fundstrat

Evidence-based research.
150 East 52nd St, 3rd Floor New York, NY 10022

Crypto Concepts

March 7, 2023

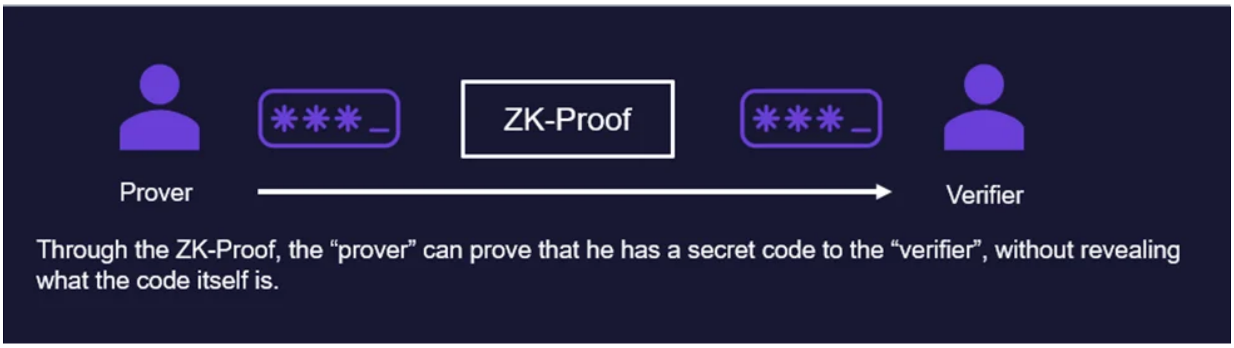
Zero-Knowledge Technology

Key Takeaways

- Zk (zero-knowledge) technology is one of the most exciting technologies in crypto today and can be very useful in situations requiring privacy and security.
- Zk-proofs enable one party to prove to another party that something is true without revealing any information beyond the fact that it is true.
- Zk-tech has a wide range of use cases in areas such as privacy, security, scalability, interoperability, and sovereign identity.
- Several promising protocols, including Polygon, Aztec, and zkSync are already implementing zk-tech.

What is Zero-Knowledge Tech?

Zk (zero-knowledge) technology is one of the most interesting technologies in crypto and can potentially be very useful in situations that require privacy and security. Zk-tech increases privacy by leveraging zero-knowledge proofs to enable one party to prove to another party that something is true without revealing any information beyond the fact that it is true. For example, imagine you have a secret code you don’t want to show to anyone, but you need to prove to someone else that you know the code to access a secure system. With zk-technology, you can prove that you know the code without revealing the code itself.


Prover
***_
ZK-Proof
***_
Verifier
Through the ZK-Proof, the "prover" can prove that he has a secret code to the "verifier", without revealing what the code itself is.

