BlockRules

BlockRules Compliance Engine

BlockRules Ltd.

MARCH 1, 2019

TECHNICAL WHITE PAPER

ABSTRACT

Blockchain ledgers are efficient, secure, and transparent, making them the ideal solution for security tokens. In addition, public blockchains can support the concept of direct ownership and facilitate trading in secondary markets. However, public blockchain implementations are inherently global, while laws and regulations vary across jurisdictions, making cross-border regulatory compliance a challenge. The BlockRules Compliance Engine provides an adaptive framework for the enforcement of multijurisdictional regulations and rules that govern the ownership and trading of security tokens without sacrificing privacy, security, and transparency. It does so by translating a set of rules provided by the issuing company into a set of abstract digital rules and implementing them entirely on the blockchain without relying on external or centralized processing. The rules set defined by the issuing company may consist of multijurisdictional regulatory restrictions, as well as any other rules the company chooses to enforce on their token.

BACKGROUND

A blockchain is a cryptographically secure method of storing data that is, by design, resistant to tampering. Initially proposed as a means of commerce, public distributed blockchains (PDBs) use the concept of distributed consensus to publicly share data that is trustworthy and not reliant on a central authority. Blockchain technology has since spawned an entirely new industry and has become an important topic of innovation among major enterprise providers and financial institutions.

The growing public interest in blockchains has fueled many new technology endeavors, some of dubious merit. To judge the value of a blockchain application, it is important to remember that the primary advantage of blockchains is to securely store data accessible by multiple parties. For example, private blockchains are well-suited to business applications, including supply chain management or efficient funds transfer between financial institutions. In contrast, PDBs, which provide data accessible in the public domain, are better-suited for proof of ownership and record of transactions. PDBs could be an ideal way of representing ledgers for financial instruments such as securities.

The advantages of blockchain ledgers are multifold:

- They provide an authoritative means to prove ownership that is not under the direct control of any central agency or intermediary.
- By providing a single, immutable, yet publicly accessible ledger, securities can be transferred securely and transparently between individuals and on primary and secondary markets.
- A complete and trusted record of securities ownership and transfers is available to anyone, including individual token holders, financial institutions, markets, and regulators.

SMART CONTRACTS

Blockchains can store almost any type of digital data. When combined with emulation technology, similar to the virtualization technology often deployed in enterprise computing, it is possible to support an entire virtual computing environment on a blockchain. A computing environment allows applications to implement complex transaction logic on a blockchain in the form of smart contracts. Through execution on a PDB, any logic provided in a smart contract is executed in a secure and verifiable manner, and all affected parties can be confident that the transaction will be faithfully executed. Furthermore, any transaction logic embedded in the smart contract is available for inspection on the blockchain.

To be of any practical use, the computing environment provided by a blockchain must respond to events outside the blockchain. In most relevant implementations, such external events are communicated by messages, which may originate from any number of entities, such as individuals involved in a transaction or organizations wishing to update data on the blockchain. To communicate with the blockchain, each entity is provided a unique address as a form of identification. Messages are cryptographically signed to ensure the identity of each sender. Addresses typically consist of a seemingly random sequence of digits and do not offer any direct clue as to the identity of the owner.

CURRENT REGULATORY LANDSCAPE[1]

Securities regulations vary between jurisdictions, but in general they seek to protect investors, maintain fair and orderly markets, and assist in efficient capital formation and allocation. As such, regulations in many countries follow a similar

[1] This information is not intended to constitute legal advice and should not be relied upon in lieu of consultation with appropriate legal advisors.

pattern. Companies who wish to issue a security to the public of a particular country (i.e. to retail investors) must register their offering with one or more national regulatory bodies and disclose details of their business plan and financial status, typically in the form of a prospectus. Certain exemptions are often allowed if the company limits their sale of securities to individuals or organizations with sufficient experience and knowledge to evaluate the investment opportunity on their own (i.e. accredited or qualified investors). The precise definition of an accredited or qualified investor depends on the jurisdiction(s) in question.

Laws restricting the sale of securities are typically territorial, that is, the law of a country applies only to transactions that occur in that country. Cross-border investment transactions may therefore be subject to regulatory and legal requirements in more than one jurisdiction. In some cases, for example in the European Union, efforts have been made to streamline cross-border registration, thereby permitting cross-border transactions. But such transactions in general remain complex. For instance, investors outside the United States may be permitted to purchase securities from a United States-based company under an exemption to registration known as Regulation S. Such investors must agree not to transfer securities sold under Regulation S to investors in the United States for a certain time period depending on the nature of the offering (e.g. one year post issuance). Yet investors in the United States may be permitted to purchase securities from the issuing company directly under a different exemption to registration, such as Regulation D.

Enforcement of regulatory rules is only possible if specific details of security holders are known (so-called "know your customer" or KYC information). Such details can vary across jurisdictions and may include place of residence, country of citizenship, and accreditation status. Furthermore, most jurisdictions require compliance with anti-money laundering (AML) standards set forth by the international Financial Action Task Force on Money Laundering (FATF) and local governments. Overall, regulatory compliance for the trading of securities requires, at a minimum, KYC/AML verification of every holder or trade participant. For security tokens, this means KYC/AML verification of the owner of each address holding the security or involved in a trade.

