Coinpit

Cryptography, Blockchain and Game Theory based Financial Systems

DISCLAIMER: NOT ALL FEATURES DESCRIBED HERE ARE COMPLETED.

FEATURES MAY BE DROPPED FOR TECHNICAL, MARKET, REGULATORY OR OTHER REASONS

Bharath Rao
coinpit.io

DRAFT 0.1.3

***Abstract*—The blockchain value proposition is that it complies with its own set of rules and does so in a provable way. Recent advances in cryptography enable the creation of systems, especially financial services that are provably compliant. On robust implementations, most of the rules may be mathematically infeasible to break. This results in substantial safety gains and dramatically reduces compliance and enforcement burdens. We describe how such systems may be built using a crypto-currency derivatives exchange that showcases some of these properties.**

Keywords—bitcoin; blockchain; compliance; cryptography; identity; safety; security; AML; KYC

I. Introduction

The confidence in accepting risk in the arena of primary focus is highly dependent on low-risk and stability in ancillary areas. For example, a hedge fund will accept market risk with greater confidence as long as they don't have to mitigate political instability, currency fluctuations, high crime and other risks that are not their principal area of focus. In the crypto world, the term *trustless* is used to denote high predictability—to a level sufficient for economic activity without regulatory protection. The regulatory landscape on the other hand, attempts to enforce a market that is *regulated*, i.e., one where most events are predictable leading to healthy and orderly conduct of business. Trustless systems seek to facilitate value exchange without relying on middlemen or state interference to govern behavior of economic actors. The regulatory position is that unchecked fraudulent and reckless behavior destabilizes the market. The goal of this paper is to demonstrate that the two sides are not mutually exclusive and can be brought together by creating mathematical models of desirable behavior and enforcing them using cryptography, blockchain and game theory.

II. Value Proposition

A *provably compliant system* prevents what can be prevented, detects what cannot be prevented and automatically remediates or mitigates further damage where possible. Such a system has very high *predictability*. Predictability precedes trust and highly predictable systems accumulate high trust and value enabling new use cases and creating a new value network.

Provability is the highest level of predictability, since an economic actor has near-certain information and low risk before committing to a course of action.

To illustrate the benefits of such an approach, let's take the example of MF Global failure in 2011. From Wikipedia: *"...MF Global probably experienced a number of trading days in 2011 during which the firm's bets on sovereign debt would have required the use of customer funds to meet capital requirements, thereby maintaining operating funds and possibly overall solvency."*[1]

In other words, the segregation of customer funds rule 17 CFR §1.20[2] was violated. Taking a preventive approach, we bake segregated accounts into the exchange operations end-to-end making it impractical to subvert this regulation.

1) A multisignature account is also created for the user where the funds are under user control.

2) A segregated account is created per user on sign up to cover trades.

3) A user action/cryptographic proof is needed to move funds from multi-signature into the segregated account.

4) Settlements are done directly among segregated accounts between losing and winning users on the blockchain.

5) The displayed user's account balance is computed using the balance in the segregated account.

6) This balance is read directly from the blockchain by the user and not from an entry in the exchange database.

Since the funds can only move from the segregated to either the user's account or to a settlement, detection of theft, embezzlement or funds movement to cover capital requirements can occur in seconds rather than days using traditional methods of whistleblowers and audits. Settlements won't be possible and the exchange will halt due to a negative balance.

Any alert is near certainty that a security incident or regulatory violation has occurred and needs to be looked into immediately. If there is a violation, there is proof of violation. If there is compliance, there is proof of compliance. This dramatically reduces compliance and enforcement burdens enabling faster and more efficient prosecutions.

III. Modeling And Enforcing System Rules

While the above is an advanced use case that incorporates cryptography, graph theory and game theory, often many rules can be modeled using simpler techniques. If a rule can be modeled mathematically, it can be enforced programmatically. The ideal option is to model what is permissible and enable only such behavior. This option should be preferred when precondition checking is a possibility. For example, United States federal regulation 17 CFR §38.152[3] lists

abusive trading practices that should be prohibited. If we can model exactly what conditions are allowable and validate before execution, we enable preventive compliance.