Source: Fundstrat

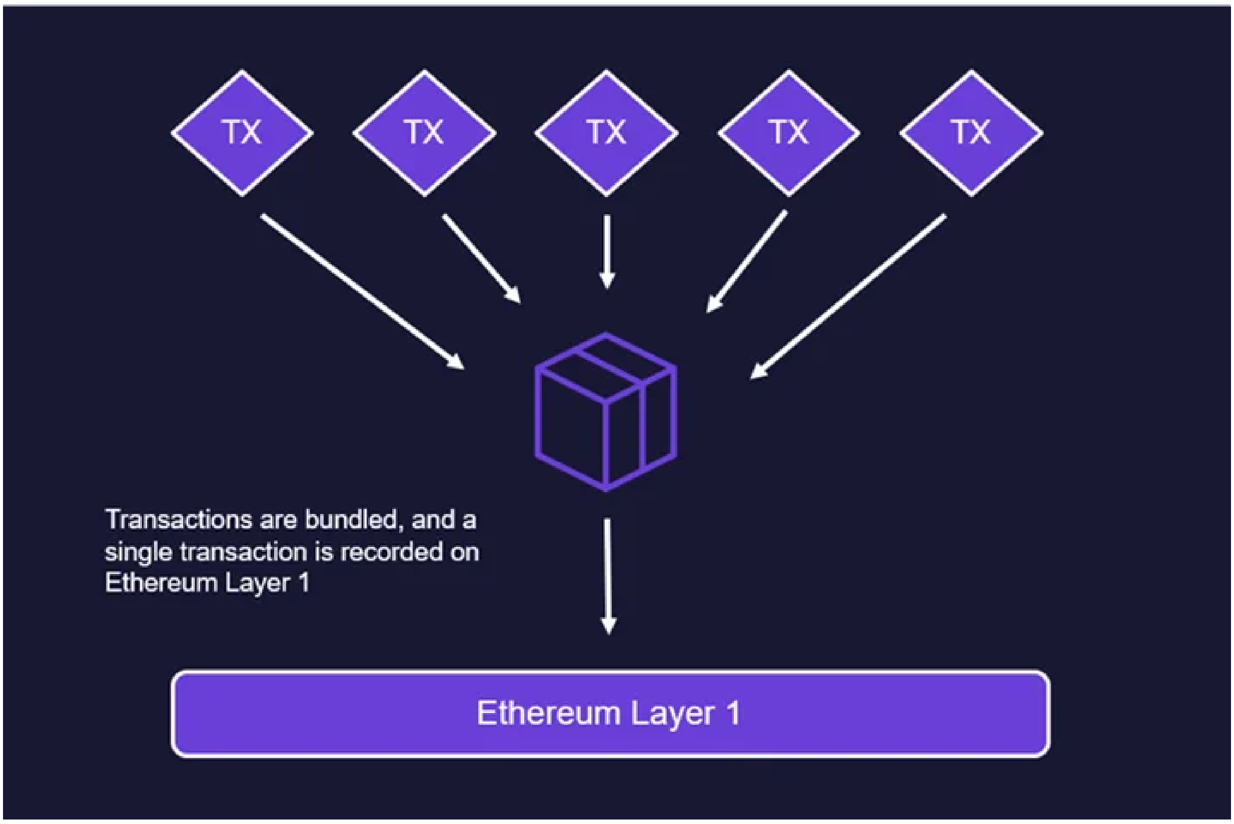
This is done by using complex algorithms to generate a "proof" that the statement is true without revealing any information about how the proof was generated. The other person can then verify the proof and be sure that the prover does, in fact, know the code without actually knowing what the code is themselves.

To qualify as a zk-proof, it must satisfy three properties:

1. Completeness: if the statement is true, an honest prover will convince an honest verifier of this fact.
2. Soundness: if the statement is false, it is impossible for a dishonest prover to convince an honest verifier that it is true (in most circumstances).
3. Zero-knowledge: if the statement is true, no verifier learns anything other than the fact that the statement is true.

