethereum-based DApps.

In the Cosmos ecosystem, decentralized applications can exist as their own blockchains, or "zones," with their own set of validators as the consensus mechanism. The zone then connects to the Cosmos Hub in order to facilitate connects to other zones. The Microtick zone runs solely the Microtick application, and is supported by its own validator set. In

practice, this group of validators will likely overlap partially with the existing Cosmos Hub validator set.

Tendermint Consensus: Understanding the Tradeoffs

As Milton Friedman was fond of pointing out, there ain't no such thing as a free lunch. In order to achieve its superior scalability and finality, Cosmos has arguably made an important (and potentially consequential) tradeoff: sacrificing decentralization for scalability. In practical terms, this means that Tendermint consensus is arguably much easier to attack than proof-of-work as currently used by Ethereum and Bitcoin.

Let's take a closer look at the two potential threat models:

Sybil Attacks. Unless validators are carefully verified in a KYC-style process, there's no way of knowing that each validator is a unique actor. A motivated attacker could thereby accrue a high proportion of voting power, while maintaining the illusion that the validator set is fully decentralized.

Cartel Formation. There is nothing to prevent groups of validators from agreeing to act as a single actor. As noted above, this type of behavior has already been observed in EOS. While the higher number of validators (100+ vs 21) and other Tendermint mechanics are designed to mitigate this issue, the threat remains. This could be exacerbated in tandem with sybil attacks; the combination of both tactics could lower the barriers to entry for malicious actors.

The potential for byzantine behavior is a significant risk for Microtick, and it will likely be viewed as such by potential traders and market makers.

As such, it's mission-critical that we proceed in a careful and methodical fashion when building our own validator set. Fortunately, the Cosmos ecosystem has an important

property: fault-attribution. This means that malicious validator behavior should be readily detectable and attributable. To the extent we can leverage the existing Cosmos Hub validator set, we'll be in better shape for our own chain; existing validators have more to lose by attacking a smaller chain, as they'd be forfeiting future ATOM earnings from the Cosmos Hub.