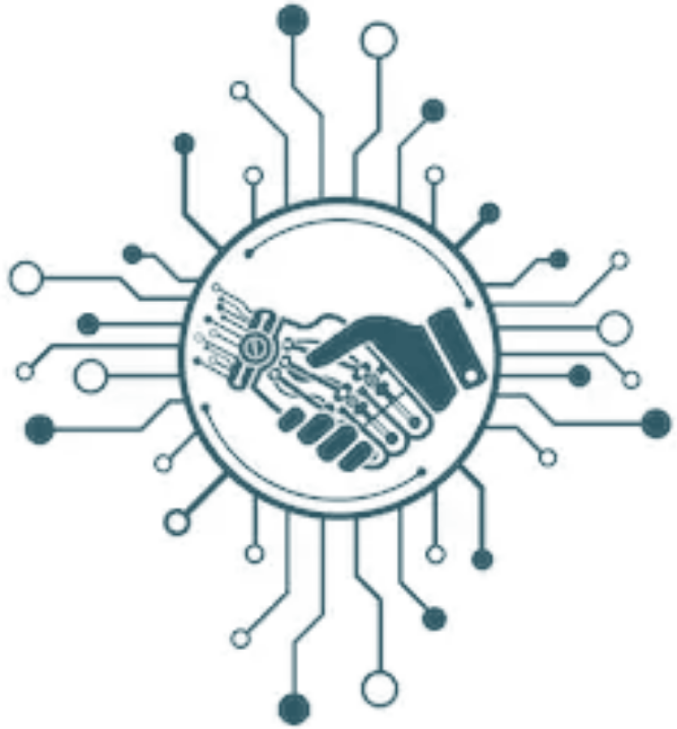
November 27, 2018

A PRIMER ON
SMART CONTRACTS

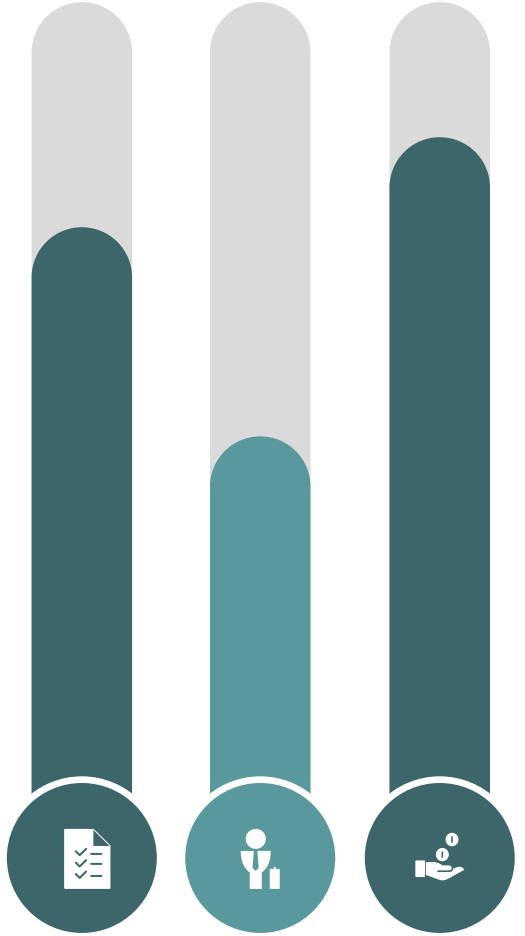


This primer format is intended to be an educational tool regarding emerging FinTech innovations. It is not intended to state the official policy or position of the CFTC, or to limit the CFTC's current or future positions or actions. The CFTC does not endorse the use or effectiveness of any of the financial products or technologies in this presentation.

The CFTC's jurisdiction over any particular smart contract will depend on specific facts and circumstances. Any examples included in this Primer are illustrative only and do not indicate a determination by the Commodity Futures Trading Commission or its staff of jurisdiction.