Issuing companies are generally responsible for developing, in concert with their legal counsel, a set of rules that implement the legal and regulatory requirements governing the ownership, issuance, and trading of a security for the desired jurisdictions (referred to herein as "compliance rules"). When implementing compliance rules on the blockchain, the challenge lies in representing these rules in such a way that they can be translated to a robust and efficient framework. This framework is necessary to reliably enforce the rules for all transactions of a security, including primary issuance and secondary trading across multiple jurisdictions. Regulatory compliance is a key issue that must be addressed for the tokenization of securities to be viable.

In addition, there may be other types of restrictions on the ownership and transfer of securities related to corporate governance that should also be considered. Some companies, for example, award restricted stock units as part of employee compensation. Others impose trading limitations to some or all of their employees around significant events, such as earning reports. While such restrictions are often implemented administratively inside a company, a blockchain solution would be an additional and reliable means of enforcement and protect against unintended breaches of policy.

SIMPLE LISTS ARE INSUFFICIENT

The simplest approach to enforce regulatory compliance on a PDB is to restrict ownership or trading of a security token to a list of addresses stored in a smart contact. Ownership or trade participation could be restricted to members of a permitted list (i.e. a "whitelist"), or, conversely, ownership could be closed to a prohibited list (i.e. a "blacklist"). Methods on the smart contract can be provided to allow messages from

authorized addresses (i.e. curators) to add or remove members from these lists. Simple lists can be used, for example, to restrict the sale of securities during a primary offering in one jurisdiction. Because of their simplicity, whitelists have seen widespread adoption on the blockchain.

However, securities offerings across multiple jurisdictions are often associated with complex, interlocking compliance rules and legal requirements. In such cases, white- or blacklists typically cannot appropriately restrict the ownership and trading of security tokens. For instance, a regulation may prevent token holders residing in country A from selling tokens to residents of country B for a certain duration. A whitelist-based approach, however, would allow trades among all token holders, regardless of country of residence and timing relative to token issuance, and would therefore not be able to enforce such a regulation.

As a consequence, most blockchain implementations resort to other methods when seeking to provide support of multijurisdictional regulatory compliance, such as centralized processing "off-chain" (i.e. outside the blockchain). To connect their off-chain processing to a blockchain smart contract, these providers deploy what are commonly known as "oracle" processes.

ORACLES ARE A POOR COMPROMISE

With oracle processes, regulatory compliance for the trade of a security token would typically operate in the following fashion (see Figure 1). A trade is requested by sending an instruction to a smart contract using the secure methods built into a public blockchain. An off-chain oracle process running on a computer server makes note of the request (e.g. by reading the event log of the Ethereum network) and runs an off-chain compliance check, using whatever rules and techniques are at its disposal, typically proprietary in nature, to evaluate whether the requested transaction is valid. It then encapsulates its decision into a second, separate message, which the