When only postcondition checks are possible, we may use detection and generate proof-of-violation and discipline the perpetrator automatically. For example, to address the issue of spoofing[14], if a trader who typically trades 10 contracts places orders for 10,000 contracts and cancels them before they are filled, it may make sense to refuse such large orders from said trader for a period of time that increases exponentially every time such orders are placed and cancelled. After detection of the cancelling of a uncharacteristically large order, it becomes a proof-of-violation that is readily available should the user turn into a habitual offender.

IV. Definitions

Proof Predicate

Proof-predicates are ordinary mathematical statements comprising of propositional logic.

Compliance Rule

A compliance rule is a mathematical expression composed of proof-predicates that defines a compliant behavior of the system.

Objective Predicate

A predicate is objective if it can be evaluated with general purpose computers. For example, *required margin* ≤ *available margin* is an objective predicate. Objective predicates can be re-evaluated, automated and archived on the blockchain.

Subjective Predicate

A predicate is subjective if it requires a human or special entity for evaluation. For example, *adequate number of compliance staff* is subjective. Subjective predicates lead to high compliance and enforcement burdens and have low effectiveness.

Compliance Proof

A compliance proof is a set of values that evaluate to true when applied to a compliance rule.

Violation Proof

A violation proof is the complement of a compliance proof—one that proves a violation has occurred when true.

Proof Anchor

For proofs to be universally verifiable, they need an anchor external to the system itself. *Without an external anchor, the system may generate proofs that have no evidentiary value.* A proof system that depends on digital signatures of participants provides robust proof-predicates secured by intractable mathematical problems.

Identity

Identity of an entity is that which threads together everything that happens to it. Changes to the entity over time and its accumulated data can be tracked using its identity. Things which do not change such as numbers are values and they are their own identity. An identity is usually reified into a tangible form called Identifier.

V. Coinpit—A Crypto-currency Exchange

We describe some characteristics of a contract market that uses crypto-compliance. We note some regulations that are enforced by them from 17 CFR §38, the USA codebook of federal regulations dealing with contract markets. Adapting to any other set of regulations can be done using a similar approach.

Coinpit facilitates exchange of derivatives between users in a trustless manner that enforces multiple standard regulatory and compliance practices currently enforced. The counterparty contracts create a zero-sum game between traders who take opposing views on the direction of a risky financial asset. The main product is BTC/USD, allowing users to hedge and speculate on the USD value of Bitcoin, with margin requirements as low as 1%. This is done in a platform design that is provably compliant.

A. Centralized Identity

Humans interacting indirectly with each other often use a an identity provided by a trusted entity. Identifiers used by such systems are tax-ids, government issued IDs and email addresses. Some of these are verifiable using special equipment such as black-lights. Authentication requires verification of both the authenticity of the identifier and lawful possession and is a labor-intensive process. Both are impractical over the internet. Email addresses can be authenticated more readily but are susceptible to a variety of attacks. A key point of friction is that a centralized identity does not belong to the bearer of the identity, but rather to the issuer. The issuer can arbitrarily revoke this identifier or a merchant using this identifier could compromise it, causing severe financial or reputational loss to the owner. For example, if your email provider decides that your email should be blocked for whatever reason or a website that uses this email id as an identifier is compromised by a hacker, you may lose access to all accounts tied to it. In many cases, you can't even change an email address at a website without clicking on a verification sent to the old address. Centralized identity is an ever present risk as demonstrated by fairly regular incidence of security breaches[4].

B. Decentralized Identity

Humans interact with each other directly using decentralized identity. On encounter with new person or entity, we create an identity for and associate all accumulated data of the entity with it. Coat check tokens are an example of decentralized identifiers in real-life. They allow economic activity to occur without a centralized identity.

From a computing perspective, a decentralized identity can just be a large random number. Computing systems automate the generation of decentralized identity for example, by generating UUIDs[5] for every entity they track.