LabCFTC cannot and will not provide legal advice. If you have specific questions regarding your activities and whether they conform to legal or regulatory requirements, you should consult with a qualified lawyer or appropriate expert. LabCFTC has no independent authority or decision-making power, and cannot independently provide, or create an expectation for, legal or regulatory relief. Communications from LabCFTC shall not create estoppel against CFTC or other enforcement actions. Any formal requests for relief must be addressed by relevant CFTC staff or, as necessary, by the Commission. LabCFTC will work with entities on such requests with the appropriate offices through established processes.

Contents



Overview of Smart Contracts

- *What is a Smart Contract?*
- *Smart Contracts and Blockchain/Distributed Ledger Technology (DLT)*
- *Benefits and Potential Applications of Smart Contracts*

What Is a Smart Contract?

- **Fundamentally, a "smart contract" is a set of coded computer functions.**
  - May incorporate the elements of a binding contract (*e.g.*, offer, acceptance, and consideration), or may simply execute certain terms of a contract.
  - Allows self-executing computer code to take actions at specified times and/or based on reference to the occurrence or non-occurrence of an action or event (*e.g.*, delivery of an asset, weather conditions, or change in a reference rate).

Character of Smart Contracts

- **“Smart contract” may be an oxymoron!**
  - A “smart contract” is not necessarily “smart.”
    - The operation is only as smart as the information feed it receives and the machine code that directs it.
  - A “smart contract” may not be a legally binding contract.
    - It may be a gift or some other non-contractual transfer.
    - It may be only part of a broader contract.
    - To the extent a smart contract violates the law, it would not be binding or enforceable.

Understanding Smart Contracts

Key attributes of a smart contract include:

Can authenticate (counter-) party identities, the ownership of assets and claims of right

Smart contracts use ***digital signatures*** – private cryptographic keys held by each party to verify participation and assent to agreed terms.

Can access or refer to outside information or data to trigger action(s)

Smart contracts use ***oracles*** – a mutually agreed upon, network-authenticated reference data provider (potentially a third-party); this is a source of information to determine actions and/or contractual outcomes, for example, commodity prices, weather data, interest rates, or an event occurrence.

Can automate execution processes

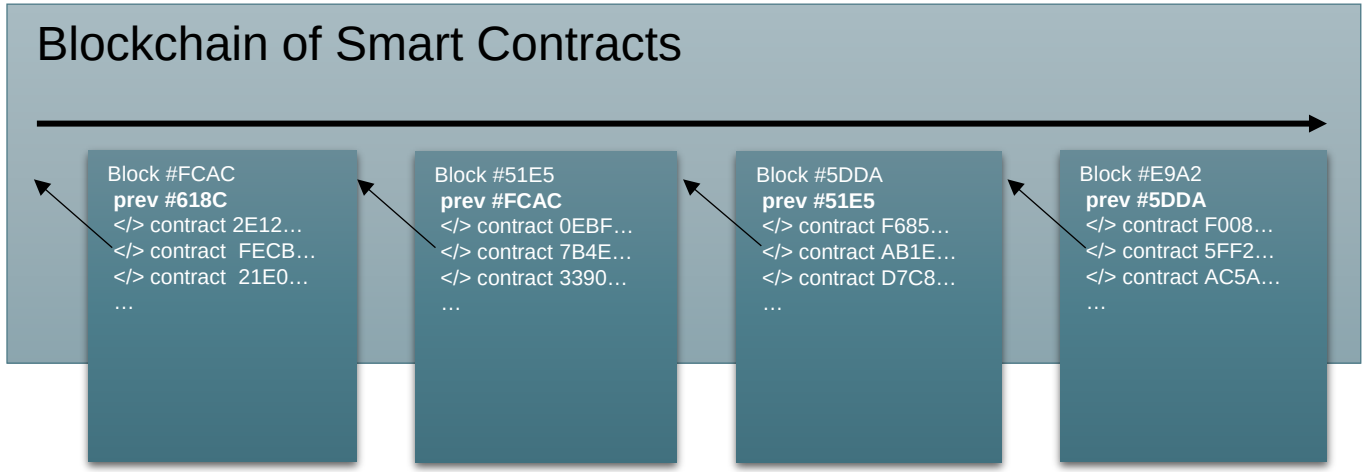
Self-execution: A smart contract will take actions, *e.g.*, disperse payments, without further action by the counterparties.