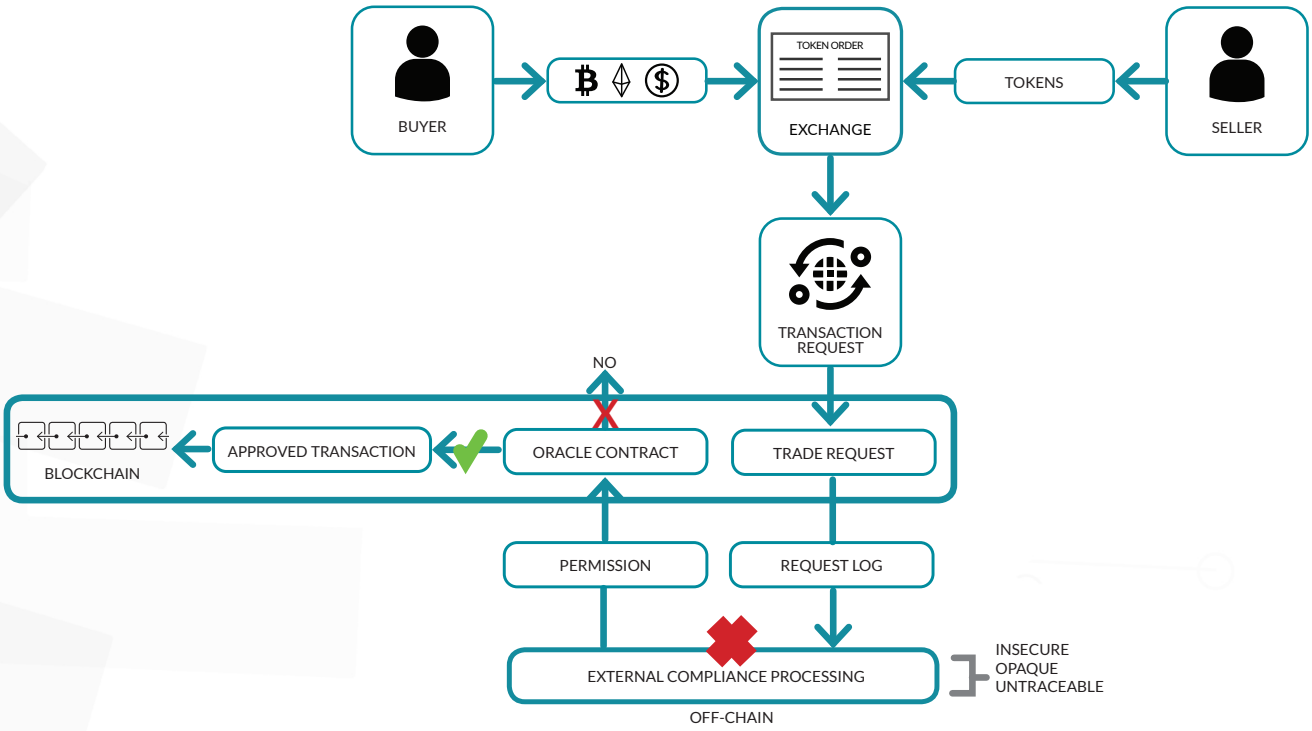

Figure 1. Operation of an oracle checking for regulatory compliance for a requested trade. This technique introduces an opaque, unverifiable, and potentially fragile off-chain process.

oracle then sends back to the oracle smart contract. The oracle smart contract, in turn, processes the second transaction. Even if this process works as intended, the person who made the original transaction request is going to experience a delay.

To understand the drawbacks of oracles, it is important to appreciate the potential weaknesses of a smart contract. Once data is stored on a blockchain it is presented faithfully to all parties, but the data is only as trustworthy as its original source. Trust is easily broken if a smart contract is programmed to receive important data from off-chain sources that cannot be verified. Providers that wish to promote the greatest trust and transparency must limit the type of external data that their smart contracts receive and how such data impacts important transactions on a blockchain.

Interrupting blockchain transactions with unverified off-chain processing to enforce regulatory compliance undermines the security and transparency of a blockchain. This is a result of introducing hidden, centralized, off-chain manipulations into what should be a verifiable and predictable blockchain transaction. In this sense, the use of oracles for regulatory compliance should not be considered a blockchain solution.

In some implementations, the actual trade may even be associated with the oracle address rather than the address of the original seller. Because the oracle has the power to perform this transaction, in principle it also has the power to perform arbitrary transactions. Effectively, this constitutes a backdoor method and poses a security risk to the investor. Smart contracts may have other vulnerabilities and investors are encouraged to learn all they can about the implementation details of a token smart contract before making an investment.

Moreover, while a properly implemented public blockchain smart contact is virtually invulnerable to manipulation, off-chain oracle processes are vulnerable to conventional hacking techniques. When an off-chain compliance process is compromised, it can be difficult or impossible to know, because the processing takes place outside the blockchain and is typically hidden from public inspection. This runs contrary to the underlying philosophy of blockchains.

Furthermore, oracle processes are centrally controlled, yet another property in stark contrast to the decentralized nature of public blockchains. If, for example, the company providing the oracle service suspended operations or their services were otherwise disrupted, the oracle process might fail to respond and submitted transaction requests would not be approved or rejected.

THE BLOCKRULES COMPLIANCE ENGINE

The BlockRules Compliance Engine (BCE) provides on-chain enforcement of multijurisdictional regulatory compliance rules governing the ownership and transfer of a security token, as instructed by the issuing company. It does so without relying on opaque and insecure off-chain processing through oracles. Instead, the BCE is implemented by converting the compliance rules assigned by issuing companies into suitable abstractions as extensible logic encoded in smart contacts. When the compliance rules must be applied, such as to authorize a trade, the appropriate code is executed directly on the blockchain in order to enforce the associated compliance rules. The general process of the BCE is illustrated in Figure 2.

Implementing regulatory compliance through investor address categories (IACs)

A key consideration when designing a smart contract is how to incorporate real-world constraints like regulatory compliance rules into an abstract set of instructions for execution on a public blockchain. The primary abstraction used by the BCE is to associate each token holder with one or more abstract groups, called investor address categories (IACs). IACs are designed to facilitate enforcement of a set of compliance rules developed by the issuing company. Each IAC corresponds to a specific functional or legal category and the precise legal definition of each IAC is established in advance.

Examples include, but are not limited to:

- A relevant aspect of an individual's regulatory status (e.g. accreditation class)
- An individual's country of citizenship
- An individual's country of residence
- A business's country of organization
- A business's country of operations
- Whether an individual is affiliated with the issuer of the security (i.e. an "insider")
- Whether a business is an exchange

IACs can also be expanded to accommodate the Cartesian products of other IACs. For example, if compliance rules for residents of a certain country depend upon accreditation status, one may choose to establish two separate IACs: one for accredited investors in the designated country and a second for non-accredited investors in the same country.