Public Key Identifier

An authentication system that uses public/private key authentication can simply use the user's public key as a decentralized identifier. One of the obvious advantages is that only the owner of the identity has complete control and responsibility to keep it safe. The risk from identity providers and third parties compromising your identity practically goes away. While such an identity is indeed transferable, i.e., you could use the same public key everywhere, there is also the possibility of using a distinct public key for different websites, preventing merchants from correlating your online behavior and thus protecting your privacy.

The private key is best stored on an affordable hardware device[6] to ensure that keys cannot be moved into a general purpose computer to prevent malware from compromising the key. However, storing the key in a file may be acceptable for small monetary values if sufficient precautions are taken.

Mutual Authentication

A user and website can mutually authenticate each other by simply exchanging public keys. ECDH[7] may be used by both parties to arrive at a shared secret, which can be used to HMAC[8] authenticate messages to each other. This will thwart all manner of man-in-the middle attacks and any attacks that depend on a secret being sent across the wire such as a password or session cookie.

Signatures as universal proofs

A financial system that uses signatures[9] from a controlling private key to spend coins can authenticate user-specified actions with the same key. This proves that the person controlling the funds in the account is the same person who authorized the action. Signatures are non-repudiable and are a very strong proof but are computationally expensive. It may be acceptable to use a separate private key on a faster curve[10] to sign messages. The faster curve public key would need to be signed by the coin private key to ensure a valid chain of proof to the owner. This faster public key could function as an API Key, with limited privileges. In particular, it wouldn't mathematically be able to move any coins. The system can never delete the corresponding public key, since it would be required to verify past transactions.

C. *Compliance proofs, Audit & Transparency*

Hash-chains as audit trail

A financial service that uses signatures as above can embed it in every user created request and embed a cryptographic hash of the object into every object resulting from a subsequent computation. For example, the user's order contains a signature; an execution contains the hash of the order; a P&L calculation contains a hash of the execution; and a settlement contains the

hash of each P&L. The settlement hash could be safely stored on a secure blockchain such as the bitcoin blockchain. This is especially desirable when settlements are directly on the bitcoin blockchain. This provides an indelible audit-trail, which can be used to go back in time and ensure that everything has executed according to the rules of the system. For example, we can examine the timestamp and price field of a limit order and ensure that the execution has filled it with the FIFO and price guarantees[11] of the limit order book. Each object can store the preconditions to create the next object resulting in compliance proofs that are embedded into every step of the trade execution.

Real-time public audit

Audit in this case would simply involve ensuring the hashes compute correctly and recomputing the expected values. If the results in each step are published on a blockchain or otherwise, this audit can be done by multiple parties in real-time. This will ensure that any mistake intentional or otherwise, is detected immediately. The system itself should halt in such a case since this indicates a programming error or other serious condition.

This level of compliance and transparency can only be accomplished when the user's identity is not published to market participants. The API Key that provides the signature can never appear on the blockchain since it uses a completely different cryptographic curve and would not compromise privacy.

User Agreement

The private key representing the identity can be used to sign the User Agreement with any additional required information such as date, home country, etc. This signature is stored with the user record. It is best to accept the minimum amount of information from the user required for them to interact with you. This also makes the system an unattractive target for identity thieves.

Median Index

Listed contracts are anchored to an index representative of the spot market. When representing a market where spot markets have large differential and any exchange can go down for maintenance or other reasons, a VWAP approach can cause the price to jerk violently. This disruption is proportional to the market share of the impacted exchange. A median index is robust against temporary exchange failures and presents a more realistic representative price of the underlying asset.

The index can also serve as a settlement price for contracts with expiry. To prevent manipulation pre-expiry, contracts are settled at the final 30 minute (or appropriate duration) TWAP of the index price.

Trading Bands

On contracts that have low liquidity, price could diverge heavily from the spot market. This can lead to price distortions, market manipulation, accommodation trading and other illegal activities. To prevent these, a trading band around the price ensures that no trades occur outside

them. Any stop orders are not triggered unless they are also in the band. The band would need to be loose enough to reflect the sentiment of the market in addition to the index price since derivatives can quote at a premium or discount to the underlying spot price depending on market conditions but tight enough to prevent price distortions.