Smart Contracts Leverage Blockchain/DLT

- Smart contracts can be stored and executed on a ***distributed ledger***, an electronic record that is updated in real-time and intended to be maintained on geographically disperse servers or **nodes**.

- Through ***decentralization***, evidence of the smart contract is deployed to all nodes on a network, which effectively prevents modifications not authorized or agreed by the parties.

- ***Blockchain*** is a continuously growing database of permanent records, "blocks," which are linked and secured using cryptography.‡



‡ Distributed ledgers may be public or private/permissioned. *See* "A CFTC Primer on Virtual Currencies," October 17, 2017, https://www.cftc.gov/LabCFTC/Primers/index.htm

Smart Contract Origins

The concept of a smart contract is not new. More than 20 years ago, computer scientist Nick Szabo stated the following:

> "A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on the other promises…. The basic idea of smart contracts is that many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher."‡

Nick Szabo,
Computer Scientist
Smart Contracts Building Blocks for Digital Markets 1996

‡ See Nick Szabo, Smart Contracts: Building Blocks for Digital Markets, 1996, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Additional Viewpoints

"A smart contract is a mechanism involving digital assets and two or more parties, where some or all of the parties put assets in, and assets are automatically redistributed among those parties according to a formula based on certain data that is not known at the time the contract is initiated."

Vitalik Buterin, Founder of Ethereum, "DAOs, DACs, DAs and More: An Incomplete Terminology Guide," (May 6, 2014), available at https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

"A smart contract is an agreement in digital form that is self-executing and self-enforcing."

Kevin Werbach, Professor of Legal Studies & Business Ethics, University of Pennsylvania, Wharton Business School, "The Promise — and Perils — of 'Smart' Contracts," (May 18, 2017), available at http://knowledge.wharton.upenn.edu/article/what-are-smart-contracts/

"A smart contract is an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code."

ISDA and King and Wood Mallesons, Smart Derivatives Contracts: From Concept to Construction (October 2018), at 5 (citing Clack, C., Bakshi, V., and Braine, L., "Smart Contract Templates: foundations, design landscape and research directions" (August 4, 2016, revised March 15, 2017))

Smart Contracts in Context

Smart contracts can be viewed as part of an evolution to automate processes with machines and self-executing code.

Increasing automation has long been a feature of our financial markets including, for example:

- Stop Loss (Conditional) Orders: "If the price falls below $X, then sell at market."
- Trading algorithms and smart order routers (machines that direct orders for execution).

Increasingly automation is a feature of everyday life.

- The ATM
- Automatic bill pay
- Touch-to-pay systems
- Instant money transfer apps

Potential Benefits of a Smart Contract

The attributes of a smart contract give rise to potential benefits throughout an economic transaction lifecycle, *e.g.*, formation, execution, settlement.

STANDARDIZATION

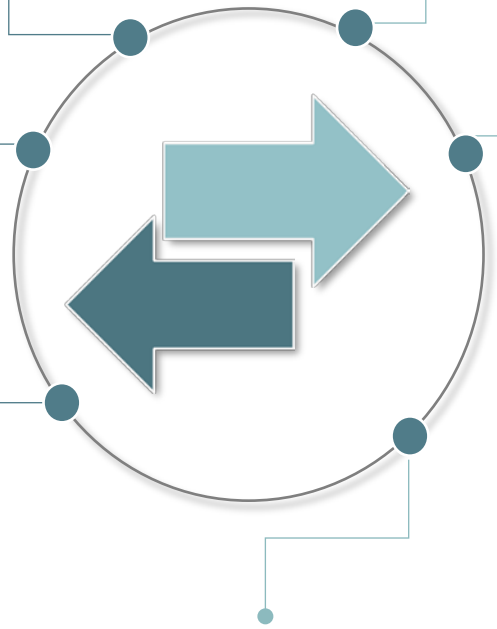
Standardized code and execution may reduce costs of negotiations and agreements.