What are Zero-Knowledge Rollups

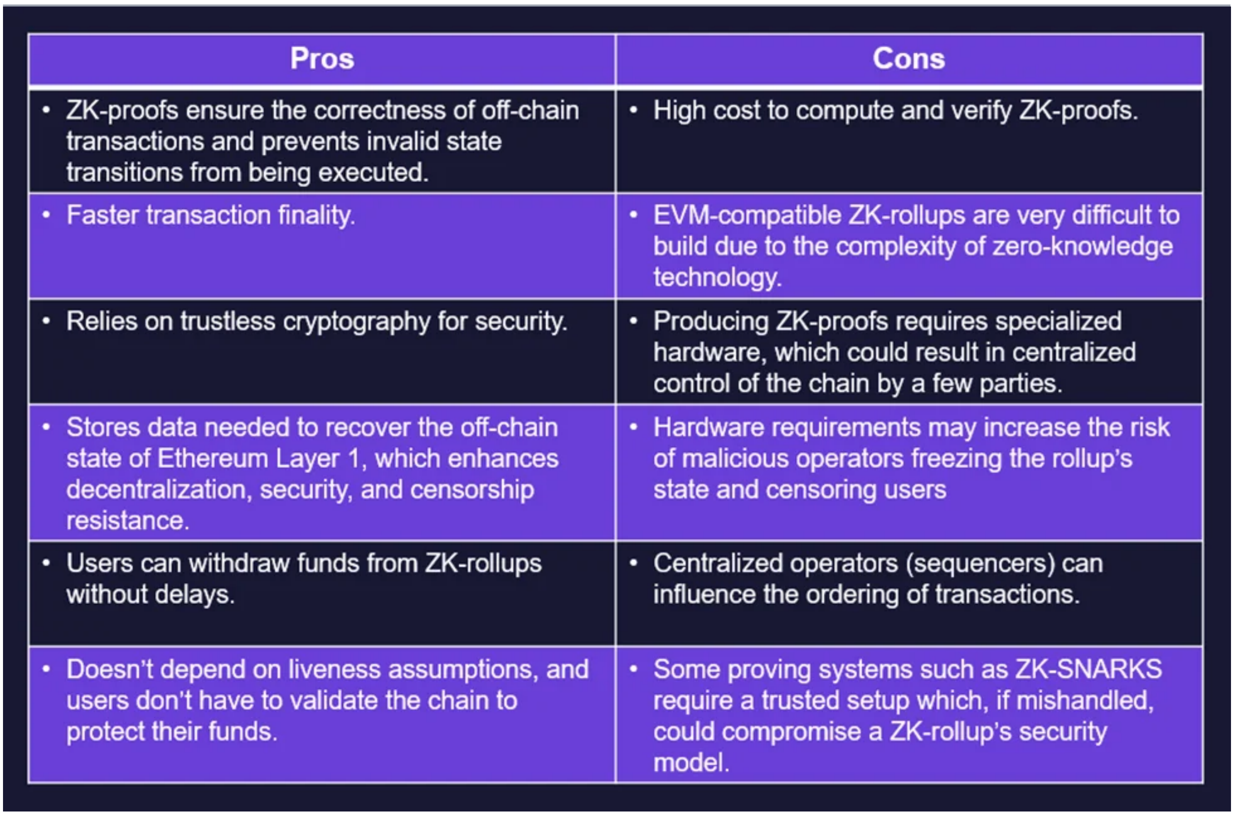
Zero-knowledge rollups (zk-rollups) are layer 2 scaling solutions that increase throughput on Ethereum Mainnet by moving computation and state storage off-chain. Zk-rollups can bundle thousands of transactions in a batch and then only post minimal summary data to Ethereum Mainnet. This summary data defines the changes to be made to the Ethereum state and includes a cryptographic proof that those changes are correct. This allows for cheaper, more efficient, and private transactions.


TX
TX
TX
TX
TX
Transactions are bundled, and a single transaction is recorded on Ethereum Layer 1
Ethereum Layer 1

Source: Fundstrat

To give an example, imagine a group of people playing poker online. They could use a zero-knowledge rollup to bundle all of their individual bets into a single transaction without revealing the identity of each person. The bundled transaction could then be recorded on-chain, proving that the bets were made and are valid without revealing personal information about the players or their bets. This application would enable privacy for the players and would make the poker game more efficient than it otherwise would be on Mainnet.

Pros and Cons of ZK-Proofs



Pros	Cons
• ZK-proofs ensure the correctness of off-chain transactions and prevents invalid state transitions from being executed.	• High cost to compute and verify ZK-proofs.
• Faster transaction finality.	• EVM-compatible ZK-rollups are very difficult to build due to the complexity of zero-knowledge technology.
• Relies on trustless cryptography for security.	• Producing ZK-proofs requires specialized hardware, which could result in centralized control of the chain by a few parties.
• Stores data needed to recover the off-chain state of Ethereum Layer 1, which enhances decentralization, security, and censorship resistance.	• Hardware requirements may increase the risk of malicious operators freezing the rollup's state and censoring users
• Users can withdraw funds from ZK-rollups without delays.	• Centralized operators (sequencers) can influence the ordering of transactions.
• Doesn't depend on liveness assumptions, and users don't have to validate the chain to protect their funds.	• Some proving systems such as ZK-SNARKS require a trusted setup which, if mishandled, could compromise a ZK-rollup's security model.