Sentiment Index

Futures prices can trade at a substantial premium or discount from the underlying price and trading bands need to take this into consideration when limiting the trading range. A market must be free to explore broad ranges in the course of price discovery, but as a system manipulation must also be prevented. A sentiment index composed of the premium or discount reflecting the leading futures markets may be more appropriate trading band anchor for some markets in addition to the spot price.

The combined effect of the median index, trading bands, and sentiment index is is to allow market participants to freely trade on a market without the fear of manipulation and other abusive trading practices by large traders on the exchange.

Abusive Trading Practices

While the bands prevent some manner of illegal activities, other abuses such as front-running customer orders require other checks. One way to front run customer orders is to hold them until sufficient orders are in and simply enter at a slightly better price and exit into customer orders. This can be somewhat mitigated by having timestamps signed by the customer and rejecting orders that are more than a few seconds away from current time. A futures commission merchant (FCM) or other intermediary would not be able to modify the user's signature on their order. This requires an accurate clock and variations in system clock can be adjusted for by the server providing its system time to users.

Quote stuffing can be mitigated by rate-limiting the users API access.

When the buy and sell orders belong to the same user, it is termed a wash trade and is prevented by cancelling the later order. These and other abusive behavior prevention can include compliance-proofs in the executions. For example, including the buyer and seller userids in the execution proves a wash sale did not occur and including timestamps prove that the exchange executed orders in FIFO order.

Realtime Integrity Verification Engine(RIVEN)

There are certain properties that always need to be true to verify the correctness of transactions. These are exchange invariants and include the following: The cumulative positions of all traders is zero; the cumulative P&L from unsettled transactions and fees is zero; every position has a stop. After every execution, the exchange performs a set of checks to verify the integrity of the system. If any check fails, the change is not committed and the exchange is halted. This ensures that the exchange never goes into a bad state due to a programming error.

D. *Systemic Risk Management*

Many exchanges estimate risk of a user position and manage risk by requiring margin that would cover a significant move. When an abnormally large volatility is likely due to external events, the exchanges require higher margins to ensure the integrity of markets. Estimating systemic risk works fairly well, but a strong unexpected price movement can bring the system into an imbalanced situation where winners cannot be paid from the losses. Some exchanges address this with a clawback where the system loss is socialized to the winners, while others use "auto-deleveraging" features to mitigate risk.

Atomic Stops

An alternative to guesstimating risk is to measure risk precisely. Mandatory stops allow the precise measurement of risk across the board and we can ensure that at no point a user will have more exposure than the margin balance. The stops are also atomic, meaning that they execute in the same book rather than being added on after triggering. Atomic stops are guaranteed to fill within a max predetermined distance from the trigger price.

Forced Termination of contracts

The other side of the filling an atomic stop is the fact that a winning contract needs to be terminated on the other side. This is likely to be a problem during extremely low liquidity. In a corner case, even a losing position can get terminated with the combination of high leverage and low liquidity during a sharp reversal. With sufficient liquidity, terminations should occur rarely.

E. *User funds Safety*

Crypto-currency exchanges in particular are prone to all manner of breaches and should be especially crafted to prevent and detect breaches. There is also the risk of exit scams and failure due to third parties such as hosting providers and API vendors. The guiding principle is to mitigate these risks is to avoid holding exclusive access to coins except under unavoidable circumstances.

Multi-signature accounts

To avoid the issues of reading the user's balance from a database entry, we place the user's funds on the blockchain. A 2-of-2 multi-signature[12] account enables both parties to know when coins have moved from the address. In particular, coins should not move from the coins without the user's signature. Any scheme where coins can move without the user's signature are susceptible to custodial risk. The multisignature address is a safe location for the coins not in a trade as long as users take safeguard their private key. It is of the utmost importance never to share this key with absolutely anyone.