SECURITY

Transactions are encrypted and stored on a distributed ledger intended to be immutable.

ECONOMY AND SPEED

Automation reduces transaction times and unnecessary manual processes.



CERTAINTY

Well-designed smart contracts execute automatically thereby reducing counterparty risk and settlement risk.

BUSINESS INNOVATION

Automating flow of digital assets and payments may foster new products and business models.

REGULATORY INNOVATION

Examples include:

- Built-in regulatory compliance (*e.g.*, cannot sell to a non-Eligible Contract Participant (ECP); cannot sell until mandated period has passed; or must report certain data).
- New regulatory reporting models (*e.g.,* smart contracts automatically report data at pre-determined intervals).
- Stress testing built into smart contracts and regulatory nodes (*e.g.,*execute scenarios on smart contracts to determine payouts across the network).

Example of Self-Executing Logic: *Vending Machine*

The machine offers pre-defined terms whereby the seller agrees to deliver immediately to buyer a product upon payment of stated sum.

Logic code is a simple loop:

If **payment (P)** received and **item (I)** selected is available, then:

- If $P \geq I_{price}$, dispense I
- If $P > I_{price}$, dispense change
- Else beep and wait.

Example Use Case I: Self-Executing Insurance

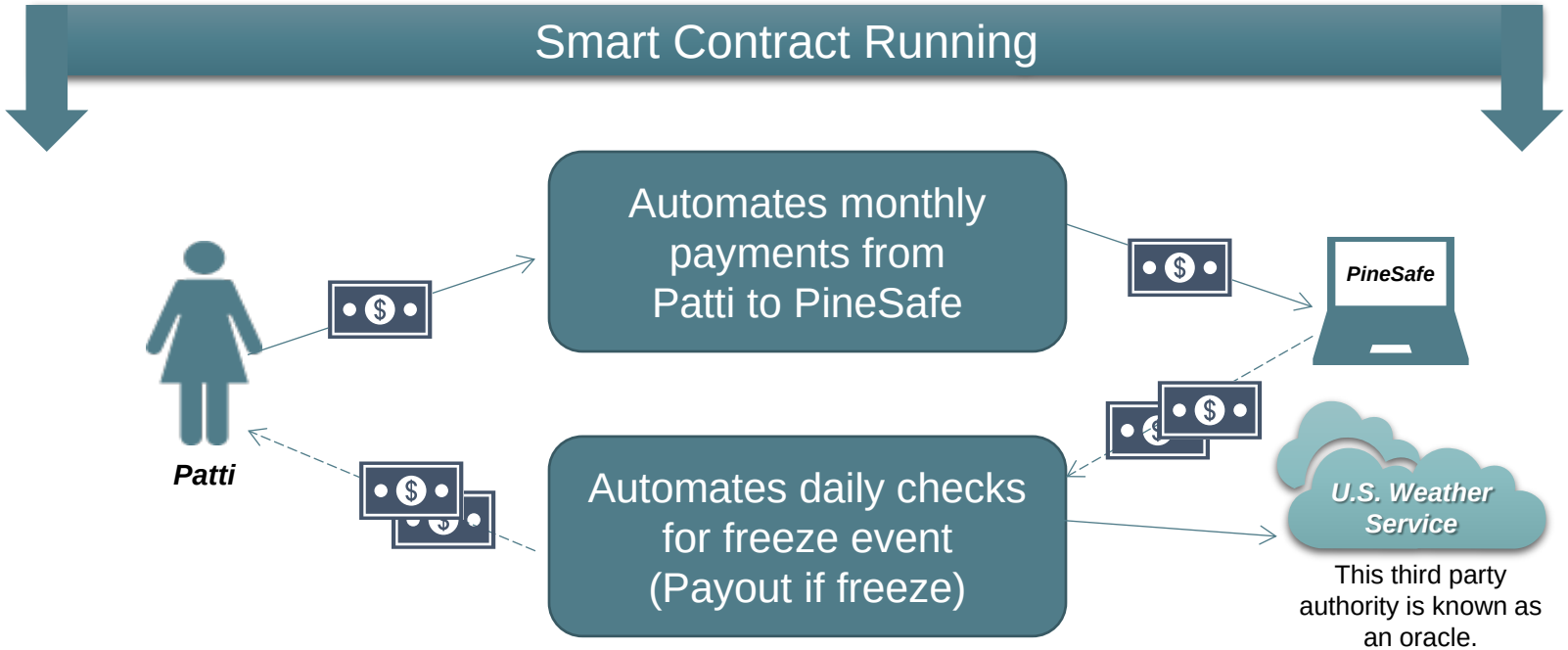
Patti buys a pineapple grove in Hawaii

Patti worries weather could jeopardize business

PineSafe offers insurance through a self-executing smart contract

Patti and PineSafe agree to terms and digitally sign a smart contract

The smart contract is stored and operates on Blockchain



This third party authority is known as an oracle.

Example Use Case II: Transportation Rental

Jane uses a smart contract to rent a ride.

Upon deposit, the smart contract unlocks bike for use.

The smart contract monitors speed and distance with ride tracking.

Jane returns bike to a different rental point.

The smart contract transfers funds to RentCo and relocks the bike.

Jane

Jane can see records of her rides on the Smart Contract Blockchain.

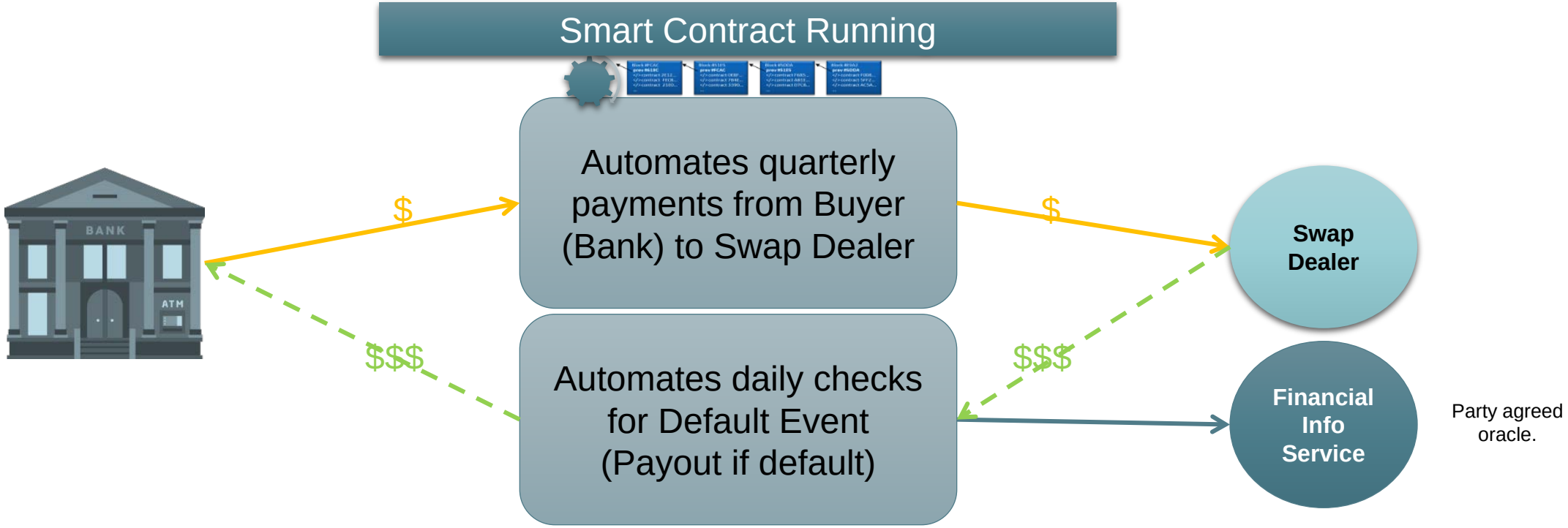
Ride Tracking Service

Oracle tracks location, speed, and accidents.

Example Use Case III: Credit Default Swap

To cover the default risk of its customers, a bank enters into a credit default swap (CDS) contract with a swap dealer.