The BlockRules Compliance Engine requires each current or potential token holder to register in advance. Potential token holders provide registration data so due diligence can be performed (KYC/AML verification) and register one or more addresses. Based on their registration data, the individual or organization is assigned to one or more IACs. Their registration data is then abstracted and anonymized in the form of a transaction authentication record (TAR). Note that data contained in the TARs are no more specific than is necessary to enforce the provided compliance rules. For example, IACs may include the country of residence of a token holder, but will not include more specific location data, such as that token holder's address, and will not include sensitive data, such as the token holder's name. TARs are associated on the blockchain with the registered address(es) representing the individual or organization, not with other publicly available identity information.

The owner of a BCE smart contract can designate blockchain addresses that are allowed to create and update TARs, for instance to reflect changes in KYC/AML information of a registered token holder or to account for regulatory changes that impact the compliance rules.

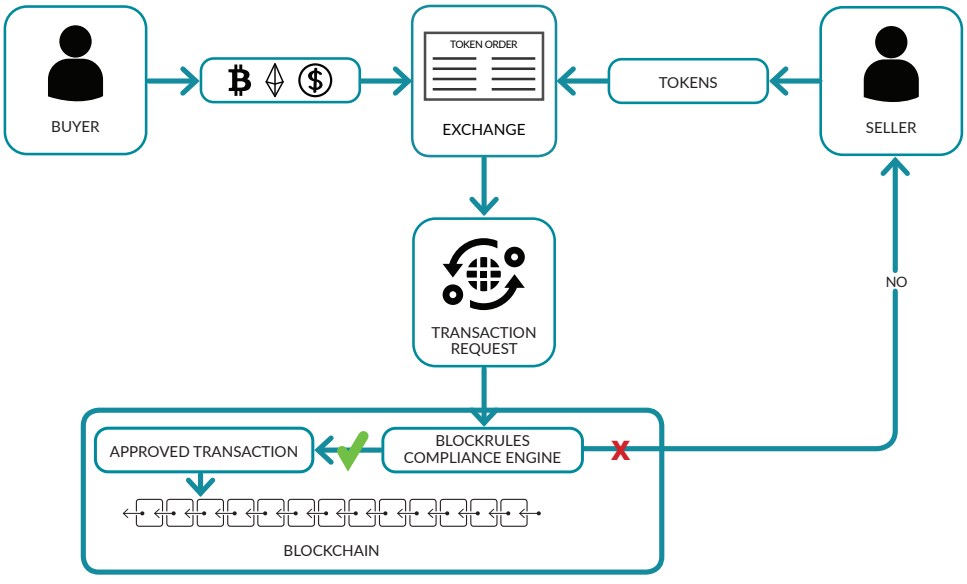

Figure 2. Processing of a trade request using the BlockRules Compliance Engine. All compliance checks are performed inside the blockchain environment without intervention from a centralized off-chain service and results of the compliance checks are written to the blockchain event log or equivalent logging facility on a PDB.

Each TAR is assigned an expiration date, which serves two purposes. First, some jurisdictions mandate regular updates of KYC/AML verification data and an expiration date on the blockchain can reliably enforce such requirements. Second, in the event of a disruption of registration services, all TARs will eventually become stale and trades will be blocked, a safer alternative than allowing potentially non-compliant trading.

The BCE includes an abstract representation of the compliance rules laid out by the issuing company. TARs are used to provide responses to transaction-related questions, including:

- Is the potential token holder allowed to own the security?
- To which IACs is the token holder allowed to transfer any portion of their holding in the security?
- To which IACs is the token holder prohibited to transfer any portion of their holding in the security?
- Is the token holder's KYC/AML information still valid?

Note that the answers to the above questions will depend on the compliance rules for each security token (as established by the issuing company) and, for that reason, each security token will typically need its own independent BCE instance.

EXAMPLES

This section discusses some hypothetical regulatory scenarios and how the BCE might handle them. Note that the BCE framework is applicable to many more scenarios than those listed here.

Example 1

Consider a fictitious United States company, ABC Co., that wishes to register and offer security tokens under a prospectus in Singapore. ABC Co. simultaneously intends to offer its securities to certain investors in the United States pursuant to Regulation D. ABC Co.'s United States residence means it must comply with additional restrictions (Regulation S) to make foreign sales, even with a registered prospectus.

ABC Co. develops compliance rules that permit both accredited or non-accredited token holders in Singapore to trade tokens to other entities in Singapore, pursuant to ABC Co.'s registration. The compliance rules further permit ABC Co. and accredited Singapore investors to sell tokens to accredited investors in the United States. However, all token holders in Singapore are prohibited from transferring their tokens to non-accredited investors in the United States for a period of one year post issuance. To increase liquidity, ABC Co. additionally wishes to permit qualified investors who live in the European Union, where ABC Co. does not intend to make any primary sales of its token, to purchase the token on the secondary market.[2]

Figure 3 shows IAC definitions, assignments, and trading permissions for four hypothetical investors. Alice, an accredited Singapore investor, may purchase tokens directly from ABC Co. during issuance. An accredited investor in the United States, Bob, may also purchase tokens directly from ABC Co. A non-accredited investor in the United States, Carol, is prohibited from purchasing tokens directly from ABC Co. Moreover, ABC Co. does not intend to sell tokens directly to investors in the European Union, so Dave is prohibited from purchasing directly from ABC Co. These permissions and prohibitions, provided to BlockRules by ABC Co., are encoded in the BCE smart contract, which allows the transfers to proceed only if they are permitted and blocks them if they are not.