Source: Ethereum Foundation, Fundstrat

zk-SNARKS & zk-STARKS

Within zk-tech, there are two primary zk-proof systems: SNARKS and STARKS.

zk-SNARKs

zk-SNARK stands for Zero-Knowledge Succinct Non-Interactive Argument of Knowledge. The word "succinct" refers to its data compression - the proof can be concise, and verified quickly. It is called "non-interactive" because the prover does not need to communicate with the verifier during the proof process. This can reduce gas fees and the computational power required. zk-SNARKs are often used to allow for private and secure transactions without revealing any personal information and are currently the most common proof system found in crypto. Protocols using zk-SNARKS include zkSync and Zcash. and A drawback to SNARKs is that they typically require a trusted setup between parties.

zk-STARKs

zk-STARK stands for Zero-Knowledge Scalable Transparent Argument of Knowledge. Unlike zk-SNARKs, zk-STARKs are "transparent" in that they do not rely on a trusted setup. This means that the proof is not dependent on a secret key that needs to be generated beforehand. zk-STARKs are also "scalable," meaning that they can be used for larger computations than zk-SNARKs. They are a newer technology and are still being developed for practical applications. Still, they have plenty of potential to be used in similar crypto applications that require security and privacy. The downside to STARKs is that the proof sizes are much larger than SNARKs, which makes implementation more difficult.

ZK Uses Cases

The innovation of zk-tech has given rise to a wide range of use cases. Below we list what we consider to be the primary ones today, although more will surely surface as more developers implement the technology.

Privacy

Zk-tech's ability to let one party prove something to another without revealing additional information makes it highly useful for privacy and anonymity.

- Private Transactions and Payments
  - On Ethereum layer 1, all transactions are public on the blockchain. While this is useful in many aspects, it isn't ideal for users who value privacy. For example, holders of large amounts of cryptocurrency may not want their finances to be publicly known for security reasons. Zk-tech offers a private alternative where users can have their transactions and account balances completely private. This allows them to use blockchains without needing to worry that anyone is invading their privacy.

- Crypto Mixers
  - Mixers, also known as tumblers, are tools that allow users to deposit some amount of crypto into a pool, which is then "mixed" with other funds so that the crypto is untraceable from the source to the destination. Crypto mixers are often associated with illegal activity, but there are legitimate use cases as well for users who value privacy and don't want their transactions traced.
  - Not all crypto mixers use zk-tech, but zk-tech is used in certain mixers to enhance privacy and anonymity. In the context of mixers, zk-proofs are used to prove that a mixer's output is valid without revealing any information about the origin of the funds or the identity of the parties involved. This provides users with an added layer of privacy.
- Authentication
  - Zk-proofs proofs can be used to authenticate a user's identity without revealing any personal information. For example, a user could prove to a service provider that they have a valid email address or phone number without disclosing the actual email address or phone number. This is very useful at a time when centralized parties suffer from data breaches on a regular basis.
- Health data
  - Zk-proofs can be used to protect sensitive health data by allowing a patient to prove that they have a certain condition or have undergone a particular treatment, without revealing any other information about their health.

Scaling

Another use case of zk-tech is that it improves scalability and reduces fees. It does this by bundling many transactions into just one, which is then recorded on-chain. By bundling hundreds or even thousands of transactions into one, the fees and computing power required are shared amongst many transactions. It does this while not compromising the security of the network. There are a number of Ethereum Layer 2 scaling solutions that utilize zk-tech including zkSync, Aztec, and StarkNet. These scaling solutions typically work by having a smart contract on the mainnet serving as a coordinator, receiving batches of transactions from a zk-rollup aggregator on the Layer 2 sidechain. The coordinator then creates a zero-knowledge proof that attests to the validity of all the transactions in the batch, which is then submitted to the mainnet as a single transaction. This significantly reduces the amount of data that needs to be stored on the mainnet and also reduces the gas fees required.