- New Quarter? The smart contract calculates and transfers premium from bank to swap dealer.
- Borrower Defaults? Check party-agreed authority (*i.e.,* oracle) for default event. If the borrower defaults, the smart contract calculates and transfers payout from swap dealer to bank.



Other Potential Smart Contract Use Cases

Smart Contracts may have potential uses in financial market operations, and likewise may be useful in a variety of other areas as well. Examples include:

- **Financial Markets and Participants**
  - Derivatives – streamline post-trade processes, real time valuations and margin calls.
  - Securities – simplify capitalization table maintenance (*e.g.*, automate dividends, stock splits).
  - Trade Clearing and Settlement – improve efficiency and speed of settlement with less misunderstandings of terms.
  - Supply Chain/Trade Finance – track product movement, streamline payments, facilitate lending and liquidity.
  - Data Reporting and Recordkeeping – greater standardization and accuracy (*e.g.*, Swaps Data Reporting, regulator nodes for real time risk analysis); automated retention and destruction.
  - Insurance – automatic and automated claims processing based on specified events; Internet of Things (IoT) enabled vehicles/homes/farms could execute claims automatically.
- **Other sample applications**
  - Public property records – maintain a "gold copy" of ownership and interests in real property.
  - Loyalty and rewards – can power travel or other rewards systems.
  - Electronic Medical Records – improves security and accessibility of data, empowering patients to control their own records while improving compliance with regulations (*e.g.*, HIPAA).
  - Clinical Trials – protects patients with timestamped immutable consent forms, securely automates sequences, and increases data sharing of anonymized data while ensuring patient privacy.

The Role of the CFTC

- *The CFTC's Mission*
- *Smart Contracts and CFTC Markets*

The CFTC – Who We Are

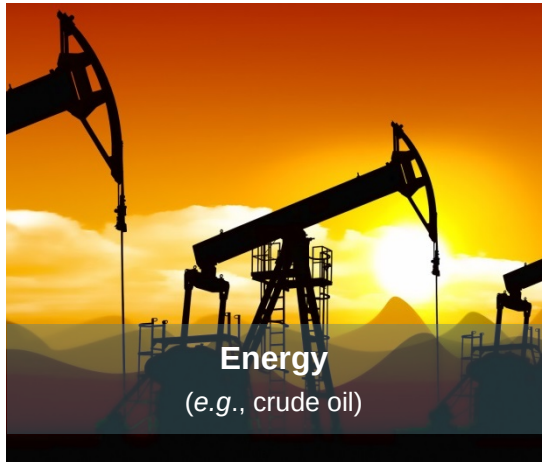
- **The CFTC's mission is to foster open, transparent, competitive, and financially sound markets.**
  - By working to avoid systemic risk, the CFTC aims to protect market users and their funds, consumers, and the public from fraud, manipulation, and abusive practices related to derivatives and other products that are subject to the Commodity Exchange Act (CEA).

- **To foster the public interest and fulfill its mission, the CFTC will act:**
  - To deter and prevent price manipulation or any other disruptions to market integrity;
  - To ensure the financial integrity of all transactions subject to the CEA and the avoidance of systemic risk;
  - To protect all market participants from fraudulent or other abusive sales practices and misuse of customer assets; and
  - To promote responsible innovation and fair competition among boards of trade, other markets, and market participants.

- **Responsible innovation is market-enhancing.**

CFTC Markets

- The CFTC regulates risk transfer and hedging markets.
- These futures and derivatives markets may include, but are not limited to, certain products based on:



Entities Registered with the CFTC

- Trading Exchanges/Organizations (*e.g.*, Designated Contract Markets (DCMs) and Swap Execution Facilities (SEFs), and Forward Boards of Trade (FBOTs)).
- Clearing Organizations (*e.g.*, Derivatives Clearing Organizations (DCOs)).
- Data Repositories (*e.g.*, Swap Data Repositories (SDRs)).
- Intermediaries (*e.g.*, Futures Commission Merchants (FCMs), Introducing Broker (IBs), Commodity Pool Operators (CPOs), and Commodity Trading Advisors (CTAs)).
- Counterparties (*e.g.*, Swap Dealers (SDs))