The BCE continues to apply the compliance rules during secondary market trading. For example, Alice may transfer her tokens to a qualified investor located in the European Union, Dave. However, if Alice attempts to transfer her tokens to Carol, a non-accredited investor in the United States, during the first year post issuance, the BCE blocks the transfer as it would violate the requirements reflected in ABC Co.'s compliance rules. However, the BCE would permit Bob, an accredited United States investor, to buy tokens from Alice. Note that a non-accredited Singapore investor would not be permitted to trade tokens to Bob within the first year post issuance.

After the conclusion of the Regulation S compliance period (one year post issuance), the tokens are no longer consid-

[2] ABC Co. might additionally prohibit insiders from selling tokens for a period of time, or limit the groups to which holders of its tokens may trade. Compliance rules enforced by the BCE can be as complex as desired by the token issuing company. However, any additional complexities are omitted from this example for clarity.

er restricted securities, and IAC assignments to the allowed and prohibited lists are updated to reflect this. This action is performed without the need to change code on the smart contract. IAC membership, however, does not change for the registered addresses of the four investors. From this time on, in this example, Alice, Bob, and Dave would be able to trade among themselves using their registered addresses.

Carol, a non-accredited United States investor could be legally permitted to trade tokens in the secondary market through a regulated exchange. Thus, the inclusion of a third party in this transaction is required by current United States regulations. The BCE can facilitate these trades through a suitable third-¬party address for a blockchain-based regulated exchange, once one is available. As the regulatory landscape evolves to accommodate security tokens, the BCE can easily adapt.

The BlockRules Compliance Engine implementation permits the enforcement of comprehensive compliance rules. By evaluating each trade on an individual basis rather than broadly permitting investors to own tokens, regulatory compliance with complex, multijurisdictional regulatory frameworks is possible.

As noted, the compliance rules implementing a multijurisdictional framework must be developed by the issuing company in concert with its legal counsel. The compliance rules may incorporate as many jurisdictions as the issuing company prefers, and may, alternatively, restrict individuals and organizations from certain jurisdictions from ever owning the issued security tokens. These rules may include additional restrictions stipulated by the company that are outside the scope of national securities regulations. The BCE can support compliance rules that replicate simple whitelists, as well as much more robust rules enforcement.

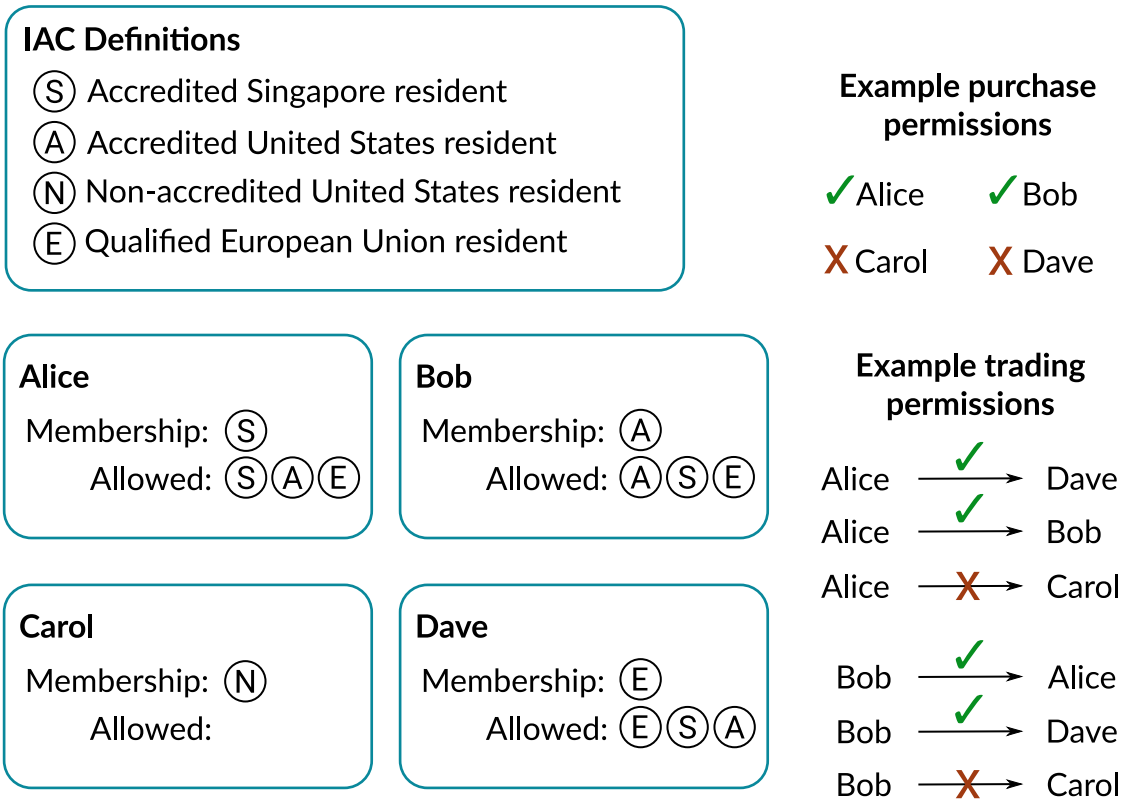

Figure 3. IAC definitions (top left) and assignments (bottom left) for four hypothetical investors (Alice, Bob, Carol, and Dave) in hypothetical company ABC Co., as described in the main text. Example purchase and trading permissions during the first year after issuance are illustrated on the right.