Bridging and Interoperability

Interoperability and bridging between blockchains are currently in their early stages and are filled with risks. According to Chainalysis, bridge hacks in 2022 accounted for $2 billion stolen or 69% of all hacks in the DeFi space in 2022. Some bridges today still rely on a centralized party to transfer changes from one chain to another. Zk-tech can potentially improve the interoperability between blockchains and enable more secure, private, and decentralized communication between them.

Instead of using centralized multi-sig committees to facilitate transfers between chains, zk-proofs can be used to bridge between blockchains by allowing a light client to verify the correctness of a transaction or state transition without having to download the full blockchain. A light client is a software program that only downloads a portion of the blockchain data needed to verify transactions, instead of downloading the entire blockchain. This makes light clients much faster and more efficient than full nodes, which are required to download and store the entire blockchain.

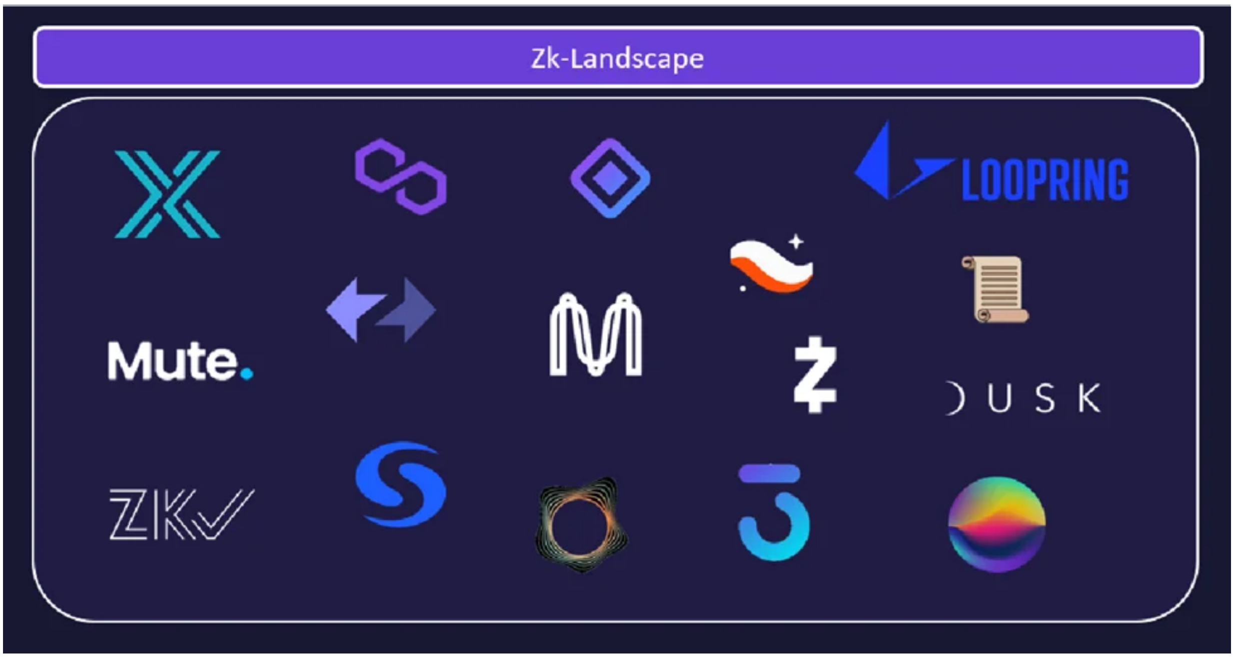
To use a zk-proof to bridge between blockchains, the proof is generated by a prover on one blockchain and then submitted to a verifier on another blockchain. The verifier can be a light client that only downloads a small portion of the blockchain data, such as the current state of the blockchain, and uses the ZK proof to verify that a specific transaction or state transition is valid without needing to download the entire blockchain. The only downside to this is that light clients are complex and expensive, sometimes too much so to host on-chain within a smart contract. A solution to this is to have the computation performed off-chain where it is less expensive, and then have a proof submitted on-chain to verify the computation.