For more information visit www.cftc.gov/IndustryOversight/index.htm

Smart Contract Use

Entities registered with the CFTC may have use for smart contracts:

- Streamline trading of products subject to oversight by the CFTC (*e.g.*, options, futures, and swaps) and enhance efficiency from pre-trade through post-trade (*e.g*., price discovery, execution, clearing, and settlement).
- Reduce duplicative confirmation.
- Reduce trade, capital, and margin risks.
- Automate fulfillment of contracts.
- Enhance compliance with internal written policies and procedures and with legal obligations and regulatory requirements.
- Improve regulatory reporting.

Smart Contracts and CFTC Markets

- Many discussions of smart contracts use derivatives as examples because they may be readily digitized and coded.
- Depending on its structure, operation, and relevant facts and circumstances, a smart contract could be a:
  - Commodity
  - Forward Contract
  - Futures Contract
  - Option on Futures Contract
  - Swap‡
- You should consult competent counsel when considering whether a smart contract may be a product subject to CFTC jurisdiction.

Risks, Challenges, and Governance of Smart Contracts

- *Overview of Challenges and Risks*
- *Legal Considerations and Frameworks*
- *Operational Risks*
- *Technical Risks*
- *Cybersecurity Risks*
- *Fraud and Manipulation*
- *Governance for Smart Contracts*

Smart Contracts: Challenges and Risks

Although Smart Contracts could:

Enhance market activity and efficiency

Verify customer and counterparty identity

Facilitate trade execution and contract fulfillment

Ensure accurate books and recordkeeping

Complete prompt regulatory reporting

Smart Contracts could also:

Unlawfully circumvent rules and protections.

Diminish transparency and accountability.

Impair market integrity.

Introduce risk, including operational, technical and cybersecurity.

Be subject to fraud and manipulation

Potentially Applicable Legal Frameworks

- Can a Smart Contract be a binding legal contract? Potentially, depending on the facts and circumstances.
- Do legal frameworks apply to Smart Contracts? Yes, smart contracts may be subject to a variety of legal frameworks depending on their application or product characterization. Examples include:
    - Commodity Exchange Act and CFTC regulations.
    - Federal and state securities laws and regulations.
    - Federal, state, and local tax laws and regulations.
    - The Uniform Commercial Code (UCC), Uniform Electronic Transactions Act (UETA), and Electronic Signatures in Global and National Commerce Act (ESIGN Act).
    - The Bank Secrecy Act.
    - The USA Patriot Act.
    - Other Anti-Money Laundering (AML) laws and regulations.
    - State and federal money transmission laws.
- ***Existing law and regulation apply equally regardless what form a contract takes. Contracts or constituent parts of contracts that are written in code are subject to otherwise applicable law and regulation.***

Examples of Prohibited Activities

Derivatives contracts, including those that are smart contracts deployed on a decentralized blockchain, must not:

- Perpetrate or effect fraud or manipulation.
- Be traded on or processed by a facility that is not appropriately registered.
- Violate the CEA or CFTC regulations, including:
  - Disruptive trading practices (*e.g.*, spoofing).
  - Failure to maintain records or reporting violations.
  - Failure to be supervised appropriately or to satisfy financial integrity requirements.
- Be traded or executed by individuals or firms that are required to be registered with the CFTC but are not and do not have an exception or exemption from registration.
- Violate the Bank Secrecy Act or USA PATRIOT Act.

Please note that this is not an exhaustive list of prohibited activities.

Smart Contracts: Operational Risk

- Smart contracts may not include appropriate or sufficient backup / failover mechanisms in case something goes awry.
- Smart contracts may depend on other systems to fulfill contract terms. These other systems may have vulnerabilities that could prevent the smart contract from functioning as intended.
- Some smart contract platforms may be missing critical system safeguards and customer protections.
- Where smart contracts are linked to a blockchain, forks in the chain could create operational problems.
- In case of an operational failure, recourse may be limited or non-existent – complete loss of a virtual asset is possible.
- Poor governance. Smart contracts may require attention, action, and possible revision subject to appropriate governance and liability mechanisms.