Example 2

For a second example, let's assume that a wealthy French citizen, Elle, wishes to invest in a security token being offered in Korea by XYZ Co., see Figure 4.

Safe harbor laws allow the issuing company to sell to professional clients in Europe. During KYC/AML registration, it was determined that Elle meets the necessary requirements. The associated BCE is updated, and Elle is allowed to purchase the security. Sometime later, Elle decides to move to Beijing, China, a country which has a broad ban on blockchain-based financial instruments for all residents. When Elle informs the issuing company's registrar of the change of address, as would be required and expected, the IACs representing Elle's transaction permissions are updated on the associated BCE instance for the issuing company's token contract to block all trading involving Elle based on her new country of residence. Elle remains in possession of the securities, but is prevented from trading with anyone as mandated by Chinese regulation, until such a time as either said regulation is changed in her favor or Elle moves to another country where trading of the XYZ Co.'s token is allowed. Even if in the future Elle is no longer banned from trading, the other participant in a potential trade must be able to receive the tokens based on their own trade permission IACs and the compliance rules of the issuing company.

IMPLEMENTATION DETAILS

A version of the BCE is currently available for the Ethereum Network and compatible blockchains. This version supports a maximum of 1024 individual IACs per BCE instance and an unlimited number of registered addresses.

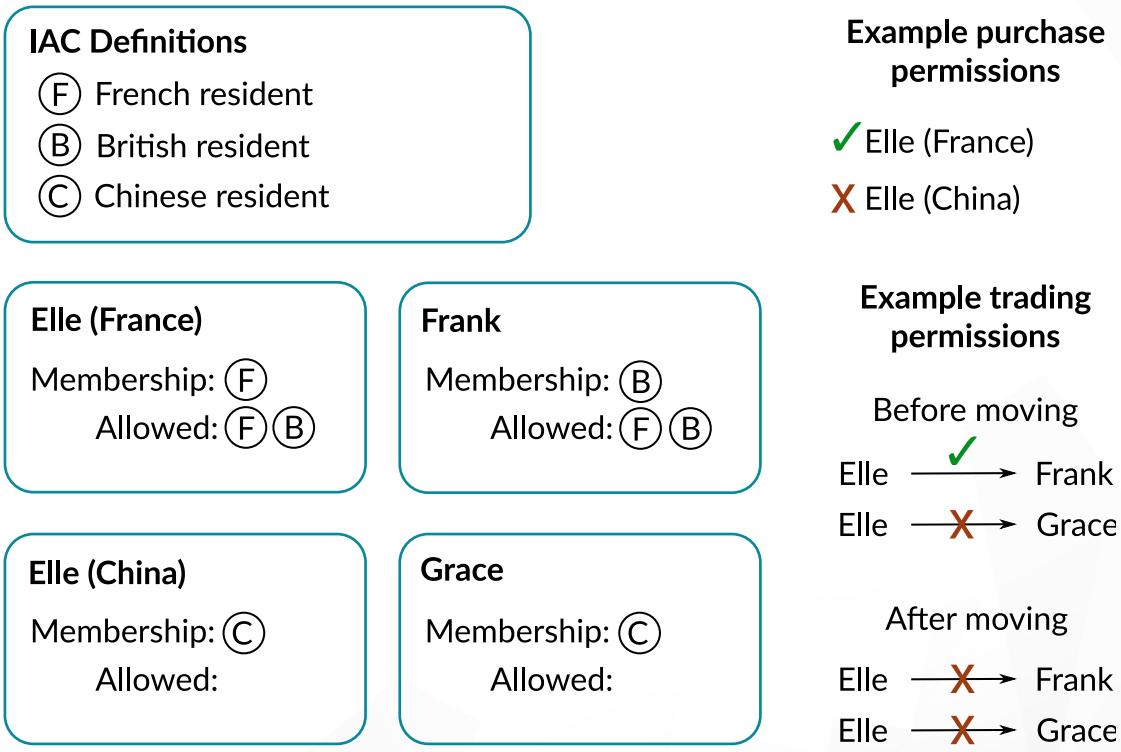

Figure 4. IAC definitions (top left) and assignments (bottom left) for three hypothetical investors (Elle, Frank, and Grace) in hypothetical company XYZ Co., as described in the main text. Example purchase and trading permissions are illustrated on the right, specifically, before and after Elle moves to China.