Sovereignty of Identity

Zk-tech opens up a realm of possibilities for digital identity by allowing for the sovereignty of identity. Sovereignty of identity is a way of managing digital identities that allows individuals or businesses to have sole ownership and control over their accounts and data. This is becoming increasingly important in today's digital age, where individuals are constantly sharing personal information online, and digital platforms collect vast amounts of data about users. It's common for massive data breaches to happen on social media sites or for individuals to be de-platformed and unable to create new accounts. Through zero-knowledge proofs, individuals are able to prove their identity without revealing any additional personal information beyond what is strictly necessary for authentication. This could be useful in a wide range of scenarios, such as on-chain loans, KYC, and authentication. It is common in some communities today to interact primarily online, and many members of these communities are pseudonymous. Zk-proofs would allow these members to verify their legitimacy without having to reveal any personal information.

Zk Landscape Today

Zk-tech is growing increasingly common in crypto, with protocols from Layer 1's, DeFi, and payments apps implementing it.



Source: Fundstrat

Polygon zkEVM

Zk-EVM (Zero-Knowledge Ethereum Virtual Machine) leverages zero-knowledge proofs to provide an off-chain computation layer that can verify the validity of on-chain transactions without needing to process them on the main Ethereum network. This allows for a huge increase in transaction throughput and reduces the cost of executing smart contracts.

By using zk-EVM, developers can build faster and cheaper applications than on the Ethereum mainnet while improving privacy and maintaining security.

Polygon is an Ethereum sidechain implementing zk-tech to improve speed and costs. Polygon has announced that they are releasing their zkEVM in late March of 2023. Polygon zkEVM is a Layer 2 scaling solution built on Ethereum that uses zero-knowledge proofs to lower fees and increase scalability while inheriting the security of Ethereum layer 1. Polygon zkEVM is fundamentally equivalent to the Ethereum Virtual Machine (EVM), meaning that it benefits from Ethereum's ecosystem and frictionlessly works with all existing smart contracts, developer tooling, and wallets.

Aztec Network

Aztec is a Layer 2 privacy-focused scaling solution for Ethereum, which utilizes zero-knowledge proofs, to allow for private transactions.

The Aztec protocol allows users to convert their ERC20 tokens into "zkTokens," which are confidential digital assets. These zkTokens can be privately traded on Ethereum without revealing the underlying token amounts or sender and receiver addresses. Aztec also allows for the creation of non-fungible confidential tokens, which can be used for a wide range of purposes, such as identity verification or supply chain tracking.

To achieve its privacy goals, Aztec uses a variation of ZKP known as "doubly efficient zkSNARKs." These zkSNARKs allow for more efficient computation and lower gas costs, which makes the protocol more

accessible for everyday users. In addition, Aztec also uses a modular system that allows developers to easily build new applications and tools on top of the protocol.

Regulatory Risk

Zk-tech’s power to make transactions anonymous on the blockchain could put it in the crosshairs of regulators and law enforcement seeking to crack down on illegal activity such as money laundering. Regulators have already targeted the decentralized crypto mixer, Tornado Cash which utilizes zk-tech through zk-SNARKs. Tornado Cash offers a service that mixes cryptocurrency funds with each other, which obscures the track back to the original source. While there are legitimate privacy use cases, mixers have also been used to launder hacked and stolen funds, leading to the Office of Foreign Assets Control and the U.S. Department of the Treasury blacklisting it in 2022. It’s possible that regulators will continue to target zk-tech and may implement anti-money laundering (AML) and know-your-customer (KYC) measures to ensure that transactions are legal.