Smart Contracts: Technical Risk

- Unintended software vulnerabilities.
- Humans! – make mi$taak3s when K0diNg.
- Technology failures – internet service can go down, user interfaces may become incompatible, or computers/servers can stop working.
- Scaling or bandwidth issues.
- Divergent/Forked Blockchains – such events can create multiple smart contracts where only one existed, or may disrupt the functioning of a smart contract.
- Future proofing – unforeseen or unanticipated future events that shock and/or stress the technology.
- Oracle failure, disruption, or other issues with the external sources used to obtain reference prices, events, or other information.

Smart Contracts: Cybersecurity Risk

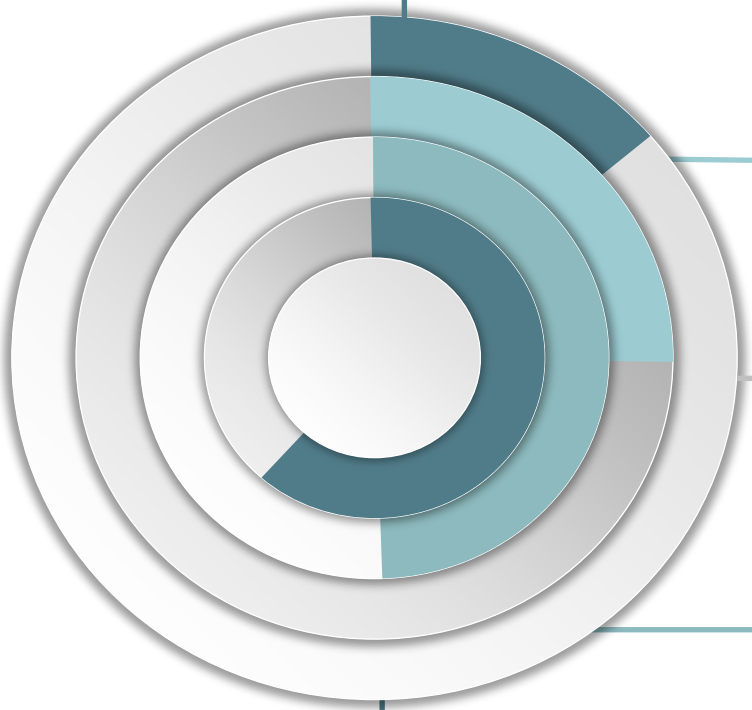
- Depending on the structure and security of the smart contract system and related wallet systems/custodian, some may be vulnerable to hacks, resulting in the theft or loss of digital assets. If a bad actor transfers digital assets to themselves or others, there may be limited or no recourse.

- An attacker may compromise the oracle (*i.e.*, mutually agreed upon, network-authenticated reference data provider) causing the Smart Contract to improperly transfer assets.

Smart Contracts: Fraud & Manipulation

- Smart contracts can include nefarious code.
- Smart contracts may be manipulated by insiders who may have “backdoors” or “kill switches” to the code or a deeper understanding of how the smart contract will react to particular events or inputs.
- Entities may solicit or offer smart contracts that do not behave as advertised.
- Oracles may accept or distribute unexpected information, resulting in outcomes that do not reflect the intent of one or more of the contracting parties when entering into the contract.
- Oracles may be subject to manipulation or themselves fraudulent, resulting in unexpected, fraudulent outcomes.

Governance for Smart Contracts



Good governance standards for smart contracts may help to address the challenges and risks that they present.

Governance standards and frameworks appear to be in early phase of development.

Such standards could create presumptions regarding the legal character of a smart contract, depending on its attributes and manner of use by market participants.

Such standards may assign responsibility for smart contract design and operation, and establish mechanisms for dispute resolution.

Governance standards may also incorporate terms or conditions for smart contracts to be enforceable.

Questions?

Contact Us at
LabCFTC@cftc.gov
www.cftc.gov/LabCFTC