The BCE associates each potential token holder with the corresponding abstract, anonymized TAR stored on the PDB ledger. The anonymized TAR contains the information shown in Table 1. Each token holder has the option to use multiple registered addresses, in which case all such addresses point to the token holder's unique TAR. By design, the BCE includes logic that permits the transfer of digital assets between any addresses associated with the same owner without restriction.

Permission to modify the TAR is restricted to a list of authorized addresses unique to each BCE instance and selected by the issuing company. This allows accounting for changes in the regulatory environment or lifting trading prohibitions after the expiration of the corresponding restriction (see also the two examples above). Each update to a token holder's anonymized TAR is saved to a permanent log on the blockchain. For computational efficiency, the BCE represents a list of IACs as a bitstream, where each IAC is assigned a specific place (or bit) in the bitstream. The membership in an IAC in the bitstream is represented as the value 1, whereas non-membership is represented by 0. Logical operations on IACs bitstreams can be efficiently represented as a combination of binary operations, such as AND, OR, or XOR. For example, to check whether the transfer of a security is allowed, three IAC bitstreams are involved:

A. the allowed trades IACs for the current owner,
B. the prohibited trades IACs for the current owner, and
C. the membership list of the intended recipient.

As part of its programming, the BCE allows a trade only if both of the following numerical requirements are satisfied:

- sum(A AND C) != 0
- sum(B AND C) = 0

where A, B, and C are the bitstream representations of the corresponding lists of IACs.

Pictorial representations of example operations taken from example 1 above are shown in Figure 5. Bob in this example is allowed to trade, among others, to Singapore residents and accredited residents in the United States. Alice, the recipient of the first transaction, is an accredited investor living in Singapore and has the corresponding bit set. In this case, the binary AND produces a nonzero value and the transaction is permitted. In the second transaction, recipient Carol is a non-accredited investor in the United States who is not allowed to participate in any trades of this token in the first year post issuance. In this case, the binary AND produces a zero value, and the transaction is blocked. Similarly, Bob and Dave would not be permitted to trade with Carol.

The BCE, implemented in a dedicated smart contract, presents a standardized application binary interface (ABI) and is associated to a blockchain ledger smart contract by reference. This allows new versions of the BCE to be substituted on demand if additional features are needed, or if a major reorganization of IACs is required, including, for example, if there is a change in securities regulations that requires an update to the original compliance rules set.

Table 1. Anonymized transaction authentication record (TAR) stored by the BlockRules Compliance Engine for each owner address.

Name	Description
Membership	The list of IACs to which the address belongs
Allowed trades	The list of IACs to which the address is allowed to send tokens
Prohibited trades	The list of IACs to which the address is prohibited to send tokens
Expiration date	The date at which the data in this TAR becomes invalid
Registrar	The blockchain address of the entity that serves as registrar for the security token

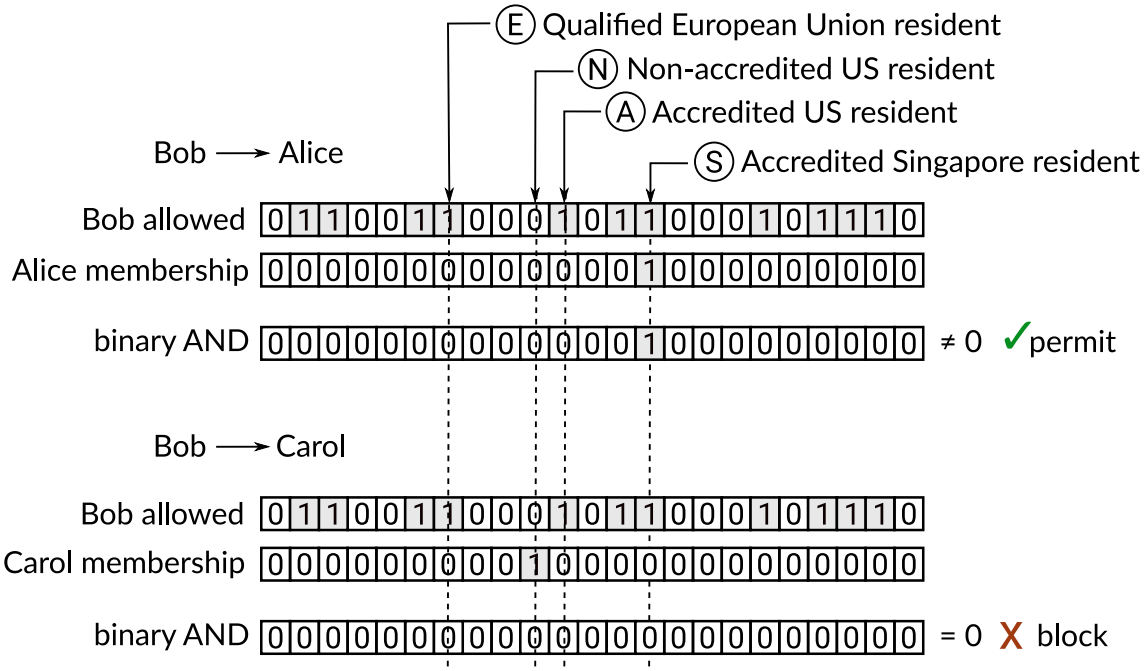

Figure 5. Bitstream operations on the allowed list for example 1, introduced above, applied by the BCE for the enforcement of transfer rules of a token. The IAC bitstream available to the BCE can currently hold 1024 IACs and is considerably more extensive than illustrated here. Four IACs are highlighted with their definition. Similar constructions would exist for other transfer pairings (e.g. Alice to Carol, Bob to Dave, etc.) and for the bitstream operations on the prohibited list.