Conclusion

Zk-tech has the potential to revolutionize a number of sectors due to its ability to provide a secure and efficient way to verify information while maintaining privacy and security. Zk-tech has already seen product market fit in use cases such as privacy and authentication, and we expect that the ways in which ZK-tech is implemented will only grow over time. In addition, it is also a promising way to scale Ethereum to the masses, allowing thousands of transactions to be bundled off the chain into one, resulting in far greater efficiency. A number of protocols have successfully implemented Zk-tech, such as Polygon, Aztec, and ZK-Sync. We look forward to seeing how these protocols do going forward and seeing which other protocols will implement the technology as well.

Disclosures

This research is for the clients of Fundstrat Global Advisors only. For additional information, please contact your sales representative or Fundstrat Global Advisors at 150 East 52nd Street, New York, NY, 10022 USA.

Conflicts of Interest

This research contains the views, opinions and recommendations of Fundstrat. At the time of publication of this report, Fundstrat does not know of, or have reason to know of any material conflicts of interest.

General Disclosures

Fundstrat Global Advisors is an independent research company and is not a registered investment advisor and is not acting as a broker-dealer under any federal or state securities laws.

Fundstrat Global Advisors is a member of IRC Securities' Research Prime Services Platform. IRC Securities is a FINRA registered broker-dealer that is focused on supporting the independent research industry. Certain personnel of Fundstrat (i.e., Research Analysts) are registered representatives of IRC Securities, a FINRA member firm registered as a broker-dealer with the Securities and Exchange Commission and certain state securities regulators. As registered representatives and independent contractors of IRC Securities, such personnel may receive commissions paid to or shared with IRC Securities for transactions placed by Fundstrat clients directly with IRC Securities or with securities firms that may share commissions with IRC Securities in accordance with applicable SEC and FINRA requirements. IRC Securities does not distribute the research of Fundstrat, which is available to select institutional clients that have engaged Fundstrat.

As registered representatives of IRC Securities, our analysts must follow IRC Securities' Written Supervisory Procedures. Notable compliance policies include (1) prohibition of insider trading or the facilitation thereof, (2) maintaining client confidentiality, (3) archival of electronic communications, and (4) appropriate use of electronic communications, amongst other compliance related policies.

Fundstrat does not have the same conflicts that traditional sell-side research organizations have because Fundstrat (1) does not conduct any investment banking activities, (2) does not manage any investment funds, and (3) our clients are only institutional investors.

This research is for the clients of Fundstrat Global Advisors only. Additional information is available upon request. Information has been obtained from sources believed to be reliable, but Fundstrat Global Advisors does not warrant its completeness or accuracy except with respect to any disclosures relative to Fundstrat and the analyst's involvement (if any) with any of the subject companies of the research. All pricing is as of the market close for the securities discussed, unless otherwise stated. Opinions and estimates constitute our judgment as of the date of this material and are subject to change without notice. Past performance is not indicative of future results. This material is not intended as an offer or solicitation for the purchase or sale of any financial instrument. The opinions and recommendations herein do not take into account individual client circumstances, risk tolerance, objectives, or needs and are not intended as recommendations of particular securities, financial instruments or strategies.

The recipient of this report must make its own independent decision regarding any securities or financial instruments mentioned herein.

Except in circumstances where Fundstrat expressly agrees otherwise in writing, Fundstrat is not acting as a municipal advisor and the opinions or views contained herein are not intended to be, and do not constitute, advice, including within the meaning of Section 15B of the Securities Exchange Act of 1934. All research reports are disseminated and available to all clients simultaneously through electronic publication to our internal client website, fundstrat.com. Not all research content is redistributed to our clients or made available to third-party aggregators or the media. Please contact your sales representative if you would like to receive any of our research publications.