Recovery Transaction

To ensure that the exchange does not lock the funds in the multisig accounts and make them inaccessible (for example if the exchange suddenly shuts down) the user should be able to get a pre-signed refund transaction that can be broadcast directly to the bitcoin network. The funds

would be sent to the address represented by the user's private key, which is also the userid in the system. This proves that the funds can only be recovered by the user who controls the private key.

Margin account

A user relinquishes control over some amount of coins when they are needed to cover existing positions and new orders. This is done by transferring coins into a margin account. This margin account is under exchange control and the exchange may let the user trade from here with zero-confirmations as long as an priority fee is paid for moving the coins (to avoid an orphaned transaction)

Settlements

Settlements occur among user margin accounts without going through an intermediary exchange account. Settlements are simply coinjoin[13] transactions with coins moving from losing accounts to winning accounts. A new settlement is not initiated if the prior settlement fails to be confirmed for any reason. In cases of severe network congestion, the settlement could be delayed by a few hours or days.

Financial Privacy

Funding transaction to multisig address, any number of moves to and from the margin account and settlements are visible to everyone on the blockchain backing the system. This enables automated accounting and tax preparation but it also means that if anyone discovers your multisig or margin address, they have potentially seen your financial history. This can be mitigated by regularly rotating these addresses, say once a week. The userid never appears on the blockchain until there is a need to extract funds from the multisig account using the recovery transaction, giving some privacy regarding actual trades performed. As with any other financial account, it's best to keep this information private.

Double-spend mitigation

The only transaction that the user could double-spend is the recovery transaction, since all other transactions require a server key. The user may try to double-spend the funds in the recovery transaction by broadcasting the recovery transaction and simultaneously moving coins to margin address. This risk is mitigated by providing normal fee to the recovery transaction and a priority fee to the add-margin transaction. RBF transactions are not accepted to avoid high-fee double spending. In addition, if there is an unconfirmed balance on the margin account, the exchange can do additional checks to detect a double spend.

Even if the double-spend succeeds, the exchange can trivially detect it and suspend operations on the user's account since the destination of the recovery transaction is fixed and equal to the userid. The exchange simply looks up the balance on the userid address and refuses to accept any operations if both the margin and recovery address have transactions with zero confirmations. As an optimization, a tiny recovery fee output could be added to every recovery transaction and the

exchange could simply monitor the recovery fee address and refuse to service new positions from users who have recently broadcast a recovery transaction.

To prevent malleability attacks, malleated outputs should not be counted against the balance.

To mitigate the risk of a miner colluding and trying to include the recovery transaction into a block without broadcasting it, progressively increasing number of confirmations are required to trade progressively larger sizes[16]. Unconfirmed outputs from settlement transactions are always available for trading.

Proof of reserves

Operators embezzling or otherwise using customer funds for speculative purposes presents a high risk for exchange failure. To prevent this, we create a segregated account per user and ensure that the user's margin is computed using on-chain balance. This prevents the exchange from allowing the user to trade while coins backing the positions have been lost to speculative activities. The user should also be able to view the balance on the blockchain at all times, enabling instant detection of any misappropriation of funds. Margin requirements and settlements are also driven from the segregated account meaning that any incorrect balance due to intentional or accidental movement of coins from a single margin account would halt the exchange.

Hardware wallets

The user can simply choose to use a private key from a hardware wallet. In such a case, the private key never leaves the hardware wallet and will simply provide signatures required for the operations described above. All compliance proofs will have the signature traceable to a hardware wallet key, ensuring malware resistant safety. Hardware wallets also allow smoother UX of trustless transfer to a multisig address. The user could sign a transfer-to-multisig transaction and request a refund transaction from the server. After the refund transaction is received and verified, the user can broadcast the funding transaction.

Hardware secured margin accounts

The server can use a 2-of-3 multisig address for margin accounts. User initiated transactions would have a signature from user's hardware key and settlements (the only exchange initiated fund movement) would have a signature from the server's hardware key. This ensures that no coins can move without a signature from a hardware wallet. The settlement signing module would verify compliance proofs before signing the transaction, ensuring that hackers cannot forge a fake settlement transaction. This security can be enhanced by programming the verification into firmware.