The compact representation of IACs via bitstreams and a reliance on read-only data makes the BlockRules Compliance Engine particularly efficient. Benchmark exercises on test Ethereum networks show a cost of approximately 5000 gas for the BCE authentication check of an ERC-20 token transfer request, or about 10% of the total cost of a simple ERC-20-compliant token transfer.[3]

DECENTRALIZATION

The BCE was built to support the ERC-20 protocol and enforces regulatory compliance directly on the blockchain. As a result, registered token holders can participate in peer-to-peer trading at their discretion as long as their registration is current. Furthermore, tokens issued using the BCE can be traded on decentralized exchanges that support ERC-20-compliant tokens without requiring any additional changes to the trading system.

The BCE was designed to accommodate multiple sources of KYC/AML verification. This provides the engine with a measure of resilience against the failure of one or more of these sources and an extra degree of flexibility. Depending on arrangements, prospective investors in a security token supported by the BCE would have multiple ways to register their identity. For example, they might register directly with certified third parties such as the issuing company, their financial advisor, or certain token exchange service. Alternatively, brokers or token exchanges may use APIs provided by BlockRules to register their investors on the BlockRules system and perform the associated KYC/AML verification.

[3] Quoted gas costs include the call on an external dedicated BCE contract address. Tests were performed on the Byzantium fork using an ERC-20-compliant token contract with a simple address-mapped ledger and no additional restrictions on token ownership.

EXTENSIONS

The BCE uses binary operations on bitstreams for simplicity and speed. Any new features that can be realized using binary operations would be relatively inexpensive to incorporate in the BCE. For example, one could incorporate so-called "global" bit streams that apply to all token holders, such as:

D. Disable the operation if the holder belongs to any of the given IACs
E. Permit the operation only if the holder belongs to any of the given IACs

The above can be implemented with the following simple rules during a transaction:

- sum(C AND D) = 0
- sum(C AND E) != 0

where C is the membership bitstream corresponding to the associated token holder introduced above. Possible uses of such a feature could include the eligibility for voting or for distributions associated with securities rights of a security token, including, for example, royalties or dividend payments. Because global bitstreams such as D and E need only be stored once for all token holders, they are quick and inexpensive to update.

If, according to an issuing company's compliance rules, there was a need to limit individual transactions sizes for specific token holders, a maximum transaction size limit could be added to the TAR. Applying this limit to each transaction would be only a small incremental expense for the BCE.

OTHER FEATURES

Compatible with established protocols

Since the BCE performs authentication checks for transaction requests directly on the blockchain using internal data, the process is operationally transparent and portable. These features allow blockchain ledgers that employ the BCE to operate within established protocols, such as the ERC-20, ERC-223, and ERC-770 token standards.

The BCE, however, does require the identification of token holder addresses with specific individuals or institutions. In transactional processes that rely on shared or intermediate blockchain addresses, such as some centralized exchanges that may initiate transactions on behalf of their clients, additional protocols will be need to be implemented.

Adaptable to changing compliance rules

Despite the fact that the BCE operates on-chain, its design can account for modifications to the implemented compliance rules. Changing regulations may require an update to the compliance rules provided by the issuing company, or the issuing company may decide to modify its compliance rules for other reasons. Such updates can be realized by adapting the IACs and their associated bitstreams in the TAR stored on-chain, but they do not require modifications in the BCE itself.

Cost efficient

Computation on a public blockchain can be expensive. To be cost effective, the BCE is designed to apply relatively simple operations on read-only data for its compliance checks. In addition, unlike conventional methods relying on oracle processes, the individual or organization that initiates the trading request is directly responsible for all transaction costs.

If a newly added security token requires complex compliance rules exhausting the current IAC limit of 1024 bits, it may be necessary to update the registration data for a large fraction of existing investors, which would be an additional expense borne by the organization performing the registration. This expense can be mitigated by analyzing the customer base in advance and carefully planning which IACs to define as early as possible. Extensions beyond 1024 bits for BCE instances are also possible if required.

CONCLUSIONS

Blockchain ledgers can only reach their full potential if compliance with regulations can be enforced. Conventional approaches that establish compliance off-chain are sacrificing many of the advantages of public distributed blockchains due to simple expediency and lack of innovation. The BlockRules Compliance Engine reverses this trend by performing all compliance processing for token trading directly on the blockchain in a secure and verifiable manner. We achieve this feat by translating compliance rules developed by token issuing companies into suitable and portable abstractions. This approach provides the flexibility needed to support complex multijurisdictional regulatory compliance and allows BlockRules to bring regulatory certainty to security tokens.