Automated Operations

Human error is a large component of operational errors and many compliance violations require human action. Any errors present in automated systems can be tested, detected, audited

and fixed but human intervention creates opportunities for hard to detect violations. As far as possible, every operation of the exchange is automated to minimize the human component.

F. *Key Compliance Issues*

Anti-Money Laundering(AML)

The standard Money Laundering model involves

- Placement: Bringing ill-gotten assets into the system
- Layering: Moving assets around to disguise origin, typically across jurisdictional boundaries
- Integration: Moving the now cleaned assets back to the owner.

We use graph theory to model the movement of assets as a directed graph with bank accounts as nodes and movements as directed edges[15]. In general, money laundering can be modeled as cycles in the graph. If substantial amounts of funds move from accounts controlled by an entity of interest via different pathways back to their control, it could potentially indicate money laundering activity. This can be easily prevented by disrupting placement by not accepting cash and equivalent deposits and only allowing withdrawals to source address, i.e., the user's multisig address.

Combating Terrorism Financing (CTF)

The New York Clearinghouse concluded that no effective financial profile for operational terrorists located in the United States is possible. Physical location using financial tracking of individuals is also not a possibility for blockchain projects. Institutions that fund terrorism use charities and banks to collect and transmit funds, which would be unnecessary on a blockchain. Layering is still a possibility, but the AML approach above would thwart it.

Know your Customer(KYC)

While decentralized identity is superior to centralized identity in most use cases, regulated business may require a centralized identity for compliance reasons. In countries such as Estonia, where government issued cards are capable of digital signatures, it's possible to simply create and sign a request for validation from the centralized identity issuer. For example, sign the decentralized identifier with a validation request on any specific attributes, for example: adult status and jurisdiction of the requestor. The centralized identity provider can certify the decentralized identity and requested attributes by signing it with their private key. The system recognizes the signature of the issuer and would store the verification as proof-of-KYC. This is similar to a TLS certificate request. The certificate is on a vendor-specific public key and would be invalid anywhere else making it an unattractive target for hackers.

G. *Future Directions*

Decentralized Exchange

A fully decentralized yet performant exchange is the ultimate goal of Coinpit. At this point, unsolved latency issues make this impractical to create a satisfactory trading user-experience

while providing trustless settlement. It may be possible to reduce the latency to acceptable levels that enable humans to trade using a network of lightning network hubs. The hubs themselves can do low latency settlements accurate to the satoshi.

Derivative Coin

Derivatives have a net position of zero, unlike normal asset based coins. A derivatives specific coin may be a faster and and easier way to create a decentralized trustless exchange. Such a coin could easily act as a global replicated order-book that settles within itself, automatically on-chain with every trade.

Acknowledgment

Nirmal Gupta for design. Chris Engel for financial theory and contract structure. Tom Taylor for product advice and usability.

References

[1] https://en.wikipedia.org/wiki/MF_Global
[2] https://www.law.cornell.edu/cfr/text/17/1.20
[3] https://www.law.cornell.edu/cfr/text/17/38.152
[4] https://en.wikipedia.org/wiki/List_of_data_breaches
[5] https://en.wikipedia.org/wiki/Universally_unique_identifier
[6] https://en.bitcoin.it/wiki/Hardware_wallet
[7] https://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman
[8] https://en.wikipedia.org/wiki/Hash-based_message_authentication_code
[9] https://en.wikipedia.org/wiki/Digital_signature
[10] https://en.wikipedia.org/wiki/EdDSA#Ed25519
[11] http://wallstreet.cch.com/cboe/rules/cboe-rules/chp_1_1/chp_1_1_6/chp_1_1_6_3/chp_1_1_6_3_6/default.asp
[12] https://en.bitcoin.it/wiki/Multisignature
[13] https://en.bitcoin.it/wiki/CoinJoin
[14] https://en.wikipedia.org/wiki/Spoofing_(finance)
[15] https://www.coinpit.io/2016/07/08/aml-without-kyc/
[16] https://bitcoil.co.il/Doublespend.